Temos um exemplo de como *transformar qualquer telefone em um dispositivo espião.*

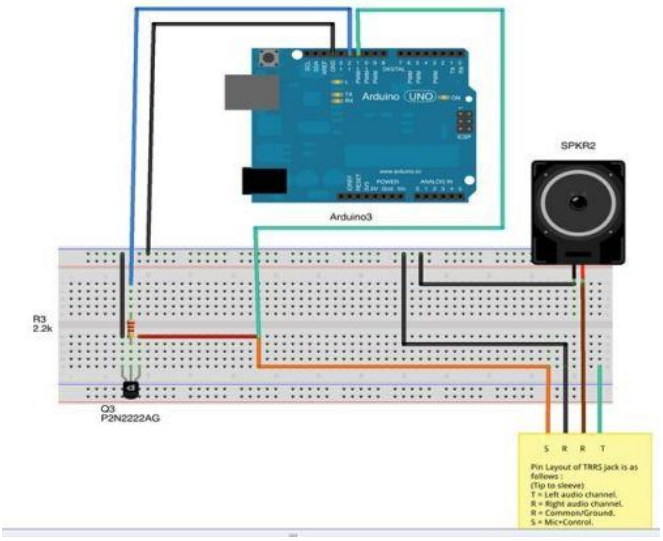
Atul Alex apresentou um artigo que cobre "o abuso da discagem por voz e a combinação do Arduino / Microcontrolador para roubar dados privados no iphone, Android, Windows Phone e Blackberry usando apenas o conector de áudio.


Tem uma forma de transformar qualquer dispositivo móvel em uma ferramenta espiã, evitando a instalação de qualquer software malicioso nele, abusando do recurso de discagem por voz que está habilitado por padrão em todas as plataformas móveis.

Dispositivos modernos são equipados com softwares poderosos capazes de interpretar comandos vocais do usuário, o dispositivo de hardware proposto é capaz de imitá-los para dar ordens ao dispositivo. A funcionalidade abre cenários futuros nos quais os hackers são capazes de controlar o telefone simplesmente enviando mensagens de texto não autorizadas para roubar dados importantes.

Quase todos os eventos no celular são notificados ao usuário com a ajuda dos tons/sons correspondentes, o pesquisador demonstrou que adicionar um **microcontrolador ao circuito do fone de ouvido** é possível:

1. Inicie chamadas sem interação do usuário.
2. Observe a duração das ligações.
3. Detecte chamadas recebidas / efetuadas, sms e assim por diante.



Nas versões futuras, o hardware também poderá integrar funcionalidades mais complexas, como gravação de ligações ou ativação remota do aparelho.

Os dispositivos semelhantes representarão no futuro uma opção privilegiada para operações de espionagem cibernética e mais em geral para operações cibernéticas.No futuro, cada interface de dispositivo móvel deve ser projetada adequadamente, cada entrada deve ser validada por um circuito especialmente projetado.

## 5. Exemplos de Ataque e Defesa em Dispositivos Móveis

Em termos de tecnologia, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil em seu glossário define ataque como sendo "qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede" [CERT.br 2015]. Isso pode ser dividido entre dois tipos, sendo passivos e ativos [Pinto e Gomes 2011]:

- Ataque passivo: esse tipo de ataque faz com que as informações sejam copiadas ou analisadas com o intuito de encontrar padrões de comunicação ou do seu conteúdo. Essa análise do tráfego se busca identificar entre quais usuários está acontecendo a comunicação, quando isso acontece, o tamanho da mensagem, a frequência da troca de mensagens. Tais dados são muito úteis para se conseguir diversos tipos de informações. Apenas constatando essa troca de informações em uma rede, já pode se revelar muito sobre os usuários.
- Ataque ativo: os ataques desse tipo são aqueles que conseguem interferir diretamente ou indiretamente no funcionamento do sistema. Ataques que utilizam táticas de engenharia social e os ataques físicos são claros exemplos.

Os atacantes são indivíduos que possuem um certo conhecimento sobre o funcionamento básico dos sistemas e tentam obter algo em relação a cada ataque. Cada invasor pode receber uma designação, segundo o seu nível de conhecimento e as intenções pretendidas em seus ataques, tais como [Dumont 2006]:

- *Hacker*: esse nome é dado àqueles que já possuem um grande conhecimento sobre tecnologias, tanto que em geral são programadores ou administradores de rede. O objetivo dos *hackers* é encontrar defeitos para resolvê-los, não buscam prejudicar ninguém em seus ataques. As tentativas de ataques basicamente são para apontar pontos vulneráveis em questões de segurança.
- *Cracker*: tal designação é dada para os invasores que tendem a prejudicar as vítimas de seus ataques. Trabalham em prol de obter ganhos ou em apenas gerar danos financeiros.
- *Phracker*: esses indivíduos são os que trabalham especificamente com telefonia, suas ações básicas são realizar ligações sem gerar custos, instalar escutas e reprogramar centrais telefônicas.
- *Larner*: são aqueles que buscam conhecer mais sobre o universo dos *hackers*. Não possuem uma única definição quanto ao tipo de ataque que realizam, podem ser com intenções de *hacker* ou de *cracker*. Seus conhecimentos são limitados, e em muitos casos recorrem aos programas ou parte deles já desenvolvidos por outras pessoas e disponíveis na *Internet*.
- *Script Kiddie*: são considerados oportunistas, de forma que buscam uma invasão que seja fácil, pois não possuem um conhecimento tão amplo quanto às tecnologias e suas seguranças. Se utilizam de métodos prontos que encontram na *Internet*, e sem um objetivo específico, tentam colocar essas formas em prática para obter acesso à conta de usuários.

## 5.1. Malware

Um programa com intenções de se instalar em um computador sem que haja a permissão do seu usuário é conhecido como *Malicious Software* (*Malware*), e possui como principal objetivo causar algum tipo de dano ao equipamento. Os principais alvos desses códigos são os ganhos econômicos em prol do seu criador, tentando captar dados confidenciais, práticas de golpes e até mesmo espalhar spam

## 5.2. Trojans SMS

Essa ameaça, também conhecida como *Trojan-SMS.AndroidOS.FakeInst.ef*, consiste em um código malicioso visando atacar apenas os telefones móveis. Ao executar o arquivo em que o trojan se encontra, ele se encarrega de enviar um *Short Message Service* (SMS) para números *premium* sem que o usuário tenha consciência do que está acontecendo. Esses números servem para efetuar cobrança, inscrevendo o usuário em certos serviços

### 5.2.1. Ransomware

Em forma de *malware* essa ameaça tem aparecido com maior frequência para usuários de diversos sistemas. Quando essa ameaça consegue controle sobre o dispositivo do usuário, ele fará a encriptação de dados pessoais com uma senha de $n$ dígitos. Também é possível comprometer a utilização do sistema todo, não apenas o acesso às informações. Com isso feito, apresentará uma mensagem para o usuário, na qual indica que a chave para descriptografia será enviada mediante ao pagamento de uma certa quantia estipulada pelo atacante [F-Secure 2014]. Obviamente é impossível saber se essa chave de fato será acessível ao usuário após o pagamento, tanto que já houve relatos em que usuários pagaram e não receberam retorno algum [Donohue 2014].

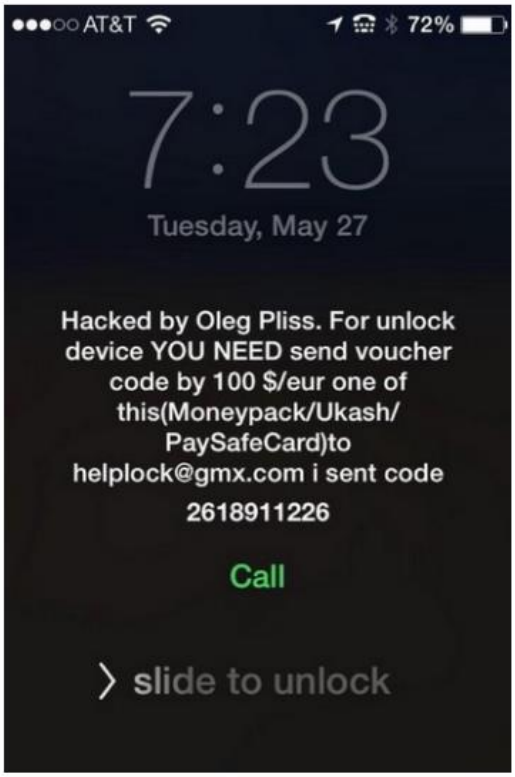



**Figura 5. Exemplo de mensagem ao usuário em um sistema iOS [Donohue 2014].**

### 5.3. Engenharia Social

A engenharia social consiste em se utilizar de conhecimentos empíricos e científicos de uma maneira sociável para obter acesso à informações pessoais. Ou seja, um atacante por meio dessas técnicas tenta atingir alguém com o propósito de conhecer alguns dados pessoais dela, sem muito esforço, fazendo com que a vítima seja induzida a fornecer seus dados sem o devido conhecimento sobre as ações que ocorrerão a partir disso.

O ataque ocorre a partir do momento em que algum usuário adquire confiança sobre o invasor, sem saber as reais ações pretendidas por ele. As técnicas de engenharia social são utilizadas em vários ramos, não se aplicam apenas à tecnologia, podendo encontrar falhas em organizações físicas e jurídicas.

Kevin Mitnick, um dos mais famosos *hackers* americanos, na década de noventa por meio de técnicas com esse conceito efetuou diversos ataques com sucesso [Pinto e Gomes 2011]. Em seu livro, A Arte de Enganar, ele cita que a empresa pode possuir os melhores sistemas para segurança que o dinheiro possa comprar, porém o indivíduo ainda estará vulnerável [Mitnick e Simon 2003]. A segurança não está ligada apenas em seus sistemas computacionais, mas envolve muito a questão das pessoas envolvidas em todo o processo. E nem sempre elas sabem a importância que possuem para a garantia da segurança.

### 5.5. Ataques na Camada de Aplicação

A *Open Web Application Security Project* (OWASP) mantém um projeto na *Internet* focado em segurança de aplicações *Web*. Em uma das vertentes de seu projeto, focam em segurança móvel, conhecida como OWASP *Mobile Security Project*. Com esse projeto eles buscam proporcionar um maior conhecimento sobre a criação de aplicações mais seguras [Open Web Application Security Project 2015].

Com o auxílio de empresas que realizam estatísticas de vulnerabilidades móveis, como *WhiteHat*, *Pure Hacking*, *Secure Network*, *Hewlett-Packard* (HP), entre outras, o grupo OWASP realizou um ranking dos 10 principais riscos móveis que envolvem autenticações remotas, recursos de computação em nuvem integrados à aplicações móveis

### 5.6. Ataques Físicos

Os ataques físicos são aqueles em que o invasor possui o aparelho em mãos para realizar a tentativa de roubo das informações pessoais. Em geral se utilizam ferramentas forenses para acessar aos dados.

Uma pesquisa realizada pela *Consumer Reports* Centro Nacional de Pesquisa nos Estados Unidos, apresentou que em 2014 houve 2,1 milhões de roubos à *smartphones*. Mesmo com um número tão alto, ainda assim foi inferior aos 3,1 milhões de 2013. A diminuição desse tipo de ação pode ser representado pelas táticas utilizadas pelas empresas, para proporcionar ao usuário uma forma de tornar o aparelho inoperável após o roubo ou extravio. Esses números representam os furtos e não quantos deles foram alvos de roubo de informação, mas é possível se pensar em quantas informações há em um dispositivo e se está sob o poder de terceiros é suscetível o vazamento de informações, por exemplo vazamentos de fotos íntimas [Deitrick 2015].

Na Califórnia o acesso remoto para inoperabilidade se tornou lei, onde diz que todos os novos aparelhos móveis do estado devem conter essa proteção contra roubos, ou até mesmo extravio. Foi conhecida como lei "*kill switch*", e obriga que a tecnologia possua algum modo de se bloquear o aparelho remotamente. Esse conceito já era uma tentativa de algumas empresas oferecerem uma maior segurança para seus clientes, onde se tinham alguns aplicativos capaz de realizar tal feito

## 5.7. Tipos de Defesas

Esta seção tem por objetivo apresentar algumas das formas de defesas que são implementadas diretamente na comunicação de sistemas computacionais. E também alguns recursos que os usuários comuns podem utilizar para diminuir a efetividade dos ataques sofridos.

### 5.7.1. Criptografia

Esse conceito de defesa acontece por meio de algoritmos, onde tentam ocultar uma mensagem ao codificá-la, mas com a mesma fórmula pode se retornar para a mensagem original. É um dos principais termos vistos quando o assunto é segurança, principalmente por ter se tornado tão importante no momento de assegurar a privacidade da informação em comunicações e nas redes públicas e privadas. Quando algum invasor tenta obter acesso aos dados que trafegam na rede ou comunicação, a criptografia dos dados tornará o acesso dele à informação muito mais difícil.

### 5.7.2. Antivírus

Depois da tamanha expansão de ataques em dispositivos, a segurança ganhou um foco ainda maior. Isso fez com que o antivírus, indispensável em computadores, passar a ser uma das formas de garantir a segurança de seus dados. Esse tipo de programa tenta se manter ao máximo atualizado quanto às principais ameaças, e foca em tentar detectá-las quando for exigido [Freire 2002].

Grandes empresas desse ramo, como *Eset*, *Kaspersky*, *Avast*, entre outras, possuem versões para a maior parte das plataformas móveis. Versões gratuitas são limitadas quanto a alguns aspectos, mas possuem uma eficiência muito boa. As versões pagas são disponíveis também, e indicadas principalmente para empresas e corporações, levando em consideração que a segurança não depende de apenas uma pessoa, e sim de um grupo

Quando aparelhos mais antigos eram roubados, o ladrão apenas trocava o chip e poderia utilizá-lo normalmente. Com o auxílio dos antivírus isso pode ser evitado, alguns deles dão a opção *Theft Protection*, ela torna possível o acesso remoto ao aparelho e dá a opção de apagar todas as informações contidas nele

### 5.7.3. Firewall

Essa técnica é utilizada para defesa no tráfego de rede, e pode ser implementada em *hardware* e *software*. Ela determina que operação de envio ou recepção de informação pode ser executada. O seu funcionamento tem uma definição simples, que é liberar acessos permitidos e bloquear os indesejados [Alecrim 2013].

pode controlar o acesso feito por qualquer tipo de rede, como no exemplo há a rede 3G, *Explicit Data Graph Execution* (EDGE), *General Packet Radio Service* (GPRS), Wi-Fi e *Bluetooth*.

### 5.7.4. Conscientização

Como já pôde ser visto na Seção 3, as pessoas são um dos principais pilares para assegurar a segurança da informação. O próprio Mitnick considera que a quebra do "*firewall* humano" é mais fácil do que se dedicar em outras técnicas para ataque [Mitnick e Simon 2003].

Por motivos como confiança demais nas aplicações ou até mesmo ingenuidade por parte dos usuários, a questão segurança não é tratada como se devia. Isso acarreta em algumas decisões equivocadas, e quando se trata da tendência BYOD nas empresas, isso ganha um tamanho mais significativo. Com o crescimento das redes sociais, os usuários passaram a expor mais suas informações. Grande parte dos usuários frequentes de redes sociais revelam informações pessoais para outras pessoas, após adquirir uma certa confiança nelas [Rosa et al. 2012]. A interação entre desconhecidos é uma tendência ainda maior via redes sociais, e os engenheiros sociais são astutos ao explorar esses meios para atingir suas vítimas.

O uso de tecnologias mais avançadas é importante para diminuir as chances de ataque. Algumas delas fornecem a visualização dos acessos pessoais, o que traz uma maior comodidade para chefes de empresas por exemplo [Kaspersky 2006].

Se as pessoas perceberem o tamanho da importância que possuem em assegurar que seus dados não serão invadidos, passarão a ter uma forma diferente de agir referente às tecnologias.

## 6. Resultados e Discussão

O presente trabalho aborda algumas formas utilizadas pelos invasores para roubo de informações ou controle de aparelhos móveis, e alguns métodos de defesas implantadas. Durante as pesquisas realizadas foi possível perceber que o sistema *Android* é o mais perseguido pelas táticas de ataques, mas não é possível comprovar se isso ocorre dado o número elevado de usuários ou por ser um sistema de código aberto, onde é possível tentar encontrar algumas vulnerabilidades (ou por alguma outra característica). O sistema iOS e *Windows Phone* possuem a seus códigos fechados, que de certa forma dificulta a ação de ataques ao sistema. Vale ressaltar que, mesmo o Android ser baseado em *Linux* e ter seu código aberto, não necessariamente isso motiva a ser um sistema vulnerável.

Uma grande parte dos ataques são por meio de táticas de Engenharia Social, e ela é uma das formas mais antigas de ataque, e eficaz. A curiosidade das pessoas é explorada de diversas formas, tanto com mensagens sobre escândalos de famosos, prêmios (atacando a cobiça..) até intimações judiciais (dentre muitas outras). Os usuários de todos os sistemas são alvos desses ataques e podem ser afetados por *malwares* com objetivos de controle das ações do aparelho ou acesso às informações pessoais.

Foi possível perceber que o fator humano é o mais suscetível aos ataques, independente das tecnologias de defesas implantadas em sistemas ou empresas. As pessoas podem derrubar barreiras que impedem o acesso dos atacantes em informações ou tarefas dos sistemas.

As defesas descritas na Subseção 5.7.1 são maneiras de se proteger de ataques, porém não garantem que as informações nunca sejam acessadas por pessoas sem as devidas autorizações. O principal motivo é a constante evolução dos ataques, que talvez não inovam a técnica, mas sim em como interagir com a vítima. Para isso há dicas que se podem seguir para evitar perda de dados, como uso de antivírus, realizar aquisições de aplicativos diretamente do repositório da empresa do sistema operacional, evitar acessos à *links* de *e-mails* suspeitos, entre outras.

O BYOD é uma realidade vivida em um número maior de empresas a cada ano, onde a responsabilidade com a segurança dos dados é mais preciosa. As vantagens nessa tendência faz com que as empresas passem a aderir ao uso dos aparelhos de seus funcionários com assuntos de trabalho. Porém qualquer perda de dados pode resultar em um prejuízo para a empresa, por isso é levado em conta tal risco quando a empresa pretende passar a utilizar esse meio de trabalho.

Com as intensas ações dos invasores sobre os dispositivos, empresas tentam encontrar formas de garantir uma maior segurança sobre os dados de usuários e corporações. Uma tecnologia que está ganhando espaço no mercado de *smartphones* é o *BlackPhone*, que se trata de um celular com características de um aparelho móvel normal, mas seu sistema é todo voltado para a segurança. Ele se baseia no *Android* puro, e com as devidas modificações constatadas como necessárias pela empresa *Silent Circle*, surgiu o *Silent OS*. O sistema dele apresenta diversas criptografias em ligações, troca de e-mails, troca de mensagens, e outros tráfegos de dados. Devido ao número de criptografias realizadas pelo aparelho seu desempenho poderia ser comprometido, mas seu projeto foi tão bem construído que os usuários não demonstram sentir uma lentidão em seu uso. Com essas criptografias a chance de alguma mensagem do usuário ser lida por um atacante é muito menor. Outro conceito utilizado nele foi o *Spaces*, que cria "espaços" representando outros dispositivos em um aparelho só, com isso é possível ter a divisão de dados da empresa com os pessoais, já que não há o compartilhamento de um espaço com o outro.

Referencias: https://securityaffairs.co/wordpress/10693/hacking/how-to-turn-any-phone-into-a-spy-device-with-hardware-hack.html

https://semanaacademica.org.br/system/files/artigos/jamilson_bine-estudo_de_seguranca_em_dispositivos_moveis.pdf