

Atendimento telefônico e autenticação segura

Por André Fucs de Miranda, CISSP, <afucs@cfsec.com.br>

IRRESTRITO / PÚBLICA / ORDINÁRIA

Grupo de Restrição: Irrestrito	Emissão: 29.01.2002
Arquivo: YSP_0001	Versão: 23.09.2002

Declaração de exoneração de responsabilidade

Este documento foi publicado pela CFSEC Security Architects com o intuito de fornecer, de forma rápida, informações precisas e atualizadas. A CFSEC Security Architects tentará corrigir qualquer erro que possa estar presente neste documento, tão logo seja avisada.

Entretanto, a CFSEC Security Architects não pode garantir que as informações apresentadas no mesmo estejam corretas.

A CFSEC Security Architects alerta ainda para os seguintes aspectos:

- O material difundido comporta exclusivamente informações de caráter geral, que não pretendem referir a situação específica de um indivíduo ou de uma entidade;
- Este documento pode incluir informações que não devem necessariamente estar completas, ser exaustivas e exatas ou estarem atualizadas;
- Este documento remete para sites externos, sobre os quais a CFSEC Security Architects não tem qualquer controle e relativamente aos quais declina todas as responsabilidades;
- As informações disponíveis neste documento não são pareceres de caráter profissional ou jurídico.

Todas as informações são providas pela CFSEC somente em uma base "no estado". Em nenhum evento a CFSEC será responsável pelos possíveis danos diretos, indiretos, especiais ou de qualquer outro tipo, derivados do uso deste web site, ou de qualquer outro web site que esteja ligado a este, incluindo, sem limitação, qualquer perda de lucros, interrupção de negócios, perda de programas ou outros dados de informação relacionados ao seu sistema, incluindo o caso de que nos seja expressamente informado a possibilidade de tais danos.

CFSEC Security Architects é marca registrada da CFSEC Sistemas Ltda. As demais marcas registradas são respeitadas.

Introdução:

Nos últimos anos, a busca de diversas empresas na otimização de seus processos, fez com que diversas soluções de atendimento a clientes através de telefones fossem automatizadas. Paralelamente, a popularização da informática nas empresas ampliou ainda mais a necessidade de suporte aos usuários.

Visando aumentar sua produtividade e desafogar suas centrais de atendimento, muitas empresas passaram a oferecer serviços automatizados de consulta a informações. Através de uma tecnologia denominada URA, Unidade de Resposta Audível, empresas possibilitaram que seus clientes fossem capazes de solicitar os mais diversos tipos de dados através de um simples aparelho telefônico. Em português simples e claro, a URA é um mecanismo de interface entre um usuário falando através de um telefone e um sistema informatizado.

O sucesso dessa solução foi tão grande que mesmo hoje, com os serviços Internet estão em plena expansão, as URAs continuam sendo utilizadas. Cientes disso, muitos gestores responsáveis pelo suporte de usuários, vislumbram nesse mecanismo uma forma de desafogar seus *call-centers*.

Ao assistir essa movimentação, uma pergunta torna-se latente. É possível automatizar de forma segura atividades sensíveis tais como a troca de senhas, cadastramento de usuários e liberação de privilégios? Como esses mecanismos automatizados poderiam ser aplicados para reduzir incidentes de engenharia social?

O que é autenticação forte?

Antes de prosseguir sobre o assunto principal desse documento, faz-se importante esclarecer o que é exatamente autenticação, como ela pode ser feita e o que faz um mecanismo de autenticação mais forte, isso é, eficiente, do que outro.

Autenticar é o termo utilizado para o ato de verificação de uma identidade. Em geral, é considerado forte um mecanismo de autenticação feito com base em pelo menos dois dos três mecanismos:

- Algo que você sabe;
- Algo que você possui;
- Algo que você é;
- Onde você está;

Algo que você sabe

De forma resumida, podemos definir esse mecanismo como a verificação de uma identidade com base em alguma informação de conhecimento exclusivo

que o sujeito da identificação saiba, como por exemplo, senhas ou algum outro dado pré-cadastrado.

Algo que você possui

É assim denominada a verificação de uma identidade através da propriedade de algum objeto ou dispositivo com essa função, tais como cartões magnéticos, crachás ou *smartcards*.

Algo que você é

Denomina-se assim o uso de características biológicas individuais, tais como padrões de voz, impressões digitais e **DNA** com o intuito de autenticar uma identidade. Através do estudo analítico de padrões individuais de dados biológicos, biometria, faz-se possível autenticar com grande precisão. Dentre os mecanismos, esse é o único cuja precisão do sistema afeta diretamente a autenticação de indivíduos.

FAR – *False Acceptance Rate* – representa a taxa de validação positiva de sujeitos não autorizados

FRR – *False Rejection Rate* – representa a taxa de validação negativa, isso é acesso negado – a sujeitos autorizados.

Essas taxas e a média delas – *Crossover Error Rate* – varia de acordo com o mecanismo e a tecnologia utilizados.

Onde você está

Talvez o mais raro dos sistemas utilizados, esse mecanismo de autenticação baseia-se na localização do sujeito da autenticação. Devido a complexidade de se implementar esse tipo de autenticação, poucos são os sistemas que o utilizam. Como exemplo, podem ser citadas a autenticação através de mecanismos de comunicação com GPS integrados e a autenticação com base em identificador de chamadas, sendo esse último, pouco confiável.

O modelo atual

Do ponto de vista da segurança, devemos observar um processo com base em três pilares, a integridade, a confidencialidade e a disponibilidade. O atendimento telefônico de chamados, seja ele automatizado ou não, leva à seguinte realidade:

- O volume de atendimento e a falta de automação de chamados, afetam diretamente a disponibilidade dos usuários e/ou clientes da empresa de acessar suas informações ou solucionar seus problemas.
- O vazamento de informações, que afeta diretamente a confidencialidade de informações da empresa ou de seu cliente.
- A manipulação de dados, tais como senhas que afeta diretamente a integridade das informações e pode nos casos mais graves levar à perda da confidencialidade das mesmas.

Além disso, o atendimento feito dessas formas esbarra nas seguintes limitações do sistema telefônico:

- Não há autenticação das partes envolvidas em uma ligação
- Não há cifragem da comunicação

Em decorrência dessa limitação o atendimento através de telefone depende obrigatoriamente de proteção adicional, cuja implementação vai desde um simples roteiro de conversa até aparelhos telefônicos seguros com capacidade de cifrar a voz e autenticar ambas as partes.

Considerando que os aparelhos telefônicos seguros são caros, esse documento irá descartá-los como uma solução de massa. Apesar disso, creio ser importante observar que a necessidade de segurança não é tecnológica e sim do negócio sustentado por essa tecnologia. Portanto, havendo necessidade que justifique o investimento nesse tipo de tecnologia, ela deve ser considerada como a solução tecnologicamente mais completa.

Ataques mais comuns

Quando se fala em proteção de sistemas de telecomunicações fala-se muito mais da proteção de serviços de telefonica como as caixas postais e os acessos remotos às chamadas de longa distância. As perdas relacionadas a esses problemas são mais facilmente percebidas por técnicos e gestores por estarem diretamente ligadas a prejuízos financeiros.

Esses problemas não são assunto desse artigo o que restringe o universo de ataques às infra-estruturas de call-center aos três ataques detalhados a seguir.

Replay

Como o nome indica, esse ataque consiste em utilizar alguma gravação obtida através de escuta com o intuito de realizar a autenticação em um sistema. No caso do atendimento telefônico, o atacante pode se concentrar na autenticação numérica, feita através do aparelho ou até mesmo na conversa. No caso das senhas numéricas, é interessante ressaltar que uma vez gravadas, essas senhas são facilmente¹ decodificadas dos tons transmitidos para os números discados no aparelho. O replay é o ataque mais simples de ser feito pois não requer grande habilidade e é de difícil rastreamento.

Engenharia Social

Kevin Mitnick, resume engenharia social² como “convencer pessoas a fazer o que elas não fariam normalmente para estranhos”. Já Sarah Granger define³ engenharia social como “a manipulação consciente, feita por um hacker, da

¹ <http://www.qsl.net/kb5ryo/dtmf.htm>

² <http://www.siliconvalley.com/mld/siliconvalley/news/editorial/4423008.htm>

³ <http://online.securityfocus.com/infocus/1527>

tendência humana a acreditar”. Seja como for a engenharia social é a técnica utilizada por um atacante para enganar e convencer um usuário a fornecer informações que possam levar a algum ganho, ou invasão.

Áreas de atendimento telefônico tais como suporte, centrais de atendimento ao consumidor, são especialmente sensíveis a esse tipo de ataque. Para um invasor experiente, essas áreas são como verdadeiras minas de ouro. Nos ataques típicos de engenharia social em centrais de suporte, o invasor se fará passar por um usuário leigo pedindo ajuda ou por um chefe exigindo, por meio de sua posição hierárquica, que um funcionário faça uma tarefa que normalmente não faria.

Muitas empresas com o intuito de se proteger desse tipo de ataque, requerem que seus usuários utilizem senhas ou verifiquem sua identidade através de dados como CPF, endereço para correspondência, telefones. Mais adiante nesse documento ficará claro porque esse tipo de autenticação não é seguro e portanto não deve ser utilizado em processos com grande necessidade de proteção.

Man in the middle

Em geral os ataques de maior sucesso se baseiam em personificação dupla - *man in the middle*. Nesses ataques, ao mesmo tempo em que o atacante se faz passar por atendente para o usuário alvo, assume a identidade do usuário alvo ao interagir com o atendente legítimo. Devido à ausência de mecanismos confiáveis de autenticação da origem e do destino de uma conversa telefônica, qualquer invasor que possua meios de interceptar uma chamada telefônica, pode em teoria, colocar-se entre as partes legítimas de uma conversa telefônica.

Os meios para esse tipo de interceptação vão desde a inserção de dispositivo na linha telefônica de outrem até variantes complexas, baseadas na manipulação de centrais telefônica e redes de sinalização das operadoras. Outra opção para esse tipo de ataque, é a engenharia social dupla, onde o atacante liga para ambas as partes simultaneamente ou não. Nessa variante, o atacante obtém do usuário senhas, dados cadastrais que serão informados ao atendente do *call center*.

Mecanismos de proteção

Procurando se proteger dos ataques apresentados, na tentativa de viabilizar o uso do telefone como canal de atendimento e até mesmo negócio, muitas empresas vêm optando por algum mecanismo de proteção. Os mais comuns serão apresentados a seguir.

Senhas estáticas

Senhas são sem dúvida alguma a forma mais popular de autenticação

eletrônica. Apesar da popularidade, não são raras as críticas ao mecanismo. Além do baixo nível de segurança em relação aos demais, as senhas podem ser roubadas e não são raras as reclamações de usuários quanto à necessidade de memorizá-las.

No caso do uso telefônico de senhas, restringe-se as combinações a um universo de 10 números e dois sinais (* e #) combinados de acordo com as necessidades de segurança da cada sistema. Sistemas alternativos que exigem que o usuário fale sua senha para um atendente são capazes de expandir o universo de caracteres das senhas, mas entretanto expõem as senhas à ameaças ainda maiores.

Apesar de senhas com um maior número de caracteres serem mais resistentes a ataques de força bruta, escutas telefônicas, interceptação de correspondência e ataques de engenharia social fazem dessa opção a mais insegura das três.

Dados cadastrais

Uma variante ao uso de senhas numéricas é a consulta a dados cadastrais, tais como número de matrícula, CPF, Cédula de Identidade, endereço de correspondência, telefones, etc. Apesar de em teoria expandirem o universo de combinações, dificilmente esse tipo de informação pode ser considerada como um mecanismo eficiente de autenticação. Obter esse tipo de dados tanto de usuário legítimo como de fontes ilícitas é extremamente simples. Como referência, considero interessante citar o caso noticiado⁴ no primeiro semestre de 2000 de vazamento de informações cadastrais de usuários de duas importantes operadoras de telefonia brasileira.

Reconhecimento de voz

Dentre as formas de se aplicar a biometria na autenticação de conversas telefônicas, esse é a única opção que não exige do usuário nenhum equipamento além de um terminal telefônico de boa qualidade. Através desse mecanismo, o usuário, previamente cadastrado, utiliza sua própria voz para confirmar sua identidade.

Características do sistema telefônico global fazem com que a qualidade do sinal que transmite a voz de um usuário varie significativamente de telefone para telefone. Considerando que em condições propícias, esse tipo de sistema já apresenta uma média de falsas rejeições e falsos aceites acima dos demais, essa solução não é muito recomendada para uso em larga escala.

Faz-se importante ressaltar que há no entanto produtos que afirmam

⁴ <http://www.estado.estadao.com.br/editorias/2000/05/16/eco645.html>

praticamente eliminar problemas com ruído e qualidade de sinais, elevando a confiabilidade desse tipo de sistema.

Identificador de chamadas

Assim como as centrais telefônicas mais modernas, certos modelos de PABX apresentam a capacidade de mostrar em um visor, o número de onde se origina uma chamada telefônica. Apesar de pouco utilizado por restringir demais a movimentação de usuários através de terminais aleatórios, o identificador de chamadas pode ser uma ferramenta interessante como auxílio à autenticação de chamadas. Deve se levar em conta que o sistema pode ser burlado e não é 100% confiável mesmo quando utilizado em ambientes ditos confiáveis, tais como malhas telefônicas corporativas.

Tokens / One Time Passwords

Sistemas que exigem uma senha diferente a cada vez que um usuário efetua um login são denominados **One Time Passwords**. Em geral esses sistemas são implementados em dispositivos portáteis com dimensões que variam de uma calculadora de bolso aos chaveiros. Através de complexas fórmulas matemáticas, o dispositivo gera senhas novas que apesar de derivadas de uma senha mestra, não são capazes de levar ao conhecimento desta.

Assim como as senhas convencionais esse mecanismo possui uma limitação, as senhas não devem possuir letras e demais símbolos gráficos. Ainda assim, o mecanismo criptográfico do token garante uma senha mais forte e protegida contra escutas. Apesar de não ser 100% seguro, o nível de proteção oferecido é relativamente alto.

O SecureID da RSA é hoje o mecanismo de one time passwords mais utilizado em telefonia estando disponível em alguns modelos de **PABX** mais modernos como o **OmniPCX 4400** da Alcatel. Trata-se de um pequeno dispositivo que em espaços de tempo pré-definidos, gera senhas numéricas de difícil quebra.

Em teoria, essas senhas não podem ser reutilizadas e em conjunto com uma senha cadastrada garantem a identidade do usuário. Dentre os mecanismos apresentados, o SecurID é o único que combina obrigatoriamente o uso de dois mecanismos de autenticação:

- Algo que você sabe
- Algo que você possui

Conclusão:

O uso de telefones para obter informações e atendimento é da forma atual, pouco confiável para aplicações que necessitem de ampla segurança. Inúmeros são os ataques possíveis aos sistemas que baseiam seu processo

de autenticação em senhas estáticas ou informações cadastrais. O problema é tão grave que grandes empresas brasileiras usam suas mensagens de espera para alertar seus usuários quanto ao risco de fornecer certas informações. Curiosamente, enquanto usuários são alertados, criminosos aproveitam falhas nos procedimentos de atendimento para obter acesso não autorizado aos mais diversos tipos de informação.

A automação de tarefas não elimina os ataques, levando a necessidade de autenticar de forma adequada os usuários desse tipo de sistema. Sem mecanismos fortes de autenticação, é pouco recomendável que aplicações citadas anteriormente nesse documento, tais como sistemas de re-emissão de senhas, liberação de acesso e privilégios façam uso de mecanismos exclusivamente eletrônicos.

Considerando também, que a tecnologia não demonstra ser capaz de garantir a segurança do processo completamente, mecanismos alternativos, tais como a determinação controles e limites pré-determinados de atividades, apesar de não garantirem a segurança do sistema, minimizam prejuízos que possam sofrer ambas as partes.

O uso responsável da tecnologia, atendendo as necessidades de segurança de um negócio, é a garantia de retorno de qualquer investimento em segurança da informação.

Sobre o autor

André Fucs de Miranda é Diretor de Tecnologia da **CFSEC Security Architects**. *Certified Information Systems Security Professional* pelo ISC2 e participante de diversos congressos e eventos no Brasil e no exterior, participou durante sua carreira de alguns dos mais importantes projetos brasileiros de Segurança da Informação. Membro do Association for Computer Machinery e do Information System Security Association, participa ativamente de diversos debates sobre a Segurança da Informação no Brasil e exterior.