UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

Seamless and Strong Authentication on Mobile Devices Based on User Activity

Luís Paulo Lemos Perez

Tese para obtenção do Grau de Mestre em
Engenharia Informática
(2º ciclo de estudos)

Orientador: Professor Doutor Pedro Ricardo Morais Inácio

Covilhã, Outubro de 2015

Dedicatória

Dedico este trabalho a todos aqueles que contribuíram para a pessoa que sou hoje, à minha família, principalmente a minha mãe, mas especialmente a minha avó. Obrigado.

Acknowledgments

This was probably the hardest time of my academic path and I could not do it all by myself. I needed friends, professors and family to make it throught and, before proceding, I wish to thank everyone who has contributed directly or indirectly this work.

In particular, I would like to acknowledge the contribution of my supervisor Professor Pedro Ricardo Morais Inácio, first for accepting to be my advisor, and then by his unequaled set of skills, knowledge, expertise, support and encouragement over the years, specially in the last year.

I would like to cease this opportunity to express my gratitude to the members of the research group Multimedia Signal Processing - Covilhã (MSP-CV) of the *Instituto de Telecomunicações*, independently of being students or professors. This group hosted my internship of my 3-years Bachelor of Science in *Tecnologias e Sistemas de Informação* also, and I would like to thank them for providing me a welcoming environment, adequate workstations and many sources of information.

I am very grateful to my fellow, André Ferraz, for his help, knowledge, support and tips.

A no less important acknowledge goes to my family, namly to my grandparents, father, mother and brother which, one way or the other, have contributed to my education and to the person I am today. My most sincerely thank you.

I am thankful to EyeSee, Lda., specially to Eng. João Redol, for partially financing this work.

Last, but not least, I would like to thank my girlfriend Viktoriya for her motivation, support and understanding during this last year. She gave me strength and inspiration to achieve my goals, even when they seem complicate.

Thank you all!

Resumo

No ano de 2015, o número de dispositivos móveis (e.g., *smartphones*, *tablets*, *phablets*, etc.) ultrapassou o número de computadores físicos a nível mundial. As características físicas destes dispositivos estão em constante evolução. O aumento da autonomia, da capacidade de armazenamento e processamento e das funcionalidades, são fatores que levam as pessoas a comprarem cada vez mais estes dispositivos. Existem milhares de aplicações para as mais diversas áreas, que podem ser instaladas e utilizadas no dia-a-dia do utilizador, desde aplicações financeiras, de saúde, jogos, filmes, utilidades, etc. Os utilizadores confiam cada vez mais nestes dispositivos, confiando-lhes dados e informações privadas e delicadas (e.g., fotos, contactos, vídeos, informações confidenciais, etc). Desta forma, os sistemas devem ser cada vez mais seguros, para que o utilizadores se sintam mais seguros com a utilização dos mesmos.

O *Android* é um sistema operativo *open source*, para o qual é simples desenvolver aplicações. ¤ data de escrita da dissertação, é o sistema operativo mais utilizado no mundo para dispositivos móveis, e os utilizadores confiam nos seus mecanismos de segurança para os proteger contra ataques de terceiros. Para além dos mecanismos de segurança que funcionam sem o conhecimento do utilizador, é possível utilizar outras aplicações opcionais de segurança, como as aplicações de bloqueio de ecrã (*lock screen*) com segredo. As aplicações de *lock screen* são sistemas de autenticação que permitem bloquear e controlar o acesso ao dispositivo. A autenticação é o processo em que uma entidade (uma pessoa ou sistema) se identifica perante outra entidade. O processo de autenticação é normalmente conseguido através da prova de conhecimento, posse ou de uma característica pessoal, fatores conhecidos na área pelas designaç¤es inglesas *something you know*, *something you have* e *something you are*, que podem ser usados individualmente ou combinados em sistemas multi-fator.

Um dos problemas dos *lock screens* e de alguns sistemas de autenticação da actualidade reside no facto de, independentemente do conceito utilizado, o código secreto para desbloquear ou para se autenticar perante o sistema ser sempre estático ao longo do tempo. Esta característica dos sistemas de autenticação da actualidade pode ser explorada por utilizadores mal intencionados. Caso o segredo de autenticação (e.g., código de uma aplicação *lock screen*) seja descoberto, e o utilizador não saiba que o seu segredo foi comprometido, o utilizador que descobriu o segredo pode autenticar-se, fazendo-se passar pelo verdadeiro utilizador, visto que o sistema pergunta sempre pelo mesmo código secreto. Nos sistemas de autenticação convencionais e mais utilizados, sistemas baseados na introdução de *username-password* ou introdução de um padrão, se o utilizador quiser precaver-se da situação descrita anteriormente, tem o incomodo de ter que alterar e memorizar com frequência um novo segredo de autenticação.

Este programa de mestrado consistiu no desenvolvimento e estudo de uma nova abordagem de autenticação em que o segredo é dinâmico, o que significa que este muda ao longo do tempo, sem ser preciso a intervenção direta do utilizador. Um dos objetivos a alcançar com esta abordagem é conciliar a segurança com a experiência do utilizador. O utilizador não tem o incómodo de mudar o segredo de autenticação nem tem que lembrar-se da mesma forma que se lembra de uma palavra-passe, Personal Identification Number (PIN), imagem, padrão, etc. Nesta abordagem, o sistema de autenticação utiliza actividade registada no dispositivo móvel para gerar o código secreto que permite desbloquear e identificar o utilizador. Este método de autenticação

é simples, porque é baseado em informação que o utilizador sabe automaticamente e não é baseado em alguma coisa em que o utilizador é obrigado a decorar. Este é um mecanismo mais seguro, pois o segredo de autenticação não é estático, contrariamente a muitos mecanismos de autenticação utilizados nos dias de hoje.

Para se testar a viabilidade da abordagem de autenticação, decidiu proceder-se à elaboração de um inquérito para obter retorno dos utilizadores sobre vários aspetos. O inquérito foi feito em formato digital e recorreu também a uma aplicação móvel para o sistema operativo *Android*. O inquérito foi divido em três partes. A primeira parte continha perguntas sobre o conhecimento e hábitos de segurança na utilização de *smartphones* e ainda perguntas relacionadas com o tema do programa de mestrado. A segunda parte do inquérito continha o teste de usabilidade. Neste teste, foram feitas várias questões relacionadas com a actividade do utilizador no *smartphone*, nomeadamente perguntas sobre as chamadas e mensagens mais recentes. O teste de usabilidade estava dividido em quatro grupos, com três perguntas em cada um: uma sobre o nome do contacto associado a *chamadas*, outra sobre a duração das *chamadas* e outra sobre o nome do contacto associado às *mensagens*. Na última parte do inquérito, as perguntas eram destinadas a conhecer a opinião do utilizador em relação ao inquérito e ao tema do mesmo.

Depois da entrega dos resultados dos inquéritos, avançou-se para a análise dos resultados. Elaboraram-se análises individuais e comparativas para diferentes aspectos. Concluiu-se que o utilizador se lembra mais facilmente de informação relativa aos nomes de contactos, tanto em relação a chamadas como a mensagens, tendo mais dificuldade em relembrar-se da duração das chamadas. Os participantes revelaram mais rapidez em responder às questões relativas a mensagens do que em relação a ambas as questões de chamadas. Através do inquérito pode-se avaliar e analisar vários outros dados, como qual o tipo de actividade de que o participante está mais ciente (últimas vs. penúltimas actividades) ou por exemplo o impacto da quantidade do número de respostas que são mostradas ao utilizador. A maior parte dos inquiridos achou a abordagem muito interessante.

Aparte o que foi mencionado antes, o resultado mais visível deste trabalho é o protótipo final para um *lock screen*, que disponibiliza dois modos de operação. Na primeira versão, o utilizador tem que responder correctamente a uma série consecutiva de perguntas para desbloquear o seu *smartphone*. Na segunda versão, são exibidos vários nomes de contactos no ecrã, o utilizador tem que selecionar o conjunto de contactos com quem tem mais frequência de interação para desbloquear o *smartphone*. Foi adicionado um segundo mecanismo de autenticação para o caso do utilizador n□o se conseguir autenticar. Nesse caso, a dificuldade é detectada pelo sistema, que envia o utilizador para um segundo sistema de autenticação, onde pode usar um código PIN por si configurado anteriormente.

Palavras-chave

Actividade Utilizador, Android, Ataque de Escuta Sobre o Ombro, Autenticação, Bloquear, Bloquear Ecrã, Controlo de Acesso, Desbloquear, Palavra-passe, Palavra-Passe Dinâmica, Segredo Dinâmico, Segurança, Segurança Móvel, Telemóvel

Resumo Alargado

Mundialmente, o número de utilizadores de *smartphones* tem crescido muito rapidamente, em particular o número de utilizadores que usa dispositivos com sistema operativo *Android*. A principal característica destes dispositivos é a sua capacidade multi-funcional, j□ que permitem funcionalidades e comunicação mais avançadas tecnologicamente que os telemóveis convencionais. Este tipo de dispositivos permitem que os utilizadores instalem aplicações que podem ser uma mais valia no dia-a-dia do utilizador, nomeadamente relacionadas com finanças, bancos, saúde, redes-sociais, entretenimento, fotografia etc. A aproximação entre os dispositivos móveis e os utilizadores é cada vez maior. Cada vez mais confiam-se a estes dispositivos várias tarefas importantes, informações e dados privados.

Desta forma, é de esperar que os sistemas operativos possam responder com sistemas de segurança robustos, fiáveis e alternativos. Para além dos mecanismos de segurança que funcionam sem o conhecimento do utilizador, o sistema operativo oferece outras aplicações opcionais de segurança, como as aplicações de *lock screen* com segredo. Estas, são aplicações de autenticação permitem bloquear o dispositivo móvel (e.g., após algum tempo sem aceder ao mesmo), e o seu desbloqueio sśe preocessa se o utilizador introduzir o código secreto definido anteriormente.

A autenticação é o processo em que uma entidade (uma pessoa ou sistema) se identifica perante outra entidade. O processo de autenticação é normalmente conseguido através da prova de conhecimento, posse ou de uma característica pessoal, fatores conhecidos na área pelas designaç□es inglesas *something you know*, *something you have* e *something you are*, que podem ser usados individualmente ou combinados em sistemas multi-fator. Os fatores mencionados anteriormente são utilizados diariamente nos mais diversos sistemas de autenticação:

- *Something You Know* - em mecanismos de autenticação que usem este factor, o utilizador tem normalmente de decorar algo (e.g., um número ou uma palavra), para no momento da autenticação lembrar-se e inserir o código. Exemplos incluem: código *Personal Identification Number (PIN)*, *username-password*, código *padrão*, etc.

- *Something You Have* - neste caso o utilizador não tem que decorar nada, mas tem que transportar algo físico, como um cartão Radio-frequency identification (RFID) ou cartão multibanco. O segredo de autenticação é guardado dentro do cartão, ou a presença e demonstração do objeto é considerado como parte do segredo.

- *Something You Are* ou *Something You Do* - para este factor de autenticação, os sistemas utilização características biométricas do utilizador para gerar o segredo de autenticação. Normalmente estas características são únicas e só o utilizador □ que as possui. Também se incluem nesta categoria sistemas baseados em algo que só determinada entidade consegue fazer. Neste tipo de sistemas de autenticação o utilizador não necessita de decorar um código secreto nem tem o fardo de transportar um objeto matérial. Apesar dos sistemas de autenticação baseados neste factor serem bastante apelativos, ainda existem algumas questões de segurança a preocupar, pois a autenticação neste tipo de sistemas não é baseada na exatidão das amostras, mas por semelhança entre a amostra da característica guardada na base de dados e amostra recolhida no momento de autenticação. Além disso,

existem muitos fatores externos que podem alterar as características biométricas do utilizador e enganar o dispositivo biométrico. *Smartphones* com leitor de impressão digital ou leitor facial são exemplos de mecanismos de autenticação baseados neste factor.

Um dos problemas dos *lock screens* e dos sistemas de autenticação da actualidade é o facto de, independentemente do conceito utilizado, o código secreto para desbloquear ou para se autenticar perante o sistema ser sempre estático, i.e., o segredo não muda ao longo do tempo. Este facto acaba por ser utilizado de forma mal-intencionada por *crackers* para obterem acesso ao sistema. Existem diversos ataques que podem ser utilizados com elevado grau de sucesso para descobrir o segredo de autenticação e aceder ao sistema.

Na solução sugerida nesta dissertação, pretende-se desenvolver e estudar uma nova abordagem de autenticação em que o segredo de autenticação é dinâmico, mudando ao longo do tempo, sem ser preciso a intervenção direta do utilizador. Um dos aspetos importantes que era desejável alcançar com esta abordagem seria o de conciliar a segurança com a experiência do utilizador. O utilizador não tem o incomodo de mudar o segredo de autenticação, e não tem que lembrar-se da mesma forma que se lembra de uma *palavra-passe* ou *PIN*, por exemplo. Nesta abordagem o sistema de autenticação utiliza actividade registada no *smartphone* para gerar o código secreto que permite desbloquear ou identificar o utilizador. Esta informação é utilizada para construir desafios de questão-resposta, em que o utilizador tem que responder positivamente para desbloquear o *smartphone*. O mecanismo de autenticação utiliza parte da informação da actividade para fornecer uma forma de desbloqueio e de identificação do utilizador mais simples e segura:

- é simples, porque é baseada em informação que o utilizador está ciente e em nada que o utilizador seja forçado a decorar;

- é segura, porque não é estática, contrariamente a muitos segredos de autenticação utilizados nos dias de hoje. O segredo de autenticação depende da actividade do utilizador, o que vai alterar o segredo a cada autenticação.

Esta nova abordagem assenta no uso da informação relativa a actividade do utilizador no seu dispositivo móvel para gerar as questões e respostas do mecanismo de autenticação. Neste programa de mestrado desenvouve-se um estudo para analisar o conhecimento do utilizador em relação a sua actividade no *smartphone*, como informação relativa a chamadas e mensagens, para que no protótipo final fossem utilizadas as melhores fontes de informação para gerar as questões e respostas. Este mecanismo de autenticação tem duas fases:

- Na 1ª fase, os dados de diferentes atividades realizadas pelo utilizador são armazenados no dispositivo por aplicações nativas. Esta informação vai ser utilizada na próxima fase;

- Na 2ª fase, vários desafios de perguntas-respostas são geradas automaticamente com base nas actividades referidas anteriormente. O utilizador deve responder corretamente a essas perguntas para desbloquear o dispositivo.

Na 1ª fase, utilizar utiliza várias aplicações do seu dispositivo, as mais utilizadas normalmente são aplicações relacionados com chamadas e mensagens. Cada vez que o utilizador usa estas

aplicações, são registadas na base de dado do sistema operativo vários dados relativos a sua utilização, como a duração de chamada, a hora, o dia, para que contato foi, se foi uma chamada recebida ou enviada, etc. Desta forma, grande parte da actividade que o utilizador faz no seu dispositivo móvel é armazenada e normalmente o utilizador está ciente de grande parte do conteúdo dessa informação armazenada. De certa forma, a 1ª fase pode ser equiparada com a fase de registo e de configuração de um mecanismo de autenticação, onde o utilizador tem que configurar o código secreto por exemplo. No nosso mecanismo o utilizador não tem que se dar ao trabalho de elaborar este passo, pois o segredo é gerado aleatoriamente, e o utilizador está ciente dessa informação.

A 2ª fase é dedicada ao procedimento de autenticação do utilizador perante o dispositivo móvel. Quando o *software* de *lock screen* é iniciado, o sistema é bloqueado até o utilizador conseguir provar a sua identidade ao sistema. Para desbloquear o utilizador tem que responder corretamente a uma serie de perguntas que o sistema faz, estas perguntas são baseadas em informação gerada na 1ª fase.

O inquérito foi elaborado principalmente por dois motivos: primeiro para conhecer o conhecimento geral da população dos participantes em relação a dispositivos móveis e a sua segurança; e segundo para testar o conhecimento dos participantes em relação à sua actividade no seu *smartphone*. Desta forma o inquérito estava dividido em 3 partes. A primeira parte com perguntas relativas ao conhecimento geral (e.g., perguntas relacionadas com os participantes, seu conhecimento em termos de segurança em dispositivos móveis) dos participantes. A segunda parte consistia no teste de usabilidade. A última parte era relativa a questões sobre a opinião e *feedback* do participante em relação ao inquérito e ao tema abordado no mesmo. A entrega deste inquérito foi feita durante várias semanas. Quando se abordava um possível participante eram efetuadas algumas perguntas iniciais, transcritas para aqui:

- Está disponível para responder a um questionário relativo a uma dissertação de mestrado?
- Tem um sistema operativo *Android*?
- A versão do sistema operativo é igual ou superior a 4.1?
- Aceita instalar a aplicação do questionário no seu *smartphone*?

A abordagem para entrega e divulgação do inquérito era feita de forma aleatória e em vários locais. A divulgação foi feita na universidade, em cafés, no grupo de trabalho, através de redes sociais como o *facebook* e *reddit*, entre outros. Além disso, era pedido às pessoas para darem a conhecer o inquérito aos seus amigos e familiares. Ao inquérito responderam 44 pessoas, com idades compreendidas entre os 16 e 54 anos de idade. A população inquirida tinha os mais diversos graus académicos e vinha das mais diversas áreas profissionais. A apresentação do questionário foi feita a um número considerável de pessoas, mas por diferentes razões, alguns participantes não responderam ou não entregaram os resultados do inquérito. De seguida, são mencionadas algumas razões que impediram determinadas pessoas de responderem ao inquérito:

- Não tinha disponibilidade (tempo) para responder;

- O *smartphone* não tinha sistema operativo *Android*;

- O dispositivo *Android* não preenchia os requisitos mínimos para se poder instalar aplicação de inquérito;

- Algumas pessoas revelaram não estar interessadas em participar e contribuir para a investigação;

- Algumas pessoas instalaram a aplicação, mas por razões desconhecidas não enviaram os resultados do inquérito;

- Algumas pessoas ficaram com dúvidas sobre os privilégios requeridos pela aplicação de inquérito para ser instalada, como por exemplo, os privilégios para aceder às chamadas e mensagens do dispositivo móvel;

O inquérito e a análise dos resultados foram a parte mais difícil e interessante do programa de mestrado. Analisou-se e avaliou-se o conhecimento dos utilizadores em relação ao tema da dissertação e ao conhecimento que os participantes revelavam sobre a sua actividade no *smartphone*. Nesta fase analisou-se de forma individual e fizeram-se a comparações de vários dados para retirar conclusões dos mesmos. Para melhor análise dos resultados foram gerados vários gráficos, estes são acompanhados de uma breve explicação e análise dos mesmos nesta disserta□□o ao longo do cap□tulo 4. De seguida são mencionadas as principais conclusões da análise dos resultados:

- A maior parte dos participantes mostraram interesse no tema da dissertação e também gostaram da abordagem proposta. Boa parte da população inquirida gostava de ver mais investimento em estudos e aplicações sobre o novo conceito (ver figuras A.11,A.12).

- Concluíu-se também que, dos três tipos de questões (*nome associado a determinada chamada*, *duração de determinada chamada* e *nome associado a determinada mensagem*), os participantes revelaram ter menos conhecimento nas questões relativas à duração de chamadas do nas outras duas. Contudo, achou-se indevido excluir totalmente as questões relativas à duração de chamadas. Participantes acertaram aproximadamente 93.5% das questões relativas a nome de contato de chamadas e mensagens. No caso das questões relativas à duração das chamadas, a taxa de sucesso ficou se pelos 53.4% (ver figura 4.9).

- Analisou-se o impacto da quantidade de possíveis respostas exibidas ao participante. Após uma analise detalhada dos dados, concluíu-se que, em determinadas questões, o número de respostas sugeridas não tinha um impacto relevante, contudo, em termos gerais, concluíu-se que a partir de 3 op□□es, por cada resposta adicional, a dificuldade em responder à essa questão aumenta aproximadamente 4% (ver figura 4.10).

- O espaço temporal de cada tipo de questão também foi avaliado. Chegou-se à conclusão que os utilizadores conseguem acertar mais às questões relativas às últimas do que a penúltimas actividades. Ou seja, recordam se mais facilmente do nome associado à última chamadas efetuada do que da penúltima (ver figura A.13).

- Para as questões sobre duração de chamadas, definiram-se 3 tempos mínimos (15, 30 e 60

segundos) de diferença nas respostas exibidas ao utilizador. O tempo era escolhido aleatoriamente durante a geração da questão. O tempo de diferença mínimo entre cada duas respostas deveria ser no mínimo esse tempo escolhido. Concluíu-se que os utilizadores têm mais facilidade em acertar a esta questão se o tempo mínimo escolhido for de 60 segundos. Os participantes revelaram ter mais dificuldade em diferenciar a duração real da chamadas das falsas se o tempo mínimo fosse de 15 ou 30 segundos (ver figura 4.11).

- Durante o teste de usabilidade, monotorizou-se (sem conhecimento do participante) o tempo que o participante demorava ao responder a cada questão. Esta avaliação foi bastante importante, porque permitiu perceber em quais questões os participantes demonstravam requerer maior e menor tempo. Além disso, foi possível perceber o tempo despendido em cada grupo do teste de usabilidade (ver figura 4.12). O tempo despendido a responder a cada pergunta pode traduzir-se na informação que está mais ou menos ciente para o utilizador, ou que pelo menos, o utilizador está mais à-vontade em responder rapidamente (ver figura 4.13).

Para testar o conceito apresentado nesta dissertação, desenvolveu-se um protótipo de demonstração, este consistia numa aplicação de *lock screen* baseada abordagem sugerida neste trabalho. Este *software* de teste é destinado a *smartphones* com o sistema operativo *Android*, mais precisamente à versão 5.0 *Lollipop* ou superior. A linguagem utilizada para desenvolver o protótipo foi Java, na *Android* Application Programming Interface (API) nível 21. O *software* foi desenvolvido utilizando o *Android Studio 2.0*. Desenvolveram-se dois modos para demonstrar a abordagem proposta. Desta forma os utilizadores podem experimentar o mesmo conceito demonstrado de duas formas diferentes e alternativas.

Na variação do protótipo designada por *modo A*, o*software* gera um conjunto de questões para o utilizador responder. A cada questão estão associados um determinados número de pontos. O sistema tem dois limites, um superior e um inferior. Se o limite superior for alcançado, o *smartphone* é desbloqueado. Caso o limite inferior seja alcançado, o utilizador é enviado para um segundo mecanismo de autenticação. O utilizador inicia com um determinado número de pontos que alteram consoante o utilizador acerte ou falhe a resposta a uma pergunta. Uma resposta correta acrescenta pontos, uma resposta errada reduz o número de pontos do utilizador. Caso o número de pontos seja reduzido até ao limite inferior, o dispositivo troca o sistema de autenticação proposto por um alternativo. Para além do sistema de pontos, existe um limite máximo de perguntas a exibir. Caso esse limite seja alcançado, o sistema troca o mecanismo de autenticação por um secundário. Este segundo mecanismo de autenticação é baseado no sistema de introdução de um PIN.

Na segunda variação do protótipo, designada por *modo B*, o sistema cria uma lista (lista A) com os 15 contatos (este número pode variar) com quem o utilizador revela ter mais interacção. Para criar esta lista o *software* utilizada informação relativa às listas de chamadas e mensagens. O *software* vai ordenar a lista A, dos contactos que o utilizador tem mais frequência para aqueles com quem ele tem menos frequência, e por fim seleciona os quatro (este número pode variar) primeiros da lista. Depois disto, o *software* vai criar de uma segunda lista (lista B). Nesta lista vão estar os quatro contatos selecionados anteriormente e mais seis contatos (este número pode variar). Para escolher estes seis contatos, o sistema vai analisar a lista (lista Z) de contatos do *smartphone* e vai escolher seis contatos aleatoriamente. Contudo, só serão válidos e adicionados

à lista B se não existirem na lista inicial (lista A). Desta forma, é formada a lista B, com quatro contactos com quem o utilizador tem mais interação e mais seis contatos com quem o utilizador não revela ter quase actividade. O protótipo vai mostrar uma lista de nomes de contatos no ecrã, representado os contatos da lista B. O utilizador tem que selecionar os quatro contatos com quem mais interage para desbloquear o dispositivo. O utilizador pode definir se os nomes devem ser escolhidos por uma ordem especifica ou n□o. Se o utilizador definir que quer que o protótipo requira uma ordem especifica na escolha dos contatos, o nível de segurança aumenta, comparado à opção de não requerer uma qualquer ordem de seleção.

Nesta dissertação apresentou-se uma nova abordagem de autenticação. É desejável continuar a investigação de possíveis mecanismos de segurança que utilizem esta abordagem. Podendo ser utilizada a abordagem de forma completa ou parcial, como ser utilizada como mecanismo complementar de um sistema de autenticação já existente. De seguida, são mencionados algumas sugest□es de trabalho futuro:

- Elaboração de um inquérito para testar o conhecimento dos utilizadores sobre outras actividades nos seus dispositivos móveis e em outros dispositivos (e.g., *smart Television (TV)*);

- Criar um protótipo em que a informação de actividade provém de uma nuvem de informação. Esta nuvem iria ter reunida informação de vários dispositivos do utilizador;

- Estudo da utilização deste conceito para *fall-back authentication*. Este conceito seria utilizado para o utilizador recuperar uma *password* ou conta esquecida;

- Elaboração de um inquérito em que fosse possivel testar a capacidade de um desconhecido desbloquear um dispositivo que não lhe pertence-se (i.e., um dispositivo de outro participante). Esta forma de proceder iria permitir estudar outros fatores de segurança relativos à abordagem;

- Num futuro próximo, seria bastante interessante estudar a combinação deste novo conceito com outras formas de autenticação.

Abstract

In 2015, the number of mobile devices (e.g., smartphones, tablets, phablets, etc.) exceeded the number of physical computers worldwide. The physical characteristics of these devices are constantly evolving. Increased autonomy, storage and processing capacity, as well as functionality are factors that lead people to buy more and more of these devices. There are thousands of applications for many different areas, that can be can be installed and used on daily-basis, ranging from finantial applications, to health, games, movies, and utilities, etc. Users increasingly rely on these devices, entrusting them with private or sensitive data (e.g., photos, contacts, videos, confidential information, etc.). Thus, the system must be ever safer, so that the users also feel safer when using them.

Android is an open source Operating System (OS), for which is simple to develop applications. At the time of writing of this dissertation, this was the most widely used OS in the world of mobile devices. and users rely on its security mechanisms to protect them against attacks from third parties. In addition to the security mechanisms functioning without the explicit knowledge of the user, it is possible to use other optional security application such as lock screens with associated secret. The lock screen applications are authentication systems that allows one to block and control the access to the device. The authentication is the process by which an entity (e.g., a person or a system) is identified by another entity. The authentication process is usually achieved by proving knowledge or possession of a personal characteristic or device, which are known as *something you have*, *something you have* or *something you are* factors. These designations that are typically used to categorize authentication mechanisms. Several factors can be combined in multi-factor systems to increase security.

One of the problems of lock screens and current authentication systems is that, regardless of the concept being used, the secret code to unlock or to authenticate to the system is always static along the time. This specific characteristic of the current approaches can be exploited by malicious users. If the authentication secret (e.i., the code of a lock screen application) is discovered, and the user is unaware of this fact, then the malicious user who discovered the secret can log in afterwards and impersonating the real user, because the system always asks for the same secret code. If the user wants to avoid the aforementioned situation while using the popular authentication systems based on username-password or patterns, he has the inconvenience of having to change and memorize a new authentication secret regularly.

This master's program consisted in the development and analysis of a new approach for authentication in which the secret is dynamic, which means that it changes over time without the direct intervention of the user. One of the main objectives that are expected from this approach is that it conciliates security with user friendliness. The user is not forced to change the secret nor has to explicitly memorize it in the same way he memorizes a password, Personal Identification Number (PIN), image, pattern, etc. In the proposed approach, the authentication system uses the activity of the user on the mobile device to generate the secret that enables unlocking it and identify the user. The data concerning user activity is stored by the OS itself. This authentication method is simple, because it is based in information that the user knows without much effort, and it is safe, because the authentication secret is not static, contrarily to many authentication mechanisms used nowadays.

To test the feasibility of the authentication approach, it was decided to proceed with the preparation of a survey to obtain feedback from users on different aspects. The survey was done in digital format and used also a mobile application for the Android operating system, specially designed for the subject at hands. The survey was divided into three parts. The first part contained questions about knowledge and safety habits in the utilization of smartphones, and also questions related to the main topic of this master's program. The second part of the survey contained a usability test. In this test, several challenge-questions related with the activities of the participant on your smartphone were asked, namely questions about the most recent calls and messages. Usability testing was divided into four groups, with three questions each: one on the contact name associated with incoming or outgoing calls; one on the duration of calls and the another one on the name associated with the most recent messages. In the final part of the survey, the questions were designed so as to obtain the opinion of the user regarding the proposed approach and the subject of the dissertation. After the delivery of the survey results, progress was made to analyze the results.

After having obtained enought users participating in the survey, the results were analysied. Several individual and comparative analysis were performed at this stage. It was concluded that users remember information about contact names more easely, both for calls and for messages, and that they find it more difficult to memorize the duration of calls. Participants were faster answering to questions related with messages than related with calls. Through this survey and its results, it was possible to evaluate and analyze various other aspects, such as the kind of activity the user is more aware of (e.g., last vs. penultimate activities), or the impact on effectiveness of the number of options displayed for every question. Most participants found the approach to be very interesting.

Apart from what was mentioned before, the most visible outcome of this work is the final prototype for a lock screen, which offers two modes of operation. In the first version, the user must correctly answer a consecutive series of questions to unlock the smartphone. In the second version, several contact names are displayed on the screen, and the user has to select the group of contacts with whom he interacts more frequently, in order to successfully unlock the device. An additional (alternative) authentication mechanism was added to the lock scree, in case the user is not able to authenticate using the first one. This secondary mechanism is triggered automatically after several failed attempts to login or incorrect answers, and it consists on the insertion of a pre-configured PIN,

Keywords

Access Control, Android, Authentication, Dynamic Password, Dynamic Secret, Lock, Lock Screen, Mobile Application, Mobile Device, Mobile Security, Password Security, Security, Shoulder-surfing Attack, Smartphone, Unlock, User Activity

Contents

List of Figures

List of Tables

Acronyms

2FA 2-Factor Authentication

ACM Association for Computing Machinery

API Application Programming Interface

APP Application

ATM Automated Teller Machine

CAS Code Access Security

CCS Computing Classification System

GPS Global Positioning System

iOS iPhone Operating System

IT Information Technology

NFC Near Field Communication

MFA Multi-Factor Authentication

OS Operating System

PIN Personal Identification Number

RFID Radio-frequency identification

ROM Read Only Memory

SDK Software Development Kit

SMS Short Message Service

TV Television

UBI Universidade da Beira Interior

USA United States of America

Chapter 1

Introduction

The work reported in this dissertation concerns the development of a lock screen for Android mobile devices based on a new authentication approach. To the best of the knowledge of the author, this approach was never explored or investigated before. This project was included in the context of the 2nd cycle of studies of Computer Science and Engineering of the University of Beira Interior, Covilhã, Portugal. This chapter contains the context for the work performed during this year in section 1.1. Section 1.2 then motivates the problem and presentes the objectives of the master's program. Section 1.3 is dedicated to a brief explaination on how the problem was solved. The contributions to the scientific community are then subject of discussion in section 1.4. Finally, section 1.5 presents the structure of this dissertation in a brief manner.

1.1 Focus and Scope

The sales of mobile devices, like smartphones, tablets and other small electronic devices has been growing over the last years [Sta15]. The beginning of 2014 is an historic moment, where the number of mobile users exceeded the number of desktop users, as shown by several statistics [Dan13, Reb14]. Two billion mobile users in the entire planet is the number expected at the end of 2015, and the trend is for sales and number of users to continue to increase [Dan13]. One of the Operating Systems (OSs) that have been most popular and increasingly gaining market share in the world of mobile devices is Android [IDC15, Net15]. The popularity is largely due to the fact that this OS is open source and allow users to install many applications, tweak several features and configurations and change home screen widgets [Mob15] according to the preferences of the user. Because the source code is open, there are modified Read Only Memorys (ROMs) also available. Other options for modern mobile devices are Windows Phone, iPhone Operating System (iOS), Symbian and Kindle [Net15], though they do not have such a large market share, when compared to Android. The latter represents more than 50% of the global market share on mobile devices [IDC15, Net15, O'C15].

Smartphones are the new mobile phones. The great advantage of these devices is that they allow the installation of a large variety of applications for several distinct objectives. Users typically have more than one choice for a given purpose, the diversity of applications in the online mobile stores is one of the factors that made smartphones so important in our daily lives. A user can find applications related with health, financial, commercial, social, kitchen, homebanking, traveling, entertainment, and many other subjects. In the case of Android, the official store holding a plethora of such applications is known as *Goolgle Play*, though several others can be found and installed in the devices. With the advent of new technologies and with the increase of useful apps, accompanied by price drops on the equipments, it can be said that people are becoming more dependent of mobile devices, and this trend is expected to continue in the for the future to come.

As smartphones become more feature rich and part of their daily lives, users rely increasingly more on these devices. As such, security of mobile devices has become increasingly important. Several applications keep personal information about the user of the smartphone, whose many times not even aware of that monitoring. To make it worst, some data is stored remotely, as the Cloud model gains momentum. This data may have different sources, meaning, and importance. It may even look innocuous from a naive point of view, but if it is private, you should be secured and the user probably does not want anyone to have access to it. On the other hand, the applications installed and configured on the mobile devices may also be important to the user, and unauthorized access may even lead to financial losses, as homebanking applications may be set up with to automatically log in or with an open session. Photos, health or work related information are other examples of critical private information that may be frequently found in mobile devices.

The user assumes that the smartphone OS keeps applications secure, and most importantly, that the data that the smartphone collects from the user is kept safe and intact. There are several ways an unauthorized user can collected and get personal information from a smartphone that does not belong to him. From complex hacking procedures, to simple actions that do not require the help of a computer or any other kind of hardware or software. It is important to keep any software updated with the latest security mechanisms, and try to be one step ahead of any possible attack technique that the system could suffer. Researches have shown that a lot of users do not use, to the full possibilities, the security mechanisms that are available to them. Due to the fact that Android is open source and distributed by several companies, OS updates and security patches cannot be generated and distributed from a single source, and many mobile users are sometimes using software with known security bugs and flaws, with no automatic and general patching mechanism, apart from reinstalling or updating those apps. One of the biggest problems with Android is the fact that one of the most important security systems, the security-by-permission mechanism, needs more documentation as well as more granular control, and it can be misused by third-party developers [JM13].

The authentication on mobile devices, performed via the lock screen, is one of the most important security mechanism that the user can use to protect the device. Text-based passwords are a common approach for authentication, and users typically choose weak passwords, and have problems to recall strong ones. In their research [SZO05], Suo et al. mention that there are not enough studies proving that the brain is better in remembering graphical passwords than text-based passwords, but they also say that is more difficult to break a password based of images and graphical data using the common attack methods, such as brute force search and dictionary attack. There is not a lot of implementation of graphical passwords, but one of the most known schemes is used on Android systems: the *Android Unlock Pattern* scheme. The user is presented with a 3x3 grid, and must draw a sequence of lines connecting the dots. That sequence represents the password of the user. Another graphical password approach is the one used by Windows OSs starting from 8.0, which uses a combination of images and touchscreen gestures to create a password system [CW13]. To perform the authentication the user must select a series of key points (e.i., previously defined by the user himself). Normally users can understand graphical schemes very easily. In practice, this subject needs more research and tests, some security aspects of these schemes are hardly studied, therefore the advantages and security offered by this type of schemes compared to text-based password remain to be identified. One problem that persists in all of the above is that their are based on a static *something you know*, mean-

ing that the secret remains the same over time (unless the user explicitly changes it). Several researchers [WWB+05] have defended that passwords have to be constantly changed in order to improve security. However, this would lead to an increase of the difficulty that the human mind has in remembering several lengthy passwords.

To the best of the knowledge of the author, the first study to perform authentication based on user activity on mobiles was performed in the scope of this master's program. This work falls within the intersection of the computer security and programming of mobile devices areas, concretely in the authentication on mobile devices topic. Under the 2012 version of the Association for Computing Machinery (ACM) Computing Classification System (CCS), a *de facto* standard for computer science, the scope of the masters program, reflected in this dissertation, is defined by the categories named:

- **Security and privacy∼Authentication**
- **Security and privacy∼Access control**
- *Security and privacy∼Mobile platform security*
- Security and privacy∼Software and application security

1.2 Problem Statement and Objectives

The main problem addressed in this master's program is related with the fact that most authentication mechanisms are based on a static secret. The users need to remember this static secret and set it up prior to using the mechanism. The secret does not often change for long periods of time, making it more prone to attacks and susceptible to shoulder surfing. The problem is obviously wider than this, and encompasses the fact that users implicitly trust that the data is secure in their mobile device. Making the users aware of this fact is one way to tackle the problem, but it is not perfect, since people should actually be able to trust the data is safe. Nonetheless, this work starts from the believe that the potential of these new devices is not being used in full. Since they are fundamentally different from previous computing devices and, specially, more personal, then different mechanisms can also be devised for all purposes, namely authentication, as it also has been proved before.

The main objective of this work is thus to study a new means to authenticate on mobile devices based on the user activity. The approach is still classified as *something you know* mechanism, but the secret is dynamically generated and it does not need to be explicitly memorized by the user. Secondary objectives include the following:

- Study existing authentication mechanisms for mobile devices, namely available lock screens for smartphones with the Android OS;
- Contextualize the proposed authentication approach within the state of the art and formalize a possible first iteration of the mechanism;
- Implement a prototype for the Android OS and assess its feasibility, usefulness and security, namely via user oriented surveys.

1.3 Adopted Approach for Solving the Problem

The adopted approach for solving the problem was focused on the proposal and development of a new authentication scheme. An Android application mimicking a lock screen for that OS was implemented and used to test its feasibility and assess its usefulness and adoption from real users, before producing a prototype for proof-of-concept. In order to achieve the proposed objectives, this master's program was divided into the following main phases:

1. The first phase consisted in the effort to contextualize with the subject of this dissertation and getting familiarized with the terminologies involved, namely with the meaning of authentication, lock screen and secret code, etc. A depth study was conducted, dominated mostly by reading and analyzing several online references and scientific articles and reports;

2. The second phase was devoted to the understanding of how the users interact with their smartphones and better defining the authentication approach according to what was learned. This part included also the identification of a preliminary set of sources of data representing the user activity;

3. The third phase included studying the technologies necessary to the development of a first prototype mimicking a lock screen for Android devices. It required an exhaustive analysis of the way Android deals with the data sources identified in the previous phases and the requirements to construct a lock screen. This phase included also the setting up of the development environment and the installation of the necessary tools;

4. The fourth phase was mostly devoted to the development of an archaic lock screen implementing the new authentication approach and conducting several tests. This prototype was to be used in the next phase and needed to be ready to be used by real users in the context of a survey;

5. The fifth phase included the elaboration of a set of questions for a user survey. It also included the dissemination of the questionnaires and assisting in their fulfillment;

6. The sixth phase corresponds to the the time period in which the answers to the survey were analysed in detail;

7. The final phase consisted in the writing of this dissertation.

Though the approach was structured as discussed above, the third and fifth tasks were the most important, and it was devoted the most time and effort . In the third phase was tried to create a good set of questions and usability prototype. In the fifth phase was study the answers and feedback/opinion of the user about the all survey. Since the knowledge of the user is one of the pillars of this programme, this approach seems to be adequate to understand the user knowledge.

1.4 Main Contributions

The main contribution of this masters program was the research, investigation and development of user authentication mechanism for mobile devices, based on user activity. The final prototype is composed by an application for Android smartphones. Apart from this prototype, a different application (a preliminary prototype) for studying user activity was also developed along the course of this work, so as to test the approach during a user survey (at this point of the research, it was a typical Android application). The final prototype was entirely built resorting to the Android Application Programming Interface (API) and does not use any third party resources, nor hacks or bugs of the system to achieve its purpose. The application for studying user activity was very important in the scope of this work because it enabled obtaining a better knowledge of the important factors affecting the mechanism and also fine-tunning the final prototype, which is a lock screen. To the best of the knowledge of the author, there is no other efforts in producing an authentication mechanism like the one proposed and studied in this work.

The main contribution can be further decomposed into the following ones:

- A review of the state of art in terms of new authentication approaches was performed. The study was mostly focused on those aiming for usage in mobile devices as lock screens, and it eventually led to analyzing and comparing existing lock screen software available for the Android OS. This part is reflected in chapter 2.

- The way smartphone users interact with their phone and the activities they perform was studied with detail via several means. The most interesting findings were incorporated in the developed prototype. One of the utilized means included devising and delivering lengthy user surveys; the other included the usage of the custom made Android application.

- A final prototype based on the proposed approach was produced.

1.5 Dissertation Overview

This dissertation is organized in five main chapters and also two appendixes. The overall structure reflects the work flow of the master's program. The three intermediate chapters are dedicated to the description of the main parts of the program, ending up with a chapter on conclusions and future work. The subject of each one of the chapters can be summarized as follows:

- Chapter 1 - Introduction - provides a context for the subject at hands and the motivation behind this work. It also defines the problem to be addressed, the objectives and the adopted approach to achieve them. It enumerates the main contributions resulting from this work and this dissertation overview.

- Chapter 2 - Revision of the State of the Art - starts with a brief discussion concerning previous works related with the topic of this dissertation. It then proceeds to an explanation on the classification of authentication mechanisms, as well as their advantages and disadvantages. It then describes a few related works and scientific papers with more detail, ending up with the outline of what was learned from this phase of the work.

- Chapter 3 - Authentication on Mobile Devices Based on User Activity - is first devoted to the explanation and design of the authentication approach proposed in this dissertation. That section is followed by a discussion regarding security, privacy, performance and other aspects of the solution. This chapter explores the details, structure and background that was used to build the prototype and the survey. A summary of the chapter was added to emphasize aspects that was used later on.

- Chapter 4 - Prototype and Usability Tests - describes one of the most important phases of this master's program and also its main output. The chapter includes the presentation of the developed prototype and the elaboration and delivery of a usability test used to study the effectiveness, efficiency and user satisfaction of the authentication approach. This chapter contains several charts summarizing the results of the survey and an extensive analysis of the main findings. In the end of the chapter, a reflection about the progress of the work is included.

- Chapter 5 - Conclusions and Future Work - contains the main conclusions and summarizes the most interesting findings of this master's program. It also discusses directions for future work.

Appendixes A and B contain many charts that were produced during the analysis of the results of the user survey. These charts complement (and are mentioned in) the discussion of chapter 4.

Chapter 2

Revision of the State of the Art

2.1 Introduction

This chapter chapter reviews important concepts about authentication in general and particularly about lock screen software. Several references included herein were key to make the research presented throughout this dissertation possible.

Authentication is nowadays under the spotlight due to the importance security in computer systems has gained in the last few years. The research presented throughout this dissertation was made within the scope of user authentication in handheld devices on an Internet of Things scenario. This chapter attempts to contextualize the reader with the current state of authentication. For that purpose, an introduction to authentication mechanisms can be found in Section 2.2, where related works are discussed. An in-depth review of the literature in terms of applications and mechanisms is available in Sections 2.3 and 2.4. Section 2.5 summarizes the chapter and enumerates the main takeaways.

Computer security is a wide field of knowledge, spanning several areas such as software security, hardware security and network security. Access control in all fronts overlies those areas, requiring the interchange of technology and a myriad of protocols to achieve a desirable level of security. User authentication has been for the last few decades and still is an important step to attain that. Most user authentication methods are based on a static factor of authentication, known as password. However, nowadays many advocate that new approaches are required due to the gradual decline of password security and due to the increase of novel approaches (e.g., biometrics) in the mobile computing vision. This chapter elaborates on this topic, revewing the state-of-the-art of authentication factors and approaches.

The strict sense of authentication is the one of enabling a system to verify the identity of a requester, may that be a user, a device or a process. Authentication has been a common requirement ever since computers and networks came to existence, as it guarantees, if well implemented, that only rightful users, devices or processes can access some service or resource. Authorization, another part of access control, covers the part of which services and resources one is authorized to view. The most common approach to authentication is the one of username and password combination. Today, this form of authentication can be seen in widespread use in software like operating systems, websites, and online services. To cope with the gradual decline of password security and to take advantage of newer technologies, researchers started exploring new approaches to authentication. Multi-Factor Authentication (MFA), as it is called, aims at using additional factors beyond the static password to identify a requester, thereby providing additional security layers. New approaches to this paradigm usually aim at providing a high-level standard of security while striving to guarantee similar quality of experience for the end-user.

Authentication is so embedded into our daily lives that it may go unnoticed for most of the times. For example, opening the door of a car with a key is a simple demonstration of the possession of the key *to the car*. In air traveling, the passport is used as a means to identify the person traveling. Using debit or credit cars with the associated Personal Identification Number (PIN) to make purchases is another instance of authentication. This one is particular, however, is a form of second-factor authentication, where the user proves to have the possession of the card itself and to know the associated PIN. Nowadays, authentication factors are usually split into the following five categories [BJR+06, SUSM09, Gem11]: *something you have* (e.g., a hardware token/credit card), *something you are* (e.g., a fingerprint, eye print), *something you know* (e.g., PIN code, a password), *somebody you know*, and *something you process* [SUSM09]. Any of these factors can be combined to make strong authentication mechanisms. Failure to protect some resource from unauthenticated or unauthorized parties can result is severe consequences, such as data breaches.

Most devices nowadays, such as computers or smartphones, are locked out when inactive or not in use, requiring the user to input a secret code configured previously to unlock the device. This mechanism is meant to let only the owner of the device that configured the unlock code to unlock it and use it freely. The supplicant, if authenticated with success, is granted access to resources, functionalities, features and data according with the level of privileges assigned to that user. Despite the fact that the first devices with touch screen technologies were created in the middle sixties, only after the invention and massification of smartphones the software for that technology has been explored by developers. Enterprises are now exploring new authentication schemes, such as the lock screen, paving the way for upcoming authentication mechanisms.

2.2 Classification of Authentication Mechanisms

Authentication is a procedure to identify entities like individuals or systems. It is a security measure designed to protect something (e.g., a website, platform or device) from unauthorized parties such as malicious actors. There are several factors and approaches available to build authentication schemes. This section overviews various well-known or less prevalent authentications mechanisms. The authentication factors reviewed ahead are illustrated in Figure 2.1.

2.2.1 Something You Know

The *something you know* factor is based on something that the user knows, typically a PIN or an alphanumeric string such as password or a passphrase. Figure 2.2 depicts two examples of authentication applications based on the something you know factor. In this factor of authentication, the user has the ability to pick and change at will the code or password. Awareness of password security is low, typically resulting in poor choices of combinations of characters that lead to fast dictionary or brute-force attacks. Ideally, passwords should be complex enough in order to increase the time it takes to brute force them, such as being long and made of different types of characters. In addition, the more random the combination of characters is, the higher the entropy is. However, typical users often make weak and easily remembered passwords by choosing something personal (e.g., pet name or birthdate), thereby making them low entropic. On top of that, users usually use the same password across several services and platforms, which is a bad practice that should be avoided.

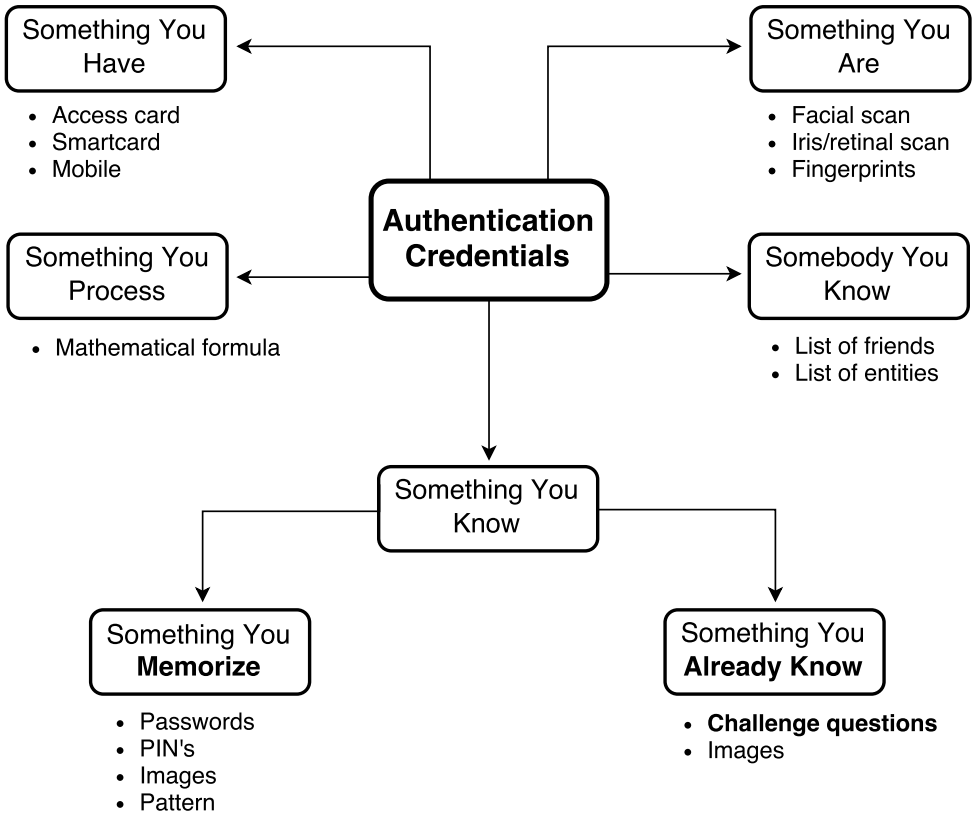

Figure 2.1: Diagram showing the types of authentication credentials (adapted from [Jus09]).

Another issue with passwords is the security awareness of people. They often lose them, pass them over to friends or work colleagues via chat or email, write them down on a piece of paper or on unencrypted computer files. Obtaining the password can therefore be as simple as reading a document or an email, making authentication solely based on passwords weak. In addition, hardware is getting faster everyday, following the Moore's Law principle, easing brute-force attacks. For these reasons, password-based authentication is being considered no longer a viable future for the mid- and long-term [Sch05].

Notice that the something you know factor can be split into two subcategories. The first subcategory, the *something you memorize*, is related with secrets the user is forced to memorize. At the time of enrollment, the user did not know the secret and must learn it in order to authenticate afterwards. Each time the secret is changed, the user is forced to re-learn the new one from then onwards. In the second subcategory, the *something you already know*, aims at re-using credentials that the user already knows or is aware of. Daily tasks, activities or other frequent process the user attends to are ways to build an authentication system following this principle. The authentication approach proposed in the scope of this work falls precisely in this category.

2.2.2 Something You Have

The *something you have* factor refers to the possession of a physical object (also known as hard token) that a user who wishes to authenticate must carry around. Figure 2.3 shows two examples of objects that are used as authentication credentials. The previously referenced example of the car keys fits this criteria. Another instance of something you have for authentication

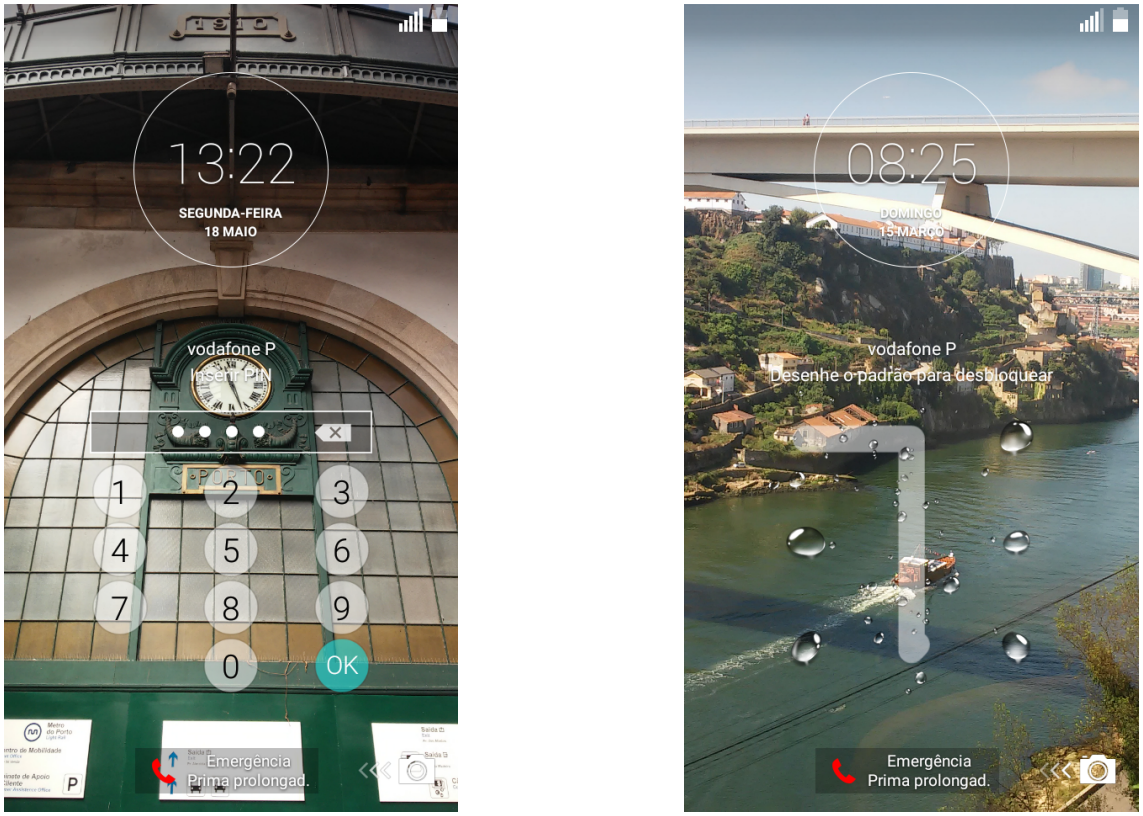

Figure 2.2: *Something You Know* factor: on the left side is depicted a PIN code lock screen, on the right side a pattern lock screen.

are Automated Teller Machine (ATM) cards which, when combined with the PIN code, makes a second-factor authentication mechanism. One of the advantages of the something you have approach is that the user does not need to memorize a probably complex secret, a burden which can be hold by the hard token itself. On the other hand, the token may malfunction, may need maintenance, and may be stolen or lost. In case of the token getting astray, it is possible to disregard it and setup a new one with ease (in a matter of minutes for soft tokens). One of the most widely used applications of hard tokens is the one associated with one-time passwords, where the secret provided by the token changes frequently from time to time (e.g., every 30 seconds). This makes it harder for a malicious actor to overcome authentication. The figure 2.3 shows 2 examples of objects that are used as authentication credentials, and are based on *something you have* factors.

2.2.3 Something You Are or Something You Do

This form of authentication is based on something intrinsic to the user being authenticated, such as the biometric traits show in figure 2.3. This type of authentication is based on unique characteristics of the user or in something that only the user can do, undeniably identifying an individual. The *something you are* is naturally inapplicable to systems or software and is hard to overcome without expensive technology and apparatus.

In password- or pattern-based authentication systems, the authentication is successful only and only if the provided input is exactly the same as the one stored in the databases. However, in the case of biometric traits, that comparison relies on the similarity between two biometric samples of the user trait, allowing a small amount of error. One sample is stored in the database, and

Figure 2.3: *Something You Have* factor: home keys [dS15] are depicted on the left side, while an Radio-frequency identification (RFID) card [img15] is depicted on the right side.

Figure 2.4: *Something You Are* factor: a facial scanner [Ham15] is depicted on the left side, on the right side a smartphone with a fingerprint scanner [dL14] is shown.

was provided during the enrollment phase, and another is obtained during the identification phase. The biometric characteristics chosen to use as a something you are must be easily and accurately measured and, if possible, difficult to spoof. Examples of biometric characteristics for authentication purposes include the retina, fingerprint, handprint, face geometry, voice print, vein geometry, among others.

The security of biometric-based authentication systems can be considered quite high. Although the proliferation of these is slowly progressing (e.g., iPhone fingerprint scanner), the cost of biometric readers is still high and the identification phase may present flaws. Biometric systems may be unreliable at times [JN12]. Human traits may change and a number of external factors (e.g., dirty finger, makeup) may incorrectly provide an unsuccessful authentication. In addition, physical injuries (e.g., face burns, eye damage by chemical burn) to the body may render a biometric trait different from the sample taken at the enrollment phase. Other external factors may also contribute to the malfunction of the biometric scanner, such as light, moisture, or reflection.

2.2.4 Somebody You Know

The Somebody You Know form of authentication explores the relationship between users (social relationship) and entities to identify a user. It is said that a user is identified and authenticated if another person explicitly identifies him or her. This action can be performed via informal channels such as the email. Nevertheless, in computer security, there is low exploration on developing mechanism of authentication combined with social networks and relationship of entities.

In [BJR+06] it is explored an authentication system where the user has a list of trustees whom (s)he chose (i.e., normally acquaintance and close friends). Authentication is therefore made if one or more of those trustees vouch for the user. This authentication method is preferentially mostly indicated for fallback authentication, where the user has forgotten the password. However, this approach can have a few problems, like the possible fact where the user forgets who is in the list of trustees.

2.2.5 Something You Process

The *something you process* factor aims at exploring the cognitive side if the user to perform authentication, requiring to perform logic in order to unveil the secret. For example, in [SUSM09] the authors proposed a logic game consisting of solving a secret mathematical formula given some values presented by the authenticator. A new code outcome is generated each time the formula is processed, meaning that the values publicized by the authenticator are different for each authenticating session.

Figure 2.5 shows a example of an authentication based on *something you process*. The user must memorize the mathematical formula to use later in the authentication process. During the authentication, the screen shows several characters associated with several numbers (i.e., the characters of the user are mixed among all the others). The user change the characters of the formula by the corresponding number and calculates the formula. In the end, the result of the formula is the secret that the user types to perform the authentication.

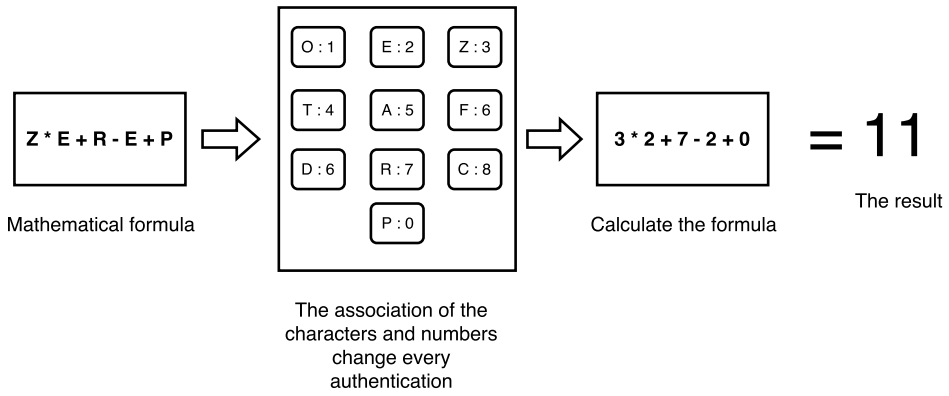

Figure 2.5: *Something You Process factor*: the image shows a calculation according to a formula.

2.2.6 Multi-Factor Authentication

MFA consists of combining any of the authentication factors described in the previous subsections. For instance, it is common to see (e.g., Google, Facebook) authentication systems based

on username and password plus a second factor consisting of an one-time password generated by a soft token.MFA is also of widespread use in online banking transactions, traditionally requiring a one-time code received via Short Message Service (SMS). Such a combination, even of the same factors, hardens the security of the system, making it more troublesome for an adversary to overcome the security layers put in place. MFA has gained attention in the last few years and is usually discussed within the scope of multi-factor authorization as well. Sometimes, researchers address both MFA and multi-factor authorization simply as *multi-factor auth*, since both of them are closely related in within the access control scope. However, MFA is not foolproof, being vulnerable to phishing [Kre06], *man-in-the-browser* and *man-in-the-middle* attacks [Sch05].

2.2.7 Two-Channel Authentication

To complement and harden the security of authentication systems, developers can opt to deploy factors over different communication channels. Such schemes are widely seen in homebanking [YLKJ10], where a challenge is sent via SMS to the mobile phone after successfully introducing the username and password. The response can be sent back to the server via the same channel or can be typed in the webpage and sent over the Internet. This can also be called 2-Factor Authentication (2FA), because the user knowns the secret and is in the possession of the mobile phone.

2.3 Related Work

Several works related with authentication mechanisms were found, which provided important clues about how to design and devise a similar job. Although not all works settle along with the lines of this proposal, they have revealed very important in the development of this work. However, this chapter does not address all the subjects that are going to be discussed in this dissertation. This section represents an important phase of the work, because through the study and analysis of other researches, it was possible improve the structure and development of the proposal.

A lock screen is a user interface element responsible for locking the device screen, which can be either from a mobile device or a personal computer. Usually, mobile devices use lock screens based on touch gesture or more recently based on image or other external factor. There are lock screens that do not have the objective of protecting the mobile device and are not related with the security of the system. This dissertation is focused on lock screen for authentication, which aims to protect the device from an unauthorized user. Normally, lock screens software are shown to the user before he accesses the OS or when the OS does not detect user absence for a certain period. The principal idea of a lock screen is to protect the device and operating system where it is installed. Additionally, it can display some features like shortcuts to applications or information like notifications from several types of content, like weather, mail or message received, date, hour, etc.

The mechanism for authentication is behind the lock screen installed on mobile devices. A lock screen is an authentication application, that relies often in the assumption that the owner of the mobile device knows the secret code. The secret can be a password as numeric or alphanumeric, or a pattern, or even the facial traits of the user. Next, some related work regarding authentication mechanisms and lock screens will be discussed.

Syed Shabih ul Hasan Naqvi and Samiullah Afzal have developed a technique named Operation Code Authentication [uHNA10], which provides more security when a user is typing his password, during an authentication procedure in public places or in case the user is in a critical position, of using his personal computer. The technique is based on the factor*something you process*. The steps of this scheme are as follows: during the sign up phase, the user will be asked to introduce two things besides the username. A passcode, with the minimum size of 3 and a maximum size of 6. A four letter word, like Oreo, which means the four arithmetic operators (i.e., division, multiplication, addition, and subtraction). The word chosen previously will be used to perform the arithmetic operations, and always in the following sequence, division, multiplication, addition and subtraction. Only the user knows the digits that are related to the arithmetic operation. During the authentication procedure the user will be prompted with a few tasks that combines the passcode and the four letter word that only he knows. They have also developed a graphical *security box* with the objective of preventing any criminal/unauthorized activity. This feature can provide multilevel security in very dangerous circumstances to the user, like being point with a gun. The user can choose one of several images, depending of the image chosen by the user the systems take or not additional security measures. This mechanism tries to be secure against *replay attack*, *insider attack*, *shoulder surfing attack*, *guessing attack* and *reconnaissance attack*. This project focuses on changing the logging mechanism present in ATM, turning them more secure and feasible for the user and harder for hackers.

In 2012, the authors of [SPLP12] developed an upgraded lock screen system, which is apt to support the authentication procedure if user wants. They have also suggested an upgrade in Android smartphones, regarding the current authentication system. In this concept of lock screen, they have created two modes, a *user mode* and *guest mode*. In the *user mode*, the user can access whatever he wants in the device, but in the *guest mode*, the user can perform fewer operations and has lower privileges, also has limited number of apps. When the device is locked, the *gues mode* can be access by shaking the mobile device. The *user mode* can be enable by unlocking the lock screen, a circle consists of 6 mini circles, where the user has to enter a given sequence, if he hits the sequence he unlocks the *user mode*. The color circles change to show whether user-entered the right sequence or not.

In 2010, Mohammad Tanviruzzan and Sheikh Iqbal Ahamed have proposed [TA14] and developed an authentication framework for smartphones is based on the idea of how a pet recognizes its owner, in other others, the possibility of the device distinct his owner automatically. During several days, the application gather several data types, using different device sensors. An internal algorithm of the application generate several owner characteristics from the data collected previously. A template of several samples is stored in the device, each sample represent a trait, is a unique set of characteristics of the owner. Authentication rules, can be computed from a subset of the of traits and an authentication verdict depends on authentication criteria. The procedure is divided in 3 phases, a first phase destined to gather user data, through the device sensors and create the database. The next phase is dedicated to the training phase, where the application will use several algorithms and functions upon the data collected previously to create patterns and criteria. The last one, is the authentication phase, where the software is ready to perform the authentication procedure without the user knowledge. The procedure consists in comparing the data (e.i., owner characteristics) that are been collected in real time with previously data. The authentication criteria should respect previously analyzes made over the data of the training phase. The positive aspect of this proposal is that require minimum in-

volvement of the user, but suffers for having a solution that makes intensive use of the battery, since the application if constantly sensing and computing the data collected using the sensors of the device.

In 2009, Mike Just wrote a paper [Jus09] about the state-of-art of challenges questions, and the importance of this mechanism to recovery a password or account. The papers describes how challenge-questions works and is divided, it is divided in two situations, in the first situation the user needs to choose the type of question (e.i., the user is presented with several different types of questions, but that are related with personal information of the user) he is more comfortable to answer, and then proceeds to register the response. The second situation, recovery process is required by the user to recovery a lost/forgotten password or account. The author also have made analyzes about the security offer by this type of security. He had conclude that using simple challenge questions as security mechanism do not offer sufficient security and account protection. It is also mention that using a single question-answer pair provides a low level of security. One way to improve the system could be by adding multiple questions or other security measures (e.g., using the email as part of the security process) to increase the security.

In their work [TA08], Hai Tao and Carlisle Adams have designed and evaluated a new graphical password scheme, inspired by an old Chinese game. In this work, the user must select an intersection on a grid, to create the password, basically, the user must draw the secret in the screen or in the input of the device. One of the main reasons to develop this scheme was the fact that normally it is very difficult for the users memorized textual passwords. They have elaborated a study about their graphical password proposal, where they had good acceptability from the users. The scheme is destined to support most applications environments and input devices. They have concluded that they need several improvements in several aspects like a solution for the *shoulder surfing attack* and the fact that after analyzing the results of the study, they have found that users have tendency to choose very long passwords, leading to an extremely large password space.

The authors of [KWSJ03] designed and developed a multimodal personal authentication system based on the union of hand-geometry and palmprint features. Same research mention that 11"%" of the biometric technologies were based in hand-based features, making it one of the most used in the biometric systems. They have chosen the multimodal biometric system over the unimodal system in spite of the fact that last one is more cost-efficient, the multimodal integrate two or more different biometric characteristics, which increase the accuracy of the decisions. One of the positive aspects of this approach was the fact that, with just one single-shot image that could extract all the necessary characteristics. They also used the palmprint biometric technology, due to the uniqueness and permanence of the palmprint features. The characteristics that they explored and used to increment the accuracy and scalability of the proposed were the use of finger-geometry, palm geometry, palmprint and fingerprint features.

The paper entitled *Design and Analysis of a Graphical Password Scheme* [GLW+09] contains a proposal for an authentication mechanism that tries to be a solution against the *shoulder surfing attack*, as also they aim to decrease the login time duration. This scheme uses a new method, based on grid of different background colors and each one has a grid of several different images. In the registration phase the user choose a color from several, and associated with that color there different images, then user choose a certain number of images. During the Authentication

Procedure, is exhibit a grid of background colors ,each one with its associated color images, this way the user only need to focus one the color chosen previously (registration phase), and focus on the images either chosen previously, the user eliminate the burden of try to find the images in other background colors.The user does not need to select the cell of the image, but the line, even if it touches the area of another color other than the chosen color. This is a big advantage because it shuffles a possible hacker that is trying to capture the secret by looking at the user.

There are a few standard and common ways to create a lock screen. Nonetheless, one must be aware that a lock screen is not always used to authenticate users to the device. Sometimes, they are just screen-savers or applications for showing useful information after periods of inactivity. An example of such a lock screen is *Slide Lock*, in which the user just needs to perform a *touch drag* to unlock the device. This lock screen does not protect the OS. Examples of security oriented screen locks can be described as follows:

- *Keypad Lock* - In the case of this type of authentication, the most frequently used method is the PIN code. Theoretically, the level of security depends on the range of possibilities, and then, depends of the choice of the user, but in practice users often choose a small and simple secret codes, reducing the number of possibilities secret. Thus, the range of available numbers for a hacker trying to figure out the secret code is much smaller. An attack that is quite frequently use and have a high success rate for this type of authentication factor is the *shoulder surfing attack*. In the study [BPA12] it was possible to conclude that, if a thief steal an ATM card with the personal information of the person, likelihood of finding the PIN code increases abruptly. The thief can guess the right code of a card every 11-18 wallets stolen. The previously research probably can also be used if the thief stole the smartphone with the wallet, the probability of finding the code to unlock the smartphone increase. Users should always use complex passwords, but these are difficult to remember and even more difficult to write on keyboards, especially in small touch screens, like those used in smartphones. The user should avoid certain characteristics when choosing a password, choosing a weak and simple password (e.i., for better memorization) can leave the system vulnerable to attacks, another mistake that occurs very often is use the same password across multiple platforms, services and devices;

- *PassPhrase* - The appearance of passphrase as password, tried to help in reducing the complexity associated with the memorization of PIN codes (e.i. only with numbers), in this case, the user chooses a combination of words and numbers (e.i., which is easily memorized). However, this method eventually leads to the same memorization problems, and adds the fact that is more complicated to input them during the authentication procedure. If the user choose a long and complex passphrase, it can be very boring in case the user needed to enter the secret several times a day on his mobile device or computer. There are some techniques that make it possible to decrease the difficulty associated with it, the user knows the secret (entirely), but only need to enter the initial part of it, the device suggests the rest. However, there is another problem that occur with this method, normally, the user tend to choose familiar words to create the passphrase, which can induce an intruder try to guess the passphrase;

- *Pattern Lock* - The pattern method is an alternative for those with mobile devices, the concept is simple, the user must connect several dots displayed on the screen in the form

of a grid. The secret is the sequence formed by the junction of the several dots. This method becomes easier to decorate than the PIN code or a passphrase, however is also strongly fragile against *shoulder surfing attack*, where the attacker discover the password by looking at the user while he is typing the password, as also, the hacker can find all or part of the secret by looking at fingerprints left on the device screen, even after the user cleans it. In the research [UDWH13], they have purpose a solution to strive against this attack, by using the same principle, but in this approach the dots change randomly, but it is most likely that creates some confusion in the mind of the user, and ultimately hinder the authentication task. Finally, due to the physical size of dots, the range of secrets is not too large, giving the user a small range of options. Furthermore, a study [UDWH13] has showed that, when users are selecting the pattern in the matrix, they usually have more preference for certain dots than others, this is translated into a decrease in the number of possibilities of patterns;

- *Smart Lock* - You can set different devices, as a pair device, to your smartphone, as Near Field Communication (NFC) tag, Bluetooth device or the face of the user, so every time the smartphone is near one of the pair device, it will automatically unlock your device, this process will lift the burden of the user to perform the unlock procedure manually [JM13];

- *Finger Scan* - one of the first [IBN13] implementing this technique and scheme was Motorola, with his smartphone, Atrix. A finger scan system, a way to unlock the smartphone, that joins the convenience and good security without touch dragging or slide. This type of technology is one of the most used among biometric systems, this mechanism uses several unique characteristics and patterns of the fingerprint (e.i., that differentiate every individual) to identity and verify the identity of the user (e.i., that is trying to perform the authentication). This technology is the oldest biometric technology in research and is used in several kinds of situations, like physical access to a building or unlock a mobile device [Spi03];

- *Facial Recognition* - This scheme uses the face of the owner to perform the authentication on the smartphone, this technique perform pretty well, but is not foolproof, it is easy to trick the system, by let the system thinking that another person is the owner of the smartphone. This mechanism is usable but not 100”%” secure. Face recognition can be used to perform other kind of tasks, beyond authentication scheme, application that check if the persons gathered at the meeting point are all those who are expected. This scheme authentication is based on *something you are*, as mention before this method of authentication is good, but not foolproof. There are several problems related with this kind technologies, for example someone with a photo of the owner of the device can probably unlock the device, also a person very similar in facial traits can deceive the device, and it will unlock it [Spi03].

2.4 Other Interesting References

This section contains references to documents and articles that, despite not being part of the related work, were important to the development of this program. Going through these documents allowed acquiring more knowledge about several subjects that are related to the main subject of this master’s program, namely important aspects regarding Android architecture and

security.

Article [KNOM12] contains a reflection on security in Android smartphone, authors discuss the vulnerabilities and limitations in the current security model of Android, principally the application permission mechanism. They have also proposed improvements for enchant of Android security model, and analyzed and discussed their strengths and weaknesses in detail. As result of the subject of the paper, they have proposed a list of security requirements that should be adopted in order to improve the design of future Android security model.

The authors of [FMS13] elaborated a study on some of the most basic security threats on Android and also, which security measures are normally used by the Android. The study was divided into 3 stages, the first stage of analysis, identification and cataloged the main threats and security breaches. In the second part they have made a demand on possible mechanisms and security solutions that could be adopted to improve the security mechanisms. They created a table that gather all the solution found on scientific works, and have compared the important facts of the several solutions. After that, they have analyzed the possibility of categorized those security measures into their classification model. They focused their research and analyses over publications of market research institutes. In a last phase of the programme they have studied and analyzed which security software solutions for smartphone can prevent or reduce threats on the system.For this, they have made analyzes and comparisons over which security measures are appropriate for which security software solution. Finally, they compared all security software options within each class, if they found many similarities and only few differences, that solution was validated.

The paper entitled *The Identifying and Quantifying the Android Devices User s Security Risk Exposure* [JM13], by Lukas Jeter and Shivakant Mishra, describes the development of an Android security test application with two purposes: first, gather information about user knowledge and aware about security threats facing their usage of Android devices, making them vulnerable to attacks; secondly, present the users with some basic knowledge of Android security to raise their security awareness, making them stronger against attacks. The application has the option of collects security settings information, various phone settings data and reports, the list of the most high-risk permission and the application regarding those permissions. There is also referred some security principles and mechanisms of Android that contribute to the security management of the device. The application sends the collected data to a server, where will be analyzed and study, at the end of the paper the authors elaborated a small discussion about the conclusions of the research.

Sebastian Uellenbeck, Markus Durmuth, Christopher Wolf, and Thorsten Holz [UDWH13] made contributions concerning the security of the Android unlock patterns, explaining for example why a three digit PIN is more secure than a 3 x 3 pattern scheme. They have found that, normally, users tend to choose a small fraction of dots, and that the probability of picking a certain dot is not linear for all points. For example, they have found that the upper left corner and three-point long straight lines are more popular than other strategies. The analysis focused on the range of possibilities that are chosen by the user, and not on all pattern possibilities. They have also suggested a small change in the pattern layout that can improve the scheme, and turns this graphical user authentication scheme substantially more secure.

In the paper describing their work [SHWH12], Lin Sun, ShuTao Huang, YunWu Wang, and MeiMei Huo, explain the basic architecture of Android. The sandbox model utilized in this OS is discussed with detail, namely on how it is used to separate running applications/programs, by controlling the resources of the programs. It is also mentioned the importance of the Code Access Security (CAS).

The authors of [FBC+13] have studied the duration of the screen timeout, with the purpose of improve the user experience and low energy consumption. The motivation to develop this study is the fact that sometimes the screen goes off in inopportune moment, or instead the screen stays on, when in fact the user is not using the device and the power consumption continues. They have elaborated a data collector to understand better the behaviour of the user and ended with suggestions to improve the initial problem. They have created a software that performs a monotonization over the device, it records minute by minute if the user is using the device, what application are open, and other aspects, like if the user turns the screen on before five seconds before the screen went off automatically. This last point is very annoyance, important and raised a flag in the software, because means that the system turn off the screen in an inconvenient moment, such as when the user is reading a website, and the device turn the screen off automatically.

Stephen Mujeye and Yair Levy, both from Nova Southeastern University, United States of America (USA), conducted a study [ML13] about how complex a password can be, principally on an enterprise environment, where the change of a password is a requirement. They have started their project by studying the problem of memorizing long and complex passwords, and by the fact that they have to remember many passwords for different devices and services, like websites, mobile devices, directories, applications, etc. They have realized tests with three different groups (two experimental groups A and B, and a control group C), to analyze the point at which a password become too complex for users and thus counterproductive. Each group has its own passwords characteristics. The A and B groups experienced increase and decrease in password strength and complexity during the experiment, respectively. Members of the control group kept the same password for the entire duration of the experiments.

During their research, Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner [EJP+14] conducted two studies. One to understand the behaviors and attitudes of users regarding the security of their smartphones data. They have analyzed why users choose or not to employ a security lock mechanism, and the user awareness and perception about the sensitive data that is stored in their mobile devices. The other study consisted of an online experiment to analyze which sensitive data could be found on mobile devices. They have observed that users are aware of both the risks and the security features available to protect them.

2.5 Summary of this Chapter

This chapter discussed several techniques and approaches related with the state-of-the-art in authentication mechanisms, enlightening on were the research stands today in terms of authentication factors and mechanisms, such as the *something you know*, the *something you have*, the *something you are* and the *somebody you know* factors. This chapter also reviewed approaches of authentication schemes with regard to lock screen software, such as *finger scan*, *face recog-*

nition and *keypad lock*, highlighting features and issues along the way. Several lock screens were reviewed during this study, allowing to identify five that are more popular and known to mobile device users, as showed in figure 4.4. One issue incurred in lock screen authentication approaches is that the authentication code may remain the same for long periods of time, unless the user changes it from time to time. As in passwords, once the unlock code or pattern is known to a malicious actor, the security of the mechanism fails. The lock screen approach proposed in the scope of this dissertation constitutes another way to authenticate the user in mobile devices, but takes into account the learned user activity. Because it is fundamentally different from existing approaches, it needs to be better studied before being considered for a real deployment.

The research work described in this chapter supported the evolution of this project in many aspects. For example, the study of the lock screens provided a clear perspective over what is already available and how they are designed. The lock screen developed along this work did certainly get some inspiration from the applications reviewed at this stage. At the final part of this stage, the author concluded that no system is unbreakable and, most importantly, that there is often a trade-off between the security level and user friendliness or time-efficiency. According to [TA14], a user is typically interested in three levels of protection: the first level offers no protection; the second offers weak protection; and the third offers maximum protection. Many users do not mind using the first two levels.

Chapter 3

Authentication on Mobile Devices Based on User Activity

3.1 Introduction

In computer science (as well as generally speaking), *authentication* is the process of identifying an individual or an entity, like a human or a device, to another system. The process (or mechanism used to achieve that purpose) should ensure that the entity is who claims to be. Authentication systems are not responsible for controlling the access rights of the user/entity that performs the authentication. Within the context of an authentication procedure, it is common to name the entity that is trying to prove its identity as *supplicant* and the one performing the verification as *authenticator*. Even though authentication schemes have been imagined and used long before computers, modern Information Technology (IT) embodies a new rich environment on which these procedures are naturally needed, and has been feeding the research and development on this field of knowledge. Despite several innovative and comparatively more secure schemes for authentication offered by modern cryptography, the most widely used mechanism is based on having the supplicant proving the knowledge of a password for a given username to the authenticator. This scheme was among the first authentication schemes implemented in computers and it is easy to implement and use, exhibiting a negligible computational overhead. Nonetheless, nowadays, it is considered one of the most weak authentication schemes available, there are several well known attacks against this type of authentication scheme, namely brute force and dictionary attacks. Despite that, it is widely used in authentication procedures and for controlling the access of an entity to a certain device, location, service and platforms.

However, in the last few years it has become clear that is needed to create innovative solutions in the area of authentication schemes, because much sensitive personal and financial information are increasingly been stored on online services and mobile devices. Additionally, devices are becoming smaller and more personal. The adoption of these devices to store sensitive information has been motivating both researchers and attackers to study the existing and new authentication means. Many have been trying to only improve the existing ones in the meanwhile. Two of the main factors that hinder the adoption of new authentication solutions are the production and maintenance costs of the technology (e.g., biometric systems are specially affected by this factor) and security related issues.

This chapter is focused in describing the logical structure of the implementation of the lock screen based in the activities of users on a mobile device. It discusses the security parameters involved, and compares the application it with other similar solutions. Several alternative parameters to build the prototype are also discussed herein, which are briefly compared with parameters used in alternative lock screens.

The chapter is structured as follows. Section 3.2 describes the mechanism and concept proposed

in this master's program, along with a more detailed explanation of several important aspects behind the proposed lock screen to be implemented. Section 3.3 is focused on the inherent security parameters. Section 3.4 is dedicated to the discussion of the overall security provided by the new approach. This discussion is performed by resorting to the comparison with other similar authentication software.

3.2 Description of the Authentication Mechanism

The authentication factor used in the proposed authentication mechanism is a *something that you **already know*** factor, which is a branch of the *something you know* factor. In this case, instead of forcing a user to choose and remember a new secret for authentication purposes, the user only has to recall information that he or she should probably already know. In other words, in this proposal, the secret is dynamically generated by the authentication mechanism based on information already known by the user. The mechanism will strive to produce secrets that are potentially easier for the user to remember than random passwords.

3.2.1 Challenge Questions

A *challenge question* consists of an interaction between a two parties: party A presents the question and party B must provide a valid response in order to perform the authentication successfully. There are several security systems that use *challenge questions*, normally as fall back authentication or password/account recovery. In common systems, the user sets up the answer to an associated question, so that it can be later used during the authentication or recovery phase.

The approach presented herein also uses *challenge questions* as a means of authentication, but instead of using a static, predefined question/answer, they are generated dynamically by the logic behind the mechanism. The data used to create the questions and answers during the authentication phase are based in information related with activities that the user perform frequently on they devices. The questions and answers can change over the time, depending of the activity of the user. The user never needs to set up or explicitly memorize answers to the questions.

The idea is that, during the authentication phase, one or more questions are displayed to the user on the mobile device screen. Each question will have several possible answers, generated by the underlying application for each one of the questions, with only one of them being correct. The authentication system possesses the information to create the questions and the answers. The user does not need to register answers, because the authentication system is installed in the same device where the activities of the user are performed (otherwise it would not be possible to create it, or appropriate additional measures would be needed). To successfully unlock the device, the user must correctly answer all questions presented during the authentication phase or fulfill the minimum criteria of the lock screen.

3.2.2 Questions-Answers

Papers [Jus04, Jus09] list some criteria for evaluation of *challenge-question* based mechanisms, which serve also as guidelines to build them. The three items they point out are as follows:

- **Applicability**, which refers to the fact that the questions should be relevant and appli-

cable to the users. Within the scope of this work, this means that the type of questions created with the source data should make sense to the user. Only questions based on activities/applications that the user uses very frequently should be created, otherwise the applicability is low. The algorithm should avoid generating question/answers pairs of which the user is not aware.

- **Memorability**, which refers to the fact that an answer to a given question should be easy to recall by the user. It is also desirable that remembering that information does not inflict psychological pain in the user. This emphasizes that, additionally to what was previously said, the questions-answers must be simple to remember. Information based on frequently used and more recent activities is more memorable. This means that accessing activities that host information of the habits and activities of the user provide suitable questions-answers.

- **Repeatability**, which refers to the property that answers should have simple representation and the same type of content for all of them. This means that the format, such as length and visual aspect, as well as the amount of informations the question contains or the number of potential answers should be as uniform as possible. The question should be precise or understandable and not confuse the user. Applied to the solution presented herein, this means that the mechanism should generate similar questions and the number or possible answers should not oscillate much (e.g., more than 1 or 2 options per question).

As can be seen, it is known that it is important that the questions and answers make sense to the user (but only to the one trying to perform the authentication). They should be strongly related with him or her, and the meaning of both the questions and the potential answers should be very clear, otherwise he or she will not be able to answer correctly. In the case of multiple choice answers, it is clear that the potential options should all look equally possible to an outsider. In the proposed approach, or at least in the prototype to be implemented and tested within the scope of this program, the data used to generate the questions and the answers concerns information regarding messages and calls. There are several activities associated with messages and calls, namely if was making or answering a call, sending or receiving a message. For each activity, different data can be used, like for example the name of the contacts involved, the duration of the activity, the date, etc.

One of the key aspects that was important to achieve was conciliating security with user experience. The user does not have the burden of change his password time to time, and the user does not need to remember authentication secret the same way he or she remembers a password, a *PIN*, a picture, a drawing, or a combination of numbers or dots. The authentication mechanism uses part of his/her activity to provide a seamless and more secure means to unblock or identify a person to a device:

- It is *seamless*, because it is based on information that the user knows by heart and not on something that (s)he needs to forcefully memorize;

- It is *secure*, because it is not static, contrarily to many authentication secrets used nowadays. The authentication depends on user activity, which changes for every authentication, and the leakage of user activity now does not imply that an adversary will be able

to authenticate later on, etc. In static *something you know* based mechanisms, the compromise of the password or PIN may lead to a latter compromise of the system. This is disruptive when compared with nowadays technologies.

The proposed approach has an obvious drawback. Authentication requires answering several questions, and this will take certainly more time than inserting a short PIN or password, or selecting a pattern in a touchscreen. To minimize this problem, the questions and answers must also be designed with that in mind. The following chapter shows that an experimental study was performed to better understand which data and type of questions were better to improve efficiency also.

One of the problems that this approach would most probably solve is the one of *shoulder surfing attacks*, where an unknown user tries to observe the user password during the unlocking of the device. Several techniques are actually employed to prevent this, staring from raising awareness, to the application of dynamic on-screen keyboards that change the position of number at each keystroke. The approach mentioned in last would at least force the shoulder surfer to be close enough to see the values on the keyboard also.

3.2.3 Authentication Mechanism Phases

From a logical point of view, the proposed authentication mechanism can be divided in two main phases: an *activity phase*, where the user is generating new data while interacting with the device; and the *authentication phase* per se, where the user tries to log in. They can be better described as follows:

- On phase 1 - *activity phase* - data from different activities performed by the user are stored in the device by its native functionalities or by the applications. Modern OSs make this automatically for many activities, and no specific monitoring application is thus required. The device is unlocked in this phase. The collected data will be used in the next phase;

- On phase 2 - *authentication phase* - questions and associated answers based on the aforementioned activities are automatically generated. The programming logic behind the mechanism needs to access the sources of data, construct the several challenges and present them to the user, one at a time, in a structured and clear manner. The user must correctly answer those questions to unlock the device;

The general work flow of the proposed authentication mechanism is illustrated in Figure 3.1. Thought several other potential applications of the proposed mechanism were considered later on, the genesis of this idea was on the potential usage of the mechanism on smartphones or tables. The mechanism should thus be put in practice as a lock screen for these devices. Assuming that, the work flow starts in the *activity phase* and evolves to the *authentication phase* as soon as the lock screen is activated, which happens often when a user turns the screen off or after a given inactivity timeout.

Notice that it can also be said that phase 1 works like the registering phase of a common lock screen or web application, where the user needs to set up and configure the secret code or password. In this approach however, the user does not need to perform that step, because that part is automatic.

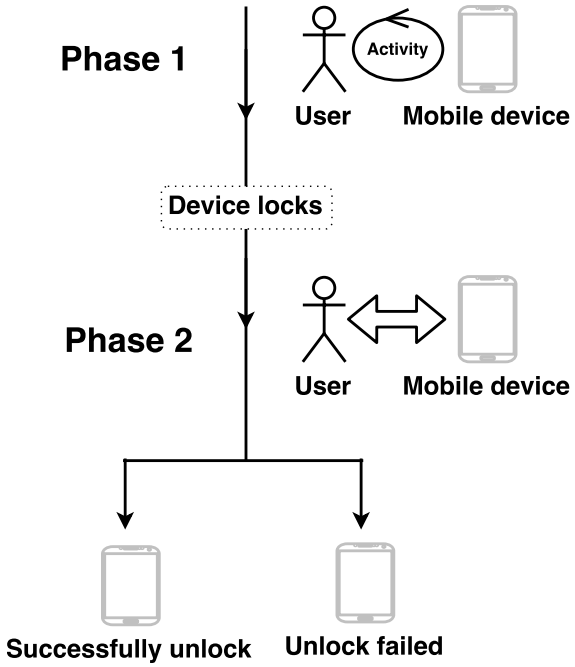

Figure 3.1: The general work flow (and phases) of the proposed authentication mechanism.

Thinking already in terms of implementation and real work flow in a device, entering phase 2 will correspond to spawning the developed prototype that needs to fetch the required data. This will need permissions from the user and the OS, and APIs with routines to query the respective applications or parts of the OS. In the case of Android, the application will need permissions to access the call and message logs, and instantiate the respective content providers to function properly. Figure 3.1 also shows that the work flow may also lead to success or failure in authenticating. Failure is the state that the prototype should exhibit if the user fails to correctly answer one or more questions (this particular aspect may be subject of research in the future). Since at least one backup plan is needed in such situations, it was defined that in the prototype to be developed, the failure state would lead the user to a screen where a PIN could be used to unlock the device (not shown in the figure).

3.3 Security Parameters

The security parameters are the ones that enable adjusting or measuring the security level offered by a system or an application against an adversary that wants to break it. Like any other security or authentication mechanism, this approach has its own set of parameters. The three fundamental parameters that regulate the security level of the proposed authentication procedure are:

- the total number of questions asked to unlock the device;
- the number of answers showed in each question;
- the difficulty and nature of each question.

The number of questions and potential answers are the dominant parameters for measuring the security level. Table 3.1 shows the number of combinations as a function of the those two numbers. The last column shows the probability that an attacker has of succeeding in authenticating by randomly selecting answers to the several questions (column named RASP - Random Attack Success Probability). As such, this probability concerns a best case scenario, since some answers may be known a priori for a particular attacker, or he may have hints for a subset of questions. E.g., consider the situation in which an attacker calls the user before trying to break into the smartphones. The last activity of the user was more probably related with the attacker.

Number of questions	Number of answers	Combinations	RASP
2	2	4	0.25
2	3	9	0.1(1)
2	4	16	0,0625
2	5	25	0.04
2	6	36	0.02(7)
3	2	8	0.125
3	3	27	0.0(370)
3	4	64	0,015625
3	5	125	0,008
3	6	216	≈0,0046
4	2	16	0.0625
4	3	81	≈0,01235
4	4	256	≈0,0039
4	5	625	0,0016
4	6	1296	≈0,00078
5	2	32	≈0,031
5	3	243	≈0,004
5	4	1024	≈0,0009
5	5	3125	≈0,00032
5	6	7776	≈0,00012
6	2	64	0,015625
6	3	729	≈0,0013
6	4	4096	≈0,00024
6	5	15625	0,000064
6	6	46656	≈0,00002

Table 3.1: The total number of combinations as a function of the number of questions and of potential answers, as well as the success probability of an attack that randomly selects answers (Random Attack Success Probability - RASP).

A lock screen application for smartphones may include a configuration utility that may let the user choose the number of questions and potential answers. Increasing the number of questions corresponds to an exponential increase in security, but it linearly increases the time required to authenticate. For example, selecting 3 questions and 4 options per question would correspond to a RASP of 0.015625, while selecting 2 questions with 4 options each would lead to a RASP of 0.04. Increasing the number of options is not as effective, security wise, as increasing the number of questions, but it does not impact time to authenticate as much either. Notice that the security provided by the aforementioned combinations should not be directly compared to that of, e.g., PINs, passwords or patterns. In this case, and since the choices are generated at each authentication prompt, the security provided is per-prompt. The compromise of the authentication information in a given try does not necessarily mean that the next is compromised

also. In the case of static secrets, the compromise is long lasting. As such, it is for example argued that using 4 questions with 6 options each is much stronger than using a PIN with 4 digits, because the PIN is compromised after a single should surfing attack. Actually, if one uses a 4-digit PIN in 4 different authentications, than the security provided in the fifth still corresponds to a RASP of 0.001 in the fifth, but the attacker already had 4 chances for obtaining the code.

3.3.1 Random Selection of Answers

Given the nature of the proposed approach, there is no static sequence of questions and answers. All questions are chosen in real-time, using a pseudo-random algorithm, thought they follow a predefined set of templates. The number of answers and the order of the questions are also randomly selected in the implemented prototypes, but this specific detail may change in the future. This implementation choice prevents better the possibility of an intrusion based on the establishment of patterns with the sequence of questions and possible answers. Even if one gets the screen location of the right answer, probably does not get the right question nor the content of the answer. In the next time the lock screen is shown to the user, the type of question, the ordering and the potential answers will be different.

In order to be effective the selection of questions and answers needs to fulfill certain requirements. The work of Mike Just [Jus04] provides some useful guidelines for this part of the work. For example, about the questions to be generated, he states that:

- *[Guessing difficulty]* it should be difficult to someone that does not know anything about the question to correctly answer to it. As such, the question should not include clues about the answer and all the answers should look equally probable to an unknown user, which means that the set of answers are uniformly distributed. As such, short questions favor the design of such mechanisms from the efficiency perspective and regarding the fact that no clues are provided. Unfortunately, the second property may not be as easy to assure as the first one, since an attacker knowing a user may also know who calls or texts him or her more often;

- *[Observation difficulty]* it should be difficult to an attacker to deduce a pattern from the observation of several logins, and it should also be difficult to obtain particular answers to several questions via investigation or eavesdropping on the mechanism.The content of the questions-answers should not come from public sources either, but from private sources, which may contain information from a single or multiple devices (e.i., but all belonging to the user). If the data used to generate the questions and answers comes from public sources, then it may be possible for someone to find, study or try to discover the correct answers. The approach proposed in this dissertation maximizes this aspect, since the answers change over time, as well as their order.

Notice that there is a privacy dimension that is not studied in the scope of this work. The fact is that the approach is based on showing some information regarding user activity on the screen during the authentication phase. This means that the screen will show names or duration of calls to anyone that grabs the smartphone and tries to turn it on. The private information that is leaked is minor, since most of the options may be fake (if the implementation supports that) and may not answer the associated question. Nonetheless, this should perhaps be subject of reflection in the future.

3.3.2 Content Storage

It was assumed from the start that the applications would have to use native functions, features, and databases of the Android OS. The information regarding the user activities is the one that Android stores, like calls and message logs. This means that no specific data collection application needs to be developed for that purpose, as Android already stored the information that is needed. It also means that no external databases or files (to temporarily store information) are created. Such external files would be a security issue. It was decided to use this approach to avoid possible leaks of information. If the suggested mechanism created a temporary file with data, and if that file was stolen or seen from an unauthorized user, (s)he could discover the possible sequence of questions and answers. The code footprint is also kept small because of this choice, which helps building security related applications.

3.4 Security Evaluation

In this section, the security of the proposed approach will be discussed and compared with other authentication schemes (i.e., with lock screens). Some arguments in favor and against it will also be put forward.

Table 3.2 compares several lock screen approaches available at the time of writing of this dissertation, mostly from the security point-of-view. For example, it contains, when possible, the maximum number of combinations one has to try to break a given mechanism, and also a brief explanation on how the combinations were calculated or on how the approach works. Some

Approach	Possibilities	Explanation
Keypad Lock	10000	A PIN code with 4 digits (numeric keypad).
Pattern Lock	3024	A connection of 4 dots (i.e., 9 dots available).
Finger Scan	Uncountable	Works by matching the fingerprint with the template.
Passphrase	>456976	4 letters long string, using only 26 characters of the keyboard.
Face Scan	Uncountable	Works by matching facescan with template.
Knock Code	256	Tap 4 times to unlock (e.i., screen is divided in 4 parts).
Proposed authentication - Mode A	Uncountable	Depends of the number of questions and answers (see table 3.1 in the previous section).
Proposed authentication - Mode B	3024	Choose 4 out of 9 options available.

Table 3.2: Comparison between lock screens approaches, security wise.

parameters of the proposed authentication approach can be adjusted in such a way it offers similar levels of security to other available lock screens. Nonetheless, one must not forget that, since the is dynamic, the strength (maximum number of combinations) should not be directly compared.

Table 3.3 compares several lock screen approaches, but this time it classifies the several alternatives in terms of convenience and security. The ones included here are the most popular ones at the time of writing of this dissertation (see also figure 4.4).

Table 3.4 is focused solely on the two modes implemented in the final prototype. More details on these modes can be found in section 4.4. After an analysis of the results of a user survey (see chapter 4 and section 4.3), it was possible to conclude that most of the questions related

Input type	Convenience	Security	Comment
Slide Lock	Good	No	No password is used.
Glass Lock	Good	No	No password is used.
Keypad Lock	Bad	Normal	Inconvenient because repeated touching is required.
Pattern Lock	Normal	Normal	A keyspace lower than keypad lock.
Finger Scan	Bad	Good	Problem with low speed of realization.
Passphrase Lock	Bad	Normal	Inconvenient because repeated touching is required.
Face Scan	Bad	Good	Problem with low speed of realization.
Knock Code	Normal	Normal	Inconvenient because repeated touching is required.
Proposed authentication - Mode A	Bad	Very good	Problem with low speed of realization, but provides more security.
Proposed authentication - Mode B	Normal	Very good	Inconvenient because repeated touching is required, but provides more security.

Table 3.3: Comparison between lock screens approaches (adapted from [SPLP12]).

	Convenience	Security
Mode A	Required to select the right answer of several questions in several screens.	Depends of the number of questions for each authentication, and the quantity of answers in each question (see table 3.1). The major benefit of this approach is the fact that the secret of the authentication can change regularly.
Mode B	Requires a few touch screens to perform the authentication in one screen.	The work flow of this mode is similar to a PIN code authentication, but, in this case, the secret changes regularly.

Table 3.4: Shows the convenience and security analyzes about the two modes of the prototype.

with the names of the contacts are responded correctly for both modes. This is a great point in favor of this proposal. Nonetheless, there are two situations that need further discussion and attention, affecting the security of the mechanism:

- Imagine that the user has a relationship. He or she will most likely be sending more messages and making more calls to that contact, than to any other. A stranger will not probably be aware of that fact, but one closest friend may have knowledge, and therefore he has an advantage in tentatives to break the system.

- Another important aspect affecting security concerns the options displayed for each question, namely in terms of names of the contacts. It was previously hinted that the selected options may not seem uniformly distributed because some names may seem more likely to be correct than others. For example, users often change the true names of family members to *father*, *mother*, *brother*, *sister*, or even to *honey*, in case of wife or husband. These type of names can give a certain edge to an impostor trying to break into the system. More research may be needed to find solutions to these problems.

3.5 Summary of the Chapter

This chapter explains and discusses several details about the structure, functionality, features, security and other aspects of this new lock screen approach. The overall work flow is the subject of section 3.2, whose two main phases are detailed in such a way that several requirements for

it to be secure are emphasized. Several aspects regarding the generation of the questions and answers were highlighted in the intermediate section of the chapters, and it was stated that the sources of data that are going to be used in the scope of this work are the call and messages logs only. The activities are thus confined to the ones of receiving or making calls, and receiving or sending messages. In the future, they may change, but these were considered to be enough to study the feasibility of the approach. The security parameters were also discussed herein. They are critical within the context of this master's program. In section 3.4 it was made a comparison between the security of the new lock screen concept and other similar currently available applications. It was compared against such as pattern schemes, PIN code based, etc. It was also mentioned a few important security details regarding the proposal. This chapter elaborates the foundations that enabled the construction of the prototype mentioned in the next one.

There are several types of lock screens, each one has its own layout, design, authentication mechanism and offer different levels of security. This authentication approach allows to achieve the level of security of any other lock screen software, but there is also a trade-off in user experience. Adding more questions and answers to the authentication phase is the same of increasingly the difficulty to guess answers and go through the entire set of questions and, as such, the security level increases. Nonetheless, this will also take more time from the legitimate user, which may render the procedure tedious.

Chapter 4

Prototype and Usability Tests

4.1 Introduction

This chapter reflects one of the most important phases of this master's programme. It concerns the implementation of two applications: one is the *survey mobile application* and the other is the *final prototype*. The first application was used in a survey and usability test. The second application is a lock screen software based on the proposed approach, similar to the first one, but optimized according with the findings of the survey. The *survey application* allowed studying the user behavior and gether knowledge about the best way to build the final prototype. This chapter describes the implementation details of the developed prototype.

The results obtained during the testing phase will demonstrate the importance of the usability tests in the software development process. Nowadays, it is argued that the process of creating software should always include user feedback and take previous investigations into account. In this chapter also presents the results of a usability survey that was delivered to a group of 44 individuals, as well as a detailed analysis of its results and several conclusions drawned from the collected data. The usability test was also used to test to the user knowledge in terms of his activity on the mobile device. These results provided the rights tools and knowledge to fine tune the final prototype.

Given the nature of its contents, this chapter contains several screenshots, charts and diagrams for showing the developed applications and the results of the survey. Section 4.2 starts with the presentation of the main objectives defined for the survey. Section 4.3 discusses the main results from the usability test, while section 4.4 is dedicated to the description of the final prototype. The most important conclusions of this part of the work are wrapped up in section 4.5.

4.2 Objectives, Delivery and Details of the Survey

The survey created within the scope of this work had the main purpose of testing and understanding the user knowledge in terms of activity on his own mobile device. Along with the survey, an application mimicking a screen lock was also developed for Android OSs starting at version 4.1. Users answering the survey were asked to use this application. The survey was divided into three main parts and, prior to the questionnaire itself, a brief explanation of its purpose and context was included. The three specific sets of questions are as follows:

- The first set concerns the characterization of the participant in terms of age, gender, etc., and the evaluation of the user knowledge in terms of mobile devices and authentication mechanisms;

- The second set was dedicated to the usability test, where several questions, similar to those that would be interesting to implement in the final prototype, were exhibited to

the user. The user would use the survey mobile application in real time while answering to the survey;

- The thirst set was devoted to obtaining the opinion of the user about the survey and about the new authentication approach.

The main objective of the usability test was to evaluate the following aspects:

- The knowledge of the participants regarding lock screens;
- The experience of the users about security on mobile devices;
- Ease of interaction with an interface similar to a possible prototype;
- How the user reacts when facing similar questions of a possible prototype;
- How long does the user take to answer each question;
- Evaluation of the understanding and ease of use of the proposed features;
- Obtain the feedback of the users regarding the survey;
- Obtain the feedback of the users about the new lock screen approach.

Each section of the survey starts with a brief explanation about its objectives. The questions of the questionnaire were carefully elaborated and discussed over several weeks, to keep it manageable and efficient, in terms of communication. The included explanations are short and the language was simplified several times. The survey was written in Portuguese, because target population was mostly constituted by Portuguese citizens.

A group of 44 people accepted to participate in the survey. They were asked to download the application from the *Google Play Store*. Following this procedure eased the deployment and provided more confidence to the respondents in terms of the security of the whole process. The survey was prepared for people from any professional or academic area, and not only for computer science or information technology. Delivering via the official store also shows that this concern was taken into consideration. The delivery and dissemination of this survey was made during several weeks. Dissemination was performed in various places and via different means, namely by directly approaching participants (at the university, at home, in coffee shops) of via Facebook and Reddit.

One of the authentication questions concerned the duration of one of the last two calls. One of the answers was true, and the others were generated in real-time. To generate appropriate call durations, an algorithm based on the exponential distribution was used [MAFL10], but with a minor modification. Since similar call durations are hard to remember, the algorithm was repeatedly outputting numbers until a minimum distance between options was achieved. Differences of 15, 30 and 60 seconds were tested in this phase. This way, it was possible to study the impact of using a certain minimum difference in the results obtained for this matter.

4.3 Results of the Survey

This section analyzes and discuses several results obtained from the survey. Many charts are included along the discussion, but to keep it manageable, some of them were included in appendixes A and B, with pointers to the figures included herein.

Participants had ages ranging from 16 to 54 (though some did not delivered the final report). They were from several professional areas, with different level of school education and were randomly chosen, without differentiating genders or race. Before starting the usability test, several questions were asked to the participant. The translation of such questions is as follows:

- Are you available to perform a questionnaire related to a master's program?
- Do you have an *Android* smartphone?
- Is the version of your Android OS equal or larger than 4.1?
- Do you mind installing an application in your smartphone for the purpose of this survey?

The survey was disseminated to a considerably larger number of people (than the aforementioned 44), but for several reasons, many did not participated or delivered the answers. Some known reasons that prevented people from responding to the survey are included next:

- No time for answer the survey;
- Did not possess a smartphone with Android;
- The android device did not fulfill the minimum requirements (version 4.1 or higher);
- Some individuals were not interested in participating or contributing to the research;
- Some people downloaded and installed the application, but for unknown reasons they did not send the report;
- Some people have doubts about the application privileges, since it needs to access sensitive data, such as calls and messages content;

4.3.1 Results Concerning General Questions of The Survey

This section discusses the results for questions related with the knowledge of the participant on the subject of the survey and on mobile security.

Figure A.1 shows that most of the participants were aged between 18 and 30 years, although the minimum age of a participants was 16 and the oldest was 54. As shown in figure A.2, 61% of the participants were males and 39% were females. The dissemination was made equally to people from both genders. The largest slice of the participants had an high-school degree, as depicted in figure A.3, even though this fact is not that relevant to the study. It was also verified (see Figure A.4) that more than 75% of the users were using the smartphone for more than 2 years, which implies that the major part of the participants is comfortable with mobile technologies

and features. Only four users had less than 2 years of experience with smartphones.

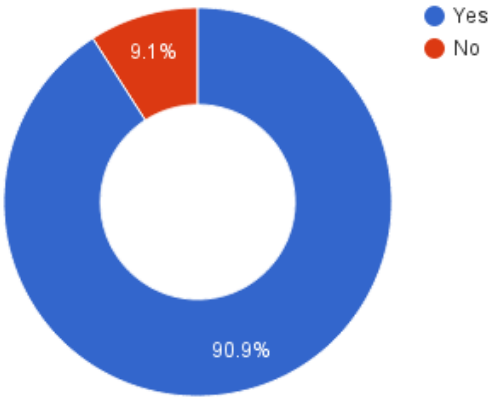

Figure 4.1: Pie chart for the results obtained for question 5: *Do you know the concept of lock screen?*.

The chart in figure 4.1 summarizes the results for the answers to question 5. Only 4 participants (9.1%) had no knowledge on the main subjects of the survey (e.i., with the concept of *lock screen* and Android security). Most of them were acquainted with both subjects.

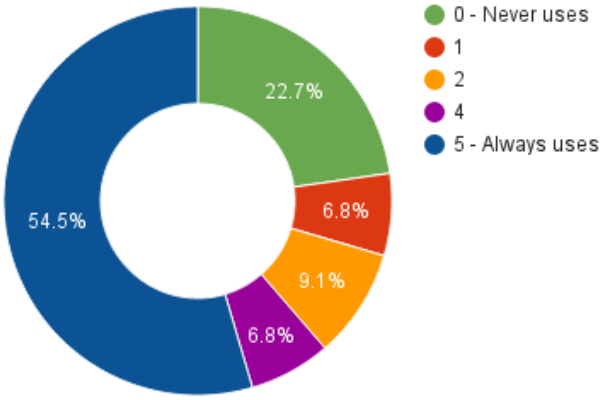

Figure 4.2: Pie chart for the results obtained for question 6: *How often do you use a lock screen with secret code?*.

The results depicted in figure 4.2 suggest that more than 50% of the participants use lock screens very frequently, which means at least half of them is concerned with the security of the mobile device. On the other hand, approximated 23% (10 users) prefer not to use any lock screen or authentication mechanism. The reasons are discussed along this section.

Question 6.1 of the survey was triggered for when the users answered *less than 2* in question 6. The chart depicted in figure 4.3 puts the possible reasons for not using the lock screen into perspective. Apart from three predefined options, there was a field for inserting a non listed reason. Around 46% of the participants prefer usability over security. As such, they disabled the need of unlock the device. Half of those users believe that they will never lose the mobile phone or that it contains no important, private and confidential data. Only one report was mentioning a different reason.

The users were then asked if they ever forgot the lock screen code and the results are summarized in figure A.5. There was only one participant answering *2 or more* on this one. For those that normally use this kind of software, 83.9% claimed that they never forgot the secret, and

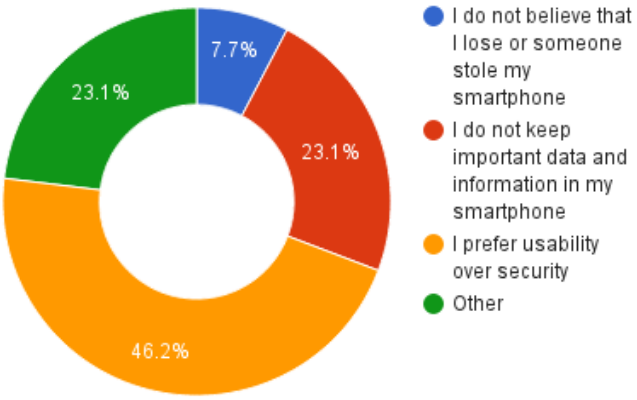

Figure 4.3: Pie chart for the results obtained for question 6.1: *Why do you use lock screen so rarely?*.

the remaining five individuals forgot the secret of the lock screen once only. This means that 26 participants never forgot the secret code of the lock screen.

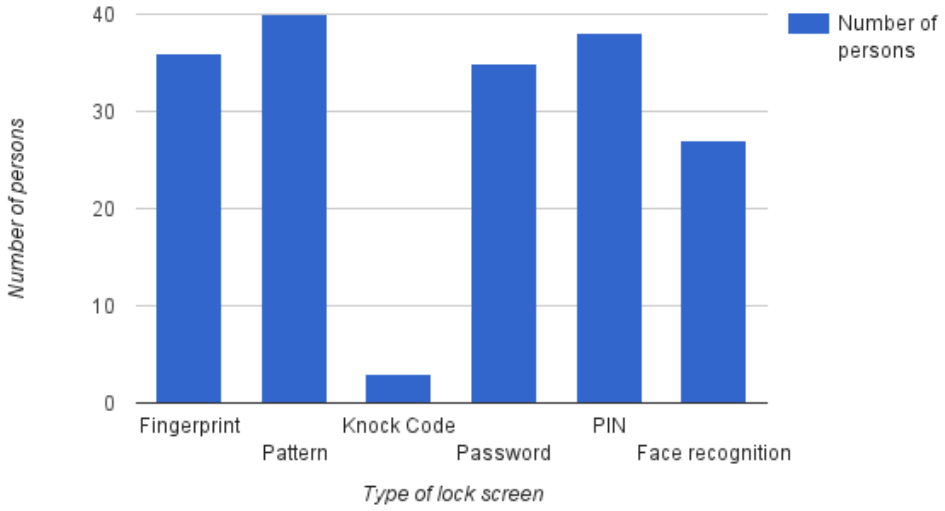

Figure 4.4: Column chart for the results obtained for question 7: *Select (multi-choice) the lock screen concepts that you know.*

As suggested by the results depicted in figure 4.4, participants seem to be aware of the available screen lock alternatives, with only one exception. The lock screen based on *quadripartite screen* (also known as *Knock Code*) was known by two participants only. At least 50% of the population knew each of the other suggested lock screen. It can be conclude that the participants are aware of the several possibilities and types of lock screens and their usefulness.

At the time of survey completion, the participants were asked if they were using any lock screen software with a secret code on the smartphone: 25 participants (56.8%) answered *yes* and the remaining 19 said they were not using one at that moment. Question 8.1 was spawn for the ones using a lock screen so as to obtain an idea of the most popular lock screen technology. The results for this question are represented in the chart of figure 4.5, revealing that the most popular approach is the one that uses a pattern with numbers. In second comes the one based on PINs. The *Nnock Code* and *Face Recognition* options were not selected by any of the participants. Earlier facts about the survey suggest that people do not really know *Knock Code*. *Facial recognition* is perceived as an inconvenient way of authentication. One of the participants was

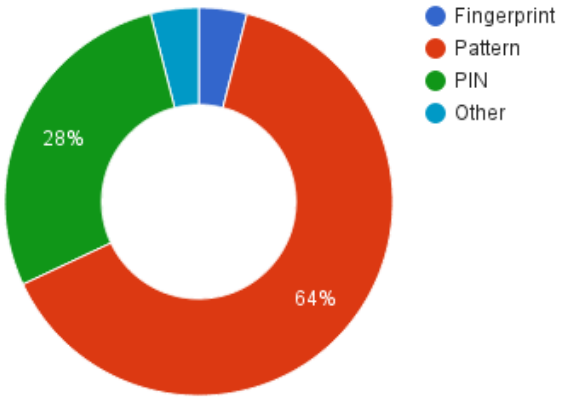

Figure 4.5: Pie chart for the results obtained for question 8.1: *Select the lock screen concept that you are using.*

using fingerprints to unlock the smartphone, and another user showed preference for an unlisted method. Notice that over 90% of the surveyed use only two types of lock screen software (i.e., the PIN code and pattern) on their mobile devices. When asked about the provenience of their code (question 8.2), about 32% of the users said it was based on some personal data (e.g., birth date, school number, etc.). Around 32% of the participants said that the secret was random (though no other details were collected regarding this matter). The remaining users (36%) indicated that their secret is related to a reason other than the two suggested ones (these results are depicted in figure A.6).

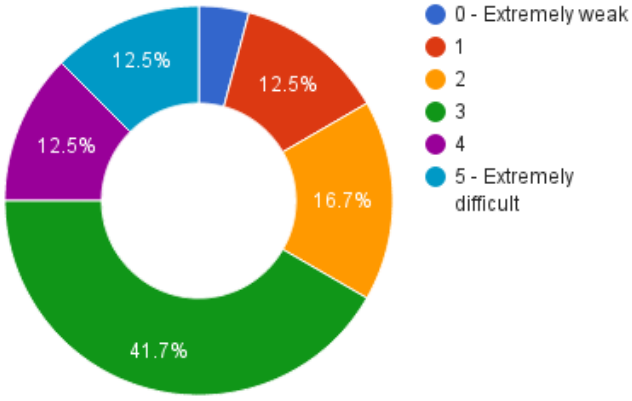

Figure 4.6: Pie chart for the results obtained for question 8.3: *What level of difficulty do you assign your secret code?.*

Participants were also asked to evaluate the security level of their secret code. The results are compiled in the form of a chart, in figure 4.6. Notice that these values reflect the opinion of the users, and they do not necessarily reflect the security of the approach. 41.7% of the participants state that the code is of medium (guessing) difficulty; approximately 30% stated that the difficulty level is low, while 1 participant chose the option *0- Extremely weak* and 3 participants, corresponding to 12.5%, stated that their code was very hard to guess. The remaining ones think the code is hard to break, but not extremely hard.

Question 9 asked the users if they had their smartphone lost or stolen before. Only four users answered affirmatively, corresponding to 9.1% of the participants (see figure A.7). From those, two have said that there was confidential data on the device at that time (see figure A.8) and

three of them stated that at least their device was set up with a lock screen when that happened (figure A.9).

The remaining part of this section is dedicated to presenting the feedback concerning the survey and the usability test. The later is then discussed in its own section, below. Perhaps the least interesting statistics collected in the scope of this survey, at least concerning its main subject, are depicted in figure A.10, which shows the perception in terms of easiness to respond to the questionnaire while using the application: 55% of users found the survey very easy to respond; while the remaining users indicated that the difficulty was easy (25%) or median (18%). No user selected the higher levels for difficulty (i.e., levels 4 and 5). It can be concluded that the survey was simple and objective, which was one of the objectives.

As for the new authentication approach, no user stated that it was *0 - Nothing interesting* or *1 - Somewhat interesting* (options went from 0 to 5, inclusively). About 11.4% selected the interesting level 2, and the interesting level 3 was selected by 36.4% of the participants, which comprises the largest share of the pie in figure A.11. 27.3% of the respondents (14) chose the interesting level 4 and the remaining 25% (11 users) attributed the maximum interesting level to the subject in study. Apparently no one found the matter of the project boring and uninteresting. The major part of the population were mildly interesting in the subject. When asked if they would like to see more investment on this project in the future, most users selected the three higher levels of interest, amounting to 88.8% of teh population (the results are summarized in figure A.12). This constitutes a quite positive feedback on the new authentication approach. Last, but not least, when inquired if they would be willing to use an improved version of the lock screen using the novel approach, approximately 75% of the users answered affirmatively or are strongly inclined to, while the remaining ones would most like not. Three users stated that they would never use this approach. The results for this question (question 13), which are depicted in figure 4.7, are nonetheless extremely promising.

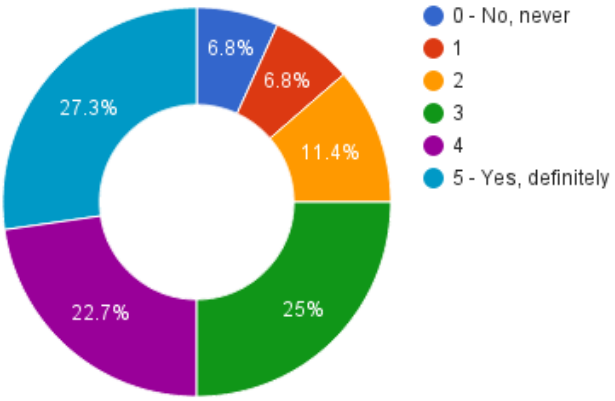

Figure 4.7: Pie chart for the results obtained for the question 13: *Would you use lock screen based on this concept?*.

4.3.2 Results of the Usability Test

The charts obtained for the results of the usability test were all included in Appendix B. This test was assessing how well would users respond to questions regarding their last or penultimate messages or calls. Users had to answer to these questions in their own smartphones when filling up the questionnaire. The application on the smartphone was mimicking a lock screen, but

was collecting also timing information and preparing a report in the background. Once the test was finished, the report was sent to the author. There were four main groups in the usability test: one for the penultimate sent messages or outgoing calls; one for the penultimate received messages or incoming calls; another one for the last received messages or incoming calls; and, finally, one for the last sent messages or outgoing calls. Figure 4.8 compares of the overall results for each one of these four groups. This chart shows the total number of questions that the users answered correctly or incorrectly. Although the results are similar across all groups, the group with more correct answers is the ones of the latest incoming calls and messages.

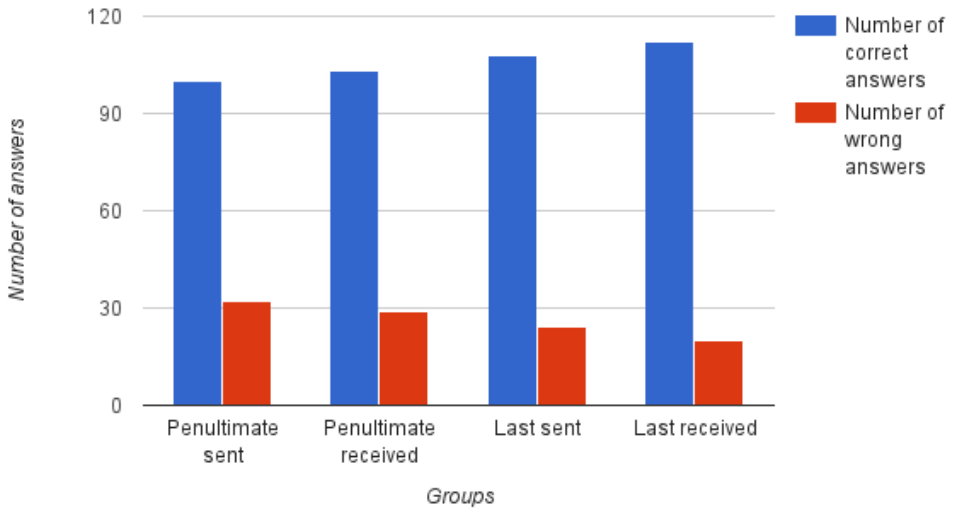

Figure 4.8: Column chart for the overall results for each group of the usability survey.

This part of the survey can be better analyzed resorting to the charts made to compare the several results obtained for the several challenge-questions. The charts in figure A.13 and A.14, for example, show that it was easier for the users to identify the name of the contact of the last outgoing or incoming calls than for the penultimate one. This also holds for the duration of the calls, as emphasized by the plots in figures A.15 and A.16. It is noticeable that knowing the duration of calls is harder than knowing the name of the contacts associated with communications. Either way, more than 50% of the answers were correct for most cases, except for the penultimate incoming call. In that situation, participants failed way more than succeeded. This suggests that that particular question may not be suitable for a challenge-question.

In terms of messages sent or received, most users were also able to correctly identify the name of the contact associated with either the last or the penultimate messages. These results are highlighted by the bar charts included in figures A.17 and A.18. Once again, users were more assertive regarding the last messages, but the difference is minimum.

The chart in figure A.19 compares results related with the contact name of outgoing and incoming *calls*. Even though the difference is not large (three persons), users seem to remember more easily the names associated with the incoming calls. In terms of the duration of the calls, the results in figure A.20 suggest otherwise. Users seem to remember significantly better the duration of an outgoing call. Probably, one is more aware of the objective of such calls, keeping a mental track of the time they take. Question-challenges based on sent or received messages seem to be very promising for authentication purposes, as corroborated by the results in fig-

ure A.21. Users typically know the contact that sent them a message or to whom it was sent to.

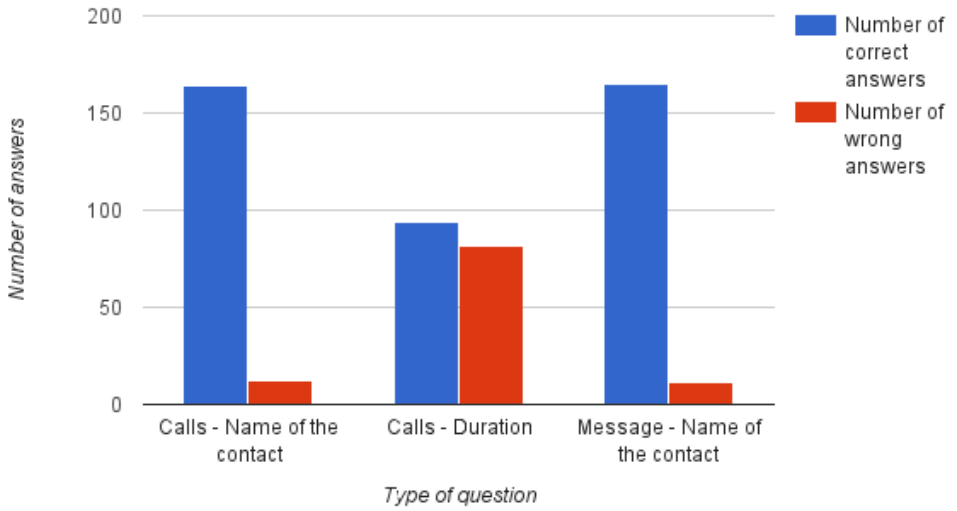

Figure 4.9: Column chart with overall results for each type of question.

Figure 4.9 exhibits the overall results for each type of question, namely *calls - name of the contact*, *calls - duration* and *messages - name of the contact*). A total number of 176 questions were made for the name of the contact associated with the last two calls, and 164 were correctly answered, corresponding to approximately 93%. As for the messages related questions, 93.8% of them were correctly answered too. The worst type of question concerns the duration of calls. In that case, there were only 53.4% of correct answers, which is low for such a mechanism. This implies that the inclusion of these question-challenges need to be carefully considered. The other two types of questions will make to the final prototype.

The Android application used in the usability was programmed to generate a different number of options for each question (three, four or five options). The results may thus be also analyzed from that dimension. Figure 4.10 plots the total number of correctly and incorrectly answered questions against the number of available options. There are some differences worth noticing. In 173 questions with three answers, there was a success rate of 85%; while for questions with four answers, that rate decreased to 79.1%. When five options were available, users were only able to correctly answer to 76.5%. The decrease from the three to the four options is larger than from four to five. Choosing three options will make the authentication mechanism more user friendly, but also more attacker friendly too.

If the results are analyzed for a particular type of question, as for example the name associated with a call, it is possible to conclude that the aforementioned difference is even larger between having three or four options, as illustrated in figure A.22. When three options are used, participants hit the correct answer 98% of the times, while for four and five options, this percentage decreases to 91.4% and 89.8%, respectively. In terms of the duration of the calls (see chart in figure A.23), the results were surprising and provide an interesting solution to the utilization of this type of question-challenge in the prototype. It was found out that the users were actually capable of correctly identifying the duration of calls often when only three options are available. Using five options would be disastrous to the mechanism, as the success rate in that case is very small.

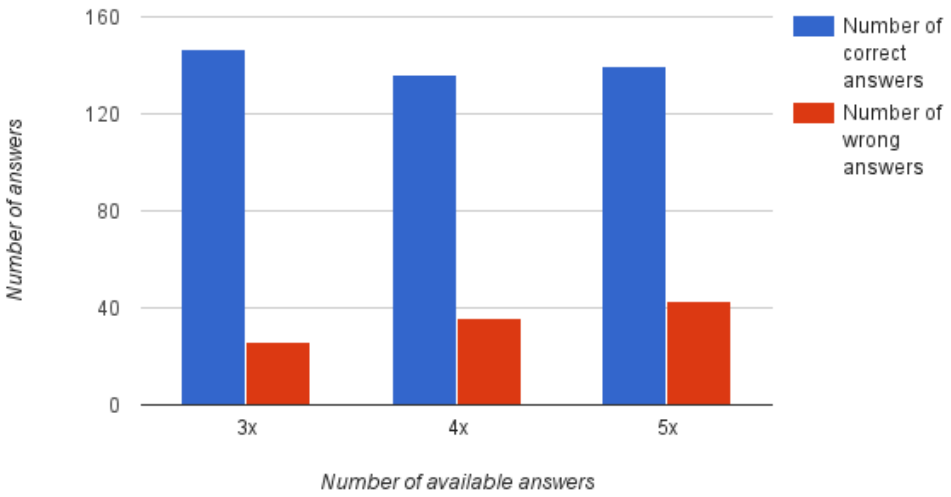

Figure 4.10: Column chart with overall results for each number of available answers.

Figure A.24 shows the overall results related with the question of *messages*, but like the two previous charts, this analyzes is about the success rate by each number of available answers. In this question either use 3 or 4 answers is quite similar, with a success rate close to 95%. In the case of presenting the user five answers, this tends to wander over, with a 91.5% success rate. Overall the use of either option offers a success rate of over 90%.

The next charts help analyzing the answers to the question regarding the duration of calls. The discussion will be mostly based on the 3 minimum intervals (15, 30 and 60 seconds) separating the potential answers of the question. Figure 4.11 shows the overall results of the *calls - duration*, this chart represents the global perspective of the impact of using different minimum times to separate the answers. The only option that achieved a positive result in the number of responses was when using 60 seconds. The remaining options the number of wrong answers is higher than the number of correct answers, where no managed have a success rate of over 48%, reaching the last option 60% of correct answers.

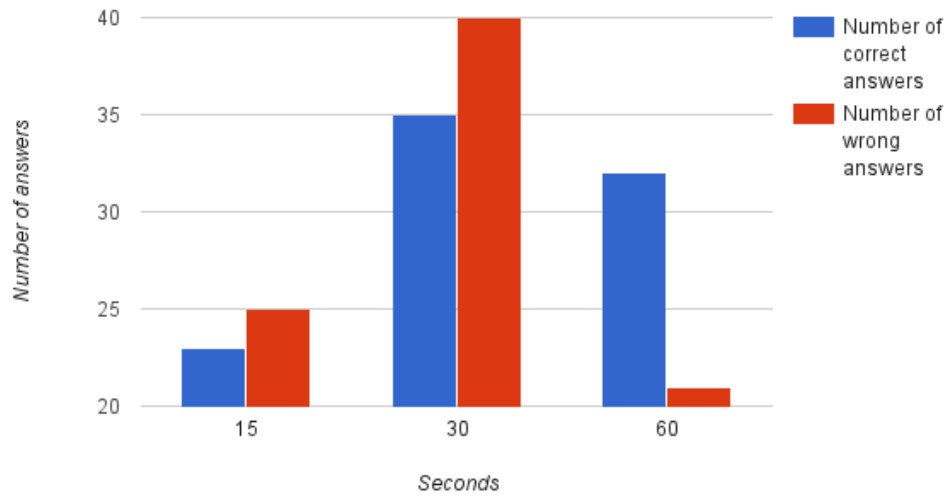

Figure 4.11: Column chart with the overall results for the three intervals separating the options in terms of durations of calls.

Figure A.25 exhibits the results about the penultimate outgoing and incoming calls. It is possible understand what is the impact of different minimum seconds between the understand in questions related with penultimate activities. Only the last option, 60 seconds ensures that at least half of the questions is answered correctly, with a rate of 66.7% of correct answers, and the options of 15 and 30 seconds below the 50% correct answers. Figure A.26 shows the results of the last call activities (outgoing and incoming calls). The results show that the users correctly answered at least 50% of the questions. The success rate is slightly higher than 50% in all options. Comapring the results of the figure A.25 on page 71 with the results of the figure A.26, the answers of the participants demonstrate that they can diferenciate easily the duration of the last call than penultimate calls. Figure A.27 shows the results concerning all outgoing calls (last and penultimate). The only option that had a rate (e.i., about 69%) of positive success was 60 seconds option, the remaining options had neutral or negative rate. Again, users seem to be able to better distinguish the call time with 60 seconds option. Figure A.28 exhibits the results concerning all incoming calls (last and penultimate). It becomes evident that irrespective of the provided minimum time, users have a tendency to err more questions than success, in any of the options the rate of correct answer is lower than the rate of wrong answers. It was concluded that users have difficulty remembering the duration of incoming calls, because in all the options the rate of failure is higher.

The average time taken by participants to respond to the questions of the usability test is analyzed next. Figure 4.12 shows the average duration to respond each group of the usability survey. Except the first group, where the average time to answer all questions exceeds the 30 seconds, all the other groups have show similar request time to answer all the questions, between 16 and 20 seconds. The decrease in the time required to answer each group decreases over time, which can be associated with the user to get used throughout the questions of the test, and thus be more quickly respond the next groups. The average time to answer each type

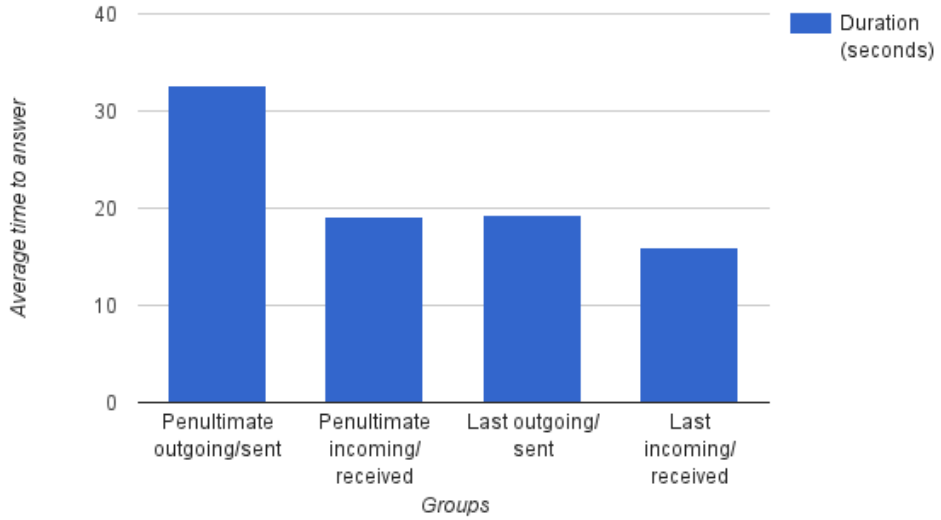

Figure 4.12: Column chart with the average time taken by the participants to respond to each group of the usability test.

of question can be seen in figure 4.13.There is a tendency to decrease the time between the various types of question, the question that requires more time for the user attempts an answer is the question related with calls - name of the contact, requiring an average of 8.5 seconds. The question related to the duration of calls requires roughly 7 seconds, the question that requires

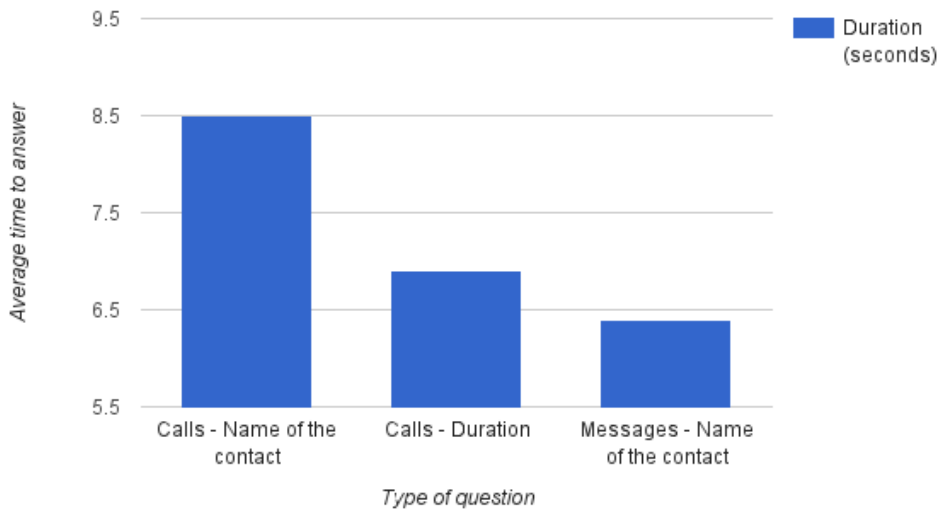

Figure 4.13: Column chart with the average time taken to respond to each type of question of the usability test.

less time is related with the messages, which on average only need 6.4 seconds. It is clearly that the question related with calls - name of the contact is the one that needs more time to be answer. Figure A.32 contains the detailed results for each question of the survey in the first group. In this group it is obvious that the first question is the one the requires more time to answer, and the answer where the user responded more quickly is the one concerning messages, with the average time to answer of 8 seconds. Figure A.33 shows the average time to answer each question of the second group of the usability test. In this group the time to answer each question is very similar. The variation between the most quick and the most slower times is 1.5 seconds. Figure A.34 exhibits the average time reuired to answer each question the third group of the usability test. The data presented allow us to conclude that all the questions required similar duration time to be answer. The answers that requires more time was the first one, with 7.4 seconds, question related with the duration of the calls required 5.7 seconds and in average users need 6.2 seconds to answer the last question. Figure A.35 shows the results regarding the questions of the last group of the survey. The average time to answer each question of this group is also similar, the maximum variation is around 1.2 seconds, with the user needs 6 seconds to answer the first question, 5.2 seconds to answer the second question and 4.8 seconds to answer the last one. Figure A.29 shows the comparison of the average time to answer a question of an outgoing call with an incoming call. The users tend to be more fast answer questions of incoming calls, and are 4 seconds show answering outgoing calls questions. From this perspective the user is more aware and confident answers questions related with incoming than outgoing calls. Figure A.30 exhibits the average time to answer a question related with sent and received messages. The timing results are very similar, and the variation is less that 1.5 seconds. It is assumed that users have almost the same confidence in responding question either related with sent or received messages, from the perspective of the above chart. Figure A.31 shows the results of the average time taken responding questions about penultimate and last calls - name of the contact. From the results show in the image, it is easily concluded that the user respond more fast to the question related with the last activity and needs more time to answer the penultimate questions.

During the analysis of the time to answer each question, very strange and unusual values were

found, for example there were questions were some users answered in less than 1 second, or even 0.1 seconds. Those values are suspicious, because in that time frame, a user does not have enough time to read the question, the answers and then press the correct answer. Opposite values were also found in the results, with some of the users needing more than 30 seconds to answer a question. In a few cases, they needed more than 60 seconds. There are no known reasons for these values, but two situations can be imagined. In the first one, concerning the case of a user answering quickly to questions, it may be due to an unintentional click on the screen. In the second case, concerning the huge delay in answering a question, probably the user pause the usability test to do something else, like watching TV.

4.4 Description of the Final Prototype

This section describes the prototype implementing the authentication approach idealized in Chapter 3, which uses the best results from the usability test.

4.4.1 Implementation Details

The implemented prototype is intended for smartphones with the *Android* 5.0 Lollipop or higher (as such, it uses the level 21 API). The programming language used to create the prototype was Java and the development environment in which it was elaborated was *Android* Studio 2.0. Initially, the prototype was tested using *Android* emulators only, but since it was easier to use the sources of data in a real device, the author moved to the usage of an LG g2 mini smartphone with Android Lollipop, making the task more easy and agile. Initially, calls and messages were simulated using two instances of emulators on the same computer.

Several prototypes were created before reaching the final prototype, though only two applications were emphasized in the discussion:

- Initially, an application to demonstrate the proof-of-concept for the layout was designed and tested. The prototype was used to analyze the messages and calls and simulate questions with multiple answers on the screen;

- Since *Google* took a while to free the entire API for Lollipop (which contains interesting resources to make lock screens), an application exploring several artifacts of the OS to lock the screen was implemented;

- The first prototype using the Lollipop API was build at a later stage, but the prototype was still not generating the questions according to the results of the survey;

- The final prototype, which comprises a fine-tunning of the previous one after analysis of the results of the survey. In the opinion of the author, this prototype fits better knowledge of the user and guarantees adequate security levels.

The user uses the mobile phone several times to make calls, access the Internet, play games, send messages, receive calls and messages, among other actions. By default, the OS and the respective applications save data from those activities in logs or databases. Given that the implemented prototype only uses data from calls and messages, it was not necessary to devise any application or background service to collect such information. The lock screen only needs

to ask for the right permissions to the OS in order to be able to generate the questions and the answers.

The lock screen application works like any other. When the screen turns off, the application is started, and when it comes on, it is displayed on the screen. To make it work like that, it was necessary to implement an Android *Service* component, that is constantly listening for when the screen is turned off. When the screen goes off, the lock screen is started and an algorithm decides what type of question will be displayed, as well as the number of questions and answers. Some of these aspects can be altered by the user, e.g., if he wants to change the level of security offered by the prototype. When the application wants to lock the device, the software will call an Android function to lock and other function to unlock the device. The function to lock is `startLockTask ()`, and the function to unlock the device is `stopLockTask()`.

4.4.2 Description of the Prototype

The implemented prototype supports two modes, previously referred to as *mode A* and *Mode B*. In the first variation of the prototype (which is considered the main output of this work), the software will create a series of questions to the user. Each question has an associated number of points and difficulty. During authentication, each time the user answers correctly to one of the questions, the respective number of points is added to a counter, or subtracted otherwise. If the user reaches a predefined superior limit, the mobile device is unlocked. If the number of points go below an inferior limit (also predefined), then the lock screen changes the flow to a different unlocking mechanism (see below). The question-challenge are the same ones discussed before, but using some of the learned facts from the survey (namely the generation of only three options for the duration of calls.) There is a maximum number of questions that a user may try to answers, to keep it manageable and avoid repetitions.

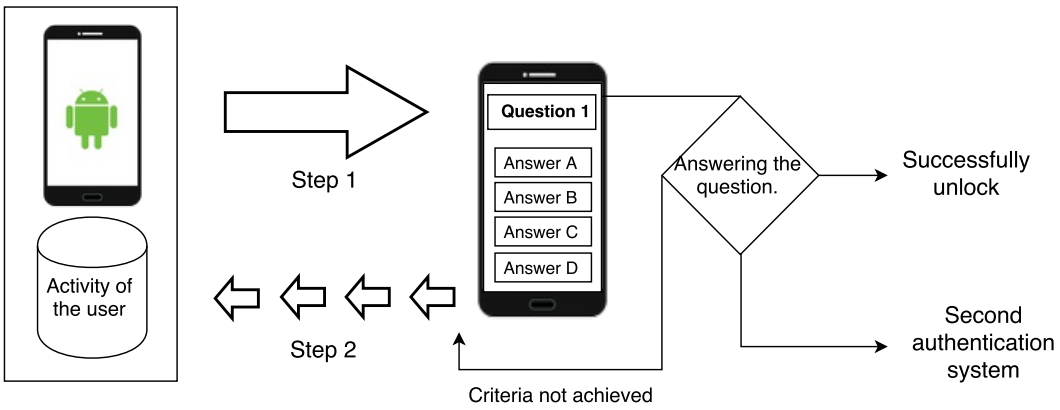

Figure 4.14: Workflow of the authentication procedure when the prototype is using mode A.

Figure 4.14 shows the general flow of the authentication procedure of the final prototype. Step 1 consists on generating the questions/answers using the activity of the mobile device. When the user responds to a certain question, either one of three scenarios may happen: the system is unlocked because the user reached the maximum number of points; the criteria to unlock the device was not fulfilled yet, and the lock screen asks for another question/answer; in the last scenario, the user reached the minimum number of points or reached the maximum number of questions, and the alternative authentication mechanism is invoked.

Some screenshots of the first variation of the prototype are included in figures 4.15, 4.16, and 4.17. They also show how the *challenge-questions* are organized and displayed to the user, as well as the options.

In this second variation of the prototype, the system creates a list (say list A) with the top 10 (but this number can change) contacts with which the user interacts more. To create that list the software uses also the recent calls and messages. The software orders the list by level of activity and then the software will choose only the top four (this number can change also) contacts. After that, the system will create a new list (list B) containing those four contacts and adds other six names (this number can change), resorting to the contact list of the smartphone (list Z), selecting names at random, but different from those of the top 10. This leads to showing a list of names in the lock screen. The user needs to select the names of the persons with which (s)he has more contact with, which should not be difficult, since the remaining ones come out of a list of contacts with which the user probably has no contact at all. From the perspective of the attacker, and since the names all come from the contacts list of the phone, the options should look like equally probable. This version of the prototype enables the user to select if it wants the list of names to be entered in a specific order (e.g., from the one (s)he interacts more with to the less popular one) or with no order. If the user sets the lock screen to required a specific order, then the level of security increases, but it is also more difficult to authenticate. Figure 4.18 shows the work flow of the second variation of the prototype, with all the different steps of the authentication and lists duly identified. In this mode, the user should feel very comfortable choosing the correct names, because its underlying idea is to use names of contacts that *say a lot to the user* against names that he is probably sure not to have been interacting with in the recent past.

The layout of this mode is very similar to that of applications implementing PIN code approaches, because the user must select the correct names of contacts amongst all the available. In terms of security, this mode is more secure than the one of the pattern based approaches, regardless of being similar in terms of operation (e.g., a user cannot choose the same option twice). The fact is that the pattern changes automatically with time in this case also. Notice that there is an implicit question in this mode also: *Can you select the names of the contacts you interact the most?*

As previously mentioned, a backup authentication procedure was included in the prototype for the case a user is unable to authenticate. It consists on entering a five digit code PIN. As a last resort, and since this is still a prototype, another fall-back was also added. It was included to prevent that someone installing the prototype for testing purposes to be locked out of its own device during this proof-of-concept stage. This last resort mechanism is boring and dull, and consists only on writing the code displayed on the screen several times. This third authentication mechanism is spawned if the user fails the backup mechanism.

4.5 Summary of the Chapter

This chapter discussed the results of the survey and analyzed the data from the usability test. With the results of the survey, it was possible to create a final prototype for this master's programme. To obtain statistically significant results, the survey was delivered to a population of 44 users. Each user answered all the questions and all of them ran the Android application

devised on purpose for this survey on their mobile device. This experiment allowed collecting information that helped in the elaboration of the final prototype. The survey application had more than 50 positive installations, but only 44 have sent the final report with all the information from the questions. One of the installations returned an error, probably due to the fact that no sufficient data was available in the messages or calls logs.

The work described in this chapter comprised one of the most import phases of this master's program, because it allowed the author to understand the user knowledge and obtain feedback about the subject. The user knowledge and the opinion of the participants about the main concept was collected. Using surveys and usability tests is one of the most reliable ways to get the real feedback from end users. The information collected during the survey provided a significant contribute to the analysis of the authentication approach, though more work is still required. The major part of the participants have shown interest in the subject and liked the proposed approach. A good part of them would like to see more investment in the future on the subject.

It was found that two of the three question-challenge explored in the usability test have more chances of being correctly answered by users and, as such, make to a final prototype of the authentication approach (e.g., see figure 4.9), but none of the options should be excluded. The most promissory questions are related with the names associated with calls and messages. Participants correctly answered to approximately 93.5% of those questions. On the other hand, in the question concerning the duration of calls, participants have failed 46.6% of the times. Questions of this type can be included if only three options are provided, and if the time difference between options is 60 seconds or more.

The final prototype was presented at the end of the chapter. The prototype includes two modes implementing complementary authentication mechanisms based on user activity. Their advantages and disadvantages were briefly described. The author hopes that they constitute a starting point for future work on this area and possibly to a mature screen lock. The prototype will run in Android powered devices starting from version 5.0.

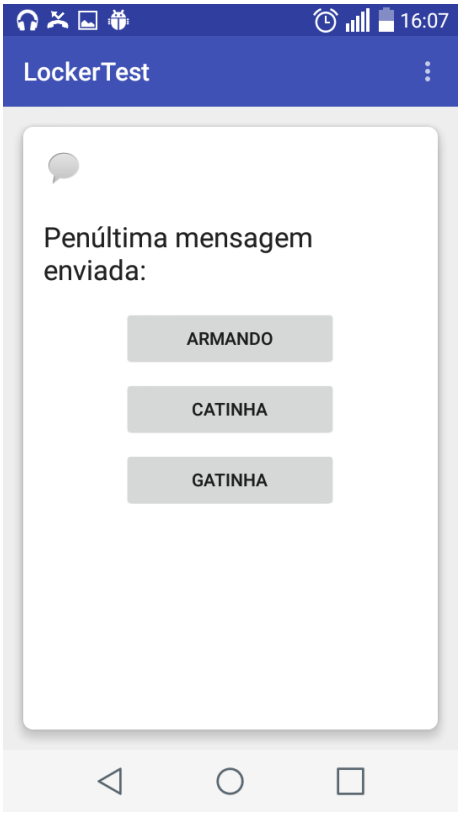

Figure 4.15: Screenshot of the prototype asking for the name of the contact of the last outgoing call.

Figure 4.16: Screenshot of the prototype asking for duration of the last incoming call.

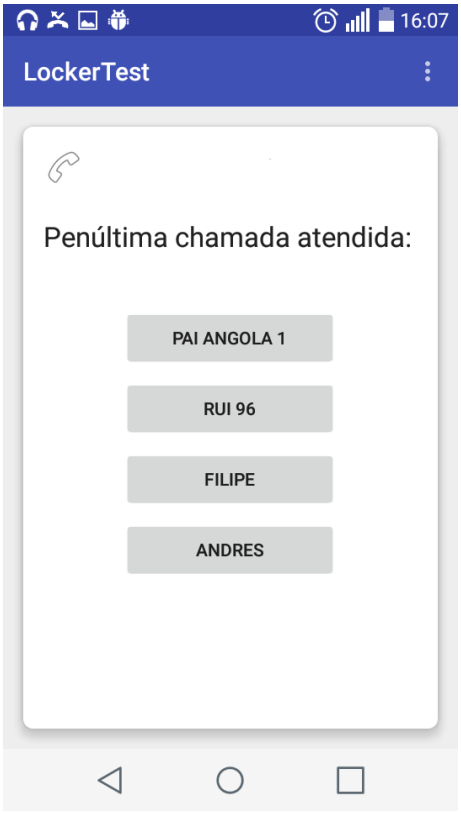

Figure 4.17: Screenshot of the prototype asking for the name of the contact associated with the last sent message.

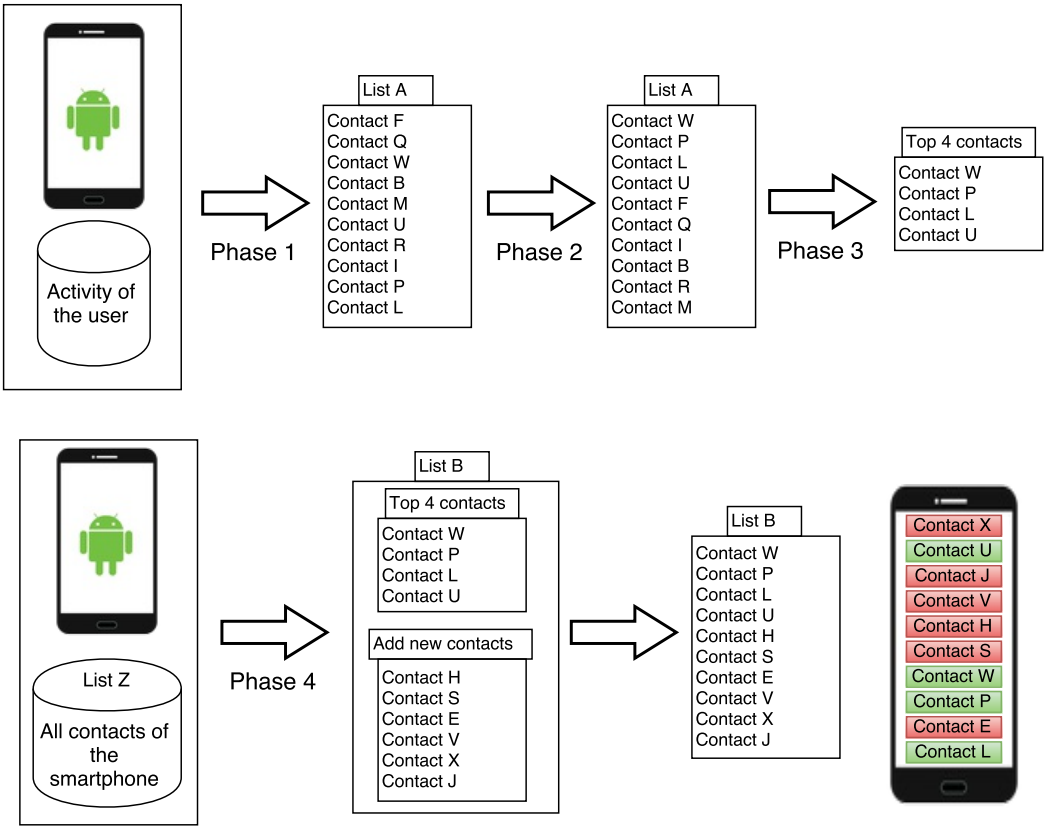

Figure 4.18: The work flow of the *mode B* implemented in the prototype.

Chapter 5

Conclusions and Future Work

This chapter wraps up the main conclusions of the work developed throughout this master's programme. It also describes several aspects and subjects that would be interesting to explore in the future. This chapter is thus composed by two sections: section 5.1 is dedicated to the presentation of the the main conclusions and section 5.2 includes the guidelines and suggestions for future work.

5.1 Main Conclusions

Authentication is an important security mechanism for computer systems and infrastructure. It is this mechanism that prevents someone to access a service, a place or a software that he or she is not authorized to. In the case of mobile devices, the lock screen comprises one such mechanism, and it actually blocks the access to personal data and applications. Most lock screens are based on a static secret (e.g., a PIN) that only the legitimate owner should know. There are several lock screens on the market, with most of them installed by default on the mobile devices by the software or appliance manufacturer which, sometimes, are also their creators. This dissertation presents an authentication mechanism that, to the best of the knowledge of the author, has never been explored and tested before. Part of the work of this program was devoted to exploring what data could used in such authentication mechanism. Its ultimate goal was the development of a prototype for a lock screen, in which the secret to unlock the device was somehow based on the previous activity of the owner in that very same device.

In the early part of this work, various types of widely used lock screens, implemented and available for smartphones, were analyzed. A discussion was included herein too, in chapter 2. In recent years, other authentication mechanisms for mobile devices have been proposed and tested by researchers. It was also shown that the most used lock screens are based on a *something you know* factor. Additionally, the secret of the authentication does not change over time, unless the user changes it explicitly. The existing implementations of lock screens are usually configured during the first utilization of the smartphone or tablet, and supposedly only the owner of the mobile device gets to known the underlying secret. Nonetheless, the design of these screens and types of code is often different depending on the manufacturers. For some, the insertion of a code is required, while for others a pattern must be drawn using the touchscreen, or even pressing previous determined points on the screen, amongst others. The problem of the code being static is common to all of them. Changing the secret requires the user to make an effort to memorize the newly configured one. One of the advantages of the mechanism proposed in the scope of this work is that the secret is constantly changing, but the user knowns it all the time. The mechanism is still based on a *something you know* factor. This aforementioned characteristics comprise actually the innovative aspects of the proposal.

Chapter 3 contains a discussion on the meaning of authentication and elaborates, from that, on the design and structure of the developed authentication mechanism. It explains the basis of the underlying concept with detail, and the work flow of the approach. The authentication concept assures that security and user privacy are maintained and it presumes that that the supplicant supplies correct answers to several questions in order to unlock the mobile device. In other words, this concept guarantees the existence of a secret that only the owner of the mobile device should know, but that is always changing. As with any other lock screen, the task of verifying the authentication procedure is guaranteed by the developed software itself. A study of possible security variables that could be used in the proposed approach was also performed in the scope of this work, and discussed therein, along with possible factors that can contribute to increasing or decreasing the security of the proposed mechanism. Additionally, a comparison between the proposal and the most common lock screen used in mobile devices was also performed, so as to emphasize the differences and similarities between them.

Thought the concept behind the authentication mechanism was simple, the work was challenging. There were two main aspects that revealed to be more difficult than expected: one was the analyses and comparison of the results of the survey, which needed much more attention and dedication to produce useful results that could be used to produce a better prototype; the other was to build the prototype following Google guidelines and using its Software Development Kit (SDK). Concerning the latter, it should be mentioned that Google only released the necessary features to build a lock screen in a more simpler way recently (e.i., in Android Lollipop), allowing one to build such application without having to resort to layout hacks or to software bugs. The main output of this master's program is an application that is ready to be installed in an Android powered device, starting from the Lollipop version. This prototype does not represent an impenetrable lock screen yet, but it can be considered a viable alternative to other similar applications, thought this one offers a fundamentally different authentication concept. Some problems were also faced during the selection of the sources of data and transformation of the raw data into questions. The Android API does not offers as many sources as initially thought, which led to abdicating of some initial ideas and focus on the available sources of data.

There are several differences between the final prototype and the application used in the survey. Some features (e.i., storing the amount of time that the user needed to respond each question in the usability test) were added to the lock screen used in the survey, so as to better measure the knowledge and reaction of the participant, when facing the several questions. The addition of partial and total times in the survey lock screen revealed to be more important that expected. The inclusion of this logic allowed obtaining a different perspective over the results. Analyzing the results with or without this feature is significantly different, as discussed in chapter 4, making it a key factor when devising the final prototype.

Most of the participants of the questionnaire found the concept and the prototype very simple and intuitive (e.g., see figure A.10), although some of the participants needed a brief explanation of some aspects of the lock screen initially. Their doubts were mostly related with the privileges of the application. After a brief explanation, the interaction with the application proceeded normally. Almost all individuals found the idea very interesting and about 21 participants (figure 4.7) ponder using a final version of this idea as an authentication mechanism on their mobile device. The elaboration of the survey and the subsequent analyzes of the results were amongst the most important steps of this master's program. The analysis over the results

helped understanding which were the most important characteristics and questions that needed to make it to the final prototype.

The survey was composed by several groups of questions: the first group concerned general knowledge regarding mobile devices, mobile security and authentication; the second group was the usability test; the third group contained questions about the opinion and feedback of the participant about the subject of the survey; and (iv), a group was dedicated to the whole experience. The usability test was divided into 4 groups, each containing 3 questions (calls - name of the contact; calls - duration; and messages - name of the contact). Each group had its own specific details, which influenced the shape of each question, e.g., whether the issue was related to any data sent or received on the mobile device, or if it was the last or penultimate action. A total number of 44 users participated in the survey, answering a total of 528 questions. A success rate of 80.1% was obtained in the usability test, which is very promissory. If the question with the lowest success rate (53.4%) is removed, the overall success rate goes to 93.5%. Interestingly, users tended to answer correctly to more questions than initially expected. It can thus be concluded that this mechanism can be applied in conjunction with other security mechanisms, or be integrated in existing solutions. Actually, there are several security services that could benefit from the usage of this concept, such as passwords recovery in web platforms.

The question related with the duration of calls obtained the worst results, revealing that the users do not usually have the explicit notion of the time a given call lasted for. Nonetheless, it is argued that the best case of this question, concerning only the last incoming or outgoing call, can still be used (see figure A.15 and figure A.16). Questions using the name of a contact, either in the case of calls or messages, have proved to be very promising. Users answered correctly to those questions 94% of the times, with only one more correct answer for the messages questions. Users are thus more aware of the names of the contacts involved in communications than with information related with duration of calls.

Comparing the 4 different groups of the usability test, it was possible to conclude that participants have higher success rate for questions regarding the last last call or message than for previous ones. Our mind also seems to store better the information regarding incoming messages or calls than outgoing communications (even though the difference is minor), which is an interesting finding for building a proof-of-concept. From the set of 12 questions, the case in which more participants failed was the one concerning the duration of the penultimate incoming call (a success rate of 45.5%). On the other hand, the question with the highest number of correct answers was the one concerning the contact name of the last incoming call, to which all answered correctly, even when the number of options was 5. This proves that for, certain questions, the number of responses is almost irrelevant.

Another parameter that was varied during the usability testing was the one of the number of responses per question. The results show a significant difference between the three options studied (i.e., 3, 4 or 5 possible answers to choose from). The tendency is to fail more when more options are available, as expected, but the variation in the success rate between using 3 or 4 answers is 6%, whereas between using 4 or 5 answers is approximately 3%. This was an important finding when developing the prototype of authentication.

The objectives drawn for this work were successfully achieved. The viability of the approach

was thoroughly studied along the course of the project and the delivered prototype is fully functional, paving the way for future research work and possibly to real-world and wider adoption of the approach.

5.2 Future Work

The program described in this dissertation concerns the development of a lock screen prototype, for mobile devices, that is based on the activity of the user. It would be interesting to explore the several possibilities where it is possible to apply this new authentication approach. This section is reserved to explain and point out some future directions that could be later investigated starting from the outputs of this program. It would be exciting to add and change some characteristics of the proposed concept, and test them practically. E.g., this could be done, again, via the usage of surveys.

Continuing the study on this topic will surely help to better understand how well the users know their mobile devices and remember their activities. To deepen such knowledge can improve the effectiveness of the authentication, add new features and contribute to increase the security of the mechanism, as well has improving the simplicity of the prototype. Next, it will be briefly described and discussed each one of the potential directions that can be used:

- **Interface** - It would be interesting to create a new interface that allows users to feel more comfortable using this authentication approach, since it will allow more users to have contact with the new concept;

- **Multi-factor Authentication** - It is desirable to study the combination of this approach with other authentication means, resulting in a new two-factor authentication. The suggestion is to use this new approach of authentication with other regular and customary authentication mechanisms, increasing the security levels of the authentication procedure. Multi-factor is already being used (partially) in several online platforms. A multi-factor process that could be explored is the combination of this approach with tracking the user device. A possible feature that has been considered during this work was to conciliate the Global Positioning System (GPS) position of the user, during the day, with the authentication concept. In such scenario, the software would not only basis its trust on the answers of the user, but also compare the values of predetermined GPS position with his current position, while trying to perform the authentication;

- **New sources of data** - One of the aspects that needs more research is related with the sources of data. The amount of sources that provide data related with the activity of the user is dependent of the Android API. Increasing the number of sources to generate the questions would be beneficial. It can be considered the option to create a mechanism (sniffer) for gathering user activity in the background too, though it needs more reflexion and testing. Some other possible data sources that can be also explored are related with the applications, as for example the last application used or installed, etc.;

- **Cloud data** - It could be interesting to create a centralized data base for gathering all data from different devices (e.g., mobile devices, smartTelevision (TV), smart Watch, Internet, etc). All of these could then be used to generate the questions and the answers of the

lock screen application;

- **An inverse prototype** - New surveys with different perspectives, but still studying the usefulness of the idea of this dissertation are needed also, as they can lead to exploring new ideas or even detect benefits or problems on the proposal. For example, it would be interesting to conduct a survey on the amount of participants that can correctly answer to questions on a phone of a stranger. To perform that study, the same application could be used, but instead of having the owner of the smartphone performing the survey, the device would be lent to someone else during the questionnaire. This study would help understanding if an unknown user could create a relation between the information displayed and the right answer. The idea of this study has emerged from the fact that, during the survey of this program, it was notice that some contact names of the mobile device can trigger more interest than others;

- **Recovery password** - Several websites and services use multiple questions to recover a lost password. The security approach suggested in this dissertation could be used to replace such mechanisms. Instead of an answer that is defined long time ago and do not change over time, the same feature could be built over this new approach. The benefits are that the secret changes along the time and is probably fresher in the mind of the user. In the existing mechanisms, a hacker can explore the past life of the user and try to figure out what is the answer for those questions.

- **Fall-back Authentication** - An idea that can be explored and tested in the future is the implementation of this authentication approach as a secondary authentication mechanism, or as a reset mechanism of a lost password or a locked system and/or device. In case a user fails authentication in a primary system, the system blocks and several questions are showed to the user. If he successfully answers a minimum amount of questions, the system is unlocked and the user can then change the password.

The previous list summarizes some ideas that would be interesting to explore in the future. The approach of this master's program is new and has never been subject of research. New ideas and research related with this new authentication approach, using part or all of it, would be very interesting.

Bibliography

[BJR+06] John Brainard, Ari Juels, Ronald Rivest, Michael Szydlo, and Moti Yung. Fourth-factor Authentication: Somebody You Know. In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS06)*, pages 168–178, New York, NY, USA, 2006. ACM. 8, 12

[BPA12] Joseph Bonneau, Sören Preibusch, and Ross Anderson. A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs. In AngelosD. Keromytis, editor, *Financial Cryptography and Data Security*, volume 7397 of *Lecture Notes in Computer Science*, pages 25–40. Springer Berlin Heidelberg, 2012. 16

[CW13] Marco Chiappetta and Alex Wawro. Research paper: Windows 8 picture passwords can be cracked [online]. February 2013. Available from: `http://www.pcworld.com/ARTICLE/2028724/windows-8-picture-passwords-their-great-untapped-potential.html` [cited Jun 5, 2015]. 2

[Dan13] Danyl Bosomworth. Mobile Marketing Statistics 2015 [online]. July 2013. Available from: `http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/` [cited June 7, 2015]. 1

[dL14] Christian de Looper. Samsung Galaxy S5 fingerprint scanner explained [online]. February 2014. Available from: `http://www.talkandroid.com/196604-samsung-galaxy-s5-fingerprint-scanner-explained/` [cited June 22, 2015]. xix, 11

[dS15] Loja de Serviços. Cópia de Chaves [online]. 2015. Available from: `http://www.lojadeservicos.com/copia-de-chaves/` [cited June 10, 2015]. xix, 11

[EJP+14] Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. Are You Ready to Lock? In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS14)*, pages 750–761, New York, NY, USA, 2014. ACM. 19

[FBC+13] José Filho, Gabriella Barros, Thun Chiu, Patricia Tedesco, Antonio Cavalcanti, Carlos Maciel, Angelia Mascaro, Fábio da Silva, and André Santos. ScreenLock: A Smart Display Management System for Smartphones. In *Proceedings of the 2013 IEEE 10th International Conference on High Performance Computing and Communications 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC)*, pages 2174–2180, November 2013. 19

[FMS13] Daniel Fischer, Bernd Markscheffel, and Tobias Seyffarth. Smartphone security: Overview of security software solutions. In *Proceedings of the 2013 8th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages

288–289, December 2013. 18

[Gem11] Gemalto. Three-factor authentication: Something you know, Something you have, Something you are [online]. September 2011. Available from: http://blog.gemalto.com/blog/2011/09/05/three-factor\-authentication-something-you-know-something-you-have-something-you-are/ [cited May 10, 2015]. 8

[GLW+09] Haichang Gao, Xiyang Liu, Sidong Wang, Honggang Liu, and Ruyi Dai. Design and Analysis of a Graphical Password Scheme. In *Proceedings of the 2009 4th International Conference on Innovative Computing, Information and Control (ICICIC)*, pages 675–678, December 2009. 15

[Ham15] Tara Hamilton. FACEBOOK AND GOOGLE DEVELOP AMAZING FACIAL RECOGNITION ALGORITHMS [online]. June 2015. Available from: http://www.mirrordaily.com/facebook-and-google-develop-amazing-facial-recognition-algorithms/22402/ [cited July 17, 2015]. xix, 11

[IBN13] IBN News HP. Motorola Atrix had a fingerprint scanner two years before iPhone 5s [online]. September 2013. Available from: http://www.ibnlive.com/news/india/motorola-atrix-had-a-fingerprint-scanner-two-years-before-iphone-5s-638036.html [cited May 13, 2015]. 17

[IDC15] IDC Research, Inc. Smartphone OS Market Share, 2015 Q2 [online]. August 2015. Available from: http://www.idc.com/prodserv/smartphone-os-market-share.jsp [cited August 5, 2015]. 1

[img15] RFID Card Keyless Door Access Control Lock With Deadbolt Latch +2 Emergency Keys [online]. 2015. Available from: http://www.dhgate.com/product/rfid-card-keyless-door-access-control-lock/179751064.html [cited June 11, 2015]. xix, 11

[JM13] Lukas Jeter and Shivakant Mishra. Identifying and quantifying the android device users security risk exposure. In *Proceedings of the 2013 International Conference on Computing, Networking and Communications (ICNC)*, pages 11–17, January 2013. 2, 17, 18

[JN12] Anil Jain and Karthik Nandakumar. Biometric Authentication: System Security and User Privacy. *Computer*, 45(11):87–92, November 2012. 11

[Jus04] Mike Just. Designing and evaluating challenge-question systems. *Security Privacy, IEEE*, 2(5):32–39, September 2004. 22, 27

[Jus09] Mike Just. Account Recovery Challenges: Secure and Usable Authentication. In *Proceedings of the Information Security Summit 2009 (ISS)*, page 6, 2009. xix, 9, 15, 22

[KNOM12] Sohail Khan, Mohammad Nauman, Abu Talib Othman, and Shahrulniza Musa. How

secure is your smartphone: An analysis of smartphone security mechanisms. In *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pages 76–81, June 2012. 18

[Kre06] Brian Krebs. Citibank Phish Spoofs 2-Factor Authentication [online]. July 2006. Available from: http://voices.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html [cited May 12, 2015]. 13

[KWSJ03] Ajay Kumar, David Wong, Helen Shen, and Anil Jain. Personal Verification Using Palmprint and Hand Geometry Biometric. In *Proceedings of the 4th International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA03)*, pages 668–678, Berlin, Heidelberg, 2003. Springer-Verlag. 15

[MAFL10] Pedro O. S. Vaz De Melo, Leman Akoglu, Christos Faloutsos, and Antonio A. F. Loureiro. Surprising Patterns for the Call Duration Distribution of Mobile Phone Users. In *Proceedings of the 2010 European Conference on Machine Learning and Knowledge Discovery in Databases: Part III (ECML PKDD'10)*, pages 354–369, Berlin, Heidelberg, 2010. Springer-Verlag. 32

[ML13] Stephen Mujeye and Yair Levy. Complex passwords: How far is too far? The role of cognitive load on employee productivity. *Online Journal of Applied Knowledge Management*, 1(1):122–132, January 2013. 19

[Mob15] Mobilecon. Advantages and Disadvantages Android mobile phone [online]. 2015. Available from: http://mobilecon.info/advantages-and-disadvantages-android-mobile-phone.html#sthash.ybpxyIUv.9pKg6KjC.dpbs [cited May 5, 2015]. 1

[Net15] Netmarketshar. Mobile/Tablet Operating System Market Share [online]. 2015. Available from: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1 [cited Jun 5, 2015]. 1

[O'C15] Fred O'Connor. Android gains share, iOS falls in 2014 smartphone OS market [online]. February 2015. Available from: http://www.pcworld.com/ARTICLE/2888532/idc-android-ios-again-dominate-smartphone-os-market.html [cited Jun 5, 2015]. 1

[Reb14] Rebecca Murtagh. Mobile Now Exceeds PC: The Biggest Shift Since the Internet Began [online]. July 2014. Available from: http://searchenginewatch.com/sew/opinion/2353616/mobile-now-exceeds-pc-the-biggest-shift-since-the-internet-began [cited June 7, 2015]. 1

[Sch05] Bruce Schneier. The Failure of Two-Factor Authentication [online]. July 2005. Available from: https://www.schneier.com/blog/archives/2005/03/the_failure_of.html [cited May 13, 2015]. 9, 13

[SHWH12] Lin Sun, ShuTao Huang, YunWu Wang, and Meimei Huo. Application Policy Security

Mechanisms of Android System. In *Proceedings of the 2012 IEEE 14th International Conference on High Performance Computing and Communication 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS)*, pages 1722–1725, June 2012. 19

[Spi03] Edmund Spinella. Biometric Scanning Technologies: Finger, Facial and Retinal Scanning. May 2003. 17

[SPLP12] Kwang Il Shin, Ji Soo Park, Jae Yong Lee, and Jong Hyuk Park. Design and Implementation of the Improved Authentication System for Android Smartphone Users. In *Proceedings of 2012 26th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pages 704–707, March 2012. xxiii, 14, 29

[Sta15] Statista Inc. Vendors' sales of mobile phone sales to end users worldwide from 2010 to 2015 (in million units), by quarter [online]. May 2015. Available from: `http://www.statista.com/statistics/263355/global-mobile-device-sales-by-vendor-since-1st-quarter-2008/` [cited May 5, 2015]. 1

[SUSM09] Fazl-e-Hadi Shakir Ullah Shah and Abid Ali Minhas. New Factor of Authentication: Something You Process. In *Proceedings of International Conference on Future Computer and Communication, 2009 (ICFCC 2009).*, pages 102–106, April 2009. 8, 12

[SZO05] Xiaoyuan Suo, Ying Zhu, and Scott G. Owen. Graphical Passwords: A Survey. In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC05)*, pages 463–472, Washington, DC, USA, 2005. IEEE Computer Society. 2

[TA08] Hai Tao and Carlisle Adams. Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. *I. J. Network Security*, 7(2):273–292, 2008. Available from: `http://dblp.uni-trier.de/db/journals/ijnsec/ijnsec7.html#TaoA08`. 15

[TA14] Mohammad Tanviruzzaman and Sheikh Iqbal Ahamed. Your Phone Knows You: Almost Transparent Authentication for Smartphones. In *Proceedings of the 2014 IEEE 38th Annual on Computer Software and Applications Conference (COMPSAC)*, pages 374–383, July 2014. 14, 20

[UDWH13] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns. In *Proceedings of the 2013 ACM (SIGSAC) Conference on Computer & Communications Security (CCS13)*, pages 161–172, New York, NY, USA, 2013. ACM. 17, 18

[uHNA10] Syed Shabih ul Hasan Naqvi and Samiullah Afzal. Operation Code Authentication preventing shoulder surfing attacks. In *Proceedings of the 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, volume 4, pages 32–35, July 2010. 14

[WWB+05] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir

Memon. PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. *Int. J. Hum.-Comput. Stud.*, 63(1-2):102–127, July 2005. Available from: http://dx.doi.org/10.1016/j.ijhcs.2005.04.010. 3

[YLKJ10] Han-Na You, Jae-Sik Lee, Jung-Jae Kim, and Moon-Seog Jun. A study on the two-channel authentication method which provides two-way authentication in the Internet banking environment. In *Proceedings of the 2010 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, pages 539–543, November 2010. 13

Appendix A

Charts Summarizing the Results from the Survey

This appendix contains part of the charts that were obtained during the analysis of the answers to the user survey. Most results were discussed in chapter 4.

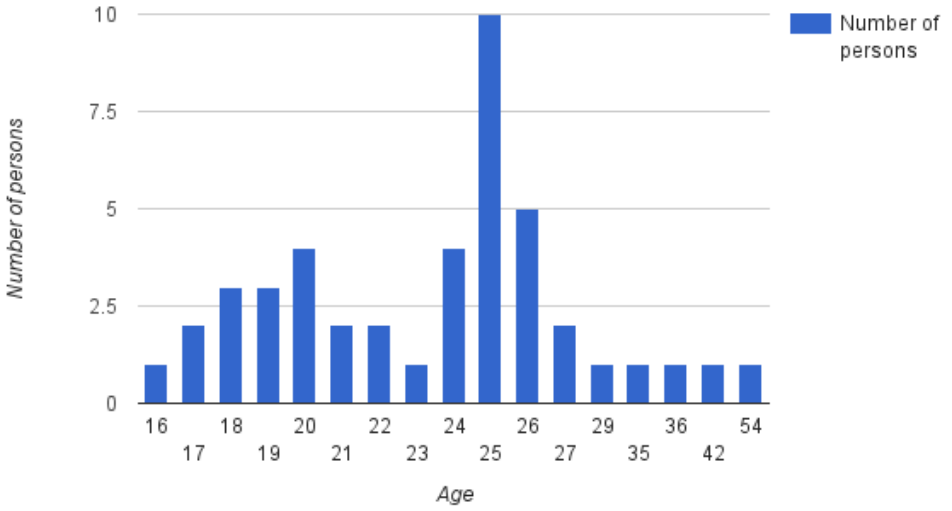

Figure A.1: Column chart for the results obtained for the question 1 (*How old are you?*) of the survey.

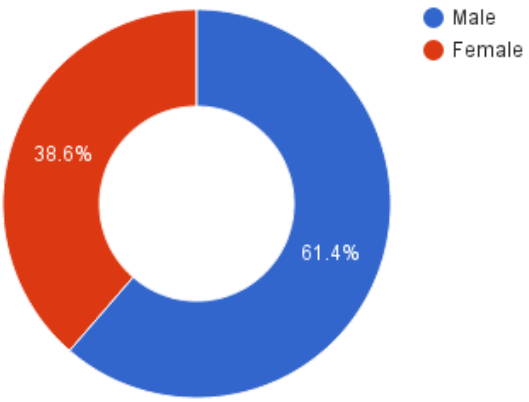

Figure A.2: Pie chart for the results obtained for the question 2 (*Gender?*) of the survey.

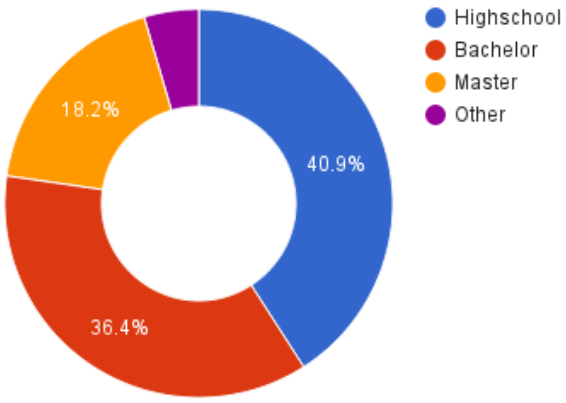

Figure A.3: Pie chart for the results obtained for the question 3 (*Academic degree?*) of the survey.

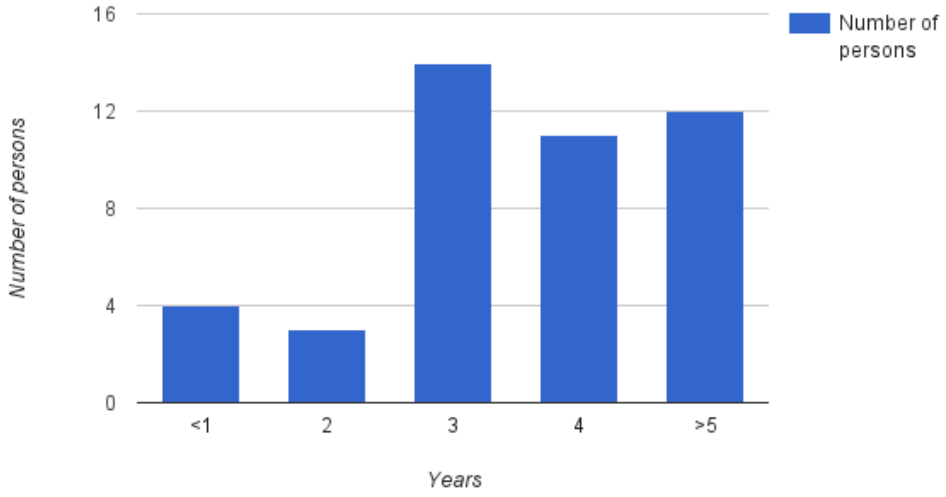

Figure A.4: Column chart for the results obtained for the question 4 (*For how long you use a smartphone?*) of the survey.

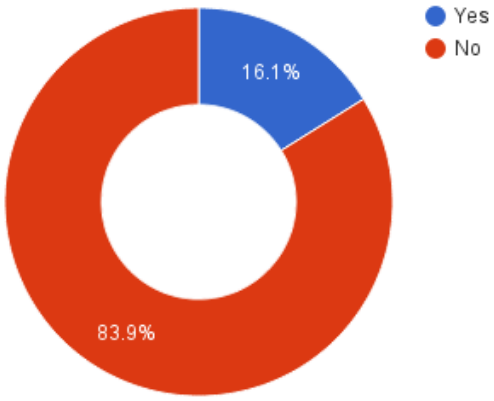

Figure A.5: Pie chart for the results obtained for the question 6.2 (*Do you ever forgot the secret code of a lock screen?*) of the survey.

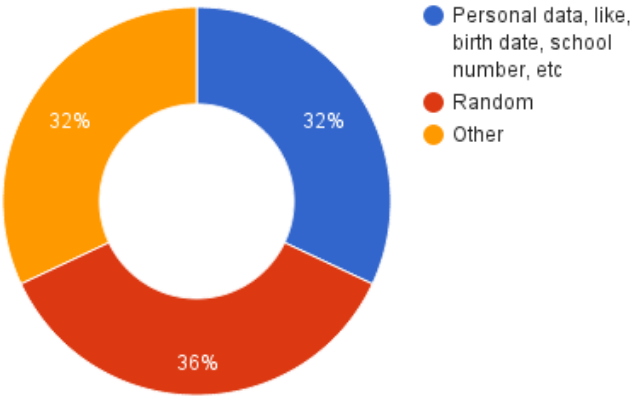

Figure A.6: Pie chart for the results obtained for the question 8.2 (implicitly given by *The secret code is related with:*) of the survey.

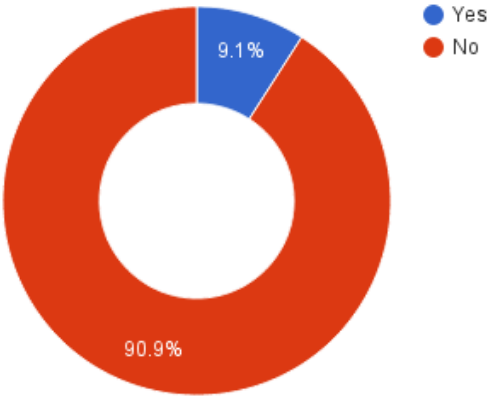

Figure A.7: Pie chart for the results obtained for the question 9 (*Did you ever lost your mobile device, or does someone stole it from you?*) of the survey.

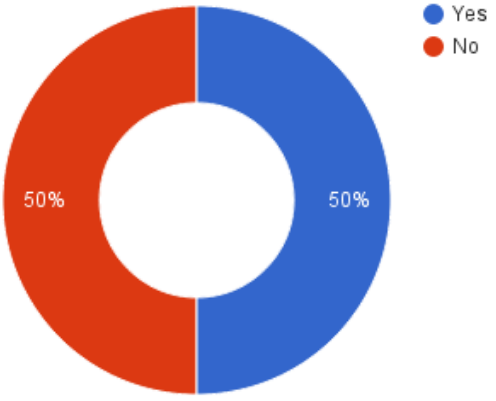

Figure A.8: Pie chart for the results obtained for the question 9.1 (*Do you have, or did you ever had, important and confidential information/data stored in your smartphone?*) of the survey.

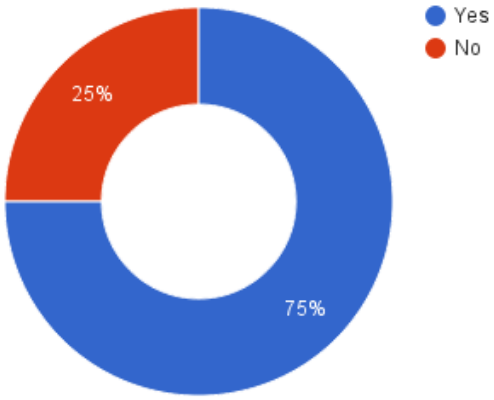

Figure A.9: Pie chart for the results obtained for the question 9.2 (*In the case you answered yes to the previous question, were you using a lock screen with a secret code?*) of the survey.

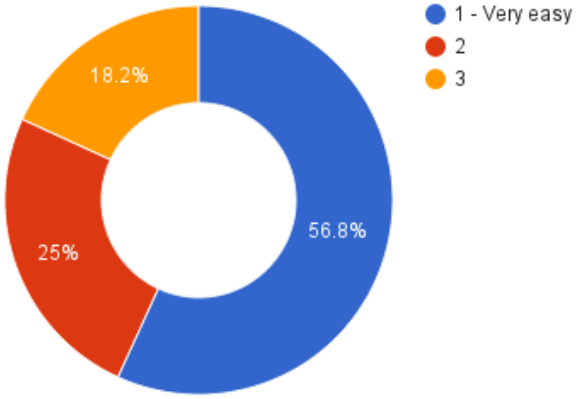

Figure A.10: Pie chart for the results obtained for the question 10 (*How do you rate the difficulty of the survey?*) of the survey.

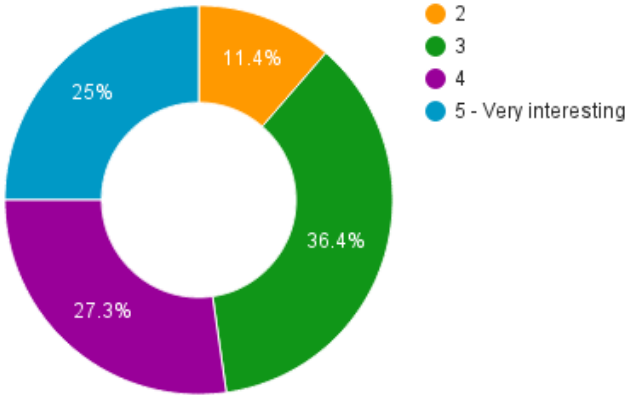

Figure A.11: Pie chart for the results obtained for the question 11 (*Did you find the authentication concept under evaluation in this survey interesting?*) of the survey.

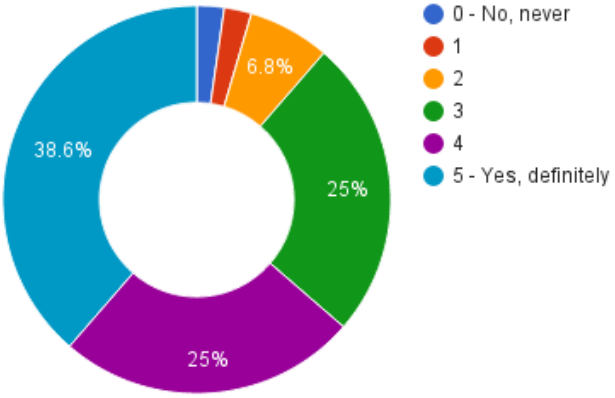

Figure A.12: Pie chart for the results obtained for the question 12 (*Do you think that we should continue investigating this concept?*) of the survey.

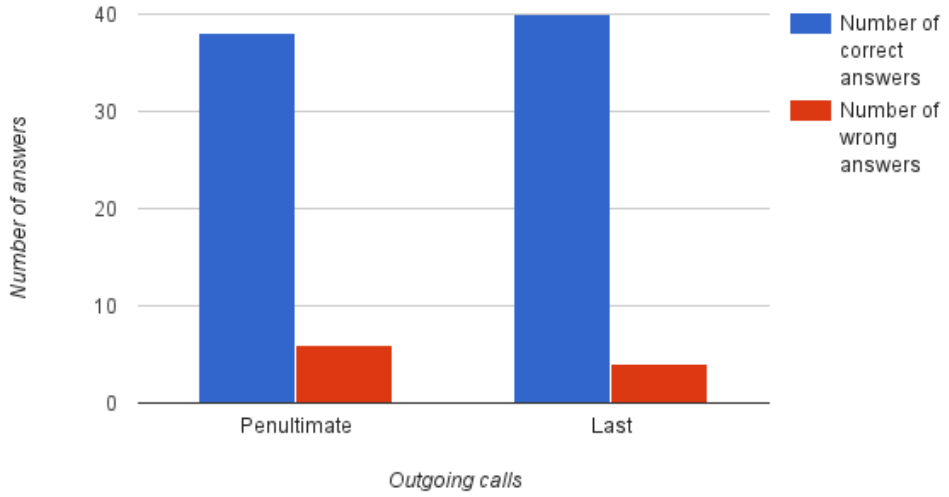

Figure A.13: Column chart showing the number of correct and incorrect answers to questions regarding the *names* associated with the last two outgoing *calls*.

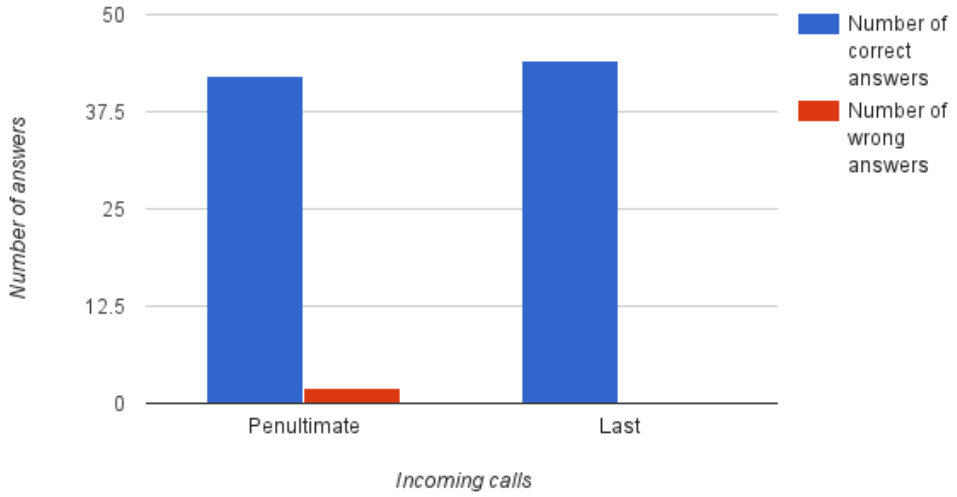

Figure A.14: Column chart showing the number of correct and incorrect answers to questions regarding the *names* associated with the last two incoming *calls*.

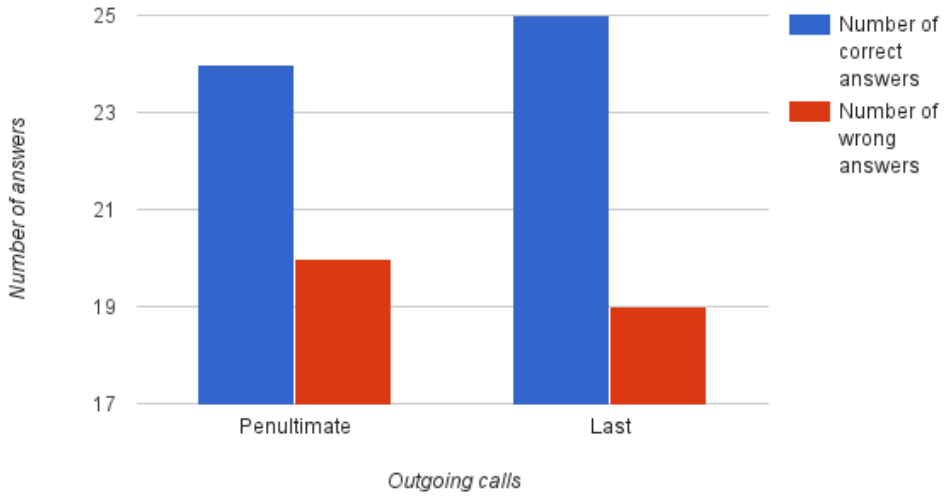

Figure A.15: Column chart showing the number of correct and incorrect answers to questions regarding the *duration* of the last two outgoing *calls*.

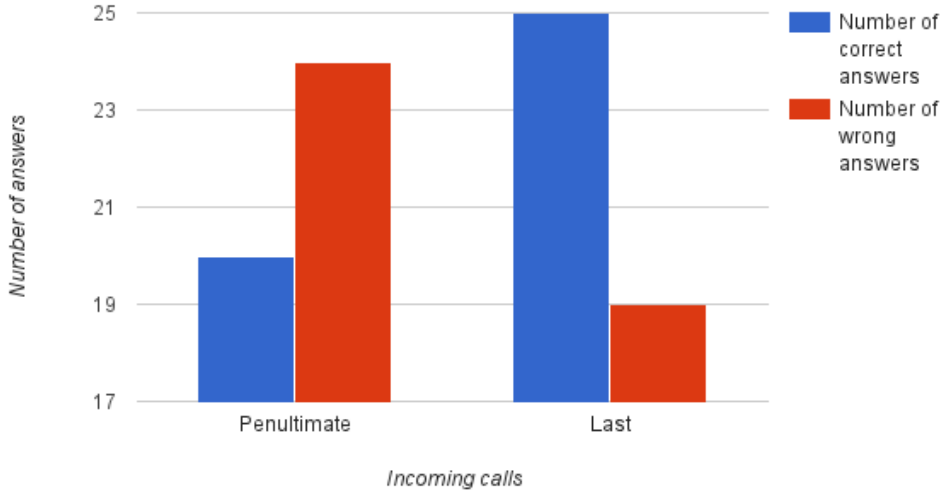

Figure A.16: Column chart showing the number of correct and incorrect answers to questions regarding the *duration* of the last two incoming *calls*.

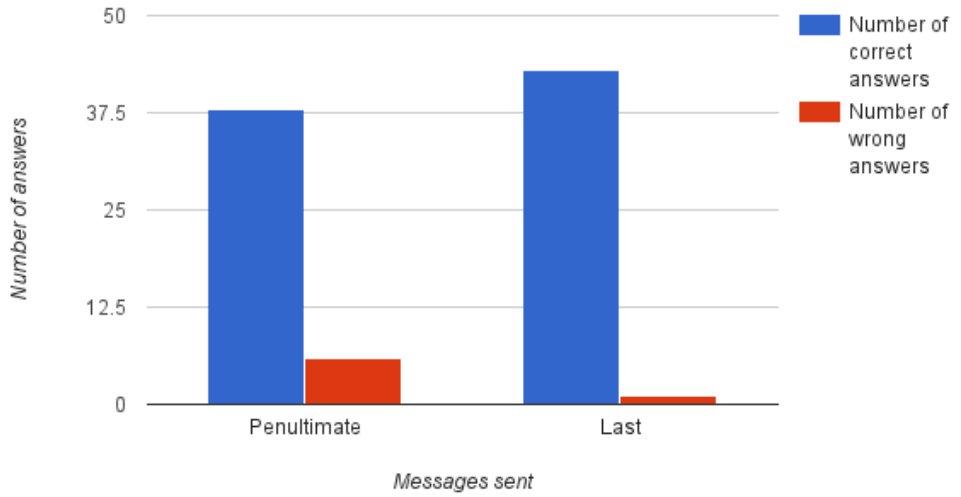

Figure A.17: Column chart showing the number of correct and incorrect answers to questions regarding the last two *messages* sent.

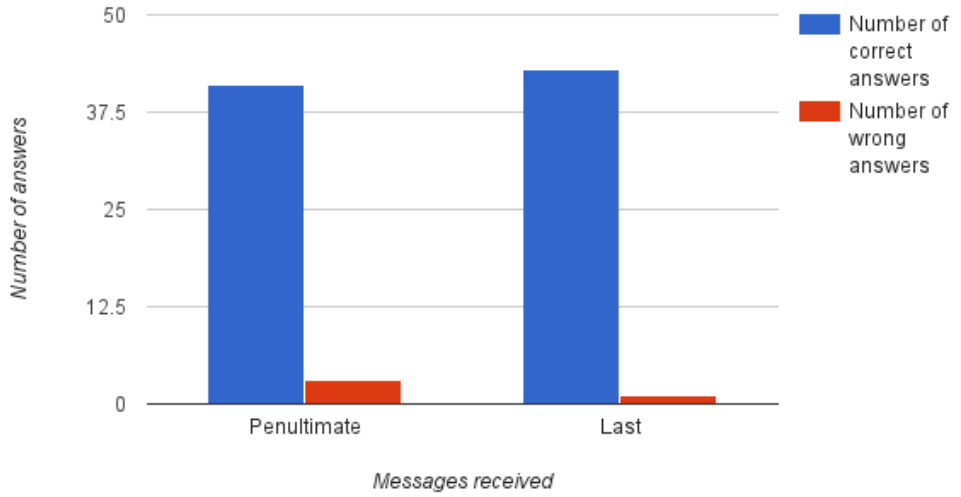

Figure A.18: Column chart showing the number of correct and incorrect answers to questions regarding the last two *messages* received.

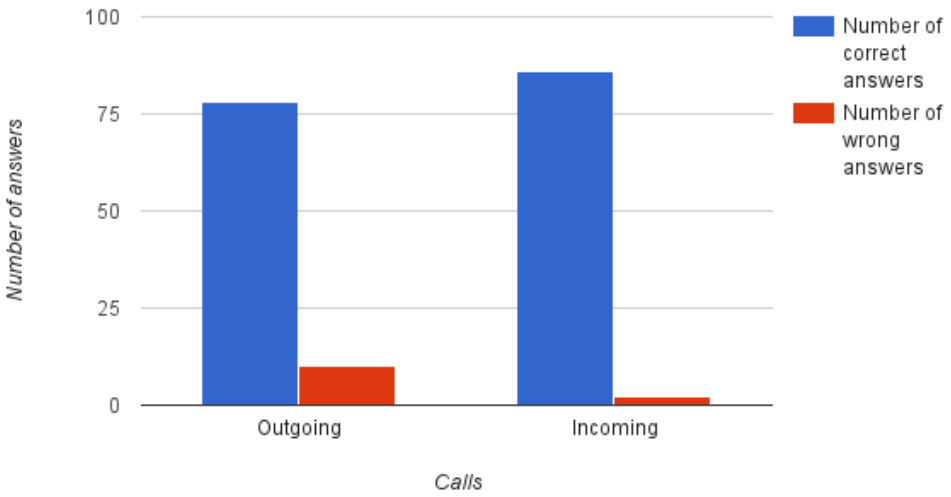

Figure A.19: Column chart comparing results for outgoing and incoming *calls* in terms of the *name of the contact*.

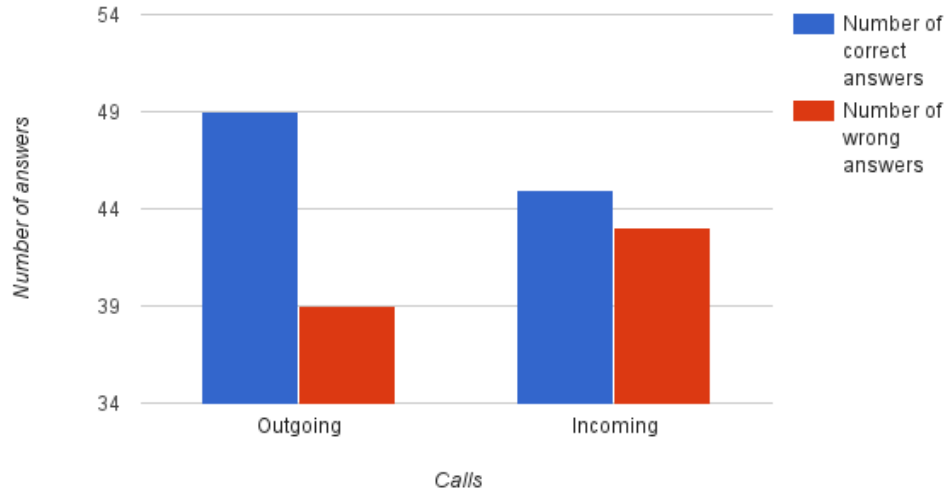

Figure A.20: Column chart comparing results for outgoing and incoming *calls* in terms of *duration*.

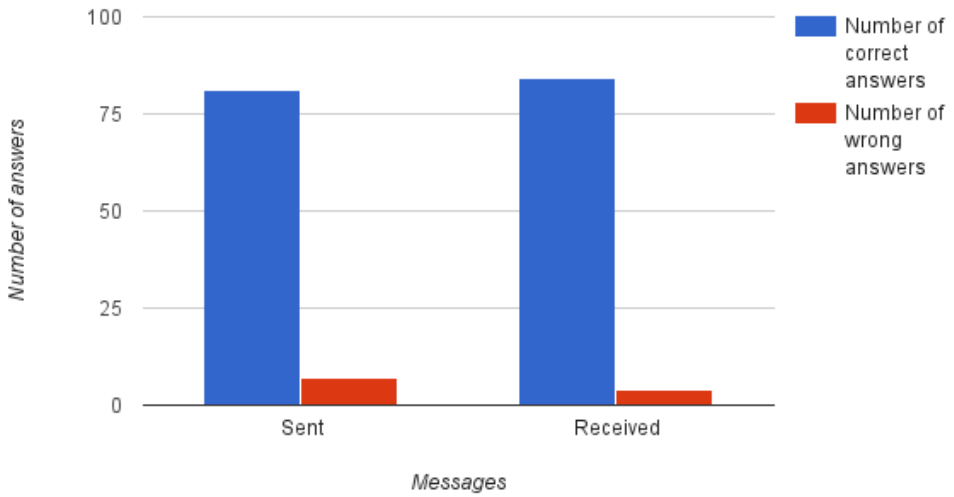

Figure A.21: Column chart comparing results for *messages* sent and received.

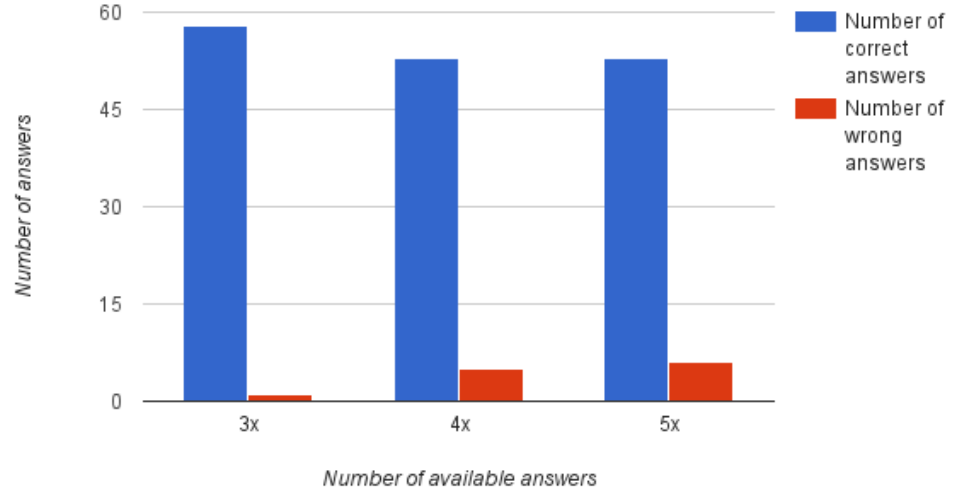

Figure A.22: Column chart with the number of correct and incorrect answers to the questions regarding the *name* associated with a *call*, segregated by the number of available options.

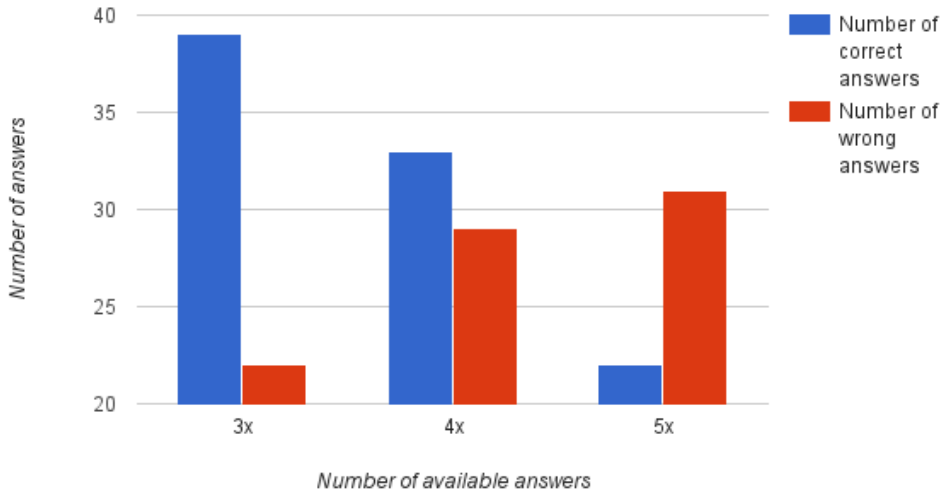

Figure A.23: Column chart with the number of correct and incorrect answers to the questions regarding the *duration* of *calls*, segregated by the number of available options.

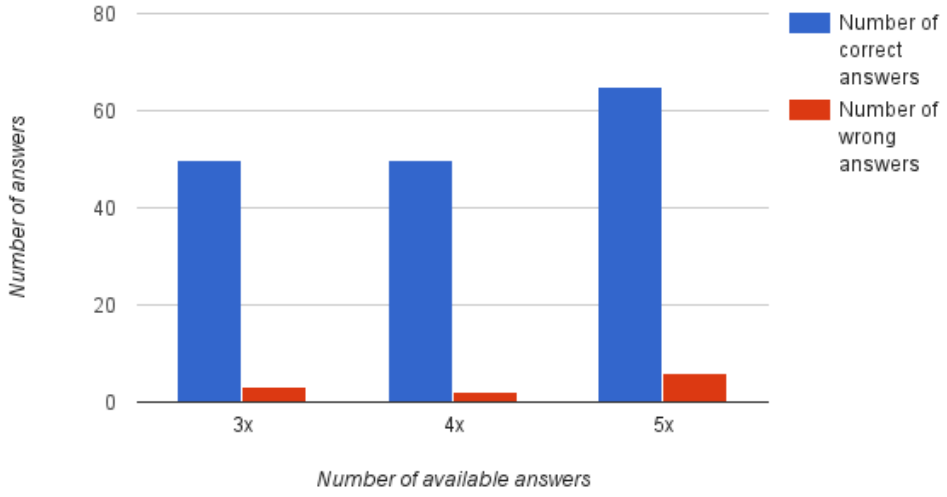

Figure A.24: Column chart with the number of correct and incorrect answers to the questions concerning *messages*, segregated by the number of available options.

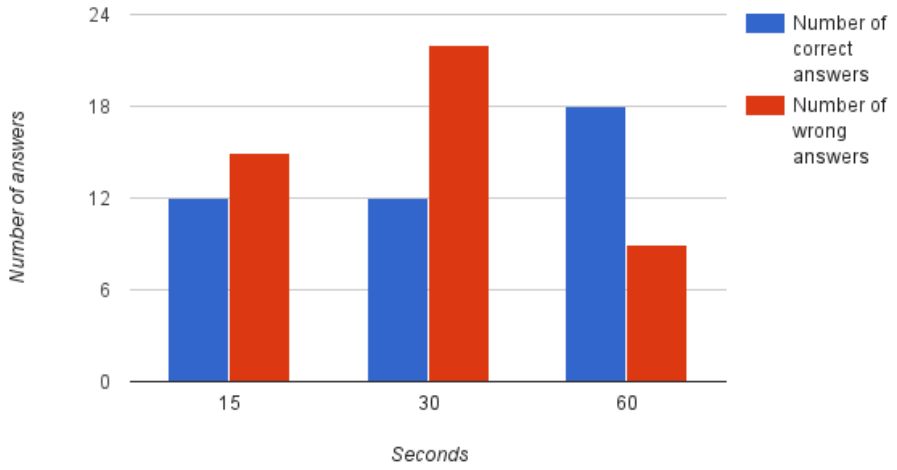

Figure A.25: Column chart comparing the number of correct and incorrect answers to questions related with the *duration* of the penultimate *call*, segregated by the several considered minimum intervals between duration provided in the options.

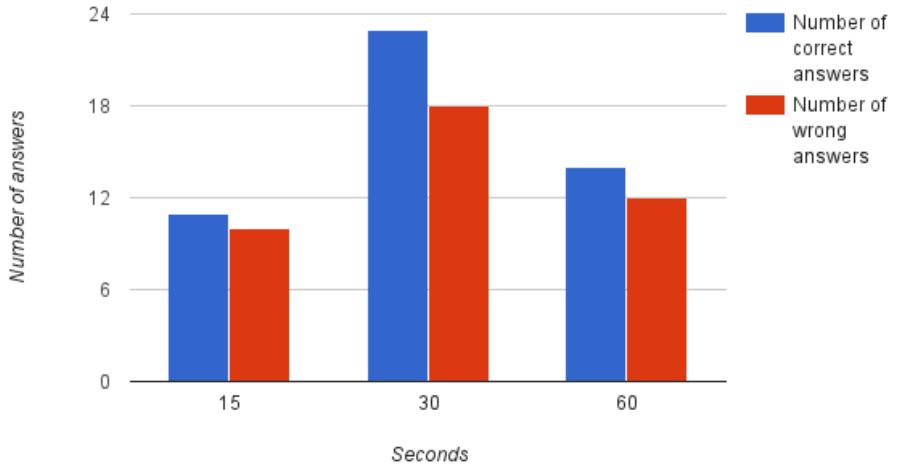

Figure A.26: Column chart comparing the number of correct and incorrect answers to questions related with the *duration* of the last *call*, segregated by the several considered minimum intervals between duration provided in the options.

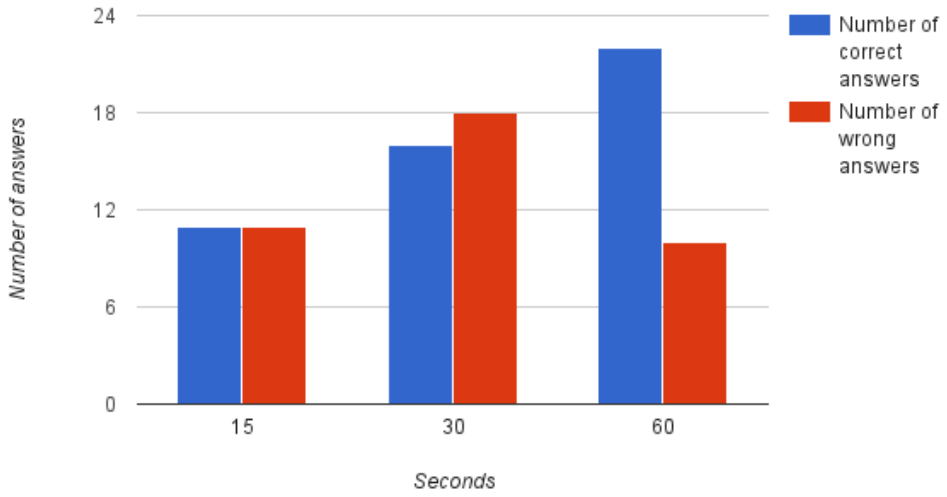

Figure A.27: Column chart comparing the number of correct and incorrect answers to questions related with the *duration* of the last two outgoing *calls*, segregated by the several considered minimum intervals between duration provided in the options.

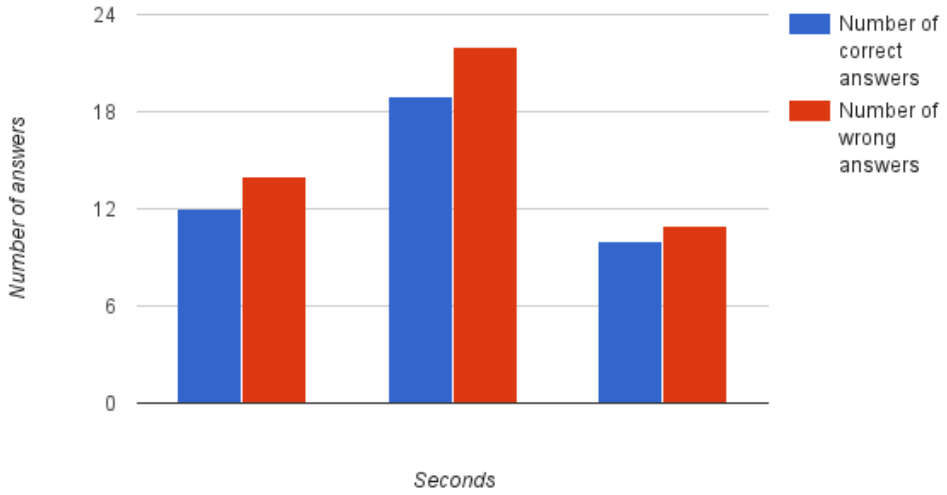

Figure A.28: Column chart comparing the number of correct and incorrect answers to questions related with the *duration* of the last two incoming *calls*, segregated by the several considered minimum intervals between duration provided in the options.

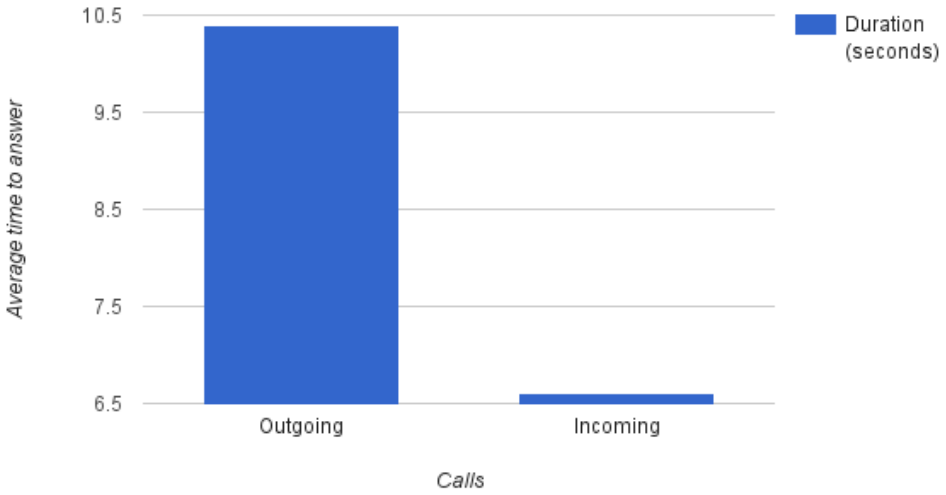

Figure A.29: Column chart with the average time that users took to answer to questions regarding the *name* associated with the last two outgoing and incoming *calls*.

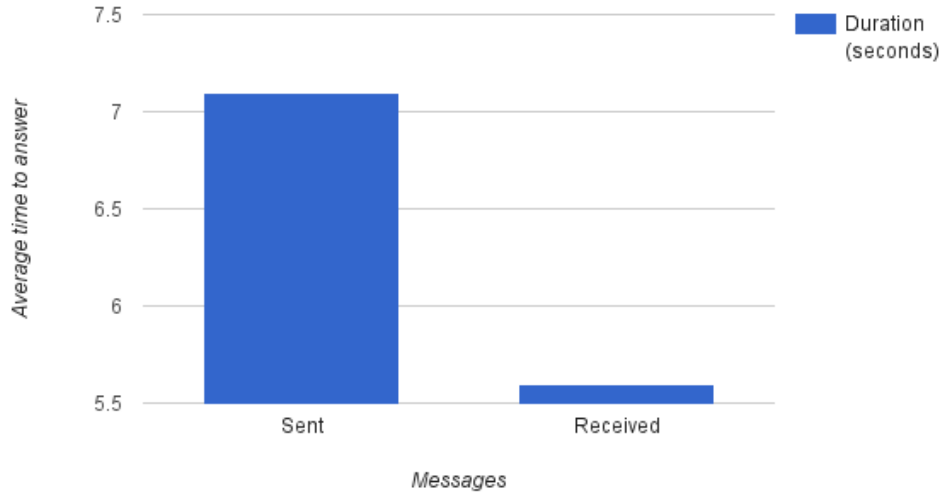

Figure A.30: Column chart with the average time that users took to answer to questions regarding *messages*, either received or sent.

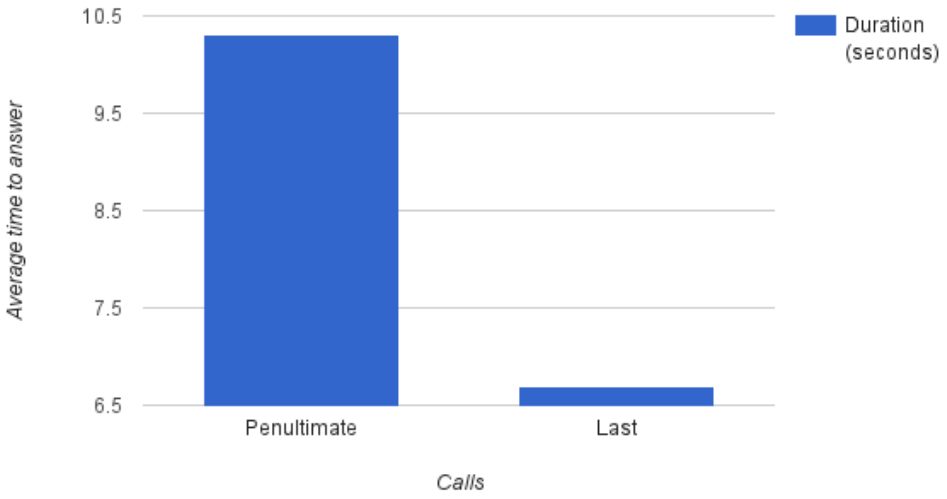

Figure A.31: Column chart with the average time that users took to answer questions regarding the *name* associated with the last two *calls*. This chart presents those times separately for the outgoing and for the incoming calls.

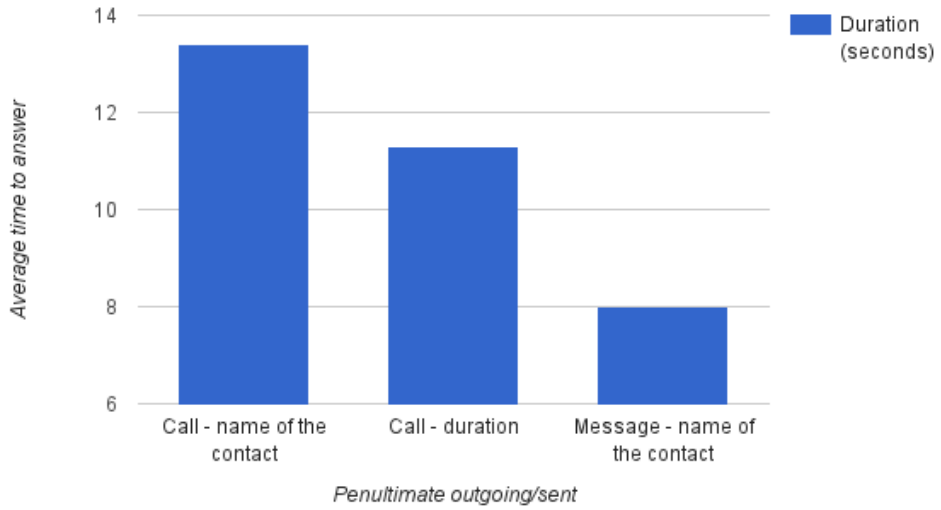

Figure A.32: Column chart with the average time users took to respond to each question of the first group of the usability test.

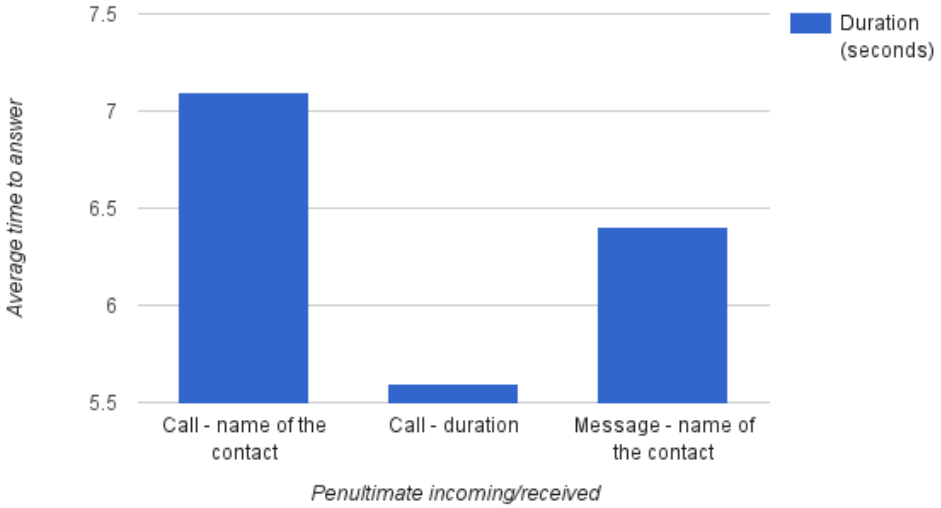

Figure A.33: Column chart with the average time users took to respond to each question of the second group of the usability test.

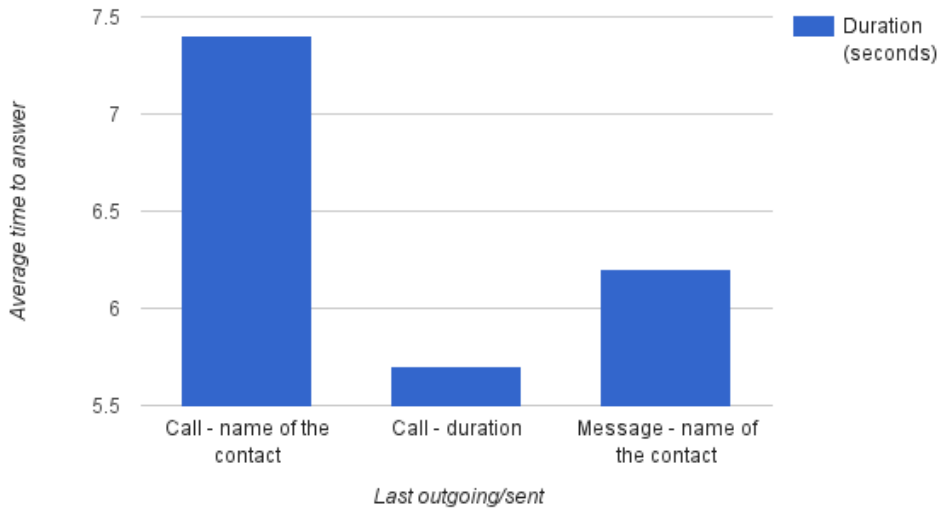

Figure A.34: Column chart with the average time users took to respond to each question of the third group of the usability test.

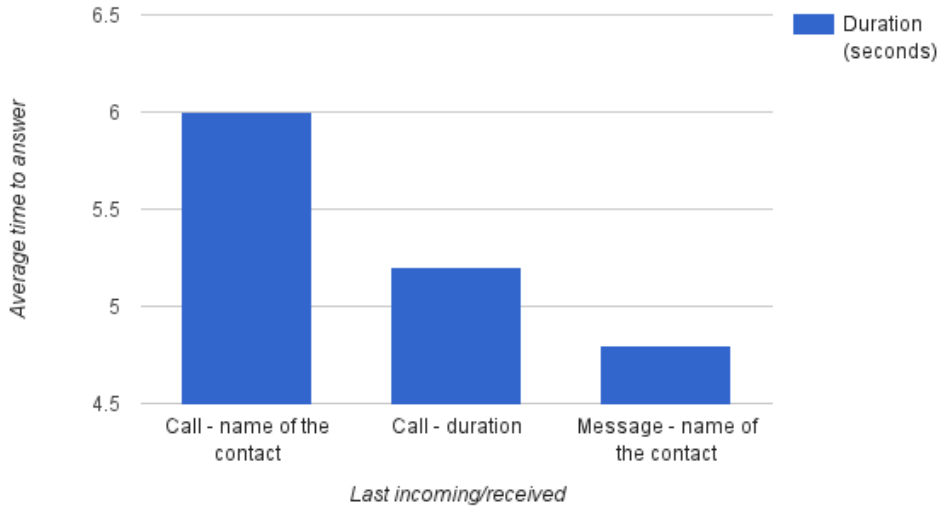

Figure A.35: Column chart with the average time users took to respond to each question of the fourth group of the usability test.

Appendix B

Results of the Usability Test

This appendix contains part of the charts that were obtained during the analysis of the answers to the user survey, but they concern the usability test part only. Most results were discussed in chapter 4.

B.1 First Group

The charts in this section are associated with the first group of questions of the usability test. The questions are related with the penultimate outgoing call and sent message.

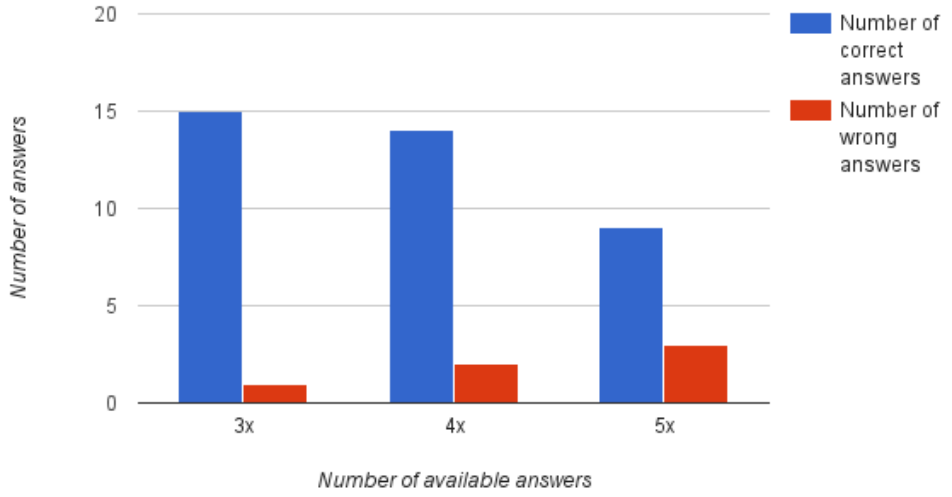

Figure B.1: Column chart for the results obtained for when the prototype was asking for the name of the contact of the penultimate outgoing call. Results are divided by the number of available options.

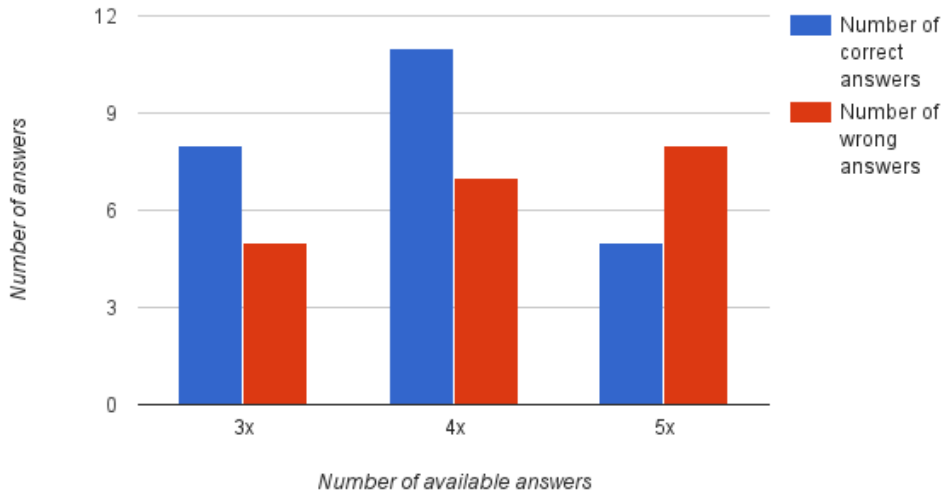

Figure B.2: Column chart for the results obtained for when the prototype was asking for the duration of the penultimate outgoing call. Results are divided by the number of available options.

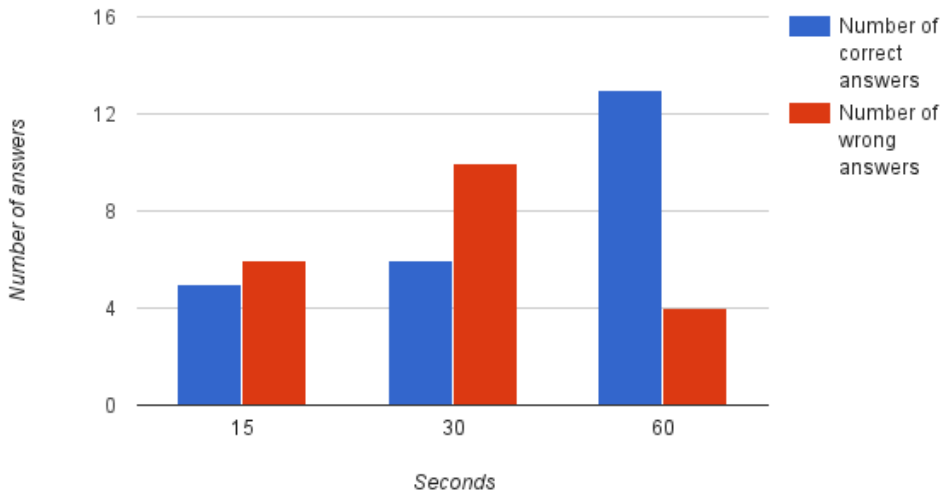

Figure B.3: Column chart for the results obtained for when the prototype was asking for the duration of the penultimate outgoing call. Results are ploted against the minimum value separating the available options.

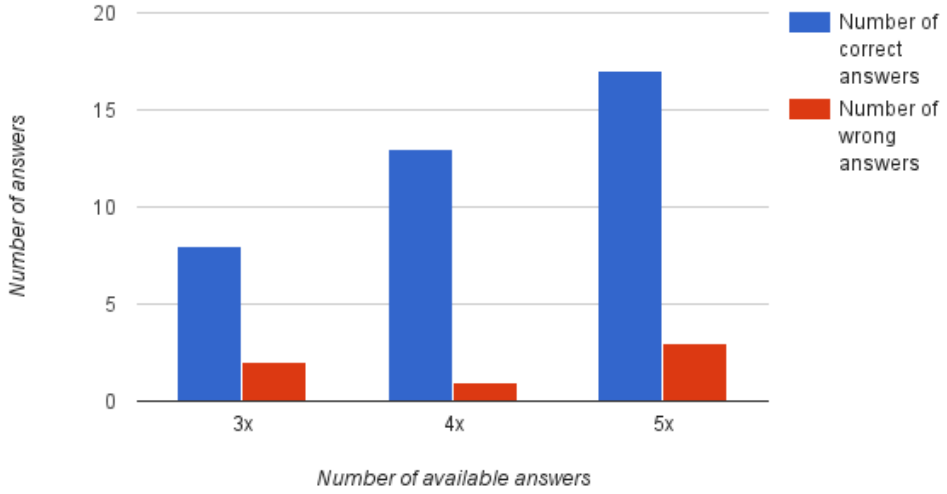

Figure B.4: Column chart for the results obtained for when the prototype was asking for the name of the contact to which the penultimate message was sent. Results are divided by the number of available options.

B.2 Second Group

The following charts are associated with the second group of questions of the usability test. The questions are related with the penultimate incoming call and received message.

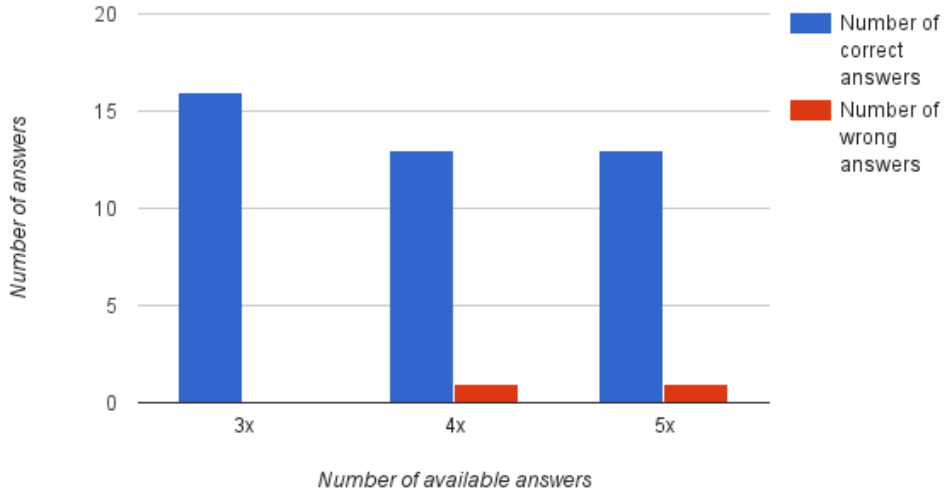

Figure B.5: Column chart for the results obtained for when the prototype was asking for the name of the contact of the penultimate incoming call. Results are divided by the number of available options.

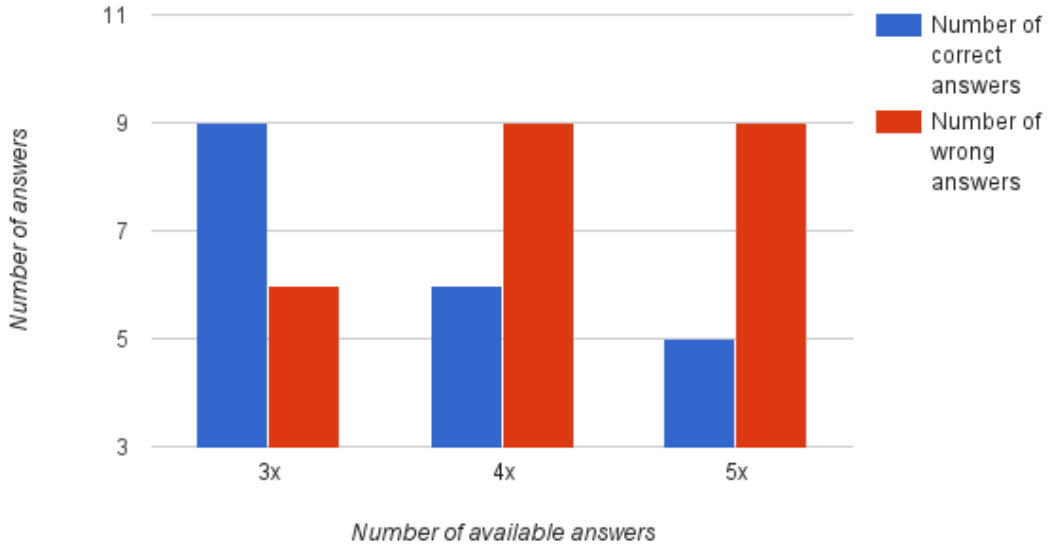

Figure B.6: Column chart for the results obtained for when the prototype was asking for the duration of the penultimate incoming call. Results are divided by the number of available options.

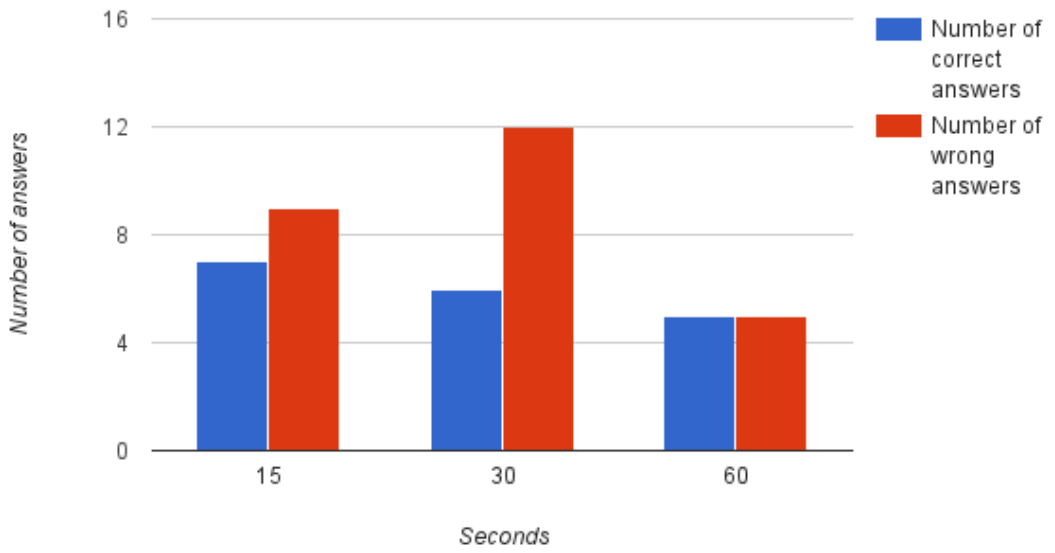

Figure B.7: Column chart for the results obtained for when the prototype was asking for the duration of the penultimate incoming call. Results are ploted against the minimum value separating the available options.

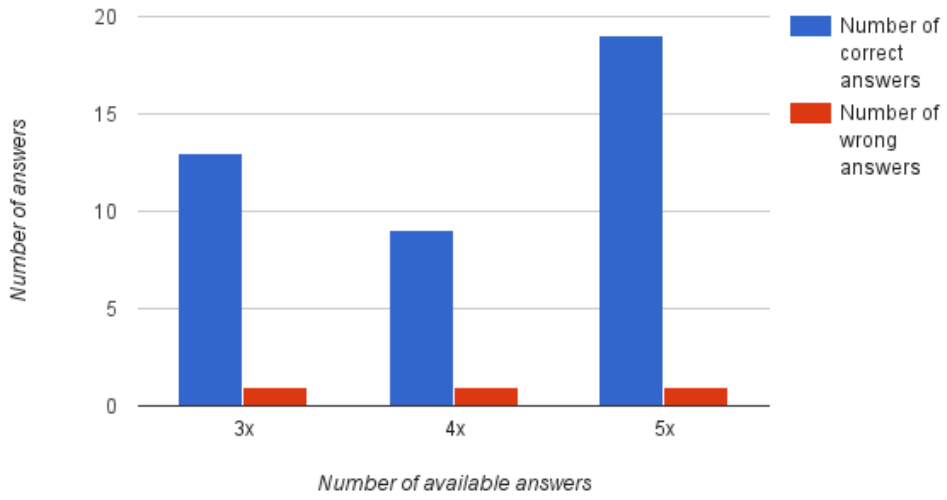

Figure B.8: Column chart for the results obtained for when the prototype was asking for the name of the contact from which the penultimate message was received. Results are divided by the number of available options.

B.3 Third Group

The following charts are associated with the third group of questions of the usability test. The questions concern the last outgoing call and message that was sent.

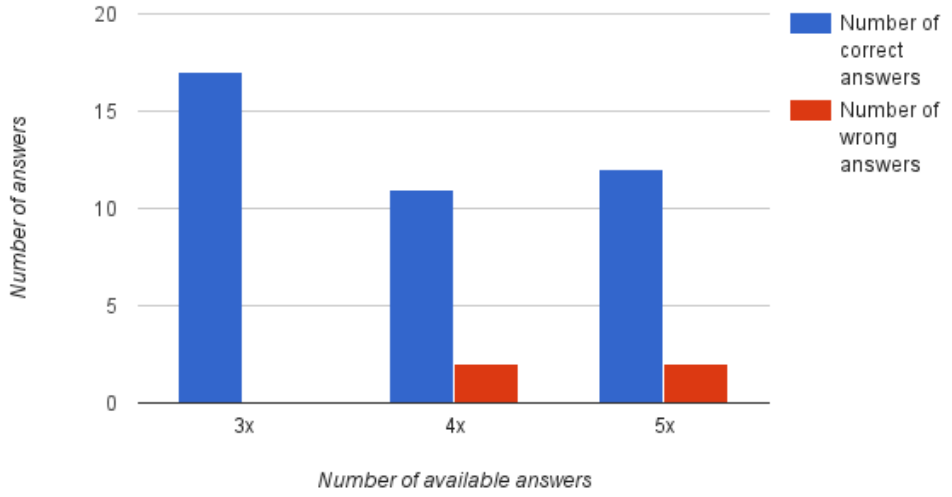

Figure B.9: Column chart for the results obtained for when the prototype was asking for the name of the contact of the last outgoing call. Results are divided by the number of available options.

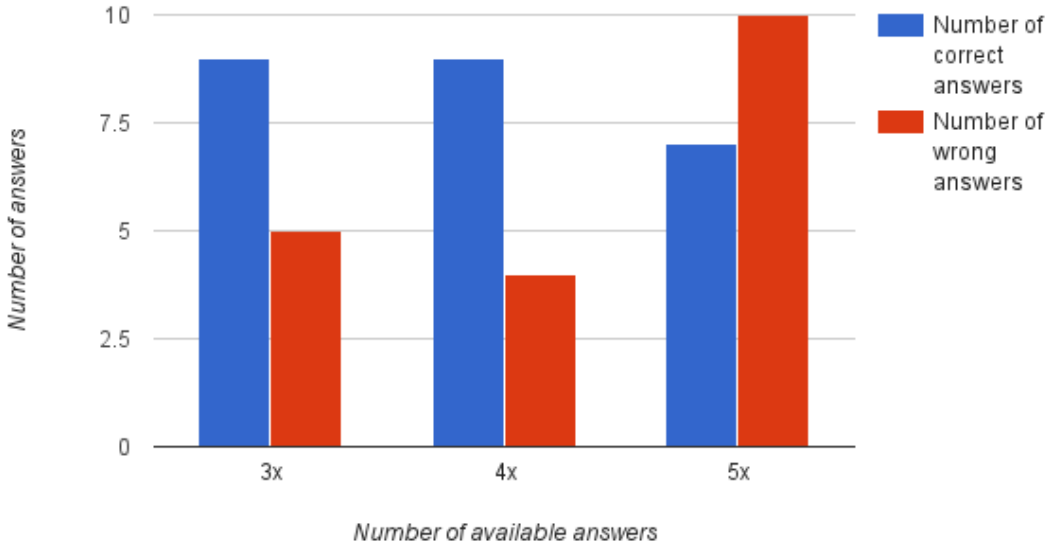

Figure B.10: Column chart for the results obtained for when the prototype was asking for the duration of the last outgoing call. Results are divided by the number of available options.

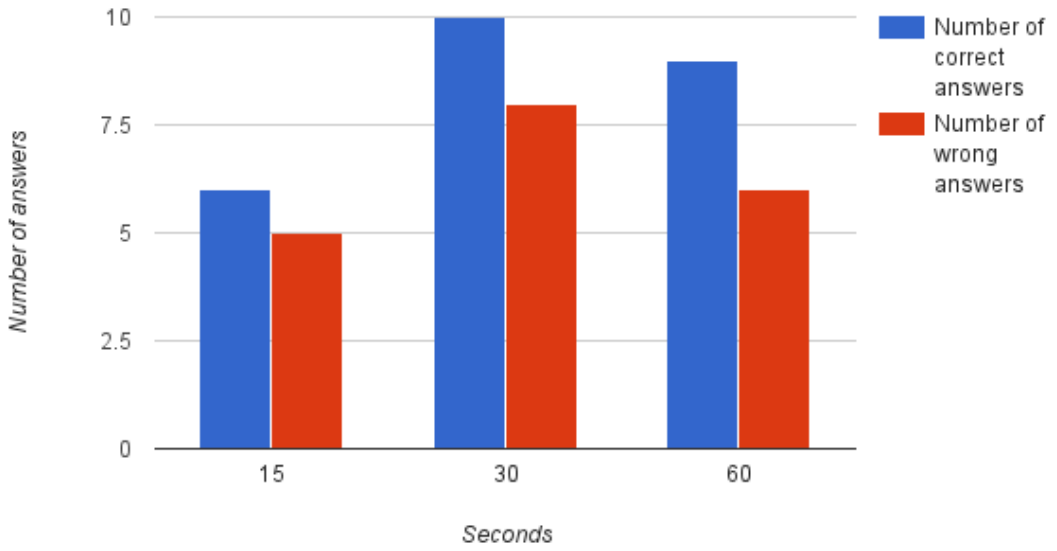

Figure B.11: Column chart for the results obtained for when the prototype was asking for the duration of the last outgoing call. Results are ploted against the minimum value separating the available options.

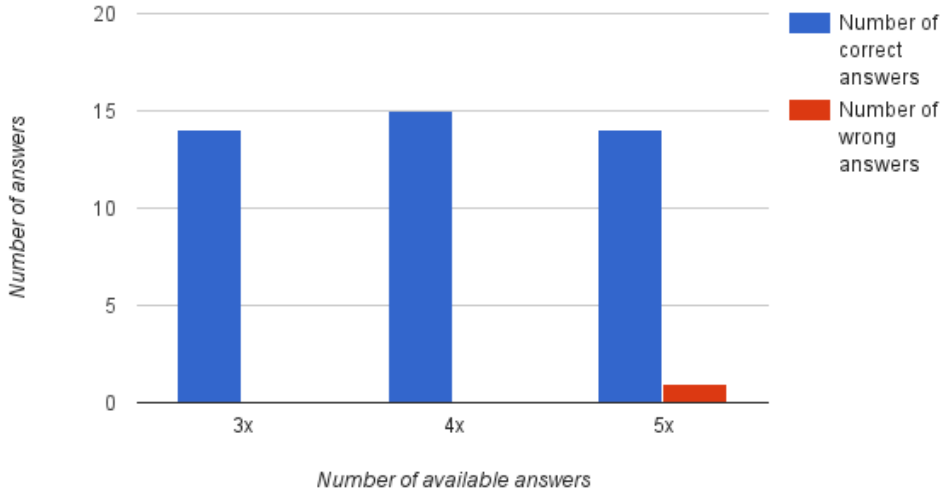

Figure B.12: Column chart for the results obtained for when the prototype was asking for the name of the contact to which the last message was sent. Results are divided by the number of available options.

B.4 Fourth Group

The following charts are associated with the fourth group of questions of the usability test. The questions are related with the last incoming call and received message.

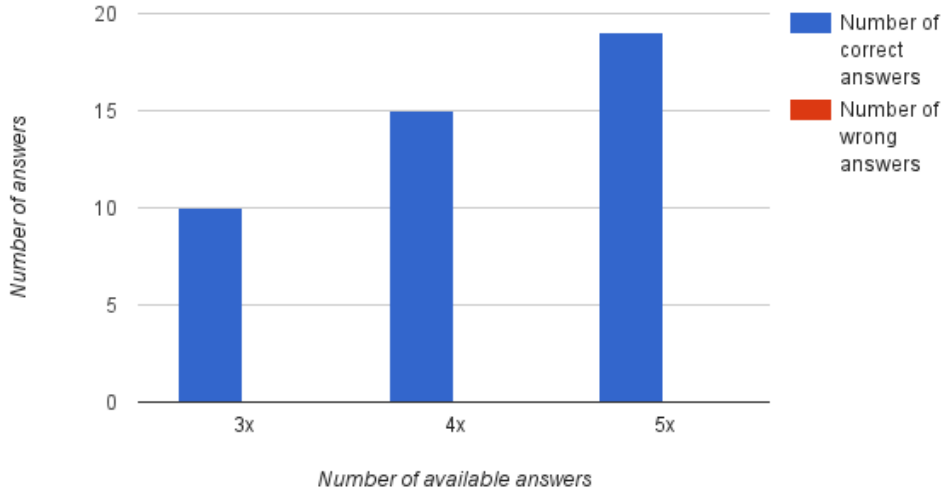

Figure B.13: Column chart for the results obtained for when the prototype was asking for the name of the contact of the last incoming call. Results are divided by the number of available options.

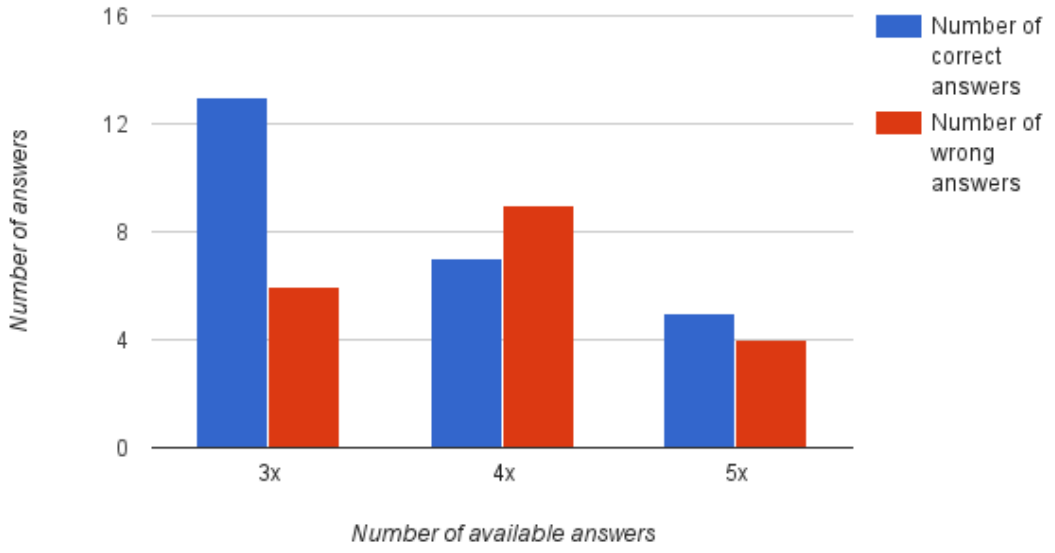

Figure B.14: Column chart for the results obtained for when the prototype was asking for the duration of the last incoming call. Results are divided by the number of available options.

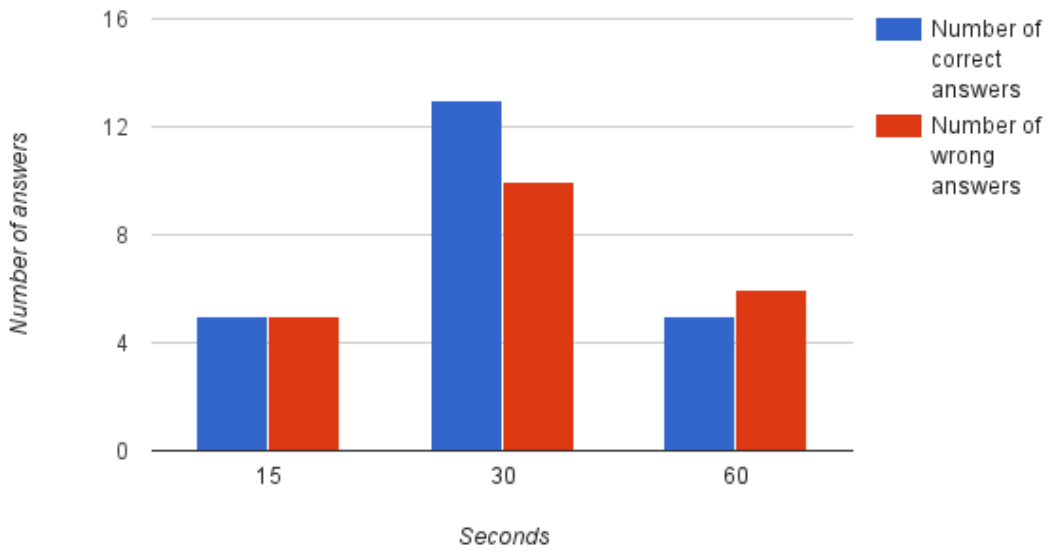

Figure B.15: Column chart for the results obtained for when the prototype was asking for the duration of the last incoming call. Results are ploted against the minimum value separating the available options.

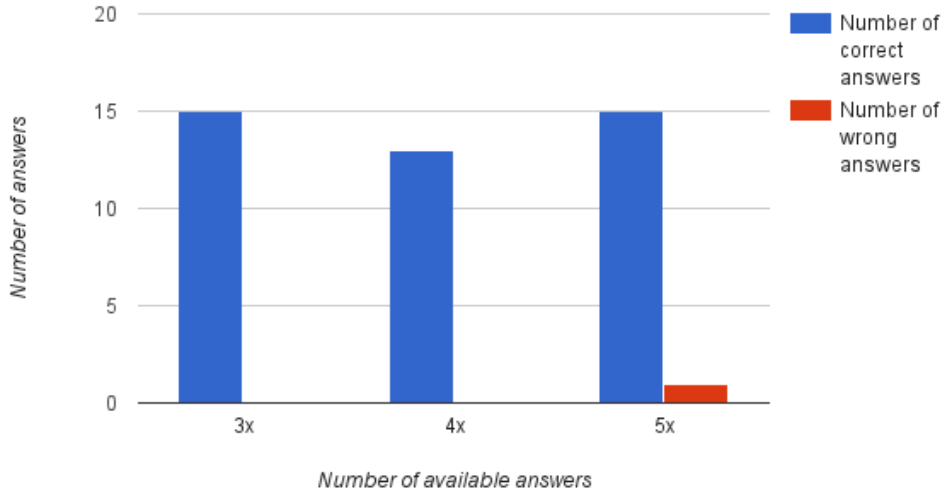

Figure B.16: Column chart for the results obtained for when the prototype was asking for the name of the contact from which the last message was received. Results are divided by the number of available options.