UNIVERSIDADE PRESBITERIANA MACKENZIE

FRANCISCO KAZO SUGO OGATHA

SEGURANÇA NA INTERNET MÓVEL

São Paulo

2011

FRANCISCO KAZO SUGO OGATHA

SEGURANÇA NA INTERNET MÓVEL

Trabalho de Conclusão de Curso
apresentado ao Curso de
Especialização em Análise de
Sistemas da Universidade
Presbiteriana Mackenzie, como
requisito parcial para a obtenção do
grau de Especialista

ORIENTADORA: Professora Kassya Rigolon de Andrade

São Paulo

2011

AGRADECIMENTOS

Agradeço a Deus por me dar saúde e todas as ferramentas necessárias para seguir minha jornada cheia de obstáculos, mas acima de tudo, com muitas alegrias.

Agradeço a minha querida mãe que me deu amor e carinho em todos os momentos de minha vida.

Agradeço a meu pai que sempre me deu força e apoio nas horas em que mais necessitava.

Agradeço a minha amada esposa por sempre estar presente e por possuir uma bondade sem fim, o que sempre me fez admira-la e ama-la cada vez mais.

Agradeço a meus irmãos e minha irmã pelos ensinamentos e pelos momentos de afeto.

RESUMO

O trabalho a ser apresentado tem como assunto a internet móvel, mais focado na parte de segurança. Como atualmente se trata de uma tecnologia em grande ascensão, é normal que o número de ataques aumente consideravelmente nessa nova forma de interação com a internet. Com isso surge a necessidade de preocupações com segurança, não somente para o público que deseja entretenimento, mas também para empresas que adotem dispositivos móveis como apoio aos processos de negócio. Há muito ainda o que se discutir e evoluir nessa área, visto que novas tecnologias, novas formas de interação e consequentemente novos tipos de ataques surgem constantemente. Porém, já existem varias soluções de padronização e tecnologias presentes no mercado para reduzir esses riscos e com certeza muito mais surgirão para que mais e mais pessoas e empresas se sintam seguras para interagir nesse novo mundo.

Palavras-chave: Internet móvel, segurança em dispositivos móveis, segurança em smartphones, segurança da informação.

ABSTRACT

The work to be presented has as subject the mobile Internet, more focused on the security. As today is a technology rising, it is normal that the number of attacks to rise considerably in this new form of interaction with the Internet. With that comes the need for security concerns, not only for the public who want entertainment, but also for companies to adopt mobile devices to support business processes. There is much still to discuss and evolve in this area, since new technologies, new forms of interaction and hence new types of attacks are constantly emerging. However, there are several standards and technology solutions in the market to reduce these risks and certainly more will rise to more and more people and companies feel safe to interact in this new world.

Keywords: Mobile internet, security on mobile devices, smartphone security, information security.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS, SIGLAS E SÍMBOLOS

AMPS	*Advanced Mobile Phone System*
ARPA	*Advanced Research Projects Agency*
CA	*Care of Address*
CDMA	*Code Division Multiple Access*
CSRF	*Cross-Site Request Forgery*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name Service*
DOM	*Document Object Model*
ETSI	*European Telecommunications Standards Institute*
FA	*Foreign Agent*
FM	*Frequency Modulation*
GGSN	*Gateway GPRS Support Node*
GSM	*Global System for Móbile Communication*
GPRS	*General Packet Radio Service*
HA	*Home Agent*
HN	*Home Network*
HSPA	*High Speed Packet Access*
HSDPA	*High Speed Downlink Packet Access*
HSUPA	*High Speed Uplink Packet Access*
HTML	*Hyper Text Markup Language*
HTTP	*Hypertext Transfer Protocol*
IDS	*Intrusion Detection System*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
ISDN	*Integrated Services Digital Network*
ISM	*Industrial, Scientific, Medical*
Java ME	*Java Micro Edition*
LTE	*Long Term Evolution*
MAC	*Media Access Control*
MIMO	*Multiple Input Multiple Output*
NCP	*Network Control Protocol*

NMP	*Nordic Mobile Telephones*
NTT	*Nippon Telephone and Telegraph*
OFDM	*Orthogonal Frequency Division Multiplexing*
PC	*Personal Computer*
PDA	*Personal Digital Assistants*
SDK	*Software Development Kit*
SGNS	*Serving GPRS Support Node*
SMS	*Short Message Service*
SMSC	*Short Message Service Center*
SQL	*Structured Query Language*
SSH	*Secure Shell*
SSL	Secure Sockets Layer
TCP	*Transmission Control Protocol*
TDMA	*Time Division Multiple Access*
UMTS	*Universal Mobile Telecommunications System*
URL	*Universal Resource Locator*
VPN	*Virtual Private Networks*
XHTML	*Extensible HyperText Markup Language*
XML	*Extensible Markup Language*
XSS	*Cross-site Scripting*
WAP	*Wireless Markup Language*
WWW	*World Wide Web*
W-CDMA	*Wideband Code Multiple Access*
3GPP	*Third Generation Partnership Project*

SUMÁRIO

1 INTRODUÇÃO

A tecnologia para dispositivos móveis está evoluindo rapidamente, não somente em aparelhos, mas também em velocidade de conexão. Juntamente com essa evolução, surgem novas formas de interação com internet. Algumas navegadas somente em sites de notícia e leitura de e-mail, deixaram de ser as poucas ações destinadas a esses dispositivos.

A evolução da tecnologia móvel se deu em vários pontos como na transmissão de dados, Bluetooth, Notebooks, Palmtop, Smartphones, mais recentemente Tablet PCs e com certeza surgirão muito mais inovações. Tal tecnologia já faz parte do cotidiano de muitas pessoas, tanto na rotina pessoal como profissional.

No início dessa evolução, surgiram os PDAs (Personal Digital Assistants), dispositivos com objetivos simples como organizar informações pessoais, contatos e tarefas. Um período mais tarde, começou a surgir os primeiros smartphones, um telefone móvel que disponibiliza funções que até aquele momento, somente eram vistas em computadores pessoais. Dentre essas funções podemos citar instalações de diversas aplicações, visualização de documentos, visualização de arquivos multimídia e acesso a internet.

Outros dispositivos que merecem destaque são os que permitiram a leitura de livros digitais, denominados e-Readers. Como evolução deste último, surgiram os chamados Tablet PCs, com maior capacidade de processamento, novas interfaces e funções semelhantes a dos smartphones, como o acesso à internet.

Aplicativos móveis, que fornecem os mais variados serviços também evoluíram e começaram a se tornarem populares. A App Store da Apple e o Market do Android, hoje as duas principais lojas de aplicativos, são exemplos dessa popularização, pois contêm milhares de aplicativos, pagos ou gratuitos e, que são consumidos de forma simples e direta no mundo todo. Estima-se um grande crescimento na movimentação dessas lojas virtuais devido ao crescente mercado de dispositivos móveis, principalmente smartphones e mais recentemente Tablets.

No mundo corporativo a computação móvel também passou a ser uma realidade. Para aumentar a eficiência de suas operações e garantir competitividade, muitas empresas estão adotando soluções que envolvem dispositivos móveis.

Mas qual o motivo dessa rápida ascensão? Com certeza foi a possibilidade de acesso a dados e informações a qualquer momento e em qualquer lugar. Com os dispositivos atuais, pode-se dizer que uma pessoa pode ter um computador na palma de sua mão, com acesso a internet, conteúdos multimídia, acesso a redes sociais e até mesmo informações de negócio.

Porém, à medida que as tecnologias evoluem, também evoluem as ameaças. É verdade que os dispositivos móveis atuais já se assemelham em muito aos computadores desktop[1]. Assim, é natural que riscos que já existiam no mundo desktop também façam parte do mundo móvel. Mas há novas ameaças que são inerentes somente a tecnologia móvel. Com isso, há a necessidade de se adotar novos mecanismos de segurança, de adaptar tecnologias do mundo desktop ao mundo móvel, de criar novas políticas de segurança e de conscientizar os usuários para essa nova tecnologia e novos riscos.

[1] Computadores de mesa

Este trabalho tem como objetivo mostrar as principais tecnologias existentes para a internet móvel e medidas necessárias para garantir a segurança. Em resumo, serão apresentados os capítulos abaixo:

Capítulo 1 – INTRODUÇÃO. Uma breve ressalva na evolução da tecnologia móvel e a necessidade de se investir em segurança;

Capitulo 2 – A INTERNET E AS COMUNICAÇÕES MÓVEIS. Neste capítulo será apresentado um breve histórico da internet até sua convergência para tecnologias móveis.

Capitulo 3 – INTERNET MÓVEL – CONCEITOS BÁSICOS. Neste capítulo serão mostrados os principais conceitos envolvidos na internet móvel.

Capiutlo 4 – SEGURANÇA DA INFORMAÇÃO. Neste capítulo serão apresentados conceitos de segurança da informação e sua importância.

Capítulo 5 – SEGURANÇA NA INTERNET MÓVEL. Neste capítulo serão apresentadas as falhas de segurança existentes na internet móvel, as soluções e práticas existentes.

Capítulo 6 – CONCLUSÃO. Neste capítulo será apresentada a conclusão do trabalho apresentado.

Este trabalho foi realizado utilizando a metodologia de pesquisa bibliográfica. Foram pesquisados assuntos envolvendo internet, tecnologia de dispositivos móveis e segurança da informação.

2 A INTERNET E AS COMUNICAÇÕES MÓVEIS

Neste capítulo, será apresentado um breve histórico sobre a internet e sua evolução para as comunicações móveis.

2.1 HISTÓRICO DA INTERNET

A internet começou a surgir por volta da década de 60 a partir de interesses militares, onde os Estados Unidos temendo um ataque russo aos meios de comunicação, idealizaram um modelo onde as informações poderiam ser distribuídas em vários pontos. Com isso se um ponto fosse atacado, a informação ali não seria perdida, pois ela estaria replicada em outros pontos (MONTEIRO, 2001).

O principal conceito criado nessa época foi a comutação por pacote. Tal conceito consiste em separar os dados em pacotes, onde cada qual possui informações sobre sua origem e destino. Esses dados segmentados percorrem uma rede de um computador a outro até que chegue ao ponto de destino correto (DIAS E SADOK, 2001).

A ARPA (Advanced Project Research Agency), uma agência norte americana, realizou experimentos com comutação por pacotes no ano de 1969. O protocolo de comunicação foi denominado de NCP (Network Control Protocol). Dez anos depois foram inseridos conceitos, como TCP (Transport Control Protocol) e IP (Internet Protocol), uma arquitetura mais sólida utilizada até os dias atuais (DIAS E SADOK, 2001).

Em 1990, surgiu a World Wide Web que possibilitou a popularização da internet. Interfaces gráficas mais ricas, formas de interação mais dinâmicas

foram cativando pessoas rapidamente (MONTEIRO, 2001). Como conseqüência, foram criados milhares de provedores de acesso, browsers, sites de busca e os mais variados portais de serviços. A internet passou a ser imprescindível nas casas das pessoas, em seus computadores pessoais.

2.2 REDES IP

TCP/IP (Transmission Control Protocol/Internet Protocol) é um padrão que possibilita a comunicação eficiente entre computadores, independente de plataforma ou distância (KUROSE E ROSS, 2006). Outros protocolos foram criados na mesma época, no entanto o TCP/IP é o mais conhecido por ser o protocolo base da internet.

Em uma primeira instância o objetivo desse protocolo era fornecer serviços de comunicação que fossem universais, ou seja, uma interface comum entre dispositivos de uma rede, independentemente da arquitetura física. Em uma segunda instância, era interconectar essas redes locais, a uma denominada grande rede, a internet. A figura 1 abaixo ilustra essa conexão de redes.

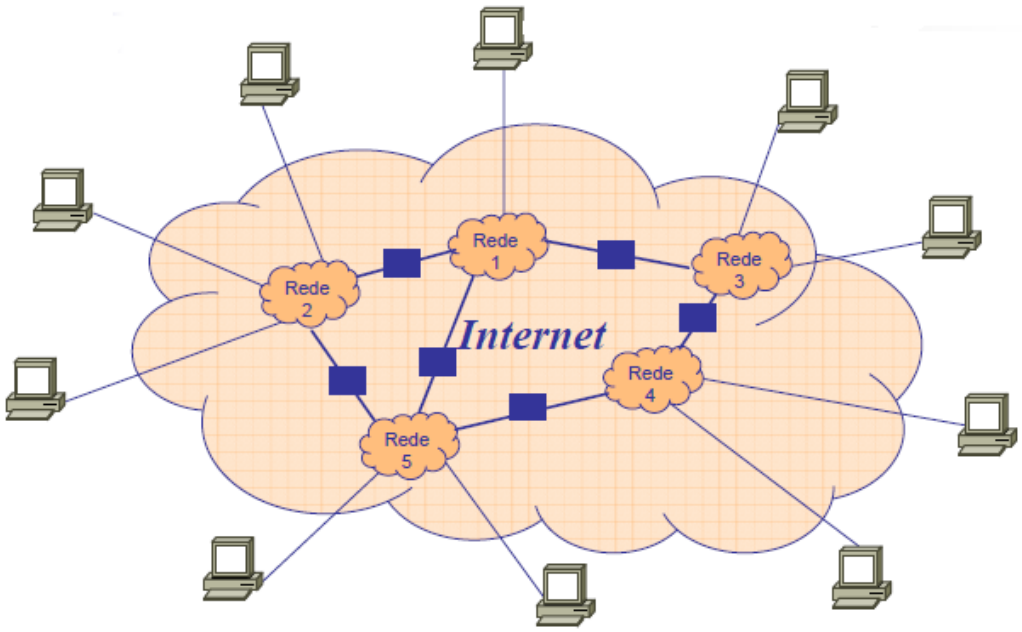

Figura 1: Ilustração das redes interconectadas, a internet.
Fonte: SARGENTO, 2004.

O endereço IP é uma seqüência de números de 32 bits que indica a localidade de um nó em uma rede (KUROSE e ROSS, 2006). Pode ser classificado em IP estático e IP dinâmico.

O IP estático ou fixo é um número permanente associado a um nó, geralmente utilizado para quem disponibiliza algum serviço (KUROSE e ROSS, 2006). Os sites da internet possuem um IP fixo, quando é digitado o nome do site, por exemplo, “www.nome.com.br”, um servidor na internet do seu provedor chamado DNS (Domain Name System), busca o IP associado ao nome e faz o redirecionamento necessário. O IP Estático está cada vez sendo menos utilizado por varias razões, que inclui problemas com segurança.

IP dinâmico é um número gerado por um servidor DHCP (Dynamic Host Configuration Protocol) e associado a um nó no momento em que se conecta a rede (KUROSE e ROSS, 2006). Toda vez em que tenta se reconectar um novo número é gerado.

Um servidor DHCP possibilita que os nós, a partir de seu endereço físico denominado MAC (Media Access Control), recebam as configurações da rede a partir de um servidor central (KUROSE e ROSS, 2006).

Atualmente o protocolo IP está na sua versão 4 o IPv4. Como descrito anteriormente, é um número de 32 bits que permite que seja gerado um grande número de endereços, mas devido a crescente demanda, está se esgotando. Para tentar contornar esse grande problema, foi desenvolvido o IPv6, que aumenta consideravelmente o número de endereços possíveis, utilizando 128 bits (KUROSE e ROSS, 2006). Essa nova versão promete ser mais segura, no entanto, como hoje se trata de uma tecnologia emergente, possui fraquezas que podem ser exploradas por hackers. Softwares devem ser revistos e gerentes de redes têm que se familiarizar com as novas regras desse protocolo para otimizar seus firewalls e outros dispositivos de segurança. Vários sites populares e sistemas operacionais já estão se preparando para dar suporte ao

IPv6. Em resumo o protocolo IPv6 é uma necessidade, promete ser mais rápido e seguro do que a versão anterior o IPv4, mas tem que ser amadurecido. Essa nova tecnologia está sendo implantada gradativamente e deverá coexistir como IPv4 ainda por alguns anos.

2.3 IP MÓVEL

Após a popularização da internet, ocorreu um grande avanço de tecnologia e informática. Computadores portáteis foram cada vez mais sendo utilizados e continuaram a serem melhorados com relação a seu tamanho, peso e capacidade. Junto a tal fato, veio a necessidade de se criar um protocolo que possibilitasse a comunicação entre computadores móveis e outros computadores, visto que os protocolos já existentes nesse período possuíam falhas nesse quesito. Nesse contexto, foi criado o conceito de IP Móvel.

O IP Móvel foi uma proposta da IETF (Internet Engineering Task Force). Tem a premissa de que deve ser independente do meio físico de comunicação e deve permitir que mesmo em deslocamento, a conexão não seja perdida e aplicações não tenham que ser reinicializadas (DIAS E SADOK, 2001). Por esse motivo, ele é utilizado nos sistemas de comunicações móveis atuais.

São definidas duas entidades para dar suporte ao conceito de mobilidade: o HA (Home Agent) e FA (Foreign Agent). O HA é associado à estação móvel de maneira estática e tem como base o endereço IP permanente da estação móvel. Já o FA é associado à estação móvel, baseando-se na localização atual da estação móvel e possui um endereço IP chamado CA (Care of Address). Os pacotes destinados à estação móvel são interceptados pelo HA, encapsulados e enviados ao FA utilizando o IP CA. O FA trata de desencapsular os pacotes os encaminha a estação (DIAS E SADOK, 2001).

Para exemplificar, vamos supor que uma estação móvel tenha se registrado inicialmente em uma rede, sua HN (Home Network). Seu registro em uma FA

também já tenha sido feito e seu respectivo IP CA já tenha sido associado à estação e enviado ao HA. A estação se desloca, e os passos abaixo são executados (DIAS E SADOK, 2001):

- Passo 1 – O Host com IP fixo envia o pacote para o HN da estação móvel;
- Passo 2 – O HA intercepta o pacote e após detectar que a estação móvel não se encontra mais em sua HN, encaminha o pacote para o CA associado à estação móvel pela FN;
- Passo 3 – O pacote é encaminhado para a estação móvel;
- Passo 4 – Quando a estação móvel envia um pacote ao Host com IP fixo, utiliza seu endereço IP registrado na HN como origem e o IP o Host como destino. O roteador encaminha o pacote normalmente, da mesma forma que faria com qualquer outra estação pertencente à FN.

Abaixo, a figura 2 representa os passos acima:

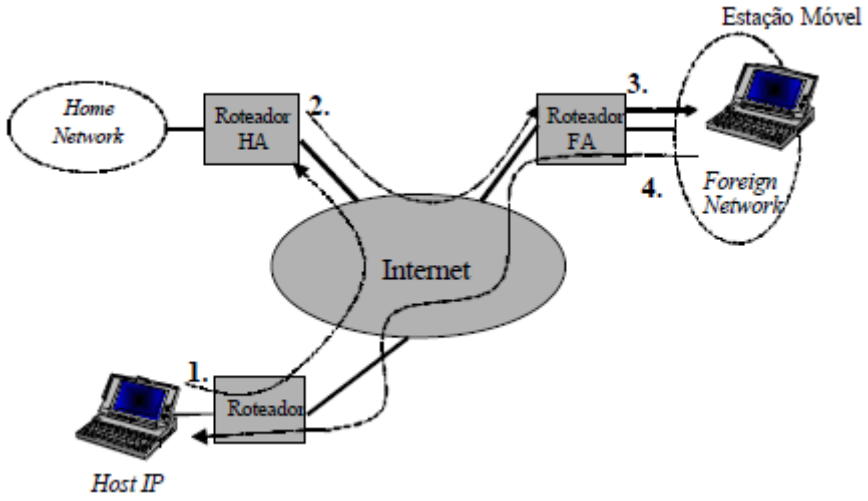

Figura 2: Roteamento com IP móvel
Fonte: DIAS E SADOK, 2001.

Em resumo o IP Móvel soluciona os seguintes problemas:

- Caso uma estação se desloque de um ponto de uma rede a outro sem alterar o seu endereço IP, ela ficará incapaz de receber pacotes em sua nova localização;
- Caso uma estação se mova e altere seu endereço IP, ela precisará terminar e reinicializar qualquer comunicação em andamento.

O IP Móvel soluciona os problemas citados acima de forma segura, robusta e independente do meio físico, sendo altamente eficiente para ser utilizado por toda a Internet.

2.4 EVOLUÇÃO DAS TECNOLOGIAS DE COMUNICAÇÃO PARA CELULARES

Os celulares atualmente podem ser considerados um dos principais meios que popularizaram a internet móvel. A seguir serão apresentadas as principais tecnologias de transmissão de dados e voz para celulares, mostrando sua evolução até os dias atuais.

2.4.1 Primeira geração

As primeiras gerações de serviços para telefonia celular eram analógicas e possuíam problemas como suscetibilidade a interferências e facilidade para clonagem. Surgiram na década de 80 e podem ser citadas as seguintes tecnologias: AMPS (Advanced Mobile Phone System), NMT (Nordic Mobile Telephones) e NTT (Nippon Telephone and Telegraph) (DIAS E SADOK, 2001).

A AMPS foi a mais utilizada e foi proposta pela AT&T em 1971. Possui transmissão em FM (Frequency Modulation) e divide a banda em freqüências de 30 kHz para cada canal. Existem dois tipos de canais nesse sistema, um de controle que coordena o acesso para que o outro canal de rádio seja atribuído

ao telefone e assim seja possível a transferência de sinal de voz (DIAS E SADOK, 2001).

2.4.2 Segunda Geração

A segunda geração de comunicações móveis ou 2G se caracterizou pelo desenvolvimento de tecnologias digitais, que promoveram grandes melhorias em relação a sua geração anterior, como codificação digital de voz, facilidade na comunicação de dados e criptografia. Três grandes sistemas digitais podem ser citados: TDMA, CDMA e GSM.

TDMA (Time Division Multiple Access) foi introduzida em 1990 nos Estados Unidos. Utiliza canais de freqüência divididos em até seis intervalos de tempos diferentes, cada um desses intervalos é utilizado por um usuário a fim de evitar interferências. Cada canal é subdividido em duas faixas de freqüência de 30 kHz, uma de ida, da célula para o telefone, e outra de volta, do telefone para célula (DIAS E SADOK, 2001).

CMDA (Code Division Multiple Access) foi utilizada comercialmente pela primeira vez em 1995. Permite o acesso simultâneo de muitos usuários em um canal, proporcionando uma maior capacidade na rede. Esse sistema espalha cada sinal com um código pseudo-aleatório que identifica cada canal de comunicação. Assim, cada telefone celular pode reconhecer seu respectivo sinal na rede através desse código. Uma das desvantagens dessa tecnologia é a certa facilidade para clonagem (DIAS E SADOK, 2001).

GSM (Global System for Móbile Communication) surgiu também na década de 90. Padrão desenvolvido na Europa e adota em boa parte do mundo tendo a maior cobertura das tecnologias de segunda geração. Utiliza uma rede digital com suporte a uma variedade de serviços denominado ISDN (Integrated

Services Digital Network). Nesse sistema, cada canal de rádio possui faixa de 200 kHz e é dividido em oito intervalos de tempo para evitar interferências.
A grande diferença do GSM é o módulo para identificação do usuário denominado SIM (Subscriber Identification Module), possibilitado através do uso de cartões de memória (“chips”) (DIAS E SADOK, 2001).

2.4.3 Terceira geração

O padrão 3G veio para substituir a tecnologia 2G devido à necessidade de maior velocidade de conexão e para oferecer uma gama maior de serviços. Nessa geração ocorreu uma maior popularização da internet móvel, pois ela permitiu o acesso em tempo real da internet a partir de qualquer localidade. O grande impulsionador para esse avanço foi a introdução da comutação por pacotes para transmissão de dados. Abaixo, serão vistos em maiores detalhes os principais padrões dessa geração: GPRS e UMTS.

2.4.3.1 GPRS

Considerada por alguns uma tecnologia de transição da 2G para a 3G, GPRS (General Packet Radio Service) é um padrão desenvolvido para comutação de pacotes em redes GSM, proposto pelo ETSI (European Telecommunications Standards Institute) (DIAS E SADOK, 2001). Possibilitou criação de novos serviços para telefonia móvel e maior eficiência na transmissão de dados.

A tecnologia 2G utilizava comutação por circuitos, onde recursos de rádio eram alocados por um usuário durante toda a chamada. Já no GPRS os recursos de rádio são alocados e distribuídos somente durante a vida dos pacotes IP. A estrutura de rede no GPRS pode ser introduzida na rede GSM inserindo dois novos tipos de nós: SGNS e GGSN (DIAS E SADOK, 2001). A figura 3 abaixo representa uma macro estrutura da rede GPRS.

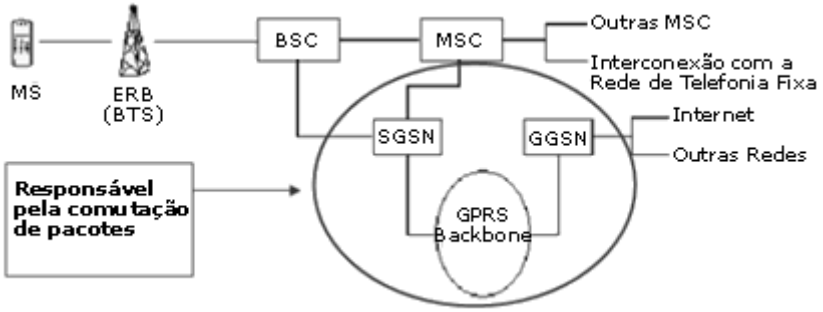

Figura 3: Rede GPRS
Fonte: TELECO, 2005.

GGSN (Gateway GPRS Support Node) é o nó que faz a comunicação entre redes de dados IP externas e o *backbone*[2] do GPRS. Pode possuir firewalls e mecanismos de filtragem (DIAS E SADOK, 2001).

SGNS (Serving GPRS Support Node) é que realiza a comunicação entre o *backbone* e a rede de rádio. Dentre as tarefas que ele executa pode-se citar: autenticação, gerenciamento de sessão e gerenciamento de mobilidade (DIAS E SADOK, 2001).

2.4.3.2 UMTS

UMTS (Universal Mobile Telecommunications System) foi desenvolvido pelo Third Generation Partnership Project (3GPP) e lançado inicialmente no Japão em 2002. Seu foco inicial era transmitir conversações de vídeo conferências, que mais tarde mudou para acesso a World Wide Web (GUEDES e VASCONCELOS, 2009).

> O padrão UMTS também prevê o tráfego de diferentes mídias sobre um mesmo canal. Ao contrário do padrão ADSL (Asymmetric Digital Subscriber Line), que apresenta limites

[2] Ou “espinha dorsal”, é a rede pela qual os dados de todos os clientes da internet passam.

> diferentes para as taxas de upload e download, o padrão UMTS usa bandas de mesma capacidade para upload e download. Isso o torna melhor adaptado para a realização de serviços como conversas em tempo real com vídeo, telefonia, entre outros (GUEDES e VASCONCELOS, 2009).

Podem ser citados dois principais protocolos para a tecnologia UMTS: W-CDMA E HSPA.

W-CDMA (Wideband Code Multiple Access) é um protocolo que provê taxas de transmissão de até 2 Mbits/s. Oferece tempos de latência muito menores e uma conexão mais eficiente. O custo por bits transmitido é mais baixo, o que permite suportar maior volume de dados e usuários (GUEDES e VASCONCELOS, 2009).

HSPA (High Speed Packet Access) pode ser considerado um avanço para tecnologia UMTS. É a junção de duas melhorias: na taxa de download o HSDPA e na taxa de upload o HSUPA.

HSDPA (High Speed Downlink Packet Access) reduz a latência e permite atingir velocidades de download de até 14,4 Mbits/s. As seguintes melhorias podem ser citadas nesse sistema (GUEDES e VASCONCELOS, 2009):

- Um menor Intervalo no tempo de transmissão, que implica em tempos de resposta menores e alocação de recursos mais ágil;
- Escalonamento rápido de pacotes que faz com que a rede se adapte às variações de qualidade e disponibilidade;
- Modulação e codificação adaptativas que também é uma adaptação da rede quanto à variação da qualidade de sinal e que pode dobrar as taxas de transmissão;
- Rápida retransmissão de pacotes com erros.

HSUPA (High Speed Uplink Packet Access) é um avanço na taxa de upload que possui as seguintes melhorias (GUEDES e VASCONCELOS, 2009):

- Retransmissão rápida de pacotes com erro;

- Menor intervalo no tempo de transmissão;
- Canal dedicado para upload;
- Escalonamento rápido de pacotes.

2.4.4 Quarta geração

Atualmente a tecnologia 4G ainda está em período de implantação e testes em alguns países. Desenvolvida pela Third Generation Partnership Project (3GPP), possui taxas de transmissão bem superiores a tecnologia 3G e baseia-se totalmente no padrão IP, o protocolo principal da internet (GUEDES e VASCONCELOS, 2009). Promete uma experiência de utilização bem mais próxima a que se tem com a internet fixa atual. Dentre os padrões principais dessa geração podemos citar o LTE.

LTE (Long Term Evolution) introduz melhorias de desempenho possibilitando uma maior disseminação de serviços móveis. Baseia-se no padrão IP e com isso a transmissão de voz é feita principalmente através da tecnologia VoIP (Voice over Internet Protocol) (GUEDES e VASCONCELOS, 2009).

Segundo Guedes e Vasconcelos (2009), podem-se citar alguns aspectos centrais do sistema LTE:

- Nova interface aérea baseada na tecnologia OFDM (Orthogonal Frequency Division Multiplexing) que possibilita alcançar altas taxas de transmissão de dados e menor consumo de energia;
- Com a intenção de aumentar a confiabilidade e capacidade dos serviços de banda larga, ao enviar dados através de diferentes caminhos, cujos sinais ocupam a mesma freqüência, a tecnologia LTE utiliza a técnica MIMO (Multiple Input Multiple Output);
- Possui eficiência no uso do espectro para suportar maior número de usuários;
- O alcance de rádio se mostra eficaz em células com raio de até 30 km;

- A interatividade pode ser maior uma vez que o tempo de transmissão de ida e volta passa a ser reduzido, o que pode impulsionar serviços de tempo real de alta qualidade;
- Possui arquitetura simplificada, interfaces abertas e possui a tecnologia EPC (Evolved Packet Core), uma importante ferramenta para comunicação com diferentes redes, garantindo uma maior compatibilidade com outros sistemas.

3 INTERNET MÓVEL – CONCEITOS BÁSICOS

Neste capítulo serão apresentados alguns conceitos relacionados ao desenvolvimento de aplicativos para dispositivos móveis, sistemas operacionais existentes e conceitos relacionados à internet móvel.

3.1 DESENVOLVIMENTO DE APLICATIVOS

O avanço das redes de comunicação e dos dispositivos móveis possibilitou um grande crescimento para a internet móvel. Com isso, o desenvolvimento de aplicativos aumentou consideravelmente, porém com algumas limitações, novos problemas e com isso novas soluções.

Atualmente o ecossistema de desenvolvimento e as ferramentas utilizadas para a web móvel não são tão diferentes da web tradicional, na verdade somente são acrescentadas novas ferramentas. Por exemplo, vamos supor que uma equipe de desenvolvimento utilize o seguinte ambiente: ferramenta gráfica de programação, ferramenta de controle de versão de código e banco de dados. Para web móvel seria incluído apenas um ambiente de teste diferente, que envolve vários aparelhos de celular ou uma máquina virtual para simular o ambiente.

Notadamente, ainda hoje existem diferenças entre os navegadores para dispositivos móveis, um exemplo, são os navegadores do Blackberry ou então o Internet Explorer Mobile, que insistem em não seguir os padrões. No entanto, pode se dizer que há uma tendência a serem adotados certos padrões, cada

vez mais próximos a web tradicional, visto que grandes empresas voltadas para dispositivos móveis, estão adotando navegadores como Safari e Chrome.

Contudo, ainda hoje, é fato que há uma diversidade muito grande no desenvolvimento de aplicativos para dispositivos móveis. Cada grande fabricante possui um sistema operacional cujos aplicativos não são compatíveis com outros sistemas operacionais. E pior, em alguns casos, os aplicativos são desenvolvidos especificamente para determinados tipos de aparelhos, não funcionando corretamente em outros, mesmo possuindo o mesmo sistema operacional.

A seguir serão apresentadas algumas linguagens de programação para dispositivos móveis e uma breve descrição de cada uma delas.

3.1.1 WML

Wireless Markup Language é uma das linguagens mais antigas para dispositivos móveis, voltada para desenvolvimento de aplicativos WAP. Baseada no padrão XML (Extensible Markup Language), foi designada para exibir textos em dispositivos monocromáticos com uma memória e poder de processamento limitados (FREDERICK E LAL, 2009).

O WML chegou a sua versão 1.3 que introduziu suporte a imagens coloridas, mas devido à evolução dos dispositivos e meios de comunicação, é considerada obsoleta.

3.1.2 HTML e XHTML

HTML (HyperText Markup Language) é a linguagem de marcação padrão na Web. Vários navegadores para dispositivos móveis suportam o conjunto

completo de tags HTML, mas podem não ter a mesma experiência de navegação de navegadores para computadores pessoais, devido a fatores como resolução de tela, largura de banda e armazenamento.

XHTML (Extensible HyperText Markup Language) combina o conjunto de tags HTML com a sintaxe rígida do XML. O XHTML é a melhor escolha de marcação para os navegadores móveis com capacidade HTML (FREDERICK E LAL, 2009).

3.1.3 XHTML-MP

Especificado pela Open Mobile Alliance, o XHTML perfil móvel ou MP (Mobille Profile) é uma linguagem de marcação derivada do XHTML, amplamente utilizada para os dispositivos móveis (FREDERICK E LAL, 2009).

Uma das grandes vantagens dessa linguagem é sua similaridade com a linguagem HTML para Web tradicional. Uma página desenvolvida em XHTML-MP pode também ser visualizada em navegadores de computadores pessoais tradicionais.

3.1.4 Java ME

Java Micro Edition é um conjunto de tecnologias e especificações que têm como objetivo criar e suportar o desenvolvimento de aplicativos para dispositivos móveis (ORACLE, 2011).

Uma das grandes vantagens dessa tecnologia é a possibilidade de rodar em qualquer tipo de ambiente, sendo por isso extremamente vantajosa para dispositivos móveis.

3.2 SISTEMAS OPERACIONAIS

Durante a evolução do mercado móvel, houve uma grande diversidade de sistemas operacionais para dispositivos móveis. Alguns fabricantes optavam por adotar sistemas próprios, otimizados para seus dispositivos. No entanto, atualmente existem alguns sistemas operacionais que estão se tornando mais populares e adotados por boa parte do mercado. Abaixo serão listados alguns dos principais sistemas.

3.2.1 IOS

Em 2005, Steve Jobs iniciou negociações com a Cingular (atualmente AT&T) o que lhe daria o direito de exclusividade dentre as operadoras de telefonia para o Iphone. No início de 2006, a Apple iniciou um processo de desenvolvimento para o Iphone OS (IOS) se baseando no sistema operacional já existente, o OSX. Em janeiro de 2007, o novo sistema operacional foi lançado com o Iphone na Macworld Conference & Expo, uma feira anual em que a Apple exibe seus produtos e novidades de cada temporada (WOOLEY, 2010).

Em um primeiro momento, Steve Jobs permitiu que apenas aplicações web fossem desenvolvidas por terceiros. No entanto, apesar de existirem mais de 200 aplicações web para o Iphone e após fortes pressões do público, em outubro de 2007 foi anunciado o desenvolvimento de um SDK (Software Development Kit), que permitiria o desenvolvimento de aplicações nativas. Em março de 2008, um primeiro beta do SDK foi lançado (WOOLEY, 2010).

Com o Iphone, a Apple trouxe várias inovações importantes que ajudaram a popularizar ainda mais a internet móvel. Suas novas interfaces, hardware bem resolvido e seu sistema operacional simplificado, revolucionaram o mercado de smartphones e se tornou um dos aparelhos mais desejados e vendidos no mundo.

3.2.2 Android

A Google adquiriu a Android Inc. em 2005 para iniciar o desenvolvimento da plataforma Android (HASHIMI; KOMATINENI; MACLEAN, 2010). Em meio a uma diversidade de sistemas operacionais já existentes, a plataforma da Google veio prometendo características como flexibilidade, código aberto, de fácil migração para as fabricantes e disponibilização de frameworks para desenvolvimento.

O sistema operacional foi proposto especificamente para dispositivos móveis. É baseado na plataforma Linux para gerenciamento de periféricos, memória e processos. A Google disponibiliza um framework para desenvolvimento baseado na linguagem Java, chamado Android SDK (Software Development Kit) (HASHIMI; KOMATINENI; MACLEAN, 2010).

Por volta de 2007, vários membros relacionados à indústria de dispositivos móveis se juntaram para formar a Open Handset Alliance, uma aliança com a intenção de criar padrões para telefonia móvel. Dentre eles podemos citar: Sprint Nextel, Motorola, T-Mobile, Samsung, Sony Ericson, Toshiba, Vodafone, Google, Intel e Texas Instruments (HASHIMI; KOMATINENI; MACLEAN, 2010).

Atualmente é um dos sistemas operacionais para dispositivos móveis mais utilizados e possui uma vasta lista de aplicativos no Android Market. Abaixo, a figura 4 representa o logotipo do Android.

Figura 4: Logotipo Android
Fonte: ANDROID, 2011.

3.2.3 Simbian

O Symbian é um sistema operacional desenhado especialmente para ambientes wireless e dispositivos móveis. Começou com a Psion, uma empresa inglesa fabricante de computadores de mão, e atualmente é mantida pela Nokia, empresa finlandesa de telecomunicações.

Propõe uma plataforma aberta para desenvolvimento de aplicações, suportando linguagens como C++ e Java. Possui vários kits para desenvolvimento como os citados abaixo (DELALANDE, 2007):

- Symbian OS Customization Kit, cujo objetivo é facilitar a integração no código;
- Symbian OS Development Kit, tipo de Super SDK, suportando qualquer tipo de desenvolvimento.

O sistema operacional Symbian também é amplamente utilizado para dispositivos móveis, dividindo mercado com outros grandes nomes como o Android e IOS.

3.3 SMS

SMS (Short Message Service) surgiu por volta de 1991 na Europa e permite que usuários de telefonia móvel enviem e recebam mensagens de texto (DIAS e SADOK, 2001).

> O SMS ponto a ponto provê um mecanismo para transmissão de e para terminais móveis sem fio. O serviço utiliza um centro de SMS (SMSC – Short Message Service Center) que atua como um sistema store and foward para mensagens curtas. A rede sem fio provê o transporte das mensagens entre o SMSC e o terminal móvel (DIAS E SADOK, 2001).

Nesse serviço a entrega de mensagens é garantida pela rede. As falhas de rede, quando são identificadas, ocasionam o armazenamento das mensagens até que o destino esteja novamente disponível.

3.4 WAP

> O WAP é um padrão para aplicações de ambientes sem fio desenvolvido pelo WAP Forum, uma organização fundada em junho de 1997 pela Ericsson, Motorola, Nokia e Unwired Planet. O objetivo básico do WAP Forum é trazer diversos conteúdos da Internet (páginas Web, push services) e outros serviços de dados (stock quotes) para os telefones celulares digitais e outros terminais móveis sem fio, como: PDAs (Personal Digital Assistants) e Laptops (DIAS E SADOK, 2001).

A tecnologia WAP faz uso de uma estrutura similar a Web convencional. Para permitir o acesso sem fio ao espaço de informação oferecido pela WWW, o modelo WAP baseia-se em tecnologias bem conhecidas da Internet, mas que foram otimizadas de modo a levar em consideração as restrições de um ambiente sem fio.

Devido à evolução das tecnologias de transmissão e dispositivos móveis, o WAP está se tornando ultrapassado, dando lugar a tecnologias cada vez mais próximas as existentes para computadores pessoais.

3.5 BLUETOOTH

Bluetooth é uma tecnologia de comunicação por ondas de rádio, sem fio e para pequenas distâncias. Surgiu por volta de 1994. Inicialmente desenvolvida pela Ericsson com o objetivo de conectarem celulares a outros acessórios como, por exemplo, fones de ouvido sem fio (CHEDE, 2002).

Essa tecnologia foi criada para ser universal e funcionar em qualquer lugar do mundo. Por esse motivo foi adotada uma freqüência de rádio aberta, a faixa ISM (Industrial, Scientific, Medical) que opera na freqüência entre 2,4 GHz e 2,5 GHz (BLUETOOTH, 2011).

Para atender as mais variadas necessidades dos dispositivos o alcance do Bluetooth foi dividido em três classes (BLUETOOTH, 2011):

- Classe 1: potência máxima de 100 mW, alcance de até 100 metros;
- Classe 2: potência máxima de 2,5 mW, alcance de até 10 metros;
- Classe 3: potência máxima de 1 mW, alcance de até 1 metro.

4 SEGURANÇA DA INFORMAÇÃO

A seguir será destacada a importância da segurança da informação, as vulnerabilidades existentes e mecanismos para controle da segurança.

4.1 IMPORTÂNCIA DA INFORMAÇÃO

A informação é um recurso que move o mundo. No mundo corporativo a informação é um bem, tem valor para a empresa e deve ser protegida. Políticas e regras devem ser criadas para proteger a informação, da mesma maneira que recursos financeiros e materiais são tratados dentro da empresa. Através do uso dos sistemas computacionais, a informação pode ser manipulada e visualizada de diversas maneiras. Pode circular pelos mais variados ambientes, percorrendo diversos fluxos, pode ser armazenada para vários fins, possibilitando ela ser lida, modificada ou até mesmo apagada.

A segurança da informação existe para minimizar os riscos do negócio em relação à dependência do uso dos recursos da informação para o funcionamento da organização. Sem a informação ou com uma incorreta, o negócio pode ter perdas que comprometam o seu funcionamento e o retorno de investimento dos acionistas (FONTES, 2006).

A segurança da informação não se refere somente a restringir seu acesso, segundo Fontes (2006, p.11), os pontos básicos que devemos tratar nesse assunto estão descritos abaixo:

- Disponibilidade: deve estar sempre disponível para usuários autorizados ao acesso;
- Integridade: manter as características originais e garantir o ciclo de vida da informação;

- Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para realização de suas atividades profissionais. Para tanto, deve existir uma autorização prévia;
- Legabilidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como os princípios éticos seguidos pela organização e desejados pela sociedade;
- Auditabilidade: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação;
- Não repúdio a auditoria: o usuário que gerou ou alterou a informação não pode negar o fato, pois existem mecanismos que garantem sua auditoria.

A figura 5 abaixo representa a relação entre esses pontos para obtenção da segurança da informação:

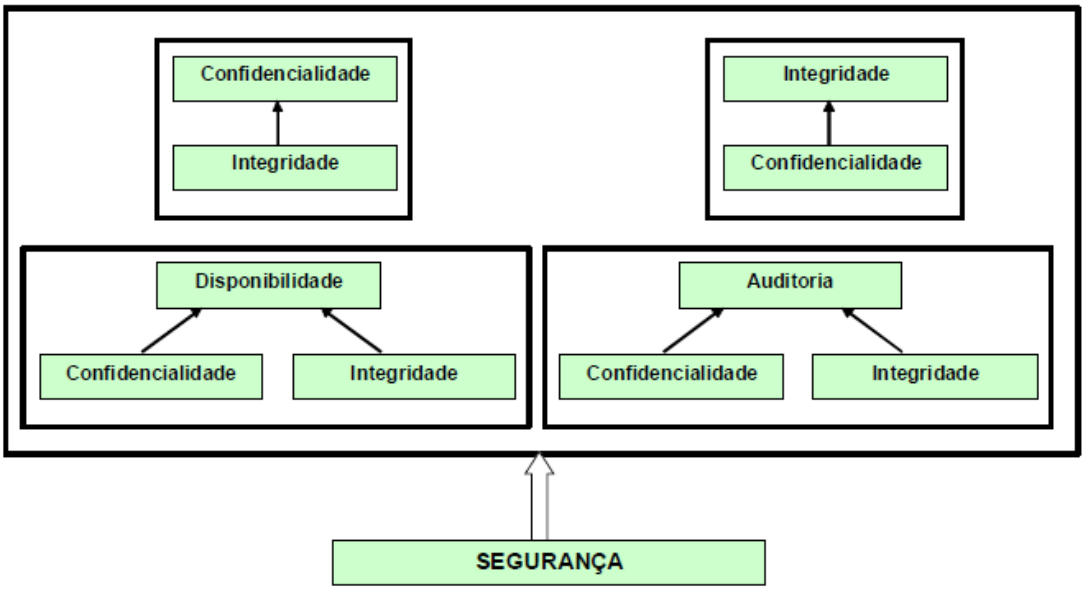

Figura 5: Pontos da segurança da informação
Fonte: LAUREANO, 2005.

4.2 CICLO DE VIDA DA INFORMAÇÃO

O ciclo de vida da informação é composto por fases em que podem ser identificados riscos quanto à sua segurança (LAUREANO, 2005). A figura 6 abaixo representa as quatro fases desse ciclo:

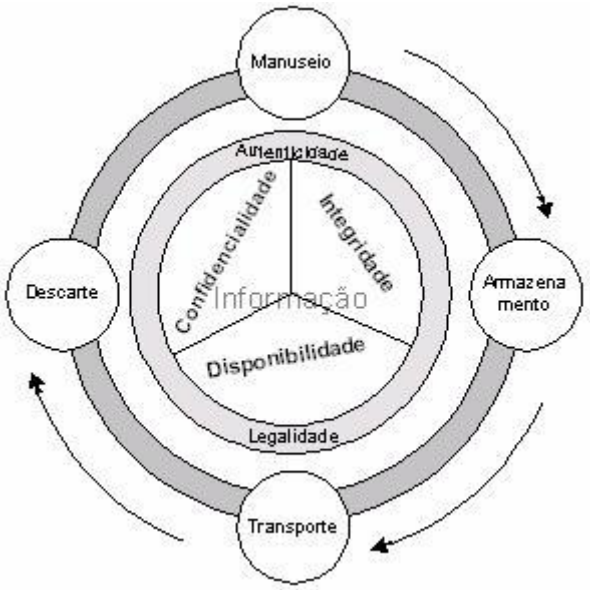

Figura 6: Ciclo de vida da informação
Fonte: LAUREANO, 2005.

- **Manuseio**: fase em que a informação é criada e manipulada;
- **Armazenamento**: a informação é armazenada para garantir a preservação dos dados. Pode ser feita através de banco de dados ou outro tipo mídia que poderá ou não aumentar a complexidade quanto à sua conservação;
- **Transporte:** fase em que a informação é transportada, podendo, por exemplo, ser por correio eletrônico ou até mesmo fax;

- **Descarte:** quando a informação fica obsoleta ela pode ser descartada. No entanto, não pode ser feita sem dar importância à segurança, para garantir que dados confidenciais não sejam recuperados.

4.3 VULNERABILIDADES À SEGURANÇA

As ameaças à segurança da informação podem vir de diferentes formas. Sistemas de informação, banco de dados e redes de computadores são alguns dos pontos que podem conter fragilidades. Para se obter segurança em uma aplicação web devem ser observados quatro elementos (SANTO, 2010):

- Segurança na estação: a estação de trabalho (cliente) é um dos pontos mais vulneráveis. Elas podem armazenar informações importantes muitas vezes sem proteção ou controle de acesso. Também estão sujeitas a vários tipos de malware;
- Segurança no transporte: a segurança no transporte da informação envolve tecnologias como a criptografia. A criptografia mascara a informação na tentativa de impedir que a informação seja reconhecida e utilizada por invasores;
- Segurança no servidor: para controlar a segurança dos servidores internos torna-se necessário o uso de firewalls que protegem o acesso através de um servidor de controle em um ponto único de acesso. O uso de firewall controla os serviços e acessos permitidos, monitora o uso e tentativas de violação e protege contra invasões externas;
- Segurança na rede: um grande número de riscos à segurança pode existir nas redes internas. As medidas abaixo podem ser tomadas para minimizar esses riscos:
    - Adotar uma política de segurança com definições das normas, diretrizes, padrões e procedimentos a serem seguidos;
    - Criar programas de treinamento e capacitação quanto à segurança;
    - Adotar ferramentas de segurança;

- Efetuar monitoração constante da intranet e realizar auditorias.

4.4 MECANISMOS PARA CONTROLE DA SEGURANÇA

Existem vários mecanismos que podem ser adotados para minimizar os riscos com segurança. Abaixo são listados alguns deles segundo Laureano (2005).

4.4.1 Autenticação e autorização

A autenticação é um serviço essencial para a segurança, pois assegura o controle de acesso e determina quem está autorizado a ter acesso à informação, além de facilitar a auditoria.

A autorização é o processo de conceder ou negar permissões a usuários ou sistemas. Dessa forma pode se ter o controle de quais atividades podem ser realizadas para cada um dos envolvidos.

4.4.2 Firewall

“Um firewall é um sistema (ou grupo de sistemas) que reforçam a norma de segurança entre uma rede interna segura e uma rede não-confiável como a Internet” (LAUREANO, 2005, p.21).

A função do firewall é permitir que informações confiáveis passem, negar serviços vulneráveis e proteger a rede interna de ataques externos. Porém, devido á possibilidade de sempre estar surgindo novas ameaças, o administrador da rede deve monitorar constantemente os eventos e alarmes gerados pelo firewall e, se necessário realizar ajustes. A figura 7 abaixo, ilustra a função do firewall.

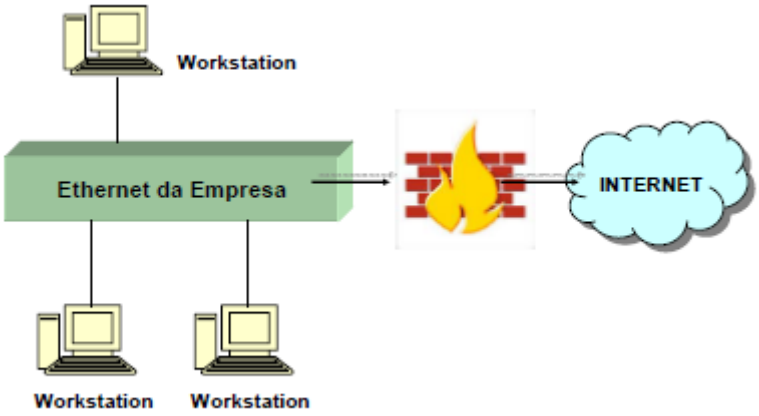

Figura 7: Firewall
Fonte: LAUREANO, 2005.

4.4.3 Detector de intrusos

Conhecida também por IDS (Intrusion Detection System), a tecnologia de detecção de intrusão tenta reconhecer um comportamento ou uma ação intrusiva, para alertar um administrador ou até mesmo disparar contramedidas automaticamente. Para realizar a detecção, são empregadas técnicas como análise estatística, inteligência artificial e data mining (LAUREANO, 2005).

4.4.4 Criptografia

> A palavra criptografia tem origem grega (kriptos = escondido, oculto e grifo = grafia,escrita) e define a arte ou ciência de escrever em cifras ou em códigos, utilizando um conjunto de técnicas que torna uma mensagem incompreensível, chamada comumente de texto cifrado, através de um processo chamado cifragem, permitindo que apenas o destinatário desejado consiga decodificar e ler a mensagem com clareza, no processo inverso, a decifragem (LAUREANO, 2005, p.25).

A criptografia das informações pode ocorrer desde o seu armazenamento até o seu transporte para que haja uma comunicação segura. Uma tecnologia de destaque existente é a chamado VPN (Virtual Private Networks), que permite a formação de redes virtuais seguras utilizando protocolos com criptografia como o SSL (Secure Sockets Layer). A figura 8 abaixo ilustra a função de proteção na comunicação entre redes através de uma VPN.

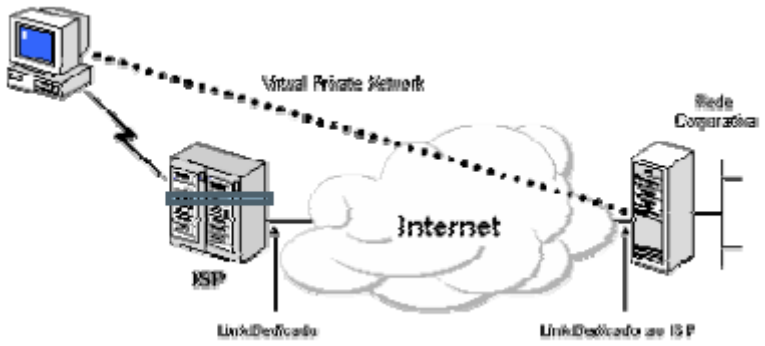

Figura 8: VPN
Fonte: LAUREANO, 2005.

4.5 A QUESTÃO HUMANA NA SEGURANÇA DA INFORMAÇÃO

O usuário desempenha um papel fundamental na segurança da informação. Podemos comparar sistemas de segurança da informação como sendo uma corrente com vários elos, onde cada um corresponde aos componentes envolvidos como software, protocolos de comunicação e usuários (SILVA E STEIN, 2007). O componente humano com certeza pode ser considerado o componente ou o elo mais fraco dessa corrente.

Do que adianta gastar milhões em recursos como firewalls, mecanismos de criptografia e dispositivos, se não há conscientização por parte dos usuários. Deve-se definir planos de tratamento de riscos, que podem incluir a instalação de ferramentas, treinamentos, campanhas de conscientização, criação de procedimentos de trabalho.

Durante todo o ciclo da informação, existe a interferência de um ser humano e se torna necessário garantir a confiabilidade humana nas partes envolvidas. No contexto da engenharia, a confiabilidade humana é a probabilidade de que um humano execute corretamente uma tarefa designada em um tempo especificado, durante um período de tempo definido em um ambiente também especificado (LAUREANO, 2005).

5 SEGURANÇA NA INTERNET MÓVEL

A segurança sempre é um fator importante para empresas ou pessoas, seja qual for o ambiente móvel ou não. Toda empresa deseja que seus dados estejam sob controle e protegidos, para que prejuízos provenientes do seu mau uso não sejam gerados. Uma pessoa, que confia seus dados pessoais em um dispositivo ou até mesmo tente acessar dados bancários através de seu celular, também quer se sentir segura realizando tais atividades. Para minimizar tais riscos com segurança, é necessário identificá-los e implantar medidas de segurança.

Esse capítulo mostra alguns possíveis ataques existentes na internet móvel, contramedidas e recomendações de segurança.

5.1 TIPOS DE ATAQUE NA INTERNET MÓVEL

Nos últimos anos a internet móvel evoluiu rapidamente e atualmente as tecnologias existentes para acesso a internet são praticamente as mesmas dos computadores pessoais. Assim, é natural que os perigos já existentes em um, passem também a pertencer ao outro. É claro, devido a alguma diferenças de arquitetura, sistemas operacionais e dispositivos, existem alguns riscos que são inerentes ao mundo móvel. Abaixo são listados alguns tipos de ataques existentes na internet móvel e possíveis contramedidas.

5.1.1 Mixed identity attack

Todo usuário de telefonia móvel possui uma identificação, onde o mesmo realiza um processo de autenticação toda vez que utiliza serviços da rede. Após ser registrado na rede, recebe seu perfil e acesso aos serviços

disponíveis para o mesmo. Se um usuário utilizar a identificação de outro ele poderá acessar e usufruir dos recursos da rede e as devidas cobranças recairão sobre o outro usuário (STRACCIALANO, 2008). A figura 9 abaixo mostra como pode ser feita essa troca de identidade entre usuários.

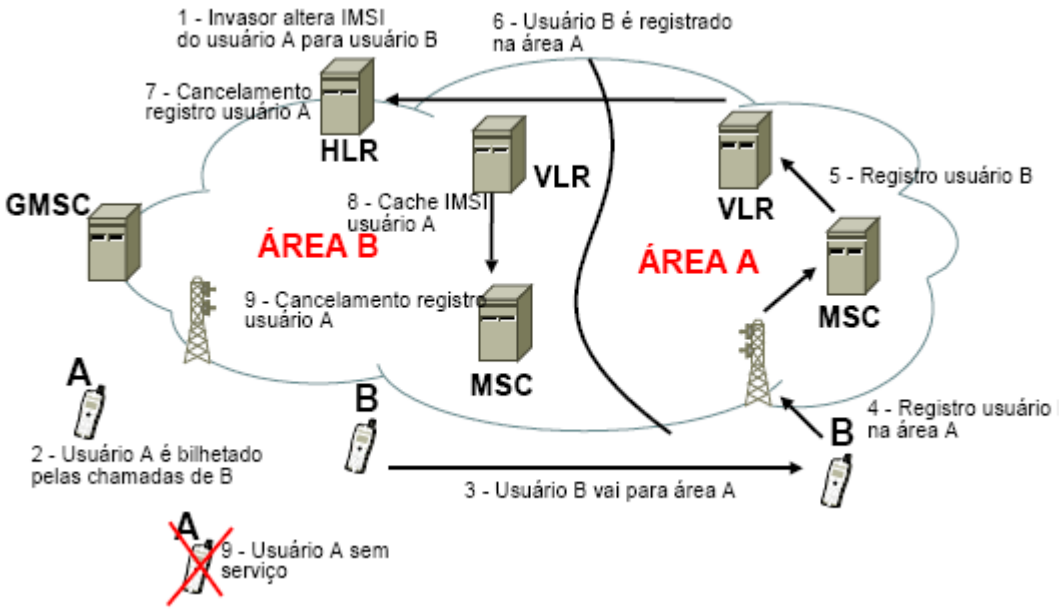

Figura 9: Mixed Identity Attack
Fonte: STRACCIALANO, 2008.

Como medida de segurança, em redes UMTS, são adotados mecanismos de identificação e autenticação que utilizam os elementos abaixo:

- RAND: número aleatório;
- XRES: resposta de autenticação;
- Ck: chave de ciframento;
- Ik: chave de integridade;
- AUTN: token de autenticação.

O processo de autenticação entre o usuário e a rede ocorre da seguinte forma (STRACCIALANO, 2008):

- Encaminhamento pela VLR/SGSN requisição autenticação para a HLR
- Resposta da requisição fornecida pela HLR

- Armazenamento pelo VLR/SGSN vetores de autenticação
- Encaminhamento da VLR/SGSN para o terminal da requisição de autenticação (RANDi) + AUTN(i)
- Verificação do AUTN(i)e geração do RES(i) pelo terminal
- Terminal envia a resposta RES(i) para a VLR/SGSN
- VLR/SGSN compara a RES(i) e XRES(i)
- Terminal gera a CK(i) and IK(i) e VLR/SGSC seleciona para uso.

5.1.2 Cross Site Scripting

Também conhecido como XSS, permite que scripts indesejados sejam executados nos navegadores. Com isso, conteúdos podem ser inseridos no sites, informações pessoais podem ser roubadas e o navegador pode ser controlado através de scripts (OWASP, 2007).

Existem três tipos de ataque XSS: refletido, armazenado e inserção DOM (Document Object Model).

No XSS refletido é adicionado um script que reflete os dados inseridos pelo usuário como retorno direto a ele (OWASP, 2007). Ocorre quando os dados são renderizados sem codificação e não há filtragem na resposta.

O tipo de XSS armazenado persiste os dados juntamente com o script malicioso em um arquivo ou base de dados (OWASP, 2007). Assim quando a vítima requisita a informação armazenada o script pode ser executado.

No XSS baseado em DOM, o código dinâmico presente na página requisitada, que pode ser em Javascript, é manipulado para efetuar o ataque. Pode ser persistente ou não (OWASP, 2007).

Para diminuir os riscos com ataques XSS é necessário que todos os parâmetros da aplicação sejam validados ou codificados de alguma forma. Na

validação de entrada devem ser utilizados mecanismos padrões de validação de entrada para validar todas as entradas quanto ao tamanho, tipo, sintaxe e regras de negócio antes de aceitar que o dado seja mostrado ou armazenado. Na codificação deve ser garantido que qualquer dado de entrada do usuário esteja apropriadamente codificado (tanto para HTML ou XML dependendo do mecanismo de saída) antes da renderização, usando a abordagem de codificação de todos os caracteres (OWASP, 2007).

5.1.3 Falhas de injeção

Esse tipo de ataque ocorre quando há a possibilidade de enviar comandos ou consultas através de formulário de dados do aplicativo web. Com falhas de injeção é possível ler, atualizar e até mesmo excluir dados.

Para tentar evitar as falhas de injeção é necessário verificar se as aplicações, quando disponibilizadas aos usuários, não permitem que os dados enviados sejam modificados para executar comandos maliciosos pelos interpretadores do sistema. No mercado existem ferramentas automatizadas para verificar se há falhas de injeção, principalmente de SQL (Structured Query Language) (OWASP, 2007).

Um método para evitar injeções, consiste no uso de bibliotecas seguras, como por exemplo, consultas parametrizadas e mapeamento objeto relacionado.

5.1.4 Referência insegura direta a objeto

> Uma referência direta a um objeto acontece quando um desenvolvedor expõe uma referência a um objeto de implementação interna, como por exemplo, um arquivo, diretório, registro na base de dados ou chave, uma URL ou um parâmetro de um formulário. Um atacante pode manipular

> diretamente referências a objetos para acessar outros objetos sem autorização, a não ser que exista um mecanismo de controle de acesso (OWASP, 2007).

Para minimizar esse ataque deve-se evitar a exposição direta a referência de objetos, utilizando índices ou outro método indireto. Deve ser criado um padrão para referenciar objetos, que seja fácil de validar e também deve ser verificada a autorização para acesso aos mesmos.

5.1.5 Cross Site Request Forgery (CSRF)

Esse tipo de ataque ocorre quando ações maliciosas são executadas como resultado do envio de scripts a partir de outro usuário logado na aplicação web. As vulnerabilidades podem ocorrer nos seguintes casos:

- Quando não são feitas verificações para ações vulneráveis;
- Caso a aplicação execute ações no envio de uma requisição de autenticação padrão;
- Se forem autorizadas requisições baseadas em credenciais que são automaticamente submetidas, como por exemplo, *cookies*[3].

Para minimizar os riscos devem ser realizadas as medidas abaixo (OWASP, 2007):

- As vulnerabilidades XSS devem ser minimizadas;
- Inserir tokens[4] randômicos em todos os formulários do sistema e quando for submetido deve ser verificado se está correto para o usuário corrente;
- Não utilizar requisições via URL (Universal Resource Locator) para dados importantes;

---

[3] Dados persistidos em arquivos, que são utilizados com freqüência por um aplicativo web.

[4] Conjuntos de caracteres que formam um padrão e possui um significado coletivo.

5.1.6 Vazamento de informações e tratamento de erros inapropriado

Alguns descuidos podem fazer com que uma aplicação web deixe vazar informações de configuração ou funcionamento interno. Tais informações geralmente são emitidas através de mensagens de erro e podem facilitar ataques (OWASP, 2007).

As medidas abaixo podem ser adotadas para evitar esse vazamento de informações:

- A manipulação de erros internos ao software deve ser padronizada;
- O detalhamento de erros deve ser limitado;
- As várias camadas relacionadas a uma aplicação, como banco de dados e servidor web, emitem mensagens de erros específicas. È necessário verificar e tratar esses erros para que não sejam explorados por atacantes;

5.1.7 Furo de autenticação e gerência de sessão

> Autenticação e gerência de sessão apropriadas são criticas para a segurança na web. Falhas nesta área geralmente envolvem a falha na proteção de credenciais e nos tokens da sessão durante seu tempo de vida. Estas falhas podem estar ligadas à roubo de contas de usuários ou administradores, contornando controles de autorização e de responsabilização, causando violações de privacidade (OWASP, 2007).

Como medida preventiva desse ataque, deve-se principalmente adotar o protocolo SSL (Security Socket Layer) para criptografia dos dados transmitidos, assim como as credenciais devem ser armazenadas de forma criptografada.

5.1.8 Armazenamento criptográfico inseguro

Dados importantes, como por exemplo, senhas de acesso, devem ser armazenadas com criptografia. No entanto, tal tarefa requer um planejamento mais elaborado, e em muitos casos isso não ocorre. Não criptografar dados importantes ou utilizar algoritmos de criptografia fracos podem acarretar sérios problemas de segurança (OWASP, 2007).

As medidas abaixo podem ser feitas para evitar essa falha:

- Utilizar algoritmos de criptografia aprovados publicamente como AES e RSA;
- Devem ser criadas chaves offline e as mesmas devem ser armazenadas com extremo cuidado;
- As credencias de acesso a recursos importantes de infra-estrutura devem estar seguras e adequadamente criptografadas.

5.1.9 Falha ao restringir acesso a endereço

Em aplicações web podem haver falhas em URL que permitem que funções sejam executadas e até mesmo dados sejam manipulados. Antes que requisições sensíveis sejam executadas, é necessário que verificações de acesso sejam feitas para garantir que somente usuários autorizados acessem a aplicação (OWASP, 2007).

Para minimizar essa falha é importante que haja um planejamento para definição das regras de acesso. Abaixo estão listadas algumas medidas importantes:

- Todos os endereços de acesso da aplicação devem estar por um mecanismo de controle de acesso;

- Testes de invasão devem ser realizados antes de liberar o sistema para o ambiente de produção;
- O acesso a todos os arquivos que a aplicação não deve executar deve ser bloqueado.

5.1.10 Malware

É natural que com o aumento da utilização de dispositivos móveis para acesso a internet, também aumente o número de malwares[5] existentes. Uma nova gama de softwares mal intencionados surge para esses dispositivos constantemente. Em muitos casos os tipos de ataques são muito similares aos existentes em computadores pessoais, mas em outros, são específicos para essa tecnologia, como por exemplo, o envio de SMS como forma de spam[6]. Abaixo seguem alguns exemplos de malwares existentes (COUTURE, 2010):

- Vírus Mabir/Cabir: pode infectar o sistema operacional Symbian por Bluetooh ou SMS;
- Trojan Dampig: corrompe configurações do sistema;
- Commwarrior: desabilita softwares antivírus;

Algumas empresas como a Apple e Android, estão adotando mecanismos de segurança como o Sandbox (Caixa de areia) para seus sistemas operacionais. Nesse conceito os processos de um aplicativo são executados de forma separada e isolada, ajudando na contenção de falhas e minimizando os riscos. No entanto, esse mecanismo tende a falhar quando usuários “desbloqueiam” seus dispositivos com intuito de instalar aplicativos não oficiais. Nesse mecanismo de desbloqueio ou popularmente conhecido como “jailbreak”, o aplicativo acaba ganhando privilégios e permissões em cima do sistema operacional. Com isso é facilitado o acesso de processos maliciosos.

---

[5] Software malicioso que pode causar dano ou roubo de informações.

[6] Mensagem eletrônica não solicitada, geralmente enviada em massa.

A fim de diminuir os riscos relacionados à malwares em ambientes corporativos, uma medida de segurança seria implantar políticas de permissão para instalação de softwares nos dispositivos, assim como realizar auditorias para verificar se aplicações não autorizadas estão instaladas.

Apesar de não haver tantos softwares comparados aos existentes para computadores desktop, é recomendável também que sejam adotados antivírus e firewalls para minimizar riscos à segurança.

Outra importante medida está relacionada à conscientização do usuário. Em muitos casos, no mundo móvel o usuário perde a preocupação com segurança adquirida com os computadores desktop. O usuário deve se conscientizar que os dispositivos móveis estão se aproximando cada vez mais aos computadores desktop e, portanto, as preocupações com segurança devem ser equivalentes.

5.2 CASOS REAIS DE ATAQUES NA INTERNET MÓVEL

5.2.1 Timofonica

> Curiosamente, a segurança é mais influenciada pela percepção que pela realidade. Muitos de nós não percebemos as ameaças à segurança que enfrentamos no dia a dia. Pessoas que têm medo de viajar de avião dirigem seus carros de maneira imprudente, sem maiores preocupações, mesmo sabendo que as chances de sofrer um acidente automobilístico é cerca de 100 vezes maior que um desastre aéreo. Outros se recusam a passar o número de seu cartão de crédito pela Internet, mas o fazem pelo telefone. Tecnologias novas despertam não apenas a curiosidade, mas geram intranqüilidade pelo próprio desconhecimento (COLCHER, 2002).

Seguindo a linha de pensamento acima, não foi surpresa que a mídia deu enorme destaque ao que seria o primeiro vírus de telefonia celular, o Timofonica. No entanto, tal vírus não se disseminava pelos celulares, e na prática era similar a outros vírus que infectavam computadores comuns. Enviava cópias de si mesmo aos e-mails encontrados no catálogo de endereços do Outlook da máquina infectada. Ao final, enviava uma mensagem para um endereço numérico gerado aleatoriamente no domínio correo.movistar.net, que possuía um serviço de transmissão de SMS. Como esse endereço podia ser um número de telefone celular, o usuário recebia uma mensagem de protesto contra a empresa telefônica (COLCHER, 2002).

5.2.2 Android.PJAPPSM

Em 2010 criminosos virtuais baixaram programas do Android Market, os modificaram infectando com malware Android.Pjapps e redistribuíram a versão em redes terceirizadas não oficiais. De acordo com a Symantec, o objetivo principal do malware era roubar informações de dispositivos infectados e inseri-las numa espécie de botnet[7] que faria novos ataques para roubar dados adicionais e infectar mais dispositivos. O malware também podia enviar mensagens SMS que geravam custos (ITWEB, 2011).

5.2.3 DroidDream

Também conhecido como Android.Rootcager foi um dos piores malwares existentes para o sistema Android segundo a Lookout, uma empresa voltada a segurança de dispositivos móveis. O DroidDream infectou cerca de 60 aplicativos do Market do Android e centenas de usuário no primeiro trimestre de 2011. O software malicioso incluiu os dispositivos infectados para um

[7] Software ou robô que executa ações automaticamente.

botnet, instalou softwares adicionais e com isso conseguiu roubar dados dos usuários (ITWEB, 2011).

5.2.4 Iphone/Privacy.A

Software malicioso que se instala em aparelhos Iphone da Apple que fizeram o que se chama jailbreak, ou seja, desbloqueio do aparelho para instalar aplicativos não oficiais. Uma vez instalado, pode roubar dados do dispositivo móvel. O malware ataca aparelhos desbloqueados que instalaram algum tipo de software que utiliza o SSH (Secure Shell), um utilitário Unix que permite conexão remota, mas que vem com senha padrão que se não for modificada, facilita o ataque (ITWEB, 2011).

5.3 RECOMENDAÇÕES DE SEGURANÇA

Conforme os dispositivos móveis vão sendo mais utilizados, é comum surgirem mitos e conceitos equivocados que comprometem a segurança em sua utilização. Abaixo serão estão listados dez desses conceitos e recomendações para segurança segundo Jon Espenschied (2007):

- Um smartphone não é apenas um celular com funções avançadas. Nos últimos anos ocorreu um grande avanço de tecnologia nos smartphones. Atualmente os aparelhos podem executar softwares avançados, equiparados a softwares desktop. No entanto, esse avanço pode ser um perigo para a segurança, já que há uma maior utilização dos serviços de comunicação e transmissão de dados. Devido a isso deve se ter um maior cuidado com as informações contidas no aparelho;

- Não deduza que a falta de atualizações e patches corretivos para sistemas operacionais e aplicativos de dispositivos móveis, indica que são estáveis e não são suscetíveis a grandes falhas. Como exemplo, pode ser citado o Symbian, sistema operacional da Nokia, que sofreu

ataques do vírus Cabir e foi amplamente criticado por isso. Da mesma forma o Windows CE, sistema da microsoft, que foi atacado pelo vírus Duts e cavalo-de-tróia Brador. Uma maneira de diminuir esses riscos é a implementação de processos e implantação de tecnologias, como educar usuários em tarefas como leitura de e-mails e tomar as corretas atitudes em relação a situações incomuns. Uma outra medida é a implementação de soluções de software anti-malware;

- Deve ser verificado se as informações estão sendo criptografadas. E-mails e outros serviços em alguns casos são criptografados somente do aparelho para o servidor da companhia e em outros sequer são criptografados. Deve haver uma maior preocupação entre os fornecedores parceiros, consultores e funcionários da organização que utilizam seus endereços de e-mail e dispositivos móveis dentro da rede corporativa;

- A conexão via WI-FI não é totalmente segura, assim como a conexão via operadora de celular. Os protocolos de dados de operadoras de celular, como GPRS ou UMTS, utilizam algoritmos de autenticação que já foram ou podem ser quebrados. É recomendável utilizar um VPN para diminuir esse risco e assegurar que os dados estejam sendo criptografadas a nível de aplicação;

- Os serviços de e-mail e mensagens devem ser monitorados quando enviados de dispositivos móveis dentro de uma rede corporativa. Se o serviço for fornecido por uma empresa neutra, verifique se há um acordo de nível de serviço que garanta a segurança dos dados;

- O uso de telefone celular como método de autenticação pode ser recusado pelo Help Desk. Uma forma alternativa para operações como recuperação de senhas, pode ser como a solução da BlackBerry, o Smart Card Reader, que permite ações de quem precisa autenticar algo utilizando somente dispositivos próprios;

- Deve haver confiança na integridade de dados e aplicativos em um dispositivo móvel. Em sistemas desktop, são comuns integrações entre servidores de arquivos, servidores de dados e de backup. Diferentemente de dispositivos móveis onde a integridade de dados se baseia em algum tipo de sincronização com um sistema fixo de servidor para backup e gerenciamento. Independente do modelo, o risco a segurança pode ser reduzido, configurando o equipamento para exigir uma senha sempre que for iniciado. Tal mecanismo pode ser útil em caso de furto do dispositivo. Com relação à integridade de aplicações, pode-se limitar as aplicações a serem instaladas nos dispositivos móveis, elaborando uma lista de softwares homologados;

- As informações não mais desejadas devem ser completamente removidas. Em dispositivos móveis, quando um arquivo é apagado, os marcadores de início e fim dos dados são removidos, no entanto, os dados em si, ficam até serem sobrescritos. Profissionais de tecnologia da informação devem se certificar de que esses resíduos sejam removidos;

- Os dados contidos em dispositivos móveis podem ser monitorados. Um software espião pode ser instalado sem muita dificuldade. Para amenizar tal risco podem ser adotados alguns softwares anti-malware e também educar usuários sobre o perigo de realizar atualizações ou instalações;

- As redes móveis não devem ser consideradas mais seguras porque seu uso é mais restrito. O interesse de criminosos virtuais aumentou nesse segmento e criatividade para burlar os mais diferentes tipos de redes e mecanismos de segurança não falta. Assim, os usuários devem considerar a transferência de dados e voz como ativo corporativo, tomando cuidados relacionados à segurança ao utilizar um dispositivo móvel.

6 CONCLUSÃO

Está evidente que a tecnologia para dispositivos móveis está se consolidando. A cada dia mais pessoas utilizam seus dispositivos móveis para funções que antes somente eram utilizadas em computadores desktop. Acesso a e-mail, redes sociais, transações bancárias, comércio eletrônico e vários outros serviços se tornaram acessíveis em dispositivos como smartphones. Somente deve haver uma conscientização de que há riscos, assim como há riscos em computadores desktop, mas que podem ser evitados se as medidas corretas forem tomadas.

No mundo corporativo, muitas empresas também estão adotando soluções móveis para que as informações de negócio possam ser acessadas a qualquer momento e em qualquer lugar. No entanto, com isso surgem dificuldades para administrar a segurança, pois devido ao acesso a uma variedade maior de redes e dispositivos, torna-se essencial a preocupação em informações como senhas, arquivos confidenciais e até mesmo e-mails relacionados à empresa, que podem cair em mãos indesejadas, sejam elas interceptadas pela rede ou pelo fato de que um terminal móvel pode facilmente ser roubado ou perdido.

É fato que esse aumento no volume de tráfego de dados na internet móvel fez surgir novas ameaças. Usuários confiam suas informações pessoais ou de negócios em dispositivos móveis e, que podem facilmente serem compartilhadas ou sincronizadas em redes diversas, exigindo uma transmissão de dados segura.

Uma ameaça cada vez mais presente são os malwares, que não somente podem corromper os dados de um dispositivo, mas também podem se espalhar

em uma rede corporativa assim que conectado na mesma, causando enormes danos à empresa.

As redes Wireless ou sem fio, também são passíveis de ataques. Um hacker pode, sem muitas dificuldades, se aproximar de uma rede com um notebook e uma antena de longo alcance, se conectar e interceptar informações de acessos de usuário que estão sendo transmitidos pelo ar. Com as informações de acesso em mãos pode acessar a rede corporativa e roubar informações valiosas.

Com toda essa gama de possíveis falhas de segurança, podem ser identificadas algumas áreas específicas quando falamos em segurança para internet móvel:

- Aplicativos móveis: o download de aplicativos pode representar ameaça à segurança. Aplicativos de terceiros em muitos casos podem conter malwares ou spywares que expõem informações, sejam ela pessoais ou corporativas;
- Redes sem fio: seja através de rede de celular ou WI-FI, existem medidas que devem ser tomadas para que ataques sejam evitados;
- Conscientização: usuários de dispositivos móveis devem ser conscientizados dos riscos existentes para a internet móvel.

Seja como for, os prejuízos podem ser enormes, assim como o desafio em tornar o acesso à internet em dispositivos móveis seguro. No entanto, na mesma medida em que os perigos evoluem, as ferramentas de segurança também estão evoluindo. Já existem muitas tecnologias disponíveis e um passo importante para se conseguir um ambiente seguro, é o fato de que usuários comuns devem se conscientizar e realizarem as mesmas práticas de segurança comuns em computadores desktop. Da mesma forma, no mundo corporativo, se faz necessário um bom planejamento antes de implantar um sistema de segurança, por se tratar de um ambiente muito mais complexo. Cumprindo tais premissas e utilizando as tecnologias e práticas já existentes no

mercado, os riscos de segurança na internet móvel com certeza são minimizados.

Como sugestão para um estudo futuro, pode ser pesquisada a utilização da computação em nuvem (Cloud computing) para dispositivos móveis. Tal recurso pode diminuir alguns riscos à informação, como roubo ou mesmo falha de hardware devido à diversidade existente no mundo móvel. Mas existem limitações e desafios que merecem ser detalhados em um próximo trabalho.

REFERÊNCIAS

ANDROID. **Android.com.** 2011. Disponível em: <http://www.android.com>. Acesso em 15 de Jun. 2011.

BLUETOOTH. **Bluetooth Basics.** 2011. Disponível em: <http://www.bluetooth.com/Pages/Basics.aspx>. Acesso em 30 de Jul. 2011.

CHEDE, Cezar Taurion. **Internet Móvel.** 2002. Disponível em: <http://www.de9.ime.eb.br/~mpribeiro/redes/Internet%20Movel%20Tecnologias,%20Aplica%E7%F5es%20e%20Modelos.pdf>. Acesso em 08 de Jul. 2011.

COLCHER, Sergio. **Internet Móvel.** 2002. Disponível em: < http://www.de9.ime.eb.br/~mpribeiro/redes/Internet%20Movel%20Tecnologias, %20Aplica%E7%F5es%20e%20Modelos.pdf>. Acesso em 02 de Jul. 2011.

COUTURE, Erik. **Mobile Security: Current threats and emerging protective measures.** 2010. Disponível em: <http://www.sans.org/reading_room/whitepapers/incident/wireless-mobile-security_33548>. Acesso em 18 de Ago. 2011.

DELALANDE, Christophe. **Symbian.** 2007. Disponível em: <http://www.wirelessbrasil.org/wirelessbr/colaboradores/christophe/symbian.html>. Acesso em 02 de Mai. 2011.

DIAS, Kelvin Lopes; SADOK, Djamel Fauzi Hadj. **Internet Móvel: Tecnologias, Aplicações e QoS.** 2001. Disponível em: <http://rolopes.com/public_html/fatec/2007_1_metodo/exemplos/artigo/Artigo_MobInternet.pdf>. Acesso em 22 de Mai. 2011.

ESPENSCHIED, Jon. **Ten dangerous claims about smart phone security.** 2007. Disponível em: <

http://www.computerworld.com/s/article/9014118/Ten_dangerous_claims_about_smart_phone_security>. Acesso em 20 de Jul. 2011.

FONTES, Edison. **Segurança da Informação**. 1a. Edição. Editora: Saraiva, 2006.

FREDERICK, Gail Rahn; LAL, Rajesh. **Dominando o desenvolvimento Web para Smartphone**. 1a. edição. Editora Apress, 2009.

GUEDES, Luís Cesar dos Santos; VASCONCELOS, Renan Ribeiro de. **UMTS, HSPA e LTE**. 2009. Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/umts/hspa.html >. Acesso em 10 de Jun. 2011.

HASHIMI, Y. Sayed; KOMATINENI, Satya; MACLEAN, Dave. **PRO ANDROID 2**. 2a. Edição. Editora: Apress, 2010.

ITWEB. **Conheça os oito ataques ao Android mais famosos.** 2011. Disponível em: <http://itweb.com.br/46003/conheca-os-oito-ataques-ao-android-mais-famosos>. Acesso em 26 de Jul. 2011.

KUROSE, James F.; ROSS, Keith W.. **Redes de computadores e a Internet – Uma abordagem top-down**. 3a. Edição. Editora: Pearson Addison Wesley, 2006.

LAUREANO, Marcos Aurelio Pchek. **Gestão da Segurança da Informação.** 2005. Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em 16 de Ago. 2011.

ORACLE. **Oracle.com.** 2011. Disponível em: <http://www.oracle.com>. Acesso em 01 de Set. 2011.

OWASP. **As 10 vulnerabilidades de segurança mais críticas em aplicações WEB.** 2007. Disponível em: <https://www.owasp.org/images/4/42/OWASP_TOP_10_2007_PT-BR.pdf>. Acesso em 05 de Ago. 2011.

PCWORLD. **New IPhone Malware Steals Data From Jailbroken Phones.** 2009. Disponível em: < http://www.pcworld.com/businesscenter/article/181906/new_iphone_malware_steals_data_from_jailbroken_phones.html>. Acesso em 28 de Jul. 2011.

SANTO, Adrielle Fernanda Silva do Espírito. **Segurança da Informação.** 2010. Disponível em: <http://www.ice.edu.br/TNX/storage/webdisco/2011/03/11/outros/2bc3b892c73868cf712dcf084ed96b8a.pdf>. Acesso em 20 de Ago. 2011.

SARGENTO, Susana. **Redes e Sistemas Distribuídos.** 2004. Disponível em: <http://www.dcc.fc.up.pt/~ssargento/aulas_2003_2004/RSD/aulas_teoricas/RSD_IP_4.pdf>. Acesso em 02 de Mai. 2011.

SILVA, Denise Ranghetti Pilar da; STEIN, Lilian Milnitsky. **Segurança da informação: uma reflexão sobre o componente humano.** 2007. Disponível em: <http://www.cienciasecognicao.org/pdf/v10/m346130.pdf>. Acesso em 22 de Ago. 2011.

STRACCIALANO, André Ligieri. **Segurança em redes 3G - UMTS.** 2008. Disponível em: <http://www.wirelessbrasil.org/wirelessbr/artigos/Seguranca-UMTS-Geral.pdf>. Acesso em 02 de Ago. 2011.

TELECO. **Telefonia Móvel Celular e sua Aplicação para Tráfego de Dados**. 2005. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialtrafdados>. Acesso em 06 de Jun. 2011.

WOOLEY, Travis. **A Comparative Study of the Android and iPhone Operating Systems.** 2010. Disponível em: <http://www.android.com>. Acesso em 10 de Jul. 2011.