SEGURANÇA E PRIVACIDADE EM SERVIÇOS MÓVEIS: UMA REVISÃO SISTEMÁTICA.

LUCIANO GONÇALVES DE CARVALHO [1]
MARIÂNGELA FERREIRA FUENTES MOLINA [2]

RESUMO

A utilização de dispositivos móveis, tais como *tablets* e smartphones vem aumentando a cada ano, seja para uso pessoal ou profissional. Seja pela escassez de recursos computacionais ou pela necessidade de acesso a recursos remotos, as aplicações instaladas nesses dispositivos precisam fazer uso de serviços móveis para atender às necessidades dos usuários, evidenciando a necessidade de suporte de uma gama de tecnologias de rede. Devido a esse cenário de alta conectividade e necessidade constante de transferência e armazenamento de dados, surgem diversas ameaças à segurança e privacidade, que exploram vulnerabilidades presentes nesse ambiente. Para que seja possível proteger o ambiente dessas ameaças é necessário conhecer as principais contramedidas de segurança adotadas. O presente artigo tem por objetivo apresentar tais contramedidas por meio da execução de uma revisão sistemática, que pode ser reproduzida e auditada por outros pesquisadores. Os resultados indicaram a preocupação com aspectos relacionados à privacidade, autenticação e disseminação de *malwares*, além de reforçar a ideia de agregação de soluções para aumento da segurança.

Palavras chave: Segurança; Privacidade; Vulnerabilidade; Serviços Móveis.

ABSTRACT

The personal and professional use of mobile devices such as tablets and smartphones is increasing every year because of due to the lack of computing resources or the need to access remote resources, the applications installed on these devices need to make use of mobile services to meet users' needs, evidencing the need to support a range of network technologies. Due to this scenario of high connectivity and frequent need for data transfer and storage, several security and privacy threats emerge to exploit vulnerabilities in this environment. To be able to protect the environment from these threats it is necessary to know the main security countermeasures adopted. The purpose of this paper is to show such countermeasures through the execution of a systematic review, which can be reproduced and audited by other researchers. The results indicated the concern with aspects related to privacy, authentication and dissemination of malwares, as well as reinforcing the idea of aggregating solutions to increase security.

Key Words: Security; Privacy; Vulnerability; Mobile Services.

[1]Docente Mestre, Faculdade de Tecnologia de Mogi das Cruzes - Mogi das Cruzes-SP. luciano.carvalho@fatec.sp.gov.br
[2]Docente Especialista, Faculdade de Tecnologia de Mogi das Cruzes - Mogi das Cruzes-SP.

INTRODUÇÃO

Com a crescente utilização de dispositivos móveis, tais como tablets e smartphones, seja para uso pessoal, normalmente relacionado à necessidade de navegação na Internet, acesso a redes sociais e compras on-line, ou profissional, principalmente como extensão do ambiente de trabalho formal ou mesmo como aumento da capacidade de trabalho nesse mesmo ambiente, que é reforçado pela política de Bring Your Own Device (BYOD) adotada por várias organizações, tem-se também um crescente aumento da necessidade de conexão de rede, nas suas mais diversas tecnologias, que dê suporte a essas necessidades. Redes de telefonia celular, redes Wi-fi e Wi-Max, *bluetooth* e infravermelho são exemplos de tecnologias que propiciam conectividade aos dispositivos móveis.

As aplicações instaladas nos dispositivos móveis, cujos recursos de processamento, memória e energia são escassos, costumam fazer uso de serviços móveis, que são um tipo de *web service* disponibilizado por servidores de grande porte, acessados por meio das redes de comunicação de dados. Como grande parte desses serviços são disponibilizados para um grande número de usuários, localizados em diversos pontos do planeta, a Internet é o meio de acesso mais utilizado para esse fim.

A associação do uso da Internet, para a disponibilização dos serviços móveis, da necessidade de uso de várias tecnologias de rede, para propiciar a conexão remota a esses serviços pelos dispositivos móveis, e o baixo poder computacional destes, torna o ambiente favorável a problemas relacionados à segurança e privacidade dos dados, já que, isoladamente, cada elemento possui seu próprio conjunto de problemas. É importante salientar, como divulgado pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que o número de problemas relacionados à segurança tende a aumentar com o tempo, fruto da melhor compreensão das tecnologias utilizadas e

suas respectivas vulnerabilidades, cuja exploração incorre em um incidente de segurança.

Como a compreensão das ameaças que exploram as vulnerabilidades apresentadas pelas tecnologias é importante para entender os tipos de contramedidas de segurança adotadas (KUMAR e RAJALAKSHMI, 2013) (KHANDELWAL e MOHAPATRA, 2015), bem como os desafios das soluções de segurança de curto e longo prazos (SAVOLA, 2009) que deverão ser desenvolvidas para novas aplicações, como por exemplo em computação para brinquedos (toy computing), faz-se necessário a realização de um estudo estruturado que permita reunir todas as ameaças atualmente documentadas e as respectivas contramedidas adotadas para evita-las, embasando adequadamente as novas propostas de contramedidas de segurança.

Este artigo objetiva apresentar e discutir o resultado de uma revisão sistemática sobre o estado da arte das contramedidas de segurança adotadas no contexto de serviços móveis, cuja forma de execução, pautada em um protocolo que define claramente as etapas de trabalho, permite que o processo seja auditado e reproduzido por outros pesquisadores. Para isso, foram analisados artigos que tratam de vulnerabilidades, ameaças e contramedidas de segurança em ambiente móvel e mais especificamente em serviços móveis disponíveis nesses ambientes.

Jana e Bandyopadhyay (2014) apresentaram uma pesquisa que reúne as principais questões de segurança e privacidade em ambiente móvel, cujo foco era no desenvolvimento de aplicações em nuvem em conformidade com o Payment Card Industry Data Security Standard (PCI DSS) e Health Insurance Portability and Accountability Act (HIPAA). Esta pesquisa se diferencia do presente trabalho por não apresentar a metodologia utilizada na pesquisa, impossibilitando sua reprodução, e por estar associada especificamente ao ambiente em nuvem, que requer uma análise mais ampla.

MATERIAIS E MÉTODOS

Para a execução desta pesquisa foi empregado um processo de revisão sistemática, cujas fases são:

1. Fase de Planejamento: estabelecimento de um protocolo para guiar a pesquisa de artigos, que teve como ponto de partida uma pesquisa exploratória para determinar a principal questão de pesquisa (“Quais as vulnerabilidades de serviços móveis, os requisitos de segurança da informação e as contramedidas que são atualmente aplicadas?”) e as palavras chaves (“mobile services”, “privacy”, “security” e “vulnerability”) empregadas no mecanismo de busca da base de dados pesquisada (IEEE Xplore), e onde foi determinado todos os critérios de inclusão e exclusão de artigos;
2. Fase de Condução: construção da string busca (“(((mobile service) AND vulnerability) AND (security OR privacy))”), execução da busca e consequente seleção de artigos baseada nos critérios de inclusão e exclusão;
3. Fase de Extração de Dados: análise aprofundada dos artigos selecionados, buscando os elementos que respondem à pergunta de pesquisa.

A busca pelos artigos retornou um total de 53 trabalhos, dois quais apenas 24 foram selecionados em virtude dos critérios de inclusão (“segurança em aplicações móveis” e “privacidade em aplicações móveis”) e o restante descartado em virtude dos critérios de exclusão (“aplicações móveis bancárias”, “publicação fora da área de computação”, “especificação de tecnologia”, “aplicações móveis na saúde”, “segurança em redes Wi-Fi”, “segurança em nuvem”, “segurança em redes Wi-Max”, “segurança em protocolos de rede”, “segurança em redes sociais” e “documentos que não sejam artigos”). É importante salientar que nenhum artigo foi rejeitado devido à sua data de publicação.

Após a análise de cada artigo, foi extraído, quando encontrado, as vulnerabilidades, requisitos de segurança e contramedidas de segurança documentadas, possibilitando identificar as principais soluções de segurança

adotadas para revolver os problemas relacionados à segurança e privacidade na utilização de serviços móveis, apresentadas na seção seguinte.

RESULTADOS

Com o intuito de compreender melhor as soluções de segurança identificadas, que são justamente as contramedidas adotadas para resolver os problemas, precisou-se extrair também dos artigos que fizeram parte da revisão sistemática as vulnerabilidades, que são exploradas pelas ameaças, e os requisitos de segurança que se deseja manter. Portanto, a contramedida de segurança é o principal elemento considerado para o resultado do trabalho, enquanto as vulnerabilidades e os requisitos de segurança são considerados elementos secundários.

Os Quadros 1, 2 e 3 apresentam um breve resumo dos 24 artigos analisados, incluindo os elementos que foram objeto da fase de extração de dados. Cada artigo foi agrupado em uma categoria conforme a contramedida de segurança adotada, descritas nas subseções a seguir.

Protocolo de Segurança

Os elementos essenciais para que haja comunicação em rede são os sistemas de origem e destino, o meio físico e protocolos de comunicação. Estes têm como função estabelecer as regras de comunicação e propiciar a troca efetiva e eficiente de dados, portanto, sendo desenvolvidos com foco nessas questões e deixando de lado outras questões importantes, como por exemplo a segurança e privacidade. A partir dessa constatação é natural que protocolos seguros sejam desenvolvidos ou protocolos considerados inseguros sejam aprimorados de forma a contemplar aspectos de segurança.

QUADRO 1 - Resumo dos Artigos Analisados.

Artigo	Vulnerabilidades	Requisitos de Segurança	Contramedidas de Segurança
Kumar e Rajalakshi, 2013	Wi-Fi and device tethering (esquema de criptografia fraco) Senhas fracas Procedimentos de controle de qualidade pobres na produção de mídias removíveis (pré-infectadas) Conectividade de rede fornecida pelos dispositivos móveis Aplicações antigas (permitir aplicações não assinadas)	Não informado	Software antivírus Software AntiSpam Filtros de Conteúdo e Gateway Malware Software de Criptografia Patching e monitoramento de vulnerabilidades Controle de dispositivo e rede Prevenção de perda de dados (Data Loss Prevention - DLP) Bloqueio de dispositivo Evitar apps questionáveis Aceitar patches de correção Efetuar backup de dados Evitar comportamento promiscuo
Tzonelih e Gope, 2013	Não garantia para VLRs comprometidos Envio de mensagem de ressincronização em texto plano	Privacidade Anonimato Proteção da identidade do assinante	Esquema de autenticação e acordo de chaves usando criptossistema simétrico
Zhijie et al., 2014	Ponto único de falha Honest But Curious (HBC) Personificação Vazamento de privacidade (dados do histórico do usuário) Redirecionamento de página web	Gerenciamento cuidadoso de identidades móveis	Controle de Acesso Criptografia
Tao et al., 2012	Facilidade em se roubar dispositivos móveis	Autenticação de usuários	Autenticação biométrica (impressão digital-implementação em hardware)
Brassil e Manadhata, 2012	Localização baseada na declaração do usuário	Identificação correta de localização	Autenticação de localização de dispositivo móvel por meio de femtocell
Le et al., 2008	Impossibilidade de se estabelecer permissões relacionadas a atividades dos usuários	Garantia da preservação de privacidade Estabelecimento correto de permissões de usuário	Protocolo de autenticação Controle de acesso baseado em atividade Autenticação baseada em imagem
Aryan e Singh, 2010	Não informado	Privacidade de localização	k-anonymization pessoal método pseudo-anonymization
Caimu e Wu, 2008	Rastreamento de localização	Privacidade	Anonymity key
Bellovin et al., 2013	Natureza inexata do desenvolvimento de software	CALEA (referente à lei)	criptografia

QUADRO 2 - Resumo dos Artigos Analisados (continuação).

Artigo	Vulnerabilidades	Requisitos de Segurança	Contramedidas de Segurança
Al-Rabiaah e Al-Muhtadi, 2012	Fornecimento de informações privadas e sensíveis (identificação e localização do usuário) Mecanismos de segurança tradicionais não são suficientes	Controle de acesso a serviços Autenticação baseada em informações do contexto	Autenticação de sensores Entrega de informação de contexto criptografada
Deshmukh e Potey, 2013	Controle de acesso all-or-nothing para dispositivos	Garantir privacidade e segurança no acesso a arquivos	Propiciar a designação de senhas por arquivos de usuário Criptografia de dados pessoais
Savola, 2009	Uso compartilhado de dispositivo Exposição a várias redes Utilização de redes sem fio	Segurança Privacidade Dependabilidade Confiança	Proteção física Segurança de Plataforma Controle de acesso Proteção de armazenamento Proteção de conexões
Zhigang et al., 2013	Atualização constante de localização Confiança em um terceiro para prover anonimato Ponto único de falha	Privacidade	Software LISA
Luyi et al., 2014	Ausência de patch Permition Harvesting Preempting Discrepancia em nomes de pacotes	Sistemas Atualizados	Aplicação de patches
Gedik e Ling, 2008	Brechas na privacidade da localização	Privacidade da localização	Abordagem baseada em política Abordagem baseada em anonimato Algoritmos de perturbação de localização
Jana e Bbandyopadhyay, 2014	Possibilidade de criação de VMs de acordo com a capacidade requerida pelo usuário Facilidade em perder o dispositivo Entrada de dados a partir de fontes inseguras Usuários sem consciência da importância das informações Validação fraca de dados de entrada Chaves criptográficas fracas APIs mal projetadas Compartilhamento de recursos físicos Falta de isolamento adequado entre VMs	Privacidade na troca de informações entre múltiplas partes	Criptografia Isolamento Gerenciamento de Acesso e Identidade Autenticação de dois fatores Serviço de Autenticação (Kerberos) Protocolo de Autenticação (Open ID) Assinatura Digital Security Gateways Tokenization de dados sensíveis
Hsiu-Sem e Tsaur, 2010	Baixa capacidade de armazenamento Baixa capacidade de processamento Eficiência energética Disseminação rápida de malware (por meio de interfaces bluetooth)	Não informado	Anti-vírus Firewall Criptografia Anti-malware Utilização de análise de comportamento baseado em ontologia para mobile malware

QUADRO 3 - Resumo dos Artigos Analisados (continuação).

Artigo	Vulnerabilidades	Requisitos de Segurança	Contramedidas de Segurança
Ghallali e Ouahidi, 2012	Facilidade de comunicação por meio de interfaces sem fio	Evitar disseminação de malwares	Assinatura Digital Análise de consumo de energia Gimpy CAPTCHA Monitores bluetooth
Dey et al., 2013	Acesso a recurso de localização comum Funcionários descuidados ou não confiáveis	Privacidade das informações do usuário Privacidade das informações transmitidas	Políticas de projeto e uso Funcionários confiáveis Software proprietário para virtualização Segurança física de servidores Esquema Seguro de Autenticação (MDA - Message Digest Protocolos de roteamento baseados em posição (criptografia de chave pública, hashing e assinatura digital) Authentication)
Xiaoxin e Nita-Rotaru, 2005	Broadcast de requisições de roteamento por toda rede	Evitar consumo de banda excessivo	Protocolos de roteamento baseados em posição (criptografia de chave pública, hashing e assinatura digital)
Choudhury et al., 2012	Transferência da identidade do usuário em texto plano	Privacidade da identidade do usuário	Conjunto elaborado de chaves para criptografia Protocolo de autenticação e acordo de chaves
Aryan e Singh, 2010	Não informado	Privacidade de Localização Privacidade da Identidade do Usuário	"Anonimizar" a localização do usuário Abordagem baseada em políticas Abordagem baseada em k-anonymity Pseudo-anonymity False dummies Landmark objects
Gelenbe et al., 2013	Uso de múltiplas tecnologias de comunicação Instalação e execução de software oriundos de fontes desconhecidas ou não oficiais Usuários desavisados	Não informado	Virtualização Infraestrutura de coleta de dados Honeypot
Khandelwal e Mohapatra, 2015	Qualquer desenvolvedor pode criar uma aplicação Android e disponibilizá-la no Android Public Market As aplicações para Android são auto assinadas e não há verificação sobre sua segurança Sandbox customizável pelo usuário no Android	Comunicação apenas com sites confiáveis Separação para aplicações (Sandbox) Somente permissões necessárias Limitação de acesso a informações	Separação de Privilégios Tipos diferentes de permissão Assinatura do código da aplicação Antimalware Firewall IDS/IPS Controle de acesso Linux Controle de acesso de permissão do Android Criptografia de dados e chamadas Filtros de Spam Checagem de certificado de aplicação Checagem de integridade Utilização de Locks Gerenciamento remoto

No trabalho de Xiaoxin e Nita-Rotaru (2005) é proposto um método para proteger a informação de posição utilizada pelos protocolos de roteamento baseados em posição, utilizando criptografia de chave pública, hashing e assinatura digital. Já no trabalho de Tzonelih e Gope (2013) é proposto um esquema eficiente de autenticação e acordo de chaves baseado em criptossistema simétrico.

Autenticação

Com o intuito de restringir o acesso a recursos e dados, faz-se necessário implementar soluções de controle de acesso, que se baseiam na identificação da entidade requisitante e sua consequente autorização de acesso. Muitos ataques visam burlar o processo de identificação para que seja possível conseguir acesso menos restrito.

Zhijie et al. (2014) apresentam um framework para controle de acesso móvel distribuído para preservação da privacidade, baseado em criptografia. A criptografia também está presente na solução de Al-Rabiaah e Al-Muhtadi (2012), que prega a autenticação de sensores no ambiente e troca de informação criptografada.

A utilização de hardware adicional para autenticação é proposta por Tao et al. (2012), para que seja possível a utilização de biometria, e por Brassil e Manadhata (2012), com a utilização de femtocell.

De forma a dificultar a automatização de tentativas de identificação, Le et al. (2008) propõem uma autenticação baseada em imagem.

Os trabalhos de Jana e Bandyopadhyay (2014) e Dey at al. (2013) abordam questões e desafios de autenticação em ambiente móvel de nuvem.

Criptografia Pura

Como a criptografia é capaz de preservar diversos requisitos de segurança, como por exemplo confidencialidade, integridade, autenticidade e não-repúdio, ela

costuma ser amplamente empregada em soluções de segurança e muitas vezes como solução única. Isso pode ser observado nos artigos de Deshmukh e Potey (2013), que utilizam criptografia de dados pessoais por meio do algoritmo AES (Advanced Encryption Standard), e de Bellovin et al. (2013), que aborda a dificuldade atual de se grampear as comunicações digitais segundo as leis norte-americanas, entre outros fatores devido à utilização de criptografia de dados.

Anonimato

Caimu e Wu (2008) além de apresentarem as principais questões de privacidade de localização, mostram um esquema que resolve os problemas do 3GPP-AKA (third generation partnership project - authentication and key agreement) que está relacionada ao endereçamento do problema de anonimato.

A crescente preocupação com a privacidade dos dados de localização é tratada nos artigos de Aryan e Singh (2010), que propõem um algoritmo para anonimato de localização, e de Gedik e Ling (2008), apresentam uma arquitetura de segurança baseada em políticas, anonimato de localização e algoritmos de perturbação de localização.

Softwares

Diversos softwares de proteção estão disponíveis no mercado, como por exemplo os anti-*malware*, solução proposta nos trabalhos de Hsiu-Sem e Tsaur (2010) e Khandelwal e Mohapatra (2015). Neste último, ainda há a indicação de uso de sistemas de firewall e sistemas de detecção/prevenção de invasão (IDS/IPS). Softwares antivírus e AntiSpam também são muito utilizados, como pregado no artigo de Kumar e Rajalakshmi (2013) para ambiente móvel em nuvem.

Para eliminar vulnerabilidades específicas, novos softwares podem ser construídos, como no caso dos trabalhos apresentados por Zhigang et al. (2013), com a utilização de um sistema de proteção da privacidade LISA, que

intencionalmente insere um certo nível mensurável de ruído nas localizações fornecidas pelo dispositivo, dificultando a inferência do próximo destino do usuário.

Outras Contramedidas

Como apresentado em Savola (2009), existem diversas tendências e áreas prioritárias de pesquisa para garantia da segurança, confiança e privacidade, além do conceito de dependabilidade (relacionado, entre outros conceitos, com a confiabilidade). Portanto, diversas outras estratégias de proteção podem ser criadas, a partir de novas abordagens ou do agrupamento de soluções já conhecidas.

Ghallali e Ouahidi (2012), que tentam apresentar o estado da arte da segurança contra a disseminação de *malware*, propõem a utilização das soluções de assinatura digital, do sistema para autenticação CAPTCHA e o monitoramento do consumo de energia dos dispositivos, que pode dar indícios de abuso.

Gelenbe et al. (2013) apresentam a abordagem NEMESYS, que faz uso da virtualização e *honeypot*, além da necessidade de uma infraestrutura de coleta de dados.

Por sua vez, Choudhury et al. (2012) discutem uma possível solução para o problema de privacidade de identidade em redes LTE (Long Term Evolution), que utiliza autenticação e controle de chave, fazendo recomendação de alteração no processo atual.

Por fim, no trabalho de Luyi et al. (2014) é enfatizado a necessidade de manter os sistemas atualizados, isto é, aplicando todos os patches de segurança disponibilizados pelo fabricante, analisando os problemas de atualização do sistema operacional Android.

DISCUSSÃO

É possível observar que muitas contramedidas de segurança objetivam resolver problemas relacionados à privacidade, seja dos dados pessoais armazenados nos dispositivos móveis, na transmissão dos dados quando se utiliza serviços móveis ou dos dados relacionados à localização dos usuários, e relacionados a questões de autenticação, visando evitar abusos em virtude da atribuição inadequada de privilégios. Uma parcela menor dos trabalhos se preocupa com a disseminação de *malware*, muito comum em ambientes de alta conectividade com presença de dispositivos com recursos limitados.

Muitas soluções de segurança propostas fazem uso direto ou indireto da criptografia, reforçando sua importância para a área de segurança da informação.

Uma questão importante evidenciada no artigo de Gelenbe et al. (2013) e que não foi tratada pelos demais artigos foi a possibilidade da inserção de novas vulnerabilidades devido à adoção da solução proposta. Essa preocupação é facilmente compreendida quando se pensa em solução de segurança em termos de linhas de código adicional, que, embora resolvam um problema específico, podem ter seus próprios problemas.

CONCLUSÃO

Devido aos requisitos de segurança desejados em ambientes móveis para acesso a serviços móveis e ao enorme número de vulnerabilidades existentes, há a necessidade de se encontrar soluções, isto é, contramedidas de segurança para evitar que as ameaças obtenham sucesso em seus ataques. Não existe uma única solução para o problema de segurança e privacidade dentro do contexto de serviços móveis, evidenciando a necessidade de se construir soluções pontuais para resolver cada um dos problemas encontrados, como por exemplo as questões relacionadas à privacidade de localização, autenticação segura e disseminação de *malware*. Em virtude da recente preocupação de segurança nesse novo contexto

de comunicação, pode-se concluir que ainda será necessária muita pesquisa para encontrar soluções amplas e adequadas para todos os problemas atuais e futuros, reforçando cada vez mais a necessidade de se utilizar um conjunto de soluções em detrimento de uma única solução.

REFERÊNCIAS BIBLIOGRAFIAS

AL-RABIAAH, S.; AL-MUHTADI, J. 2012. **ConSec: Context-Aware Security Framework for Smart Spaces**. Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on, 580 – 584.

ARYAN, A.; SINGH, S. 2010. **Protecting location privacy in Augmented Reality using k-anonymization and pseudo-id**. Computer and Communication Technology (ICCCT), 2010 International Conference on, 119 – 124.

ARYAN, A.; SINGH, S. 2010. **Securing location privacy in Augmented Reality**. Industrial and Information Systems (ICIIS), 2010 International Conference on, 172 – 176.

BELLOVIN, S. M.; BLAZE, M., CLARK, S.; LANDAU, S. 2013. **Going Bright: Wiretapping without Weakening Communications Infrastructure**. Security Privacy, IEEE, 62 – 72.

BRASSIL, J.; MANADHATA, P. K. 2012. **Securing a femtocell-based location servise**. Mobile and Wireless Networking (iCOST), 2012 International Conference on Selected Topics in, 30 – 35.

CAIMU, T. and WU, D. O. 2008. **Mobile Privacy in Wireless Networks-Revisited**. Wireless Communications, IEEE Transactions on, 1035 – 1042.

CHOUDHRY, H.; ROYCHOUDHURY, B.; SAIKIA, D. K. 2012. **Enhancing User Identity Privacy in LTE**. Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 949 – 957.

DESHMUKH, N.; POTEY, M. 2013. **Providing Data Security on Cell Phones**. Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on, 12 – 16.

DEY, S.; SAMPALLI, S.; QIANG Y. 2013. **Message digest as authentication entity for mobile cloud computing**. Performance Computing and Communications Conference (IPCCC), 2013 IEEE 32nd International, 1 – 6.

GEDIK, B.; LING L. 2008. **Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms**. Mobile Computing, IEEE Transactions on, 1 – 18.

GELENBE, E.; GORBIL, G.; TZOVARAS, D.; LIEBERGELD, S.; GARCIA, D.; BALTATU, M.; LYBEROPOULOS, G. 2013. **Security for smart mobile networks: The NEMESYS approach**. Privacy and Security in Mobile Systems (PRISMS), 2013 International Conference on, 63 – 69.

GHALLALI, M.; OUAHIDI, B. E. 2012. **Security of mobile phones: Prevention methods for the spread of malware**. Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), 2012 6th International Conference on, 648 – 651.

HSIU-SEN, C.; TSAUR, W. 2010. **Mobile Malware Behavioral Analysis and Preventive Strategy Using Ontology**. Social Computing (SocialCom), 2010 IEEE Second International Conference on, 1080 – 1085.

JANA, D.; BANDYOPADHYAY, D. 2014. **Management of security and privacy issues of application development in mobile cloud environment: A survey**. Recent Advances and Innovations in Engineering (ICRAIE), 2014, 1 – 6.

KHANDELWAL, A.; MOHAPATRA, A. K. 2015. **An insight into the security issues and their solutions for android phones**. Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on, 106 – 109.

KUMAR, R. and RAJALAKSHMI, S.. 2013. **Mobile Cloud Computing: Standard Approach to Protecting and Securing of Mobile Cloud Ecosystems**. Computer Sciences and Applications (CSA), 2013 International Conference on, 663 – 669.

LE X. H.; HASSAN, J.; RIAZ, A. S.; RAAZI, S. M. K.; WEIWEI, Y.; CANH, N. T.; TRUC, P. T. H.; SUNGYOUNG, L.; HEEJO, L.; YUSEUNG, S.; FERNANDES, M.; MISO, K.; YONIL, Z. 2008. **Activity-based Security Scheme for Ubiquitous Environment**s. Performance, Computing and Communications Conference, 2008. IPCCC 2008. IEEE International, 475 – 481.

LUYI, X.; XIAORUI, P.; RUI, W.; KAN, Y.; XIAOFENG, W. 2014. **Upgrading Your Android, Elevating My Malware: Privilege Escalation through Mobile OS Updating**. Security and Privacy (SP), 2014 IEEE Symposium on, 393 – 408.

SAVOLA, R. M. 2009. **Current and Emerging Security, Trust, Dependability and Privacy Challenges in Mobile Telecommunications**. Dependability, 2009. DEPEND '09. Second International Conference on, 7 – 12.

TAO, F.; ZIYI, L.; CARBUNAR, B.; BOUMBER, D. and WEIDONG S. 2012.**Continuous Remote Mobile Identity Management Using Biometric Integrated Touch-Display**. Microarchitecture Workshops (MICROW), 2012 45th Annual IEEE/ACM International Symposium on, 55 – 62.

TZONELIH, H.; GOPE, P. 2013. **Provably secure mutual authentication and key agreement scheme with user anonymity**. Information, Communications and Signal Processing (ICICS) 2013 9th International Conference on, 1 – 5.

XIAOXIN, W.; NITA-ROTARU, C. **On the Security of Distributed Position Services**. Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on, 35 – 46.

ZHIJIE, W.; DIJIANG, H.; HUIJUN, W.; BING, L.; YULI D. 2014. **Towards distributed privacy-preserving mobile access control**. Global Communications Conference (GLOBECOM), 2014 IEEE, 582 – 587.

ZHIGANG, C.; XIN, H.; XIAOEN, J.; SHIN, K. G. 2013. LISA: **Location information ScrAmbler for privacy protection on smartphones**. Communications and Network Security (CNS), 2013 IEEE Conference on, 296 – 304.