ISSN: 1984-3151

# SEGURANÇA NA CONECTIVIDADE WIFI EM DISPOSITIVOS MÓVEIS: ESTUDO DE CASO DO IPHONE

# SAFETY IN WIFI CONNECTIVITY IN MOBILE DEVICES: A CASE STUDY OF THE IPHONE

**Pedro Micael T.L.N Pinto[1]; Antônio Ricardo Leocádio Gomes[2]**

1 Analista de Segurança da Informação (Ciência da Computação). Uni-BH, 2011. MRV Engenharia. Belo Horizonte, MG. pedromicael@gmail.com.

2 Especialista em Novas Tecnologias em Educação e Treinamento. UniBH. 2000. Professor. Centro Universitário de Belo Horizonte. Belo Horizonte, MG. antonio.gomes@prof.unibh.br.

Recebido em: 16/07/2011 - Aprovado em: 20/11/2011 - Disponibilizado em: 30/12/2011

*RESUMO: Este artigo discute sobre como a sociedade atual é altamente dependente de dispositivos móveis e como é a segurança em tais dispositivos. Este trabalho visa demonstrar como a utilização de um celular para transmitir informações pode revelar dados sensíveis de seu utilizador.*
*PALAVRAS-CHAVE: Segurança da Informação. Dispositivos Móveis. Ataques. iPhone.*

*ABSTRACT: This article discusses how today's society is highly dependent on mobile devices and how the security is on these devices. This paper demonstrates how the use of a cell phone to transmit information can reveal sensitive data to users.*
*KEYWORDS:* Security Information. Mobile Device. Attack. iPhone.

---

## 1 INTRODUÇÃO

O mundo atual está cada vez mais dinâmico e exigente no que diz respeito à capacidade das pessoas de se manterem conectadas e disponíveis todo o tempo. De acordo com dados da ANATEL (Agência Nacional de Telecomunicações, 2011), o Brasil fechou o mês de janeiro de 2011 com 205 milhões de celulares, levando-se em consideração, que o número de seus habitantes, segundo a última pesquisa do Senso, é de 190 milhões de habitantes, o país possui 1,05 celulares por brasileiros.

O país experimenta também uma expansão considerável do número de aquisições do serviço 3G que proporciona conexão à Internet com uma maior velocidade de transmissão de dados.

Mas o que pode parecer por um lado um ponto positivo pode tornar-se um grande vilão, pois, o uso indiscriminado de uma tecnologia, sem os devidos cuidados, pode oferecer grande risco.

Os celulares deixaram de ser utilizados apenas como meros comunicadores, que só transferem voz. Hoje em dia os mesmos são utilizados para acessar a

Internet, pagar contas, realizar conferências, acessar e-mails, agendar reuniões etc.

Com a multiplicidade de recursos que um celular pode prover, são cada vez mais constantes os casos de vazamento de informações oriundos da perda de um telefone celular, como por exemplo, a publicação de fotos na Internet de cunho privado, o que pode levar a uma exposição da vida íntima de seu proprietário.

Os fabricantes de celulares e mais recentemente desenvolvedores espalhados pelo mundo, constroem aplicativos diversos, proporcionando aos seus utilizadores uma gama de serviços enorme e uma conectividade e integração nunca antes disponíveis.

De acordo com Cheng (2010), o lamentável desta situação é que, quanto maior o ganho em funcionalidades, mais os celulares se tornam vulneráveis aos mesmos tipos de ataques, que sofrem nossos laptops e desktops. Criou-se, então, um problema que vem crescendo que é como prover meios que efetivamente resguardem tais dispositivos, de acessos indevidos a informações que os mesmos armazenam, trafegam e criam.

Este artigo tem como objetivo analisar as questões de segurança referentes ao iPhone, telefone celular desenvolvido pela Apple, discutindo sobre a importância na utilização de métodos que provenham segurança ao se desenvolver aplicativos e de alertar a população de como os dados trafegados através de aplicativos podem estar vulneráveis.

Segundo a adMobile Mobile Metrics, empresa de consultoria americana, o iPhone é responsável por 43% do tráfego de dados na Internet em sua categoria. Segundo a Apple, até o ano de 2010, foram realizados mais de 10 bilhões de downloads para a plataforma iOS - sistema operacional do aparelho.

Este artigo avaliará as questões de segurança referentes a aplicações desenvolvidas para a plataforma do iOS, analisando-as ao que se refere à transmissão de dados.

## 2 Entendendo a Segurança e os Riscos na Rede de Computadores

O mundo real não se difere tanto do mundo tecnológico, se forem retirados os termos técnicos e as interfaces gráficas com o usuário diversas semelhanças podem ser encontradas. Segundo Schneier (2005) o crime no mundo virtual inclui tudo o que poderia ser encontrado no mundo físico: roubo, extorsão, vandalismo, exploração, fraude etc.

Existem até possibilidades de ataques ao meio físico, uma vez que os diversos controles anteriormente manuais se tornam cada vez mais informatizados e interconectados, possibilitando, por exemplo, a situação hipotética de se desligar a energia fornecida a milhares ou milhões de pessoas, tendo em vista que tais sistemas são altamente informatizados.

Segundo Gomes (2010) existem cinco pilares no que se refere à Segurança da Informação.

**Confidencialidade**: Característica que visa garantir que determinada informação não pode ser obtida ou revelada para pessoas não autorizadas. Exemplos: senhas em transações na Internet, prontuários médicos, dados de um novo produto de uma empresa.

**Integridade**: É a garantia de que a informação não foi alterada intencional ou propositalmente. Ela se mantém integra, consistente. Em uma sociedade onde a quantidade de informações produzidas, trafegadas e armazenadas é enorme, tal característica se torna cada vez mais importante.

**Autenticidade**: Garantia de que a informação só será criada ou enviada por pessoas autorizadas. Os processos de autenticação estão presentes no cotidiano das pessoas, por exemplo: senhas de bancos, senhas de e-mail, ligações de celulares,

crachás que restringem a entrada em instituições diversas.

**Disponibilidade**: De nada adianta as informações estarem integras, confidenciais e se para acessá-las é necessário autenticar-se, se a mesma não estiver disponível quando necessário, a disponibilidade é característica fundamental para acesso a determinada informação.

**Não – repúdio ou irretratabilidade**: Atributo que visa proteger contra a intenção de um dos participantes do processo de comunicação ou transação refutar sua ocorrência. Exemplos: envio de e-mail, postagem de comentários em blogs ou sites de relacionamento.

Existem diversos ataques direcionados aos pilares da segurança mencionados.

Segundo Néto (2004), quando se trata de segurança em redes, três tópicos devem ser abordados: os potenciais ataques à segurança, os serviços de segurança e os mecanismos de segurança.

Os ataques constituem em métodos que podem ser empregados por um atacante para quebrar determinado serviço de segurança, já os serviços provêem funcionalidades requeridas para a segurança de uma rede e por fim os mecanismos de segurança que são os componentes básicos desenvolvidos, para que ela seja alcançada.

## 2.1 Ataques à Segurança relacionados à Tecnologia

Segundo Gomes (2010) os ataques podem ser classificados em passivos ou ativos.

### 2.1.1 Ataques passivos

São aqueles onde a informação é analisada ou copiada na tentativa de se identificar padrões de comunicação ou de seu conteúdo. Bruce Schneier define a análise de tráfego como o estudo dos padrões de comunicação.

> Quem se comunica com quem? Quando? Qual o tamanho das mensagens? Com que velocidade as respostas são enviadas e qual o seu tamanho? Que tipo de comunicação acontece após certa mensagem ser recebida? Todas estas são questões de análise de tráfego, e suas respostas podem revelar muita informação. (SCHNEIER, 2005).

Como é possível perceber o simples fato de se observar a comunicação pode revelar informações sensíveis sobre os comunicantes. Schneier (2005) cita como exemplo o fato de uma pessoa ligar para um terrorista toda semana, pode ser mais importante que os detalhes de sua conversa, isso deixa claro como é importante manter a confidencialidade também do processo de comunicação.

#### 2.1.1.1 *Packet Sniffing*

Esta técnica consiste em se "escutar" o tráfego passante em uma rede. Existem diversos protocolos de comunicação que não empregam em sua arquitetura nenhum tipo de criptografia, ou seja, enviam seus dados através de texto claro, utilizando-se de um software *sniffer,* um atacante pode obter tais dados o que pode revelar diversas informações, tais como usuários, senhas, nomes de computadores dentro da rede interna entre outras coisas.

#### 2.1.1.2 *Port Scanning*

O processo de comunicação entre dois *hosts* na Internet tem como premissa basicamente o protocolo TCP/IP, que tem como uma de suas especificações a implementação de um endereço e uma porta que determinam, respectivamente, uma identificação para um *host* na Internet e um aplicativo sendo executado no mesmo. Levando em consideração este processo tem-se então o software *Port Scanning* que "varre" um *host* à procura de portas que estejam esperando por

conexão, desta maneira é possível verificar os possíveis serviços que estão sendo executados em tal máquina, se a aplicação que está sendo executada tiver algum tipo de vulnerabilidade pode servir para um atacante realizar algum tipo de exploração e ganhar acesso ao sistema do alvo.

#### 2.1.1.3 *SCANNING* DE VULNERABILIDADES

Da mesma maneira que existem os *scanners* de portas existem também os que visam descobrir uma vulnerabilidade especifica da aplicação que está sendo executada em um *host.* Este tipo de *scan* visa informar a um atacante sobre as possíveis vulnerabilidades que uma aplicação pode ter.

#### 2.1.1.4 IP *SPOOFING*

Segundo Gomes (2010) este é um ataque no qual o endereço IP real do atacante é camuflado através de técnicas especificas, na tentativa de se passar por uma máquina na rede. Pode ser utilizado para se explorar a relação de confiança entre duas máquinas de uma rede, onde uma só permite a conexão, se esta partir de outra máquina especifica.

### 2.1.2 ATAQUES ATIVOS

De acordo com Gomes (2010) os ataques ativos são aqueles que interferem de alguma forma no funcionamento do sistema, conforme descrito adiante.

#### 2.1.2.1 ATAQUES DE NEGAÇÃO DE SERVIÇOS

Os ataques de negação de serviços ou em inglês – *Denial Of Service* (DoS) fazem com que os recursos de determinados sistemas sejam explorados de forma tão contundente, que os serviços disponíveis naquele servidor fiquem paralisados, causando negação dos serviços válidos para usuários legítimos do sistema (GOMES, 2010). Schneier (2005) faz uma analogia no mundo real com as greves de motoristas de ônibus, controladores de tráfego aéreo, bancários que inviabilizam tais serviços.

## 2.2 ATAQUES À SEGURANÇA NÃO RELACIONADOS À TECNOLOGIA

### 2.2.1 ENGENHARIA SOCIAL

Kevin Mitnick que já foi considerado pelo FBI um dos *hackers* mais procurados do mundo e hoje trabalha como consultor em segurança define a engenharia social como sendo um conjunto de técnicas que um engenheiro social utiliza para obter acesso a informações confidenciais aproveitando-se do fator humano, ou seja, enganando determinada pessoa ou grupo. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

Mesmo que uma empresa se resguardasse de todos os tipos de ataques descritos até agora, ainda assim, poderia ser vulnerável a este tipo que é definido por Gomes (2010) como uma técnica que explora as fraquezas e vulnerabilidades humanas.

De acordo com Mitnick (2003), por mais que uma empresa invista nas melhores tecnologias disponíveis no mercado, além de dispor de pessoal especializado e treinado em tais ferramentas, seguir à risca as melhores práticas recomendadas pelos especialistas em Segurança da Informação, ter seus sistemas configurados, contendo as últimas atualizações de segurança recomendadas pelos desenvolvedores de seus produtos, ainda assim tal empresa poderá estar vulnerável a esta prática.

Segundo Gomes (2010), através desta técnica, o atacante tenta ludibriar os funcionários da empresa, se passando por outro, hierarquicamente superior, para que desta forma, possa obter informações. Nas

organizações há orientação e treinamento para que os funcionários colaborarem com seus clientes, fornecedores ou outros funcionários, o que fortalece este tipo de ataque.

> À medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo. (MITNICK, 2003)

É possível perceber o quanto é necessário se investir em treinamento das equipes que operam informações em uma empresa, uma vez que um dado às vezes sem importância pode comprometer a segurança de uma corporação.

### 2.2.2 Ataques Físicos

Estes ataques baseiam-se em furto de informações, dispositivos de armazenamento, hardware entre outros. Para tanto se faz necessária à presença do atacante nas instalações do alvo ou a subtração de notebooks fornecidos a executivos, profissionais de informática, que os tem disponíveis fora do ambiente de trabalho. Mas, muitas vezes, a comodidade caminha em rumos diferentes ao da segurança.

### 2.2.3 Informações Livremente Acessíveis

A Internet funciona também como um grande banco de dados com informações disponíveis a quem tenha em mãos algum dispositivo que se conecta a mesma. Para o funcionamento de diversos protocolos na Internet ou para manter um canal mais aberto com seus clientes, informações de corporações ou redes ficam disponíveis para acesso público, o que muitas das vezes pode conceder a um atacante, informações importantes da estrutura de uma organização ou de um histórico de uma pessoa, em especifico.

As informações obtidas em bases de dados públicas podem ser utilizadas em conjunto com outras para se determinar um plano de ataque a determinada empresa.

## 3 Criptografia

De acordo com Neto (2004) a criptografia visa garantir alguns dos princípios básicos da segurança da informação, definidos anteriormente, que são confidencialidade, autenticação e integridade das informações.

A criptografia consiste em uma técnica de codificação que se utiliza de algoritmos e chaves criptográficas de tamanhos variáveis, na tentativa de garantir a confidencialidade das informações. Os tipos de chaves, assim como os algoritmos utilizados, garantem a robustez da criptografia usada. De acordo com Neto (2004) são duas as principais técnicas de criptografia que serão apresentadas a seguir.

### 3.1 Criptografia Simétrica

Tal técnica consiste em transformar uma mensagem de texto claro ou legível em texto cifrado, utilizando um algoritmo de encriptação e uma chave criptográfica secreta, que é compartilhada entre quem protegeu a mensagem e quem a irá recebê-la.

O algoritmo matemático de criptografia realiza operações utilizando, também, a chave no texto claro transformando-o em texto cifrado. O processo neste tipo de técnica só pode ser revertido, através da utilização da mesma chave para tornar o texto cifrado legível novamente.

Para garantir a segurança do processo como um todo deve haver o compartilhamento da chave criptográfica o que muitas vezes não é viável, já que para trocar mensagens cifradas com determinado número de pessoas seria necessário que todas dispusessem da

chave. Em outra análise, se a chave for capturada por alguém no processo de comunicação, todas as mensagens trocadas podem ser reveladas. Para solucionar problemas como este foi criada a criptografia assimétrica.

### 3.2 Criptografia Assimétrica

Também conhecida como criptografia de chave pública, a criptografia assimétrica é diferente da simétrica onde as partes comunicantes não mais compartilham a mesma chave criptográfica.

Neste processo são utilizadas duas chaves, a pública que fica de posse de quem transforma a mensagem de texto claro para cifrado, ou seja, é responsável pela encriptação dos dados e, a outra, a chave privada responsável pela decriptação do texto cifrado gerado com a sua respectiva chave pública.

Para que aconteça o processo de troca de dados em ambas as direções, ou seja, entre os dois pares comunicantes é necessário que ambos disponham cada um de uma chave privada e uma pública.

## 4 Telefonia Celular

Um telefone celular pode ser definido como sendo um transmissor de baixa potência, onde frequências podem ser reusadas dentro de áreas geográficas determinadas. A telefonia celular teve início com as redes analógicas AMPS(*Advanced Mobile Phone Service)* de primeira geração, oferecendo serviços de caixa postal e fax.

### 4.1 Cenário Atual

Atualmente vive-se a plenitude da 3ª geração de telefonia celular e a transição para a 4ª geração no contexto mundial.

Celulares deixaram de ser apenas meros comunicadores para exercerem muitas outras atividades, os aparelhos atuais são capazes de acessar a Internet em altíssima velocidade (7,2 Mbps) proporcionando acesso a diversos tipos de conteúdo.

### 4.2 Iphone

De acordo com o seu *site,* a Apple, empresa norte-americana fundada em 1974 com sede em Cupertino na Califórnia, introduziu o iPhone no mercado em 29 de Junho de 2007. O aparelho tinha como característica principal a tecnologia *multitouch,* uma desenvolvida pela Apple que permite controlar o aparelho através de toques na tela eliminando-se os botões, anteriormente conhecidos.

A empresa contabiliza a venda de 108,624 milhões de iPhones.

O aparelho tem também como grande diferencial a possibilidade de executar aplicativos que podem ser baixados diretamente da loja da empresa a *"App Store".*

### 4.3 Desenvolvimento de Aplicações

O desenvolvimento de aplicativos para o iPhone se dá através de um SDK (*Software Development Kit)* o *Xcode*, que é um conjunto de ferramentas que auxiliam no processo de desenvolvimento de aplicativos.

Os softwares são desenvolvidos para o aparelho através da Linguagem *Objective-C*, que é uma linguagem orientada a objetos, além de outras melhorias em relação a sua predecessora a Linguagem C.

Para o desenvolvimento de aplicações no aparelho faz-se necessário, além de obter um computador da Apple, uma licença de desenvolvimento conforme pode ser visto na Tabela 1.

**Tabela 1 - Licenças de desenvolvimento**

| | iOS Developer Program | | | | |
|---|---|---|---|---|---|
| Access | Individual | Company | Enterprise Program | University Program | Apple Developer |
| Dev Center Resources | ✓ | ✓ | ✓ | ✓ | ✓ |
| iOS SDK | ✓ | ✓ | ✓ | ✓ | ✓ |
| Select Pre-Release Software & Tools | ✓ | ✓ | ✓ | | |
| Ability to Create Development Team | | ✓ | ✓ | ✓ | |
| Apple Developer Forums | ✓ | ✓ | ✓ | ✓ | |
| Test on iPad, iPhone, and iPod touch | ✓ | ✓ | ✓ | ✓ | |
| Ad Hoc Distribution | ✓ | ✓ | ✓ | | |
| In-House Distribution | | | ✓ | | |
| App Store Distribution | ✓ | ✓ | | | |
| Price | $99/year | $99/year | $299/year | Free | Free |

Conforme pode ser observado na Tabela 1 as licenças são distribuídas de acordo com o tipo de desenvolvedor tendo, cada um, suas especificidades.

Desenvolvedores do mundo todo que tenham acesso à plataforma de desenvolvimento e a licença de desenvolvedor podem produzir aplicativos e submetê-los à apreciação da Apple. A empresa é responsável por analisar o aplicativo de acordo com seus critérios, tais como, desempenho, privacidade, segurança, publicidade etc. Com esta análise, em um cenário ideal, fica difícil a disseminação de aplicativos maliciosos através da loja da empresa.

Ao disponibilizar um aplicativo para venda na loja da empresa, ela fica com 30% do dinheiro arrecadado e, o restante, 70% são remetidos ao desenvolvedor.

Por mais que a empresa tente se bloquear, a venda de aplicativos não advindos de sua loja, práticas conhecidas como *Jailbreak* ou em uma tradução literal "sair da prisão" exploram vulnerabilidades no aparelho possibilitando a instalação de aplicativos não oriundos da loja oficial da Apple.

## 4.4 JAILBREAK

Segundo Seriot (2010) o *Jailbreak* pode ser definido como sendo uma configuração que permite ao iPhone executar softwares não assinados digitalmente pela Apple. Isto é conseguido através da exploração de vulnerabilidades no IOS, sistema operacional do aparelho.

Os aplicativos da loja da Apple têm valor inicial de US $ 0,99 variando até US $99,00, o Jailbreking oferece a possibilidade de se instalar aplicativos não oriundos da App Store, e com isso não pagar por eles.

Além da questão financeira, as políticas da Apple para aprovação dos aplicativos são determinantes para alguns usuários realizarem o procedimento e com isso conseguirem liberar recursos bloqueados pelo iOS (*iPhone Operation System*, o sistema operacional padrão do aparelho). Muitas características só estão presentes nos iPhones mais novos por questão de desempenho de hardware, a empresa bloqueia funcionalidades para não impactar negativamente o desempenho do aparelho ou pelo simples fato do mesmo não suportá-las.

Com o *Jailbreak* é possível, mesmo que perdendo em desempenho, liberar tais características no iOS.

## 4.5 ARQUITETURA DO IOS

O sistema operacional iOS, que roda nos dispositivos iPhone, iPod touch e iPad é similar ao sistema operacional OSX dos computadores da Apple. Tal sistema é responsável por controlar o hardware do aparelho e prover recursos para as aplicações desenvolvidas para o mesmo.

O sistema é composto pelos seguintes componentes: Bootloader, Kernel, bibliotecas compartilhadas, e duas partições HFS sendo uma (apenas leitura) para o sistema operacional e outra para utilização geral.


**Figura 1 – Camadas de acesso**

É possível verificar na Figura 1 que todo acesso aos recursos do iPhone é feito através do iOS.

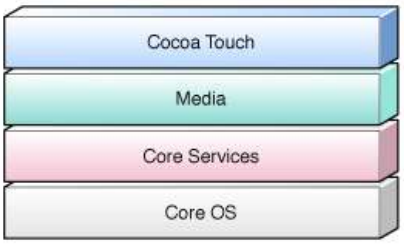


**Figura 2 – Camadas do iOS**

Fonte: APPLE, 2010.

Com a divisão em camadas do iOS é possível para o desenvolvedor escolher entre os níveis de implementação, sendo o *Cocoa Touch* o nível de abstração mais alto, ou seja, nele são tratadas as questões da interface visual do aparelho, sendo possível definir os controles por gestos que o dispositivo irá responder, multitarefa, notificações etc. Nesta camada temos os seguintes *frameworks: Address Book UI, Event Kit UI, Game Kit, iAd, Map Kit, Message UI* e *UIKit.*

A camada *Media* é responsável por prover recursos multimídia ao aparelho. Nesta camada temos os seguintes *frameworks: AV Foundation, Core Audio, Core Graphics, Core Text, Core Video, Image I/O, OpenAL, OpenGL ES* e *Quartz Core.*

Os serviços que praticamente toda aplicação utilizará são providos pela camada *Core Services* que é composta pelos seguintes *frameworks*: *Address Book, CFNetwork, Core Data, Core Foundation, Core Location, Core Media, Core Telephony, Event Kit, Foundation, Mobile Services, Quick Look, Store Kit* e *System Configuration.*

E por fim, tem-se a camada *Core OS,* a camada de mais baixo nível do iOS, responsável pela comunicação com o *Kernel* ou o núcleo do sistema. Nesta camada estão presentes os seguintes *frameworks: Accelerate, External Acessory, Security* e *System.*

## 4.6 WIRELESS

Tecnologia presente em muitos dos dispositivos atuais o *wireless* traz consigo grande mobilidade em relação ao seu predecessor as redes cabeadas. O padrão mais utilizado por redes *wireless* é o 802.11, padrão este definido pelo IEEE (*Institute of Electrical and Electronics Engineers*), instituto responsável por estabelecer padrões para computadores e dispositivos. De acordo com Amaral e Maestrelli (2004) o padrão 802.11 atingia a velocidade de 1 Mbps a 2 Mbps, projetado em 1997, ele foi logo aprimorado para o 802.11ª, desenvolvido em 1999. O mais novo propiciava uma taxa de transferência maior que chegava a 54Mbps e operava a uma frequência de 5GHz. Ainda em 1999 foi criado o padrão 802.11b que opera na faixa de 2,4 – 2,48GHz e transmite até uma velocidade de 11Mbps.

Outro padrão bastante utilizado é o 802.11g que corrige alguns problemas encontrados nos padrões anteriores, ele trabalha na mesma faixa de frequência do 802.11b, reduzindo, assim, os custos com uma possível migração entre os dois.

**Tabela 2 – Características do Padrão 802.11**

| Característica | Descrição |
|---|---|
| Camada Física | *Direct Sequence Spread Spectrum*(DSSS), *Frequency Hopping Spread Spectrum*(FHSS) e infravermelho (IR). |
| Faixa de Freqüência | 2,4GHz (11b, 11g) e 5GHz (11a) |
| Largura de Banda | 1Mbps, 2Mbps, 5.5Mbps, 11Mbps (11b), 54Mbps (11a, 11g) |
| Segurança de informação | Autenticação, confidencialidade e integridade baseada no algoritmo de encriptação RC4, porém com gerenciamento da chave limitado. |
| Distância de Operação | Aproximadamente 50m (ambientes fechados) e 400m (ambientes abertos). |
| *Throughput* | Aproximadamente 5.5Mbps (11Mbps) e 25 - 30Mbps (54Mbps). |
| Aspectos Positivos | Velocidade de rede Ethernet, porém sem cabo, muitos produtos diferentes de empresas diferentes. *Access Points* e *Wireless Client Cards* estão diminuindo de preço. |
| Aspectos Negativos | Segurança baixa na configuração padrão, o *throughput* cai muito com a distância e a carga. |

Fonte: AMARAL; MAESTRELLI, 2009.

Na Tabela 2 podem-se verificar algumas características do padrão 802.11.

O padrão 802.11b, que é o mais utilizado, provê dois métodos de conectividade o P2P(*Peer to Peer*) e o AP (*Access Point*). No primeiro, a conexão ocorre entre dois dispositivos diretamente, não necessitando um intermediador, utilizam-se para isso de NICs (*Network Interface Card*), hardwares responsáveis por realizarem a comunicação. Na conexão via AP a comunicação ocorre utilizando-se também de NICs mais é necessário um hardware para intermediar a troca de dados entre os dispositivos.

De acordo com Amaral e Maestrelli (2004) as redes wireless possuem uma área de transmissão de 29m (vinte e nove metros), trafegando dados à velocidade de 11Mbps, em áreas fechadas e de 400m (quatrocentos metros), trafegando a 1Mbps em áreas abertas.

Os benefícios em relação às redes cabeadas são evidentes, uma vez que proporcionam maior mobilidade e flexibilidade ao seu utilizador.

## 4.7 Segurança em Redes Wireless

A transmissão em redes Wireless é feita em *broadcast,* ou seja, os dados são enviados em todas as direções e é responsabilidade do destino identificar que os dados trafegados são direcionados a ele, e tarefa dos demais dispositivos conectados ao AP descartarem o que não for endereçado aos mesmos.

Uma vez que os dados são enviados para todos é possível capturar as informações que estão sendo trafegadas sem nenhum tipo de proteção, obtendo desta maneira informações sensíveis.

Desta maneira é necessário prover meios para proteger os dados trafegados em redes *wireless,* isto é conseguido através da criptografia.

## 4.8 Wireless em Dispositivos Móveis

Com a rápida expansão mundial do wireless, logo a tecnologia foi incorporada aos dispositivos móveis. Atualmente vários modelos de celulares dispõem de tal tecnologia. No iPhone, objeto de estudo deste artigo, esta tecnologia está presente desde sua primeira versão o iPhone 1.

## 4.9 Tráfego wireless no iphone

Para realizar o estudo desenvolvido neste artigo foi utilizado o *Wireshark,* que é um software livre baseado na licença GPL(*General Public License).*

O *Wireshark* é um analisador de pacotes de rede (*Sniffer)* capaz de capturar os pacotes trafegados em redes cabeadas e *wireless*.

Para a realização do estudo foi utilizado um iPhone 3G com as configurações de fábrica. A rede utilizada não dispunha de métodos de criptografia do tráfego.

Na Tabela 3 são apresentados os *apps* aplicativos utilizados.

**Tabela 3 - Aplicativos**

| Aplicativo | Categoria | Versão | Data de download | Valor |
|---|---|---|---|---|
| **BestBuy** | Estilo de Vida | 4.4.0 | 1/6/11 | Gratuito |
| **Skout** | Redes Sociais | 2.6.0 | 1/6/11 | Gratuito |
| **Anima ID** | Educação | 1.1 | 1/6/11 | Gratuito |
| **Jobs** | Negócios | 2.2.2 | 1/6/11 | Gratuito |
| **123Diagnosis** | Medicina | 1.0 | 4/4/11 | Gratuito |
| **AtZip** | Redes Sociais | 1.2.4 | 2/6/11 | Gratuito |
| **Badoo** | Redes Sociais | 1.6.1 | 3/6/11 | Gratuito |

Todos os aplicativos apresentam algum tipo de conexão a Internet, utilizando para isto a rede *wireless.* O tráfego foi capturado pelo *Wireshark* 1.4.2v em uma rede aberta.

## 5 RESULTADOS

No apêndice A é possível verificar que dados que deveriam ser sigilosos são transmitidos em texto puro, ou seja, sem nenhum tipo de criptografia em nível do aplicativo.

Serão apresentados alguns aplicativos utilizados para análise neste artigo.

Para cadastro e utilização dos aplicativos apresentados neste artigo foram usadas as informações da Tabela 4.

**Tabela 4 – Informações utilizadas**

| Informações utilizadas | |
|---|---|
| **Usuário** | testepoc |
| **Senha** | testepoc123 |
| **Email** | teste@poc.com |
| **Data de Nascimento** | 5/4/87 |

No caso do aplicativo da Ânima como é necessário ser estudante de alguma das instituições de ensino do grupo foram utilizadas as informações do próprio autor do artigo.

No Apêndice A é possível verificar o tráfego completo realizado entre os aplicativos e os servidores.

### 5.1 APLICATIVO ANIMA ID

O aplicativo Anima ID, desenvolvido pela Ânima Educação, para disponibilizar aos alunos das instituições de ensino superior UNIBH, UNA e UNIMONTE o acesso a informações acadêmicas como notas, faltas, calendário letivo etc.

O Anima ID trafega dados que deveriam ser privados em texto claro possibilitando a qualquer um que esteja na mesma rede “escutando” a transmissão capture estas informações.

Vale ressaltar que o usuário e senha utilizados para acesso aos dados do aplicativo são os mesmos utilizados para se acessar o SOL (Serviço online), serviço disponibilizado pela Instituição para administrar a vida acadêmica do aluno, sendo possível verificar dados como endereço, extratos financeiros, boletos pagos e a pagar, além de ser possível fazer diversos tipos de solicitações.

### 5.2 APLICATIVO SKOUT

O aplicativo Skout (Tabela 5) é voltado para as redes sociais sendo o 14º mais popular da loja App Store americana, desenvolvido pela empresa Wichoro. O app proporciona a seus utilizadores criar uma rede de amigos na qual é possível comunicarem entre si.

**Tabela 5 – Aplicativo Skout**

| Aplicativo Skout | |
|---|---|
| **Categoria** | Redes Sociais |
| **Atualização** | 19-Apr-11 |
| **Versão atual** | 2.6.0 |
| **Tamanho** | 11.1 MB |
| **Idioma** | Inglês |
| **Empresa** | Wichro |
| **Usuário** | testepoc |
| **Senha** | testepoc123 |

O Skout trafega o usuário e senha em texto claro assim como o Anima ID, além disso, também trafega as conversas realizadas no chat que ele disponibiliza sem utilizar nenhum tipo de criptografia, sendo possível ver na integra as conversas trocadas entre o utilizador e as pessoas envolvidas.

### 5.3 APLICATIVO JOBS

O aplicativo Jobs (Tabela 6) desenvolvido pela empresa Careerbuilder.com tem o intuito de auxiliar seus utilizadores na colocação no mercado de trabalho.

**Tabela 6 – Aplicativo Jobs**

| Aplicativo Jobs | |
|---|---|
| **Categoria** | Negócios |
| **Atualização** | 19-Abr-2011 |
| **Versão atual** | 2.2.2 |
| **Tamanho** | 2.8 MB |
| **Idioma** | Inglês |
| **Empresa** | Careerbuilder.com |
| **Usuário** | criptografado |
| **Senha** | criptografado |

O Jobs, ao contrario dos anteriores, protege com criptografia informações como usuário e senha do utilizador, mas por outro lado tudo que o mesmo procura através do aplicativo é enviado em texto claro.

O que pode parecer, por um lado, algo mínimo se levar em conta a severidade dos dados trafegados pelos anteriores, pode ser muito inconveniente dependendo do contexto. Por exemplo, se um funcionário de uma empresa, acessando e procurando informações sobre novos postos de trabalho de outra empresa, e a empresa do mesmo controla tudo que seu funcionário utiliza, inclusive através do celular, tal atividade poderia não ser vista de maneira correta.

## 5.4 APLICATIVO BADOO

O aplicativo Badoo (Tabela 7) segue a mesma linha do Skout apresentado anteriormente. É desenvolvido pela empresa Badoo Services Ltd.

**Tabela 7 – Aplicativo Badoo**

| Aplicativo Badoo | |
|---|---|
| **Categoria** | Redes Sociais |
| **Atualização** | 20-Mai-2011 |
| **Versão atual** | 1.6.1 |
| **Tamanho** | 7.6 MB |
| **Idioma** | Inglês |
| **Empresa** | Badoo Services Ltd |
| **Usuário** | testepoc |
| **Senha** | testepoc123 |

Além de trafegar usuário e senha em texto claro o app em questão trafega informações cadastrais como aniversário, e-mail e preferência sexual, também sem nenhum tipo de criptografia. Dados como orientação sexual são importantes para o objetivo do *site*.

Informações como estas não deveriam ser trafegadas sem nenhum tipo de proteção, pois ferem questões de privacidade do utilizador.

## 5.5 APLICATIVO ATZIP

O aplicativo AtZip (Tabela 8) desenvolvido pela empresa ATZIP na mesma categoria dos aplicativos Badoo e Skout, ou seja, redes sociais, tendo o mesmo objetivo prover meios para o relacionamento de pessoas.

**Tabela 8 – Aplicativo AtZip**

| Aplicativo AtZip | |
|---|---|
| **Categoria** | Redes Sociais |
| **Atualização** | 25-Mai-2011 |
| **Versão atual** | 1.2.4 |
| **Tamanho** | 11.2 MB |
| **Idioma** | Inglês |
| **Empresa** | ATZIP |
| **Usuário** | criptografado |
| **Senha** | criptografado |

Ao contrário dos anteriores utilizou-se de criptografia em todo processo de comunicação com os servidores.

## 6 ANÁLISE DE RESULTADOS

É possível perceber a gravidade da falta de criptografia no transporte de dados no iPhone, como mostra a Tabela 9.

**Tabela 9 – Situação dos aplicativos**

| Aplicativo | Vulnerável |
|---|---|
| BestBuy | não |
| Skout | sim |
| Anima ID | sim |
| Jobs | parcialmente |
| 123Diagnosis | parcialmente |
| AtZip | não |
| Badoo | sim |

Na Tabela 9 é possível verificar que apenas dois dos aplicativos não apresentaram nenhum tipo de vulnerabilidade referentes à transmissão de dados.

De acordo com a Apple em seu documento sobre desenvolvimento de código seguro o iOS por padrão não fornece métodos para criptografia no transporte de dados sendo necessário a utilização da biblioteca CFNetwork.

Fica a cargo do desenvolvedor utilizar recursos que resguardem as informações dos utilizadores de seus produtos.

Foge ao escopo do artigo a demonstração de métodos de programação segura, pois seu foco foi alertar aos desenvolvedores e utilizadores dos perigos do uso de recursos tecnológicos sem levar em conta aspectos de segurança.

## 7 CONCLUSÃO

A utilização de recursos tecnológicos pode contribuir muito para melhorar os problemas encontrados no mundo atual, no entanto, a utilização de tais recursos sem a verificação adequada dos critérios de segurança, tanto por parte do utilizador, quanto por parte do desenvolvedor, podem levar a problemas graves.

O estudo proposto por este artigo pode ser estendido para outros dispositivos da Apple como o iPad e iPod touch, que utilizam o iOS como sistema operacional, além de utilizarem o mesmo SDK para desenvolvimento, ampliando assim o impacto de tais ações, uma vez que a expansão dos produtos citados vem crescendo muito, mundial e nacionalmente, levando o Brasil a trazer para si uma fábrica de produtos da empresa norte-americana.

O artigo tratou o lado da aplicação que deveria prover meios que resguardassem os dados independentemente do canal de comunicação utilizado, mas é possível dar outro foco ao estudo analisando os aspectos de segurança dos protocolos *wifi*.

As empresas responsáveis pelos aplicativos listados como vulneráveis foram devidamente notificadas das falhas encontradas. A extensão da pesquisa para outras plataformas, como a da Google, que vem crescendo fortemente com o sistema operacional Android se dará em data posterior.

## AGRADECIMENTOS

Os autores agradecem a todos que tornaram possível a realização deste trabalho.

## REFERÊNCIAS

AMARAL Bruno Marques; MAESTRELLI Marita.;**Segurança em Redes Wireless 802.11.** Disponível em: http://biblioteca.cat.cbpf.br/pub/apub/nt/2004/nt00204.pdf>. Acesso em: 10 abr. 2011.

CHENG, Michael K.; **Iphone Jailbreaking Under The DMCA: Towards a Functionalist Approach in**

**Anticircumvention.** Disponivel em: <http://www.btlj.org/data/articles/>Acesso em: 15 fev. 2010.

GOMES, ANTONIO RICARDO L.; **Auditoria de Segurança de Sistemas**. Disponível em: <http://www.unibh.br>. Acesso em: 29 set. 2010.

LAS. **Segurança em Dispositivos Móveis**. Disponível em: <http://www.las.ic.unicamp.br/~edmar/>. Acesso em: 29 set. 2010.

MACFEE. **Malware móvel: Ameaças e prevenção**. Disponível em: <http://www.mcafee.com/us/local_content/white_papers/threat_center>. Acesso em: 28 set. 2010.

MITNICK, KEVIN D.; **A Arte de Enganar**. 1.ª Edição. São Paulo: Pearson, 2003. 290p.

NETO, JOAO CARLOS.; **Segurança em Redes Móveis AdHoc**. Disponível em: <http://grenoble.ime.usp.br/movel/monosegurancaadhoc.pdf> Acesso em: 10 jan. 2010.

RUFINO, Nelson Murilo de Oliveira. **Segurança em Redes Sem Fio**. São Paulo : Editora Novatec. 2007. 208

SCHNEIER, BRUCE; **Segurança e Privacidade**. 1.ª Edição. São Paulo: Abril, 2005. 180p.

SERIOT, NICOLAS.; **iPhone Privacy.** Disponível em: <http://seriot.ch/resources/talks_papers>. Acesso em: 10 abr. 2010.

---

## APÊNDICE A – TRÁFEGO CAPTURADO PELO WIRESHARK

Em vermelho são apresentados os dados enviados pelo Iphone e em azul os enviados pelo servidor do aplicativo.

### APLICATIVO MATCH.COM

POST /REST/user/xml HTTP/1.1

Host: g3.match.com

User-Agent: match.com/2.0.1 CFNetwork/485.12.7 Darwin/10.4.0

Authorization: (null),MatchFD51DE89D449, 5, 1

Content-Type: application/x-www-form-urlencoded

Accept: */*

Accept-Language: en-us

Accept-Encoding: gzip, deflate

Content-Length: 343

Connection: keep-alive

password=testepoc123&mobile=&uage=35&smsAlerts=1&postal=&mailMe=1&bday=1987-04-05T09%3A00%3A00&lage=18&email=mjionr%40yahoo.com.br&ClientOS=4.2.1&DeviceModelNumber=iPhone%20OS&ClientAppVersion=2.0.1&mobileid=f990038b1289bdd121e8b1ac7d803201e592f24b&gender=1&emailAlerts=1&country=United%20States&seeking=2&discloselocation=true&handle=testepoc

HTTP/1.0 200 OK

Date: Wed, 30 Mar 2011 00:56:50 GMT

Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET

X-AspNet-Version: 2.0.50727

Cache-Control: private

Content-Type: text/xml; charset=utf-8

ntCoent-Length: 294

Content-Encoding: gzip

Content-Length: 205

X-Cache: MISS from amon

Via: 1.1 amon:8080 (squid/2.7.STABLE9)

Connection: keep-alive

.....0.Dw$.!.N...PZ...!XXC1%R.TvJ..'.....|z~.+qE b.]&.DI..'..L..<..y>..=....Cn.c..s<....%.f..u].M.O%..J..^.... fd...._.....*.^.yz.1l.....J)

}.Wkd6%..M|.]@.w..x.&..D...G....X.....K...&...

PUT /REST/analytics/xml HTTP/1.1

Host: g3.match.com

User-Agent: match.com/2.0.1 CFNetwork/485.12.7 Darwin/10.4.0

Authorization: (null),MatchFD51DE89D449, 5, 1

Content-Type: application/x-www-form-urlencoded

Accept: */*

Accept-Language: en-us

Accept-Encoding: gzip, deflate

Content-Length: 225

Connection: keep-alive

otherUserId=0&returnPixelPath=false&appVersion=2.0 .1&analyticsId=0x72E09B2FB21BE9B2&deviceos=4.2. 1&pageName=RegFailfromSpotlightStartNow&eventN ame=RegFailfromSpotlightStartNow&mobileid=f99003 8b1289bdd121e8b1ac7d803201e592f24bHTTP/1.0 200 OK

Date: Wed, 30 Mar 2011 00:56:51 GMT

Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET

X-AspNet-Version: 2.0.50727

Set-Cookie: __utmmobile=0x72E09B2FB21BE9B2; expires=Fri, 29-Mar-2013 00:56:51 GMT; path=/

Cache-Control: private

Content-Type: text/xml; charset=utf-8

Cteonnt-Length: 239

Content-Encoding: gzip

Content-Length: 186

X-Cache: MISS from amon

Via: 1.1 amon:8080 (squid/2.7.STABLE9)

Connection: keep-alive

.....=..0.....Z.....N..Y\I.B.h..|.{kb.\.....I....p..h.Q..... V...t...Y..$%...xC;.m.x.m.X%.un.)..9.w.....r.e.}.(m].%. W....WB.k.v.....:...c.F..)[..`...r.....w4..N_H.t/.....N..Y\I.B .h..|.{kb.\.....I....p..h.Q.....V...t...Y..$%...xC;.m.x.m.X%.u n.)..9.w.....r.e.}.(m].%.W....WB.k.v.....:...c.F..)[..`...r.... ...w4..N_H.t/....

**APLICATIVO ANIMA ID**

POST /AnimaIDCardServices/Services/validarLoginSenha.as px HTTP/1.1

Host: carteirinha.animaeducacao.com.br

User-Agent: Anima%20ID/1.1 CFNetwork/485.12.7 Darwin/10.4.0

Content-Length: 59

Content-Type: application/x-www-form-urlencoded

Accept: */*

Accept-Language: en-us

Accept-Encoding: gzip, deflate

Connection: keep-alive

codInstituicao=1&matriculaAluno=406103279&senhaA luno=398772

HTTP/1.0 200 OK

Date: Wed, 30 Mar 2011 00:20:03 GMT

Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET

X-AspNet-Version: 2.0.50727

Cache-Control: private

Content-Type: text/html; charset=UTF-8

Content-Length: 296

X-Cache: MISS from amon

Via: 1.1 amon:8080 (squid/2.7.STABLE9)

Connection: keep-alive

{"Aluno":{"CodAluno":"132018","NomeAluno":"PEDRO MICAEL THEOSA LUCAS NOGUEIRA PINTO","NomeCurso":"CI..NCIA DA COMPUTA....O","UrlFotoAluno":"http://sistemas.animaeducacao.com.br/img/padrao/profile_m.png","Token":"3D7ACCB3E33CAFBA92144727D7CEEF7D"},"DscErro":null,"Retorno":null,"Status":"SUCESSO"}