COMPUTAÇÃO MÓVEL: NOVAS OPORTUNIDADES E NOVOS DESAFIOS

GABRIEL LUIZ OLIVEIRA QUINTAES, GUILHERME PADOVAM, LUCAS MENDES DE OLIVEIRA, VINICIUS PONTES, NARUMI ABE, ELIANE CRISTINA AMARAL, ELINEY SABINO

RESUMO

O objetivo do artigo é mostrar a dificuldade ao acesso aos dados e informações independente do lugar onde você está, com ajuda das redes sem fio o alcance fica maior e mais acessível.

Os celulares, tablets e entre outros dispositivos moveis tem seus defeitos como a bateria ser bem limitada tem a rede sem fio que ajuda porem é limitada e tem suas taxas de erros, em questão de processamento ou segurança os celulares são inferiores aos computadores.

Com essa pesquisa feita em livros e artigos queremos mostrar que os celulares têm seu benefício e defeito, oque grande vilão e herói são os aplicativos que podem ter como benefício ou querer se aproveitar do usuário para ajudar terceiros, que a internet para celular é boa, porem tem seu limite que é pequeno, mostra a evolução dessa tecnologia que vem crescendo em questão de uso e tecnologia.

Palavra-Chave: processamento, segurança móvel, infraestrutura, informação, tecnologia.

ABSTRACT

The purpose of the article is to show the difficulty of accessing data and information regardless of where you are with the help of wireless networks the reach becomes larger and more accessible.

Mobile phones, tablets and among other mobile devices have their defects as the battery is very limited has the wireless network that help but is limited and has its error rates in a matter of processing or security the cell phones are inferior to computers.

Regarding this research done in books and articles we want to show that the cell phones have their benefit and defect, what great villain and hero are the applications that can have as a benefit or want to take advantage of the user to help others, that the mobile internet is good, But it has its limit that is small, shows the evolution of this technology that has been growing in question of use and technology.

Key words: Independence, processing, security, mobile, data, infrastructure, information, technology.

Introdução

Segundo Nakamura (2015), a partir da década de 90, ocorreu um crescimento no desenvolvimento de tecnologias para comunicação celular, redes locais sem fio e via satélite. O avanço dessas tecnologias permitiu o acesso a informações onde quer que esteja. Nos últimos anos, houve um grande avanço e popularização dos dispositivos computacionais móveis, como *notebook*, *Personal Digital Assistants (PDAs)* - assistente pessoal digital, celulares, que nos trazem a estimativa de que em alguns anos as pessoas no mundo todo terão um desses dispositivos como comunicação remota. Esse ambiente traz a ideia de computação móvel.

Segundo Hecke (2013), para um aparelho ser definido como computador móvel, ele deve ter capacidade de processamento, conseguir se comunicar via rede sem fio, e ser transportado pelo usuário. Então é necessário que esses aparelhos sejam menores que os computadores de mesa, usem uma bateria ou pilha para que não necessite usar a fonte de energia elétrica, e se comunicar na rede sem fio. Alguns desses dispositivos são *laptops ou notebooks*, *PDAs*, celulares e *tablets.*

Segundo Kuszka (2014), um notebook, é um computador pequeno, leve e portátil, feito para ser usado transportado e com facilidade. Um *notebook* contém uma Tela de Cristal Líquido (LCD), teclado, mouse (*touchpad* – área onde se desliza o dedo), unidade de disco rígido, portas para conectividade local, Porta Universal (USB), gravadores de *Compact Disc* – disco compacto / *Digital Versatile Disc* – disco digital versátil (CD/DVD). Também possuem capacidade de processamento e de armazenamento comparáveis a de um *Personal Computer* (PC). Apesar disso, um *notebook* ainda não é a melhor opção para uso ágil, pois, necessita que a pessoa pare em algum lugar que tenha uma mesa ou algum apoio, tire ele de alguma bolsa ou maleta e ligue-o, o que pode demorar um pouco, e depois de usar guarde-o novamente. Outro fator a ser levado em conta, é que esses *notebooks* usam baterias que não duram muito tempo (umas 3 horas de uso), então, o usuário precisa de acesso constante com a rede elétrica para recarregar a bateria.

PDAs são dispositivos de mão, que parecem muito com uma agenda, onde os usuários podem anotar seus compromissos, e consulta-los em qualquer lugar, pois esses dispositivos são pequenos, de fácil utilização e podem ser carregados no bolso. Entretanto, por serem de tamanho bem reduzido, suas capacidades de processamento e armazenamento são bem limitadas, não possuem mouse ou teclado, e necessitam de uma pilha ou uma pequena bateria para serem utilizados. Por serem limitados e serem construídos para que haja o mínimo de consumo de energia possível, as baterias duram várias horas e ás vezes até dias.

No começo, os celulares eram usados apenas para conversação por voz, porém, com o avanço da tecnologia, esses dispositivos adquiriram capacidade de processamento e a capacidade de comunicação através da internet.

As limitações apresentadas pelo celular são iguais aos outros dispositivos citados acima, por serem pequenos, também precisam de uma bateria, que com o uso prolongado pode descarregar rápido, necessitando de uma fonte de energia para carrega-lo.

Hoje em dia os celulares não são só usados para conversar por voz, mas também contam com bastante aplicativos, como jogos, músicas, vídeos entre outros.

O celular passou a ser um computador do tamanho da palma da mão, pois pode fazer muitas coisas que o computador também faz, até navegar na internet tendo acesso à informação em qualquer lugar que esteja.

De acordo Kuszka (2014), no final dos anos 80, surgiram os equipamentos baseados em sistema operacional UNIX, onde ocorreu a migração do mainframe para equipamentos baseados em padrões abertos, os chamados "*Open Systems*", principalmente por razões de custos e possibilidade de ficar um pouco menos dependente do fabricante; afinal de contas, o UNIX, um sistema operativo portável, multitarefa e multiutilizador, prometia uma plataforma aberta e intercambiável, coisa que nunca aconteceu em sua plenitude. E esforços de migração entre UNIX continuam ocorrendo até hoje. Estamos agora na era do *Cloud Computing*, computação nas nuvens, o *Data Center* perdeu aquela identidade de centro de processamento de dados, até mesmo por razões de normas que exigem que você tenha seus dados replicados em mais lugares. O acesso via internet e via navegadores já é um padrão e os dispositivos móveis estão extremamente evoluídos e sofisticados, mas as empresas estão abrindo o acesso aos seus sistemas para qualquer dispositivo, mas com cautela. As empresas inicialmente a ignoraram por razões de segurança, mas, com a disponibilidade de tecnologias maduras de VPN (acesso via rede com criptografia) para dispositivos móveis, todo o meio corporativo começou a entender que acessar as ferramentas de trabalho pelo dispositivo que o usuário ficar mais confortável trará um aumento de produtividade, motivará o colaborador e permitirá o acesso a qualquer hora, em qualquer lugar e com segurança.

Gerações da telefonia celular

Segundo Jean (2017), as gerações de telefonia celular são classificadas da seguinte maneira:

- A primeira geração foi a 1G, formada por sistemas analógicos, onde só era possível a transmissão de voz.

- Na segunda geração a 2G, surgiram as tecnologias com a codificação digital de voz, melhor qualidade de voz, facilidade a comunicação de dados e a criptografia. Nessa geração, começam a se formar dois grupos: *Code Division Multiple Access (*CDMA) ou Acesso Múltiplo por Divisão de Código é um método de acesso a canais em sistemas de comunicação. E o Global System for Mobile Communications (GSM), ou Sistema Global para Comunicações Móveis, nele as chamadas são designadas a um determinado tempo dentro da frequência, contando com a diferença de que a transmissão é toda criptografada.

- Na terceira geração, a tecnologia 3G aprimora a transmissão de dados e voz, oferecendo velocidades maiores de conexão, além de outros recursos, como vídeo chamadas e transmissão de sinal de televisão.

- A geração 4G é um aprimoramento da 3G, é algo ilusório pois ainda está sendo implementada, é voltada para Internet, ou seja, aos serviços de dados móveis, a intensificação do uso dos smartphones, com a perspectiva de velocidades finais próximas aos dos serviços de banda larga fixa.

Segundo Nakamura (2015), é necessário ter uma infraestrutura que permita a comunicação entre dispositivos móveis e a rede, para que possa haver troca de informações. Temos dois tipos de infraestrutura, interna e externa, a principal diferença entre elas é o tamanho da área de cobertura da rede. Alguns exemplos de tecnologias de rede sem fio para infraestrutura interna são:

- Redes Locais Sem Fio (*WLAN – Wireless Local Area Network*). O padrão que vem sendo mais difundido é o IEEE 802.11 (Wi-Fi), para a formação de redes locais sem fio, e será melhor descrito posteriormente.

- Infravermelho – Mesma tecnologia adotada em controles remotos de eletrodomésticos. Possui baixa largura de banda e dificulta a comunicação com a existência de obstáculos, como uma parede, por exemplo.

- Laser – Permite comunicação com elevada largura de banda, porém, ela deve ocorrer com os dispositivos muito bem alinhados devido ao feixe extremamente direcional do laser.

- HomeRF – Especificação de um sistema de comunicação sem fio para o compartilhamento e troca de dados entre dispositivos de consumo, tais como PCs, periféricos, telefones e eletrodomésticos. (Nakamura, 2015, s/n)

Conforme foi descrito por Nakamura (2015), infraestrutura externa é limitada a áreas pequenas. A cobertura pode estender-se a áreas metropolitanas ou até mesmo globais. Alguns exemplos de tecnologias de rede para esse fim são:

- Radiofrequência – *Links* de rádio podem ser formados entre estações que desejam trocar dados. O alcance pode ser de quilômetros, porém, depende de visada direta, ou seja, sofre influência de barreiras (ex: prédios ou morros) ou da própria curvatura da terra.
- Satélites – Permite a comunicação a longas distâncias, uma vez que têm a capacidade de cobrir países e até continentes. Uma cadeia de satélites interligados torna possível cobrir todo o globo terrestre.
- Redes celulares – Infraestrutura da telefonia celular. A área a ser coberta é dividida em células, e cada célula é atendida por uma estação rádio base. Essas estações são interconectadas geralmente por fibras ópticas, formando uma rede fixa, e toda a comunicação entre dispositivos móveis passa por ela.

Ataques a redes WIFI

Segundo Mendes (2014), a ingenuidade ou despreparo das pessoas podem causar grande prejuízo. Engenharia social é o termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, abusando da confiança ou ingenuidade do usuário, para obter informações pessoais. Alguns modos de prevenir contra-ataques de engenharia social são: desconfie de chamadas que solicitem muitas. Caso desconfie, tente verificar a identidade diretamente com a empresa ou pessoa, para verificar se a solicitação é legítima.

Segundo Pasqualini e Marcondes (2012), na prática de wardriving é necessário um veículo automotor, um computador (*notebook*, *PDA*) com interface wireless e um software capaz de efetuar uma varredura nos canais utilizados pelas redes 802.11. O mapeamento é feito passeando-se com o veículo em uma região, enquanto o computador registra as redes em seu alcance. Com as informações dos pontos de acesso coletadas pelo software é possível extrair dados tais como nome das redes, canais de freqüência, tipos de criptografias, modos de operação, entre outras. Alguns modos de se prevenir

contra-ataques *wardriving:* mudar regularmente a senha do roteador, ative a criptografia, desligar a rede sem fio quando não estiver em casa, use um *firewall.*

Malenkovich, (2013) o conceito por trás do ataque Man in the Middle (MITM) é bastante simples e não se restringe ao universo online. O invasor se posiciona entre duas partes que tentam comunicar-se, intercepta mensagens enviadas e depois se passa por uma das partes envolvidas. O envio de contas e faturas falsas poderia ser um exemplo desta prática no mundo off-line, o criminoso as envia ao correio das vítimas e rouba os cheques enviados como forma de pagamento. No universo online, os ataques são mais complexos. Apesar de basear-se na mesma ideia o invasor deve permanecer inadvertido entre a vítima e uma instituição verdadeira para que o golpe tenha sucesso. Na forma mais comum de MITM o golpista usa um *router WiFi* como mecanismo para interceptar conversas de suas vítimas, o que pode se dar tanto através de um router corrompido quanto através de falhas na instalação de um equipamento. Numa situação comum o agressor configura seu laptop, ou outro dispositivo wireless, para atuar como ponto de WiFi e o nomeia com um título comum em redes públicas. Então quando um usuário se conecta ao "router" e tenta navegar em sites delicados como de online banking ou comércio eletrônico o invasor rouba suas credenciais. Alguns modos de se prevenir contra-ataques MITM: utilize dispositivos de autenticação, como tokens ou outras formas de autenticação de dois fatores para acessar contas que contém informações sensíveis e confidenciais, trate e-mails de remetentes desconhecidos com um alto grau de ceticismo e não clique em links para acessar sites seguros (digite o endereço Web no navegador).

Segundo Vinícius (2017), o conceito por trás do ponto de acessado falso é aproveitar falhas nos sistemas operacionais e a falta de atenção do usuário. A partir da utilização de um software para transformar a placa wireless em um ponto de acesso, o notebook se comporta como um *Access Point* ou Ponto de Acesso (AP). Assim, é só ligar ele em uma rede cabeada para fornecer à vítima o acesso à internet. Isto é possível porque o invasor configura o *notebook* com o mesmo nome do ponto de acesso, sendo que o sinal do computador é mais forte que o sinal do AP verdadeiro. Como o *Windows* sempre se conecta com o sinal mais forte então acaba se conectando no ponto falso, o *Windows* irá mandar os dados como se fosse para o verdadeiro. Um modo de se prevenir desse tipo de ataque é prestar atenção ao nome da rede Wi-Fi pública que você irá se conectar. Existem pessoas mal-intencionadas que criam redes com nomes falsos para se passar, por exemplo, por uma loja com o intuito de roubar os arquivos do seu dispositivo. Por isso, certifique-se de que o nome do ponto de acesso não é falso.

Segundo Amilto Júnior (2010), *sniffers* são programas que tem como princípio capturar pacotes de rede. Ele analisa o trafego de rede e identifica áreas vulneráveis. Se sua rede está enfrentando lentidões, quedas ou corrupções de dados é provável que esteja sofrendo com um ataque de *sniffers*. Os sniffers capturam pacotes de rede colocando a interface de rede *Ethernet*. Em redes locais os dados trafegam de uma máquina a outra por meio do cabo em pequenas unidades chamadas *frames*. Esses frames são divididos em seções que carregam informações específicas. Os *sniffers* impõem um risco de segurança pela forma como os *frames* são transportados e entregues. Se uma interface de rede da estação de trabalho operar em modo passivo, ela pode capturar todos os pacotes e frames na rede. Uma estação de trabalho configurada dessa forma é um *sniffer*. Uma forma de se proteger de um sniffer é usar um antivírus, que permita que você verifique problemas em sua rede. No entanto, a melhor forma de se proteger é criptografar todos os dados sigilosos transmitidos *on-line.*

Considerações Finais

Como base no levantamento bibliográfico, observou-se a necessidade de manter os usuários em qualquer ambiente bem informados por meio da utilização dos aparelhos de mão. Aproveitando a inclinação da sociedade ao uso de dispositivos moveis sobre as técnicas e conceitos dos desenvolvimentos de celulares, tablets, ipads que estão evoluindo com o passar dos anos. Tal feito oferece possibilidade aos alunos de se especializarem cada vez mais no assunto, dando continuidade a este trabalho.

Referências Bibliográficas

Anselmo, Luciana, http://www.apptuts.com.br/tutorial/android/problemas-comuns-do-android-como-resolve-los/ **Acessado em:** 30/03/2017

Cavallini, Ricardo; Xavier, Léo e Sochaczewski, Alon **Mobilize: O Potencial dos dispositivos móveis.**

Ferreira, Marcos, https://www.trustsign.com.br/blog/o-que-e-engenharia-social-6-dicas-para-se-proteger-das-armadilhas/index.html **Acessado em:**15/05/17

Hecke, Caroline, https://www.tecmundo.com.br/tendencias/45649-como-dispositivos-moveis-estao-mudando-forcas-de-trabalho-ao-redor-do-mundo.htm **Acessado em:** 30/03/2017

Jean, Gideon, https://portaldeplanos.com.br/tipos-de-tecnologias-telecomunicacoes/ **Acessado em:** 09/05/2017

Júnior, Amilton, http://dicasemgeral.xpg.uol.com.br/dicas-em-geral/12471/sniffer-entenda-como-funciona/ **Acessado em:**15/05/17

Kuszka, Boris, https://corporate.canaltech.com.br/coluna/mobile/Dispositivos-moveis-a-interface-com-o-mundo/ **Acessado em:** 13/05/17

Luca Pretto, Nelson.de. **Inclusão digital**. Edufba,2011.

Malenkovich, Serge, https://blog.kaspersky.com.br/what-is-a-man-in-the-middle-attack/462/ **Acessado em:**14/05/2017

Melo,Pollyanna,http://www.administradores.com.br/noticias/negocios/confirarecomendacoes-sobre-como-se-proteger-de-ataques-man-in-the-middle/21931/ **Acessado em:**15/05/17

Mendes, Priscila, https://prezi.com/3p93ybojkq73/engenharia-social/ **Acessado em:**14/05/17

Novaes, Rafael, http://www.psafe.com/blog/o-wardriving-como-manter-sua-rede-segura/ **Acessado em:**15/05/17

Pasqualini, Anderson L. e Marcondes Augusto C. https://revistatis.dc.ufscar.br/index.php/revista/article/download/28/31 **Acessado em:**14/05/17

Pressman, Bruce M. R**. Engenharia de Software**. AMGH,2016.

Vinícius, Marcos, https://www.passeidireto.com/arquivo/6696501/artigo---a-fragilidade-das-redes-sem-fio/2 **Acessado em:**15/05/17