**UNIVERSIDADE FEDERAL DE PERNAMBUCO**

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

CENTRO DE INFORMÁTICA

2015.1

**Análise de Vulnerabilidades no protocolo HTTPS em dispositivos da plataforma Android**

Proposta de Trabalho de Graduação

**Discente:** Luana Martins dos Santos

**Orientador:** Ruy José Guerra Barreto de Queiroz

Recife, Abril de 2015

**Sumário**

[1. Introdução 3](#_Toc417079088)

[2. Objetivos 4](#_Toc417079089)

[3. Cronograma 5](#_Toc417079090)

[4. Bibliografia 6](#_Toc417079091)

[5. Possíveis Avaliadores 7](#_Toc417079092)

[6. Assinaturas 8](#_Toc417079093)

# **Introdução**

O uso de smartphones aumentou de maneira significativa particularmente na plataforma Android. Segundo o ministro das comunicações (1), a internet móvel cresceu 416% em aproximadamente 4 anos, de dezembro de 2010 a janeiro de 2015. Este passou a ser um dos principais dispositivos de comunicação envolvendo diversas maneiras de interação, inclusive ações cotidianas como pagamento de serviços. Para essas formas de comunicação é importante frisar a segurança de tais dados trafegando por redes. No caso de dispositivos móveis, onde o poder de processamento é reduzido ao comparar com notebooks, prover criptografia para assegurar o acesso devido aos dados é imprescidível (2).

As aplicações requisitam informações de servidores externos e geralmente utilizam dados sensíveis do usuário. Torna-se, portanto, importante identificar a segurança das conexões estabelecidas para evitar que pessoas não autorizadas acessem tais dados (3).

Muitas técnicas foram utilizadas para prover segurança pro Android em várias áreas como (ICP, Binder), Network security (cryptographic providers) e outras. Uso o desses mecanismos podem dificultar o acesso de dados sensíveis por pessoas não autorizadas, mas é imprescindível que estes sejam corretamente implementados.

Os protocolo SSL (Socket Secure Layer), uma versão mais recente é denominada TLS (Transport Layer Security), é um protocolo criptográfico utilizado para prover segurança nas comunicações entre cliente e servidor, considerando um canal de comunicação inseguro (4).

O uso adequado do protocolo garante as três propriedades seguintes: autenticação, confidencialidade e integridade. O primeiro se refere a identificação do host ao qual será estabilizada a conexão, por exemplo, o cliente identificar que o servidor é legítimo, ou vice-versa. O segundo refere-se as mensagens que são trocadas entre os membros da conexão e que não devem ser acessadas por outros. Enquanto a integridade, também se refere às mensagens trocadas, mas quanto ao fato desta ser modificada durante a transferência (4).

Verifica-se portanto que a falta de segurança ou a implementação inadequada de tais protocolos proveem formas de acesso aos dados sensíveis do usuário. Aumentando assim a necessidade de análise mais aprofundada dos aplicativos que são utilizadas diariamente pelos usuários.

# **Objetivos**

Neste trabalho, algumas aplicações *Android* serão analisadas quanto ao uso de bibliotecas criptográficas para prover segurança aos dados móveis. Os protocolos analisados serão as versões da biblioteca SSL (*Socket Security Layer*) e outras versões mais recentes, como TLS (*Transport Layer Security*), que as aplicações utilizem. Como visto, as aplicações utilizam de certificados para conferir aos hosts autenticação, confidencialidade e integridade dos dados. Alguns problemas podem surgir caso essa verificação não seja feita adequadamente como explanado anteriormente.

Para análise estática do código-fonte dessas aplicações, serão utilizadas algumas ferramentas auxiliares open-source. A intenção é verificar através de *control-flow analysis*, *data-flow analysis* possíveis vulnerabilidades que, por ventura, durante o desenvolvimento tenham sido inseridas nos projetos.

Posteriormente, categorizar as vulnerabilidades encontradas e prover possíveis resoluções para as falhas de segurança encontradas.

# **Cronograma**

Estabelecimento de um cronograma indicando as atividades a serem seguidas para desenvolvimento deste trabalho de graduação.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Atividade | Março | Abril | Maio | Junho | Julho |
| Levantamento bibliográfico e leitura | X |  |  |  |  |
| Elaboração da proposta do projeto  |  | X |  |  |  |
| Obtenção de aplicações Android |  | X |  |  |  |
| Identificação das vulnerabilidades  |  | X |  |  |  |
| Estudo sobre frameworks de análise estática de código  |  | X | X |  |  |
| Análise estática dos aplicativos Android |  |  | X | X |  |
| Estabelecimento dos resultados |  |  |  | X |  |
| Escrita da monografia |  |  |  | X |  |
| Apresentação do Trabalho de Graduação |  |  |  |  | X |

# **Bibliografia**

1. **Comunicações, Ministério das.** Bernardo: Crescimento da internet móvel 'salta aos olhos'. *Ministério das Comunicações.* [Online] 26 de Março de 2014. [Citado em: 15 de Abril de 2015.] http://www.mc.gov.br/sala-de-imprensa/todas-as-noticias/institucionais/30310-crescimento-da-internet-movel-salta-aos-olhos-afirma-bernardo.

2. **Fahl, Sascha, et al., et al.** *Why Eve and Mallory love Android: an analysis of Android SSL (in)security.* North Carolina : In Proceedings of the ACM conference on Computer and communications security, 2012.

3. **Tendulkar, Vasant e Enck, William.** *An application package configuration approach to mitigating android ssl vulnerabilities.* San Jose : In Proceedings of the 2014 Mobile Security Technologies Conference, 2014.

4. **Edgecombe, Graham.** *Detection of SSL-related security vulnerabilities in Android applications.* Cambridge : Pembroke College, 2014.

# **Possíveis Avaliadores**

* Profº Paulo André da Silva Gonçalves (pasg@cin.ufpe.br)
* Profº Djamel Sadok (jamel@cin.ufpe.br)

# **Assinaturas**

Luana Martins dos Santos

**Discente**

Ruy José Guerra Barretto de Queiroz

**Orientador**