TATIANA TEIXEIRA CARLOS DE MENEZES

SELEÇÃO DINÂMICA E ADAPTATIVA DE AUTENTICAÇÃO PARA TRANSAÇÕES BANCARIAS

São Paulo
2015

TATIANA TEIXEIRA CARLOS DE MENEZES

SELEÇÃO DINÂMICA E ADAPTATIVA DE AUTENTICAÇÃO PARA TRANSAÇÕES BANCARIAS

.

Monografia apresentada à Escola Politécnica da Universidade de São Paulo referente ao MBA em Governança e Inovação de Tecnologias Digitais com Sustentabilidade – LASSU: Laboratório de Sustentabilidade da Escola Politécnica da Universidade de São Paulo.

São Paulo
2015

TATIANA TEIXEIRA CARLOS DE MENEZES

SELEÇÃO DINÂMICA E ADAPTATIVA DE AUTENTICAÇÃO PARA TRANSAÇÕES BANCARIAS

Monografia apresentada à Escola Politécnica da Universidade de São Paulo referente ao MBA em Governança e Inovação de Tecnologias Digitais com Sustentabilidade – LASSU: Laboratório de Sustentabilidade da Escola Politécnica da Universidade de São Paulo.

Área de Concentração:
Sistemas Digitais

Orientador: Prof. Dr. Fernando Frota Redígolo

São Paulo
2015

DEDICATÓRIA

Dedico este trabalho a minha família, em especial a minha mãe, que apesar de não ter tido a oportunidade de estudar, vem ao longo da minha vida me incentivando na busca do conhecimento. Assim como eu, ela acredita que por meio do conhecimento adquirimos poder para mudar a nossa vida.

AGRADECIMENTOS

Agradeço a Deus por toda sua bondade, pelas oportunidades com as quais Ele tem me proporcionado até aqui.

"*Bem-aventurado o homem que acha sabedoria, e o homem que adquire conhecimento"* (Provérbio 3:13)

RESUMO

Atualmente pessoas e dispositivos computacionais estão conectados 24 horas ao dia, e de qualquer lugar. A área da segurança da informação vem se destacando pela sua relevante atuação diante de ações criminosas como roubo de identidade, fraude bancária, espionagem, coleta de informações sigilosas praticadas por criminosos cibernéticos dotados de características e identidades diversas, cujo acesso é difícil e complexo – são protegidos pelo anonimato.

Este trabalho tem como foco compreender algumas soluções inovadoras de segurança da informação, desenvolvidas para empresas e instituições, especificamente as que atuam na área financeira utilizando canais digitais.

A explanação do tema tem o intuito despertar nas organizações o desejo de conhecer e mensurar a importância da inovação tecnológica voltada para soluções de segurança da informação, bem como motivar a novos estudos e pesquisa sobre o assunto.

Neste trabalho, também será apresentado um estudo de caso realizado em um Banco Digital, que buscou soluções de segurança da informação, visando à prevenção de fraudes, consequentemente, a fidelização de seus clientes.

.

Palavras chave: Autenticação Adaptativa, Risk Minder, Segurança da Informação, Prevenção a Fraude, Banco Digital, Pinpoint,

ABSTRACT

Nowadays, people and devices are connected 24 hours a day, and from anywhere. The information security of the area has stood out for its important role in the face of criminal activity such as identity theft, bank fraud, espionage, collecting sensitive information, practiced by cyber criminals endowed with characteristics and diverse identities, to which access is difficult and complex - They are protected by anonymity.

This work focuses on understanding some innovative solutions for information security, developed for companies and institutions, especially those working in finance using digital channels. It is technology that once was just science fiction, those shown in movies. Today, it is pure reality.

The theme of the explanation is intended to awaken in organizations the desire to know and measure the importance of technological innovation focused on information security solutions as well as motivate further studies and research on the subject.

In this work, we will also be presented a case study in a digital bank, which sought to create information security solutions for the prevention of fraud, hence the loyalty of its customers.

Innovation is a permanent mission when it comes to information security, as the company to make that commitment, also takes on the major challenge of the quest for improvement of its services and protection of information related to your account.

Key words: Adaptive Authentication, Risk Minder, Information Security, Fraud Prevention, Digital Bank, Pinpoint,

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CA	*Computer Associates Technologies*
EMC	*EMC Corporation (empresa de gerenciamento de informações)*
IBM	*International Business Machines*
IP	*Internet Protocol*
OTP	*One Time Password*
PIB	*Produto Interno Bruto*
PIN	*Personal Identification Number*
PPCD	*Pinpoint Criminal Detection*

SUMÁRIO

1 INTRODUÇÃO

Com o advento da internet, novos hábitos e comportamento humano vão sendo adotados à medida que vantagens e comodidades são reveladas no mundo virtual. Cada vez mais sites de compras, de relacionamentos, redes sociais, bancos, órgãos públicos e demais entidades fornecedora de bens, serviços e lazer, conquistam usuários que primam pela economia de tempo e dinheiro, o que significa que locomover-se e enfrentar filas, tornou-se ultrapassado para compras e serviços: basta sentar-se diante de um computador, até mesmo com um celular nas mãos, apertar algumas teclas e tudo estará ao rápido alcance.

No contexto bancário, os serviços bancários *online* são uma maneira fácil, rápida e segura para realizar diversas transações, não apenas como uma estratégia econômica de interagir com os clientes, mas também de promover seus produtos e serviços. O modo pelo qual os clientes interagem com um banco mudou significativamente ao longo da última década. Atualmente, as instituições financeiras devem prestar serviços 24 horas em um ambiente envolvendo múltiplos canais de relacionamento entre o banco e seus clientes; com o avanço da Internet, o *Internet Banking* (acesso a partir de um computador pessoal) e *o Mobile Banking* (acesso a partir de um *smartphone* ou *tablet*) tornaram-se os principais canais de relacionamento. Em uma pesquisa realizada pela FEBRABAN (Figura 1) pode-se verificar o crescimento dos canais de *Internet Banking* e *Mobile banking,* e diminuição de outros canais, como por exemplo os caixas eletrônicos (ATMs) e atendimento em agências (CABRAL, A. Crimes Cibernéticos, slide 7,2015).

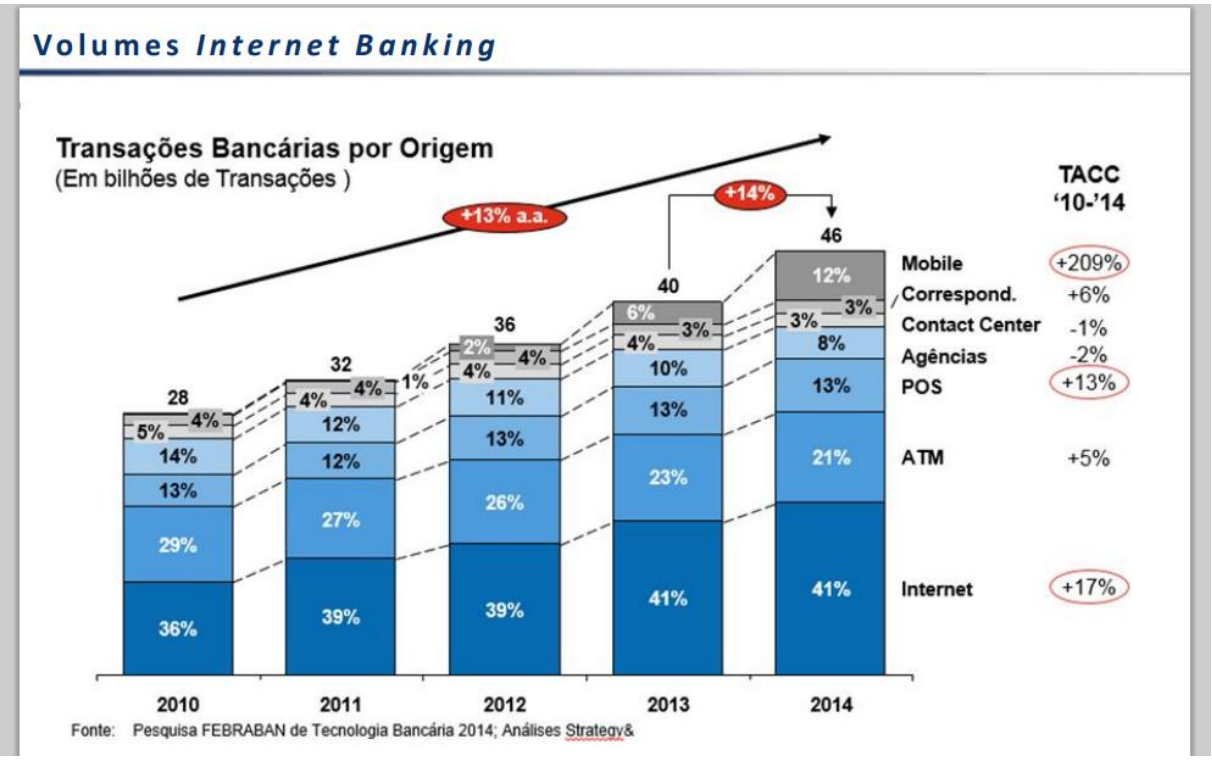

Figura 1: Pesquisa FEBRABAN de Tecnologia Bancária

Tal realidade trouxe consigo uma preocupação maior com a segurança das transações. Um dos principais tipos de fraude atuais é o roubo de identidade: Onde inicialmente, alguém rouba as suas informações pessoais e em segundo lugar, o ladrão usa essas informações para se fazer passar por si e cometer fraude. O roubo de identidade acarreta em um problema nestas operações online: como se assegurar que o usuário efetuando a compra ou consumindo o serviço é quem ele diz ser, e não um criminoso fazendo-se passar por ele ?

É portanto vital que os bancos busquem soluções tecnológicas confiáveis com alto grau de segurança para garantir ao cliente, titular da conta, que o acesso aos serviços seja realizado exclusivamente pela sua pessoa. Todas as transações devem ser incontestáveis, pois no caso de uma transação não autorizada, ou com valores alterados por um *malware* ou um *hacker*, o dano poderá ser irreparável tanto para o cliente quanto para a instituição financeira, que poderá ainda sofrer penalidades legais.

Diante dessa nova realidade, a segurança da informação tornou-se o foco deste trabalho, tendo como propósito a troca de experiências tecnológicas inovadoras na

área de segurança da informação, cujo desafio das organizações é assegurar a idoneidade moral de quem está do outro lado da Internet, evitando assim a possibilidade de fraudes, principalmente quando se tratar de roubo de identidade.

1.1 Objetivo

O objetivo deste trabalho é evidenciar a relevância da inovação de tecnologias aplicadas à segurança da informação, especificamente as que tangem às soluções de segurança, apresentar alguns conceitos e estruturas lógicas construídas por uma instituição financeira – banco digital – focada em seu cliente, a fim de garantir-lhe o sigilo de suas informações no momento da transação bancária.

Explanando este assunto, também visa à oportunidade de dar uma pequena contribuição a novos estudos e pesquisas com interesse na busca de soluções eficientes e eficazes na autenticação de usuários.

1.2 Justificativa

De acordo com a pesquisa realizada pela empresa McAfee o Brasil perdeu entre US$7 bilhões e US$8 bilhões em 2013 com ataques de hackers, roubos de senha, clonagem de cartões, pirataria virtual, além de espionagem industrial e governamental, entre outros crimes cibernéticos. Esse valor equivale a 0,32% do PIB brasileiro em 2013 (SCIARRETTA, 2014).

Diante desse panorama, os problemas de segurança vão aumentando e na mesma proporção se diversificando. O roubo de identidade tem sido preocupação constante de usuários, empresas e órgãos governamentais. Especialistas e peritos da área focam no desenvolvimento de tecnologias objetivando alcançar soluções eficazes no combate à fraude eletrônica, como por exemplo, a criação de dispositivos e sistemas de autenticação para verificar a identidade tanto dos usuários quanto dos sistemas e processos.

1.3 Metodologia

A metodologia adotada para este trabalho consiste na revisão de textos e bibliografias de autores especialistas na área da Segurança da Informação, dispostos em sites que abordam o tema, e ainda o aproveitamento da experiência de profissionais, consultores, incluindo o autor do presente trabalho, voltados às soluções de segurança, que atuam em instituição financeira.

Incialmente, é feita uma abordagem sobre a questão do roubo de identidade e suas consequências. No segundo capítulo trata-se da apresentação de algumas soluções de segurança da informação, especificamente soluções de autenticação.

No terceiro capítulo, trata-se da apresentação de alguns mecanismos de seleção dinâmica e adaptativas de autenticação.

No quarto capitulo, trata-se de um estudo de caso – Banco X – e o processo de implantação de arquitetura de segurança para canais digitais.

Por fim, as considerações finais, cuja abordagem reflete a experiência do próprio autor deste trabalho durante a participação da seleção de fornecedores, bem como da implantação das soluções selecionadas para o banco digital.

2 SOLUÇÕES DE AUTENTICAÇÃO

As soluções de autenticação consistem em mecanismos utilizados para validar a identidade dos usuários de uma operação online. Normalmente são categorizadas de acordo com a fonte da confiança no qual se baseia a solução. São elas:

- ✓ O que se sabe: segurança baseada no conhecimento de um segredo compartilhado entre o usuário e o provedor do serviço, tais como uma senha, um PIN (*Personal Identification Number*) e uma informação cadastral;
- ✓ O que se possui: baseados na posse de um dispositivo físico ou lógico pelo usuário, como uma chave criptográfica, um crachá ou um *token*;
- ✓ O que se é: baseados em características físicas do indivíduo, tais como a impressão digital, a voz, a íris, entre outros. Tais mecanismos normalmente são denominados mecanismos biométricos.

Cada tipo de mecanismos apresentam vantagens e desvantagens, que acabam por determinar um grau de segurança associada à solução. Normalmente estes mecanismos são utilizados de forma combinada, de maneira a mitigar as desvantagens de cada mecanismo, aumentando assim o grau de segurança final da autenticação: por exemplo, ao acessar o canal Internet Banking e tentar realizar uma transação bancária, o canal pode solicitar uma senha pessoal (algo que se sabe) com uma informação que é gerada a cada 30 segundos no *Token* (algo que se possui).

A seguir são apresentados os principais mecanismos de autenticação usados atualmente.

2.1 Senhas / PINs

A Senha é uma autenticação feita por meio de um segredo compartilhado apenas entre o usuário e o sistema, composta por uma combinação de letras, dígitos e outros caracteres. Alguns sistemas utilizam um tipo especial de senha denominado

PIN, composto unicamente por dígitos, para cenários onde não se deseja ou onde não é possível digitar senhas alfanuméricas.

A principal vantagem das senhas é que se trata de uma tecnologia de fácil implantação pelas empresas, tendo porém como principal desvantagem a possibilidade da senha ser capturada, roubada ou inferida.

Um dos problemas da senha é o uso de senhas consideradas fracas, ou seja, que possam ser facilmente descobertas por um atacante. Dado que a senha precisa ser lembrada pelo usuário, milhares de pessoas usam senhas básicas em suas contas para que sejam capazes de se lembrarem com facilidade, cadastrando senhas como data de aniversário, nome de animais de estimação, as quais são possíveis de serem descobertas ao serem acessadas nas redes sociais. Por esse motivo, devem ser avaliadas as regras para que as senhas cadastradas sejam consideradas fortes, a fim de dificultar que sejam descobertas.

A senha, no mercado financeiro, é utilizada para que os clientes possam ser autenticados inicialmente junto aos canais e/ou para efetivar uma transação. Em alguns casos, elas são associadas a um recurso adicional, o teclado virtual, de maneira a dificultar que os dados sejam capturados e enviados a outros computadores por meio de algum código malicioso, como o Cavalo de Tróia, por exemplo, que é capaz de gravar todos os dados digitados em teclado convencional, inclusive senhas.

2.2 Token

Os Sistemas de autenticação por *Tokens* utilizam-se do princípio de senhas de uso único (OTP – *One Time Password*), ou seja, o dispositivo de *token* gera uma senha que só pode ser usada uma única vez para a autenticação. Há vários mecanismos para a geração desta senha única. O mecanismo mais utilizado pelas instituições financeiras é a autenticação sincronizada no tempo: trata-se de um algoritmo proprietário que roda tanto no dispositivo *Token* quanto no servidor da instituição e gera números idênticos que mudam no decorrer do tempo. Ao entrar no sistema, o usuário informa sua senha de seis dígitos, fornecida no momento pelo *Token*. Ao receber a senha, o servidor localiza a chave do usuário, calcula a senha de acesso

para aquele momento, comparando-a com a que foi enviada. No caso de serem iguais, libera o acesso ou autoriza uma transação.

Atualmente, as empresas estão disponibilizando dois tipos de *Token*, ambos podendo ser utilizados sem o uso internet. O mais tradicional é o dispositivo físico, que consiste no mínimo de uma tela para exibir a senha a ser utilizada. Com a proliferação de *smartphones*, surgiu também um tipo denominado *Mobile Token*, onde o dispositivo físico é substituído por um aplicativo executado no celular, configurado e/ou sincronizado de forma apropriada com o servidor da instituição.

A solução *Token* normalmente é utilizada para uma autenticação híbrida: é utilizado tanto "algo que se possui" (o próprio dispositivo de token), como "algo que se conhece" (senha de 4 a 8 dígitos).

2.3 Autenticação via Push

A solução de autenticação via *Push* é uma tecnologia inovadora, que apesar de suas características serem menos complexas, é considerada poderosa com relação à autenticação avançada de usuários. Possui o mesmo nível de segurança do *Token* e está integrado ao *Mobile Token*. Em casos específicos para transação, essa funcionalidade previne fraudes ao associar informações sigilosas relacionadas à transação (número da conta, valor, nome destino) que ao serem processadas em determinado canal da instituição financeira serão enviadas para o *smartphone* do cliente. Após receber a notificação, o cliente verifica os dados da transação, podendo aceitá-la ou recusá-la.

Essa tecnologia exige o uso da internet para recebimento das notificações, porém de fácil usabilidade para os clientes. A Figura 2 ilustra o funcionamento da autenticação p*ush, conforme exemplificado no fluxo, mesmo que exista uma transação interceptada por um fraudador realizando "man in the middle", a confirmação ou não confirmação, é enviada para o aplicativo instalado no dispositivo cadastrado, e o retorno da confirmação ou não confirmação, somente é recebida através do mesmo dispositivo.*

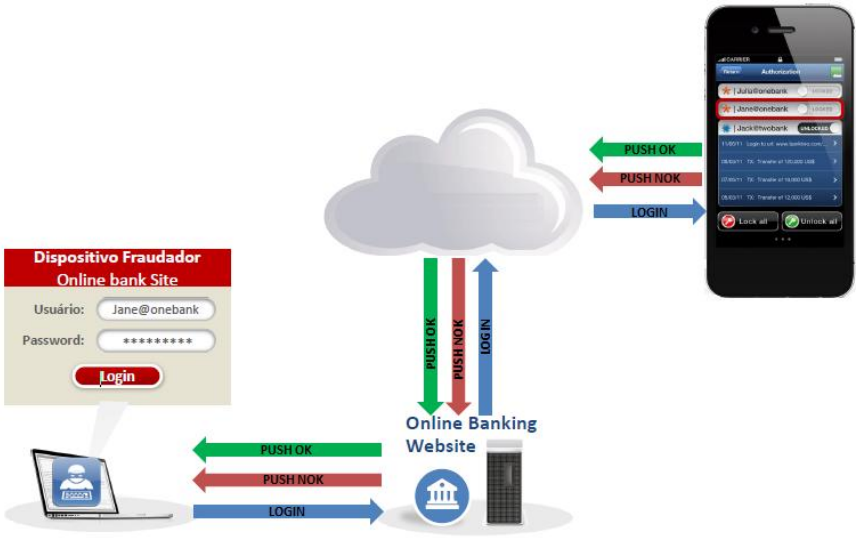

Figura 2: Autenticação via Push

2.4 Biometria

A solução biométrica consiste na verificação ou reconhecimento de pessoas por meio de alguma característica física do usuário, como por exemplo, a impressão digital, a voz, o padrão de íris, ou algum aspecto comportamental, como a escrita ou padrão de digitação. Os sistemas biométricos podem ser usados para alcançar uma identificação positiva cujo resultado possui alto grau de confiança.

O mecanismo de autenticação por biometria possui dois momentos: captura e verificação. O processo de captura consiste na digitalização e armazenamento de uma característica biológica do usuário (física ou comportamental). Na etapa de verificação da identidade efetua-se uma nova digitalização desta característica biológica, que é comparada com a informação armazenada previamente para se determinar se a pessoa é mesmo o usuário registrado e autorizado ao acesso.

Os seguintes requerimentos são utilizados para a identificação de pessoas:

- ✓ Universalidade: significa que todas as pessoas devem possuir a característica;
- ✓ Singularidade: indica que esta característica não pode ser igual em pessoas diferentes;
- ✓ Permanência: significa que a característica não deve variar com o tempo;

- ✓ Mensurabilidade: indica que a característica pode ser medida quantitativamente.

Além disso, há requerimentos importantes do sistema, tais como:

- ✓ Desempenho: refere-se à precisão de identificação, os recursos requeridos para conseguir uma precisão de identificação aceitável e ao trabalho ou fatores ambientes que afetam a precisão da identificação;
- ✓ Aceitabilidade: indica o quanto as pessoas estão dispostas a aceitar os sistemas biométricos;
- ✓ Proteção: refere-se à facilidade/dificuldade de enganar o sistema com técnicas fraudulentas.

A Tabela 1 demonstra, comparativamente, tecnologias biométricas com relação aos seus requerimentos.

Tabela 1: Comparação de tecnologias biométricas quanto aos requerimentos.

Biométricos	Universalidade	Singularidade	Permanência	Mensurabilidade	Desempenho	Aceitabilidade	Proteção
Face	Alto	Baixo	Médio	Alto	Baixo	Alto	Baixo
Impressão Digital	Médio	Alto	Alto	Médio	Alto	Médio	Alto
Geometria da Mão	Médio	Médio	Médio	Alto	Médio	Médio	Médio
Veias da Mão	Médio	Médio	Médio	Médio	Médio	Médio	Alto
Íris	Alto	Alto	Alto	Médio	Alto	Baixo	Alto
Retina	Alto	Alto	Médio	Baixo	Alto	Baixo	Alto
Assinatura	Baixo	Baixo	Baixo	Alto	Baixo	Alto	Baixo
Voz	Médio	Baixo	Baixo	Médio	Baixo	Alto	Baixo

Segundo Roberto Junqueira, membro da ABREP (Associação Brasileira de Empresas Fabricantes de Equipamentos de Registro Eletrônico de Ponto), é possível resumir as vantagens da biometria em duas palavras: segurança e conveniência.

Conveniência para os clientes, pois não necessitam decorar senhas ou portar dispositivos, porém garantem a segurança por ser características pessoais e intransmissíveis, exigindo a presença física da pessoa.

Entretanto, existem algumas desvantagens como o auto custo para implantarem eficazes sistemas biométricos e falso reconhecimento de algumas leituras biométricas quando o sistema não foi parametrizado corretamente.

3 MECANISMOS COMPLEMENTARES PARA A AUTENTICAÇÃO DE SELEÇÃO DINÂMICA / ADAPTATIVA DE AUTENTICAÇÃO

Para aplicações bancárias, entende-se que cada transação realizada pelos clientes possui um cenário diferente, levando-se em consideração, inúmeras variáveis, como por exemplo, o canal que está sendo realizada a transação; se existe valor envolvido (e o montante deste valor); se está sendo realizada a transação por meio de um dispositivo conhecido pela organização e, concomitantemente a isso existem outros fatores de segurança da informação que precisam ser considerados, a fim de evitar fraude. Cada cenário traz consigo riscos diferenciados; por este motivo, atualmente há necessidade de flexibilizar e/ou selecionar as autenticações de acordo com cada risco classificado.

As soluções de segurança combinadas servem de elementos para reduzir fraudes e impactos de uma má experiência dos legítimos clientes.

3.1 Análise Comportamental

A idéia de uma solução de Análise Comportamental é monitorar e analisar as sessões do usuário, de maneira a se inferir um risco associado àquela sessão. Durante uma transação, as informações da sessão são coletadas e usadas para gerar uma espécie de “impressão digital” do usuário, ou seja, o comportamento do cliente gera um perfil histórico. Também durante a transação são efetuadas análises em tempo real tendo por base os perfis criados anteriormente, de maneira a se identificar um risco associado à autenticidade da transação (isto é, quanto maior a certeza que a transação está sendo feita pelo próprio cliente, menor o risco associado).

Dentre as informações que podem ser usadas para se analisar o contexto encontram-se:

- Dados do dispositivo de acesso: sistema operacional, navegador, endereço IP, tipo do dispositivo (computador pessoal, *smartphone, tablet*), identificador

do dispositivo (ex.: celulares contam com um código único chamado IMEI - *International Mobile Equipment Identity*);

- Dados do acesso: localização, horário, tipo de acesso (ex.: a partir de um provedor de Internet doméstico ou de uma rede celular);
- Informações cognitivas do usuário: o estilo de digitação, o movimento do mouse, se é realizado por uma pessoa canhota ou destra;

Estas informações são armazenadas, de maneira a se criar um perfil histórico de utilização pelo usuário, facilitando a detecção acessos anômalos que podem indicar tentativas de fraudes. O perfil histórico pode envolver, entre outros, frequências de acesso (diário/semanal/ mensal) bem como dispositivos de acesso, dias, horários, localizações e tipos de acesso usuais (ex.: o usuário normalmente acessa o banco de casa, no período noturno, a partir de um computador Windows, usando o provedor NET).

De maneira análoga, a análise de contexto pode envolver uma comparação do perfil de acesso do usuário com o perfil de acesso de todos os usuários da instituição: pode-se utilizar dados do conjunto de usuários da instituição para se determinar comportamentos anômalos (ex.: um usuário demora ao menos X segundos em cada tela/página do sistema, valores menores podem indicar que é um programa malicioso efetuando a transação).

Este tipo de solução normalmente envolve uma etapa de aprendizagem, essencial para permitir a detecção de fraudes precisas, já que é necessário a criação de um perfil dos padrões de acesso às contas para estabelecer uma linha de base da atividade do cliente normal, perfeitamente diferenciada da atividade suspeita. O tempo de aprendizagem é muito variável, pois depende da aplicação protegida, dos padrões de acesso dos clientes, frequência e da qualidade dos relatórios de fraudes confirmadas fornecidos pelo cliente, outros fatores adicionais. A aprendizagem normalmente possui um lapso temporal de até três meses, mas podem existir casos que demandam maior tempo.

Uma vez tendo o perfil criado, as transações são analisadas de maneira a se detectar problemas. Dentre as análises que podem ser realizadas destacam-se:

- ✓ Detecção de Dispositivos Falsos (*Spoofed*): Coleta uma variedade de atributos, tais como: sistema operacional, navegador e endereço IP, para

gerar uma "impressão digital" única para cada dispositivo que acessa o site protegido. Os criminosos tentam alterar essa impressão digital por falsificação de atributos do dispositivo. A solução pode identificar as tentativas de falsificação, que são um forte indicador de acesso fraudulento e, se identificados, podem ser adicionados a um repositório global compartilhado entre as organizações;

- ✓ Detecção de *Phishing*: Criminosos costumam copiar o conteúdo da página da aplicação *web* autêntica e usá-lo para criar uma réplica. Algumas soluções disponibilizam um conjunto de um ou mais trechos de código para serem incorporados na aplicação web da instituição de maneira a facilitar a detecção da origem da fraude e o seu caminho a sites de *phishing*;
- ✓ Correlação de Dispositivos e Detecção de Controle: Somente a impressão digital do dispositivo é, muitas vezes, insuficiente para detectar de forma conclusiva que a conta está sendo controlada. Neste caso, podem ser correlacionados a fatores de risco de dispositivo com dados em tempo real sobre as infecções de *malware* da conta e incidentes de *phishing* para detectar com precisão o acesso criminal. Por exemplo, o acesso a partir de um novo dispositivo logo após o *malware* ser detectado em um dispositivo diferente usado com a mesma conta é uma indicação conclusiva de fraude: a conta está sendo controlada.
- ✓ Cobertura dos vetores de ataques em tempo real: Transações fraudulentas podem ser geradas através de dois vetores de ataque: de *malware* no dispositivo do cliente e transações sendo realizadas por criminosos usando credenciais roubadas e informações pessoais. Algumas soluções procuram detectar a infecção de *malware* em tempo real, parando a transação pela detecção do acesso criminal utilizando correlação de risco do dispositivo e histórico da conta do cliente.
- ✓ *Login* e Detecção de Anomalias em Transações: Detecta anomalias durante o *login* ou transações. Durante o *login*, os criminosos frequentemente apresentam características do dispositivo e de sessão anormais, como falsificação (*spoofing*) do navegador, inconsistências no idioma do sistema operacional, hora de acesso, localização geográfica ou o uso de proxies. Quando uma transação é submetida, a solução compara os detalhes da

transação para o histórico da conta e considera quantia, beneficiário e outros desvios em conjunto com outros fatores de risco.

Dentre os produtos atuais que apresentam funcionalidades de análise de contexto destacam-se: *Security Trusteer Pinpoint Criminal Detection Engine* - PPCD (IBM*), Behavioral Authentication (Biocatch) e RSA Risk-Based Authentication (RSA).*

3.2 Análise Adaptativa

A solução *Análise Adaptativa* permite realizar uma avaliação de risco em tempo real das transações e em seu resultado sugerir os dispositivos que deverão ser requisitados. Realizando a avaliação de risco da transação que está sendo executada e indica qual autenticação deverá ser realizada, sendo necessário possuir outras soluções de autenticação a serem integradas.

A solução identifica atividades suspeitas antes mesmo da ocorrência de fraude. Sendo possível, a análise de riscos adaptativos para cada fraude em potencial e, de acordo com o resultado do risco em tempo real, permitir a transação, solicitando uma autenticação adicional, ou simplesmente, negar a transação.

Durante a avaliação de risco, uma solução de *Análise Adaptativa* verifica vários fatores, incluindo a identificação do dispositivo, a localização geográfica, endereço IP e atividade do usuário, entre outras como:

- Sistema operacional utilizado pelo usuário;
- Navegador e suas respectivas versões;
- Resolução de tela;
- Java (linguagem de programação);
- Reprodutor de *flash* instalado;
- *Cookies* dos clientes;
- Tipo de conexão;

- Código ID (IMEI) do aparelho *mobile* pelo qual o cliente acessou o site e/ou aplicativo;
- Frequência de acesso;
- Padrão de utilização diário ou semanal;
- Histórico das informações referentes à data e horário de uso do site e/ou aplicativo por um determinado usuário, a partir de um determinado endereço IP.
- Análise de Comportamento;
- Configurações-padrão predefinidas;
- Mecanismo de regras configuráveis;
- Dispositivo de identificação;
- Localização geográfica/dados de velocidade;
- Gerenciamento de caso;
- Gerenciamento de fraudes multicanal.

A solução permite uma análise de risco confiável, segura e não intrusiva, pois possui capacidade de integração com multicanais, que de acordo com a estratégia da empresa, permite criar regras de negócios para cada tipo de canal.

A partir de tais informações, consegue diferenciar o processo de autenticação em relação ao risco. E quanto maior for o risco, maior deverão ser os controles para garantir a identificação do cliente.

Dentre os produtos atuais que apresentam funcionalidades de análise adaptativa destacam-se: *Risk Authentication (CA) e RSA Risk-Based Authentication (RSA).*

4 ESTUDO DE CASO – BANCO X

Neste capítulo será apresentado um estudo de caso envolvendo uma instituição financeira de São Paulo, denominada “Banco X” por razões de sigilo comercial.

4.1 Breve Histórico

O Banco X tem como objetivo ser um banco 100% digital. Tal objetivo apresenta muitos desafios relacionados à Segurança da Informação, de maneira a reduzir a ocorrência de fraudes que pode abranger desde a abertura de contas online até as transações realizadas em diferentes canais, garantindo que as transações realizadas nos principais canais como a *Internet Banking e Mobile Banking,* sejam realizadas por seus legítimos clientes.

O Banco X priorizou buscar soluções inovadoras e de alta tecnologia para a implantação de componentes corporativos de arquitetura de segurança da informação, bem como para implementar as funcionalidades de segurança relacionadas aos canais, suportados por:

- ✓ Processo de autenticação seguro, flexível, não intrusivo e inovador em relação ao mercado;
- ✓ Utilização de mecanismos multicanais, que considerem uma classificação de risco dos acessos, transações e características comportamentais dos clientes.

De acordo com o levantamento efetuado pela instituição, o Banco X identificou que até então nenhuma instituição financeira brasileira possui em suas soluções tecnológicas uma que possa avaliar o comportamento do cliente em tempo real para as transações.

A solução por elas adotada é a instalação de programas de proteção, que permita monitorar e controlar o acesso dos clientes, evitando o ataque de códigos maliciosos ou de fraudadores. Tal tipo de solução porém não foi considerada pelo Banco X, por considerá-la intrusiva.

Na Figura 4 apresenta *Benchmark* entre os bancos que atuam no Brasil

Figura 3 – Benchmark entre os bancos brasileiros.

4.2 Requisitos de Segurança e Soluções Consideradas.

Do ponto de vista do negócio as soluções de segurança deveriam contemplar os seguintes desafios:

- Soluções não invasivas, ou seja, os clientes não deveriam ser obrigados a instalar *plug-ins* administrativos em suas máquinas que pudessem interferir na rotina de acesso às máquinas e sistemas do próprio cliente, dificultando o processo para realização de outras operações que não àquelas relacionadas ao banco;
- Evitar que o próprio fraudador soubesse da existência de uma dada proteção, impedindo assim, a descoberta de pistas que poderiam revelar-lhe a solução que está por trás e incluí-la como um dos vetores de ataque;
- Detecção de transações iniciadas por códigos maliciosos (*Malware*) no dispositivo do cliente;
- Detecção de transações a partir de dispositivos do criminoso (contas comprometidas);
- Agregar decisões baseadas no risco da transação associado a regras de negócios.

O Banco X realizou uma pesquisa com algumas empresas que desenvolvem soluções de segurança, os quais estavam de acordo com a proposta de valor. A Tabela 2 apresenta as principais soluções consideradas.

Tabela 2: Produtos Considerados.

Empresa	**Produto**
EMC	*RSA Risk-Based Authentication*
CA	*Risk Authentication*
Entrust	*Identity Guard*
Biocatch	*Behavioral Authentication*
IBM	*Security Trusteer Pinpoint Criminal Detection Engine - PPCD*

4.3 Solução Implantada

De acordo com o que foi observado no estudo, o Banco X avaliou os fornecedores e motivados pela proposta de valor oferecida, decidiu utilizar uma solução de Análise Comportamental em conjunto com uma solução de Análise Adaptativa gerando um *score* de risco (em tempo real) para cada transação realizada pelos clientes.

As soluções escolhidas foram: CA *Risk Authentication* e IBM *Security Trusteer Pinpoint Criminal Detection.*

Agregar essas duas soluções permite diferenciar o processo de autenticação do Banco X em comparação aos utilizados por bancos brasileiros, gerando o diferencial. As soluções devem ser inovadoras, porém, não devem colocar em risco os acessos dos clientes e a credibilidade do banco, mas sim a redução de tentativas de fraudes.

A arquitetura funcional de segurança implantada permite que seja realizada a avaliação de risco para multicanais e de acordo com o resultado, será informado ao canal qual dispositivo de segurança deverá ser solicitado ao cliente. A Figura 3 representa a arquitetura funcional de segurança.

Na arquitetura definida, o cliente poderá realizar operações de qualquer canal, e de forma online a transação é processada, chamando os serviços *web services* da solução de análise de contexto. O retorno da análise de contexto é um dos inputs para o serviço web service da autenticação adaptativa e seu resultado é o score da avaliação de risco, sendo indicada por: baixo, médio, alto e altíssimo. De acordo com cada risco, o canal informará ao cliente qual ou quais dispositivos de segurança deverão ser solicitados como fator de autenticação.

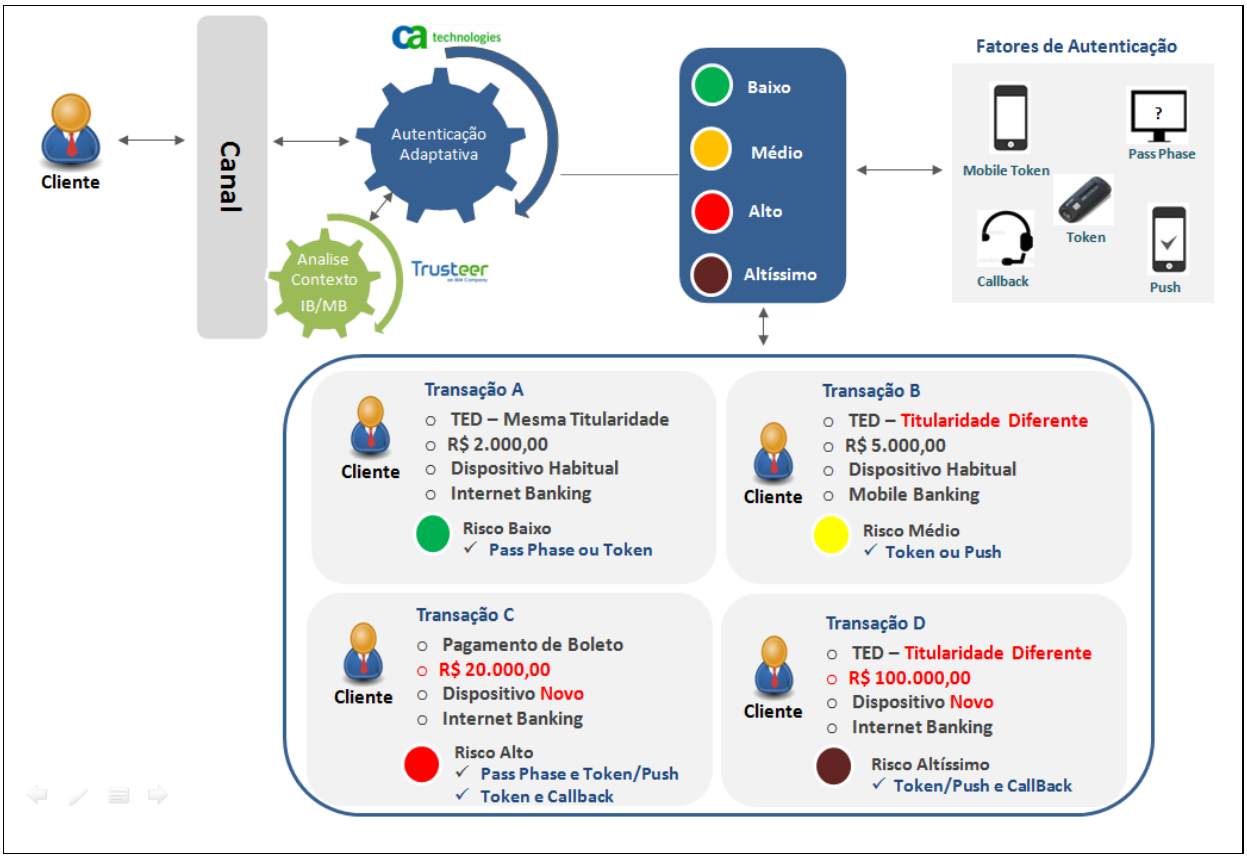

Figura 3: Arquitetura Funcional de Segurança - Banco X

Conforme descrito acima, um cliente pode apresentar diferentes comportamentos e nem por isso, significa não ser um cliente legítimo, e o outro fator, é que cada cliente terá um tipo de comportamento, e o banco precisa tratar esses comportamentos de forma diferenciada.

Desta forma, presume-se que as pessoas tendem a agir de acordo com seu comportamento anterior. Por exemplo, um cliente que acessa frequentemente da cidade de São Paulo pode ser razoavelmente esperado que continue esse comportamento. É certo que o cliente poderia se mover, mas isso é um evento incomum. Da mesma forma, as pessoas tendem a expressar uma preferência na

escolha do navegador. Se eles (os clientes) costumeiramente usam o *Chrome*, então é razoável supor que eles continuarão a fazê-lo. Assim, pode ser definido cada um deles como uma probabilidade com base em dados históricos e, em seguida, calcular uma "*Score*" (Pontuação de Anormalidade) baseada na coleção de aspectos da transação que podemos medir.

Devido, em grande parte, à iniciativa global da indústria de empregar aumento de autenticação, quando necessário em determinadas transações, os clientes rapidamente aceitam que as variações no seu padrão de comportamento impliquem em autenticação adicional. Isso tudo baseado no dispositivo do cliente (quando o cliente usar um novo dispositivo do site, a ele será informado e será solicitada a autenticação adicional).

Considera-se que a transação com mais desvios comportamentais gerais será percebida pelo cliente como sendo o mesmo fluxo. Na maioria dos sites, hoje em dia, o cliente não é informado sobre a razão da necessidade da autenticação adicional.

Para ser uma ferramenta eficaz, o modelo deve mostrar qualidades, como a consistência do comportamento atual do cliente em relação ao seu comportamento histórico. Outra qualidade importante pode ser considerada de Inteligência adicional, visto que o modelo deve gerar dados adicionais úteis para o cliente, como por exemplo, a quantificação da distribuição geográfica dos acessos do usuário (índice de mobilidade), entre outros.

Desta maneira, através da solução, após o aprendizado do comportamento, é possível estipular modelos de *score* para os cenários.

4.4 Resultados e Evoluções

De acordo com o levantamento de resultado, constatou-se que a implantação das duas soluções está sendo desafiadora, visto que cada país possui suas particularidades locais com relação à fraude. Por esse motivo, necessitam aprender

com o dia a dia e calibrar as regras de negócio para que a médio prazo possam chegar no modelo ideal.

Para o Banco X, em sua primeira fase, foram criadas aproximadamente 750 regras de negócios, sendo elas monetárias e não monetárias, cuja manutenção para essas regras exigiu um trabalho minucioso e complexo.

Neste momento, a parceria com a empresa CA, que visa dar continuidade ao desenvolvimento de *plugin* de regras e para reduzir a 100 a quantidade de regras, além de permitir melhor agilidade na manutenção das regras de negócio.

A meta da próxima fase, já com a base histórica do comportamento dos clientes, é viabilizar a criação de regras de negócios, mais complexas, cujo resultado seja 100% seguro, a ponto de assegurar que trata-se do legítimo cliente, eliminando a necessidade de autenticação de dispositivos de segurança.

Espera-se também, que essas informações sejam fatores que, através de soluções como *Big Data,* permitam o melhor relacionamento com os clientes, oferecendo a eles uma experiência única.

5 CONSIDERAÇÕES FINAIS

Este trabalho teve por objetivo compartilhar a experiência obtida pelo seu autor, com relação às atuais tecnologias de segurança da informação e prevenção à fraude disponíveis no mercado, a fim de contribuir e disseminar o conhecimento as corporações, não somente com as que atuam na área financeira, mas com as demais, presentes nos diversos segmentos do mercado de fornecimentos de bens, serviços e lazer.

Com relação ao estudo de caso do Banco X, vale ressaltar a importância de se agregar novos conceitos e valores à Segurança da Informação, com foco na manutenção e proteção de informações sigilosas das pessoas, clientes ou clientes em potencial. E ainda, há de se considerar que, as soluções relacionadas à Segurança da Informação faz parte da estratégia de negócio das empresas, não somente como prevenção, mas como uma proposta de conduta diferencial para seus clientes.

Assim, vale reafirmar que as pessoas estão cada vez mais conectadas, fazendo que as instituições sejam ágeis, flexíveis, modernas e inovadoras, sem deixar de serem simples e transparente na relação cliente e empresa. Principalmente as que atuam na área financeira, promovendo transações monetárias, como os bancos que oferecem serviços *online,* fazendo parte da vida cotidiana da maioria cidadãos. Em contrapartida: vitrine atraente para os fraudadores.

Dentro deste contexto, utilizar tecnologias avançadas é fundamental diante de inúmeros modos e meios de fraudes que vêm surgindo a cada momento, por isso, a necessidade de buscar soluções inovadoras como as que focam no comportamento do cliente e com base no seu histórico comportamental, identificar desvios.

De posse das peculiaridades de cada cliente, avalia-se a necessidade de exigir ou não uma autenticação forte para as transações bancárias quando da sua realização no canal. Considerando que o comportamento é acumulado ao longo do tempo, torna-se extremamente difícil para um fraudador representar o cliente, uma vez que o mesmo deve determinar o comportamento existente dele e imitá-lo exatamente.

Assim, com base nas experências adquiridas na implantação de soluções de segurança no BancoX, o autor deste trabalho percebe uma tendência no mercado

de empresas digitais: a utilização dos tipos de soluções de análises de riscos abordados neste trabalho. E ainda, que é de fundamental importância a inovação de soluções que buscam melhorias constantes e concomitantemente à criação de diversos modos e tipos de fraudes digitais, observando e considerando as peculiaridades existentes em cada país – eis aqui a diferença do negócio.

Essa tendência visa combater as fraudes digitais e também para proporcionar aos clientes uma nova experiência de usabilidade, sendo umas das principais das soluções fundamentadas em análise de comportamento e contexto.

REFERÊNCIAS

CURSO DE ETHICAL HACKING. **CEH**,Outubro, 2015.

MITNICK, K.D. ; SIMON, W. L. **A arte de invadir.** São Paulo: Person Prentice Hall, 2005. 236 p.

CA Risk Authentication. Reduce the risk of improper access and fraud without burdening valid users. Disponível em:< http://www.ca.com/us/securecenter/ca-risk-authentication.aspx >Acesso em 13/10/2015.

CA Risk Authentication. Disponível em:<http://www.ca.com/us/~/media/Files/DataSheets/ca-risk-authentication.PDF> Acesso em 13/10/2015.

CA RiskMinder. Disponível em:<http://www.ca.com/us/~/media/Files/ProductBriefs/CA-RiskMinder-product-brief-key-features.pdf> Acesso em 13/10/2015.

CA Security. Disponível em:<http://rewrite.ca.com/us/expertise/security.html?intcmp=headernav>Acesso em 13/10/2015.

CA Risk Analytics. Disponível em:<http://www.ca.com/us/securecenter/ca-risk-analytics.aspx> Acesso em 13/10/2015.

IBM Security Trusteer Pinpoint Criminal Detection. Disponível em: <http://www.trusteer.com/pt-br/node/182> Acesso em 13/10/2015.

REPORT, R. Risco cibernético e de reputação preocupam executivos. Disponível em: <http://www.decisionreport.com.br/publique/cgi/cgilua.exe/sys/start.htm?infoid=20971&sid=41> Acesso em 24/10/2015.

RSA Risk-Based Authentication. Disponível em: <http://www.emc.com/collateral/data-sheet/h11506-rsa-rba-ds.pdf> Acesso em 24/10/2015.

Entrust IdentityGuard . Disponível em: <http://www.entrust.com/products/entrust-identityguard/> Acesso em 24/10/2015.

CABRAL, A. Crimes Cibernéticos. Disponível em: < http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/audiencias-publicas/audiencia-publica-dia-24-09.2015/adriano-cabral-volpini-diretor-setorial-da-comissao-executiva-de-prevencao-a-fraudes-da-federacao-dos-bancos-brasileiros-febraban> Acesso em 25/10/2015.

OLIVEIRA, D. Bancos apertam o cerco contra crimes cibernéticos.Disponível em: <http://www.bandtec.com.br/index.php/bancos-apertam-o-cerco-contra-crimes-ciberneticos/ >Acesso em 25/10/2015.

SCIARRETTA, T. Brasil perde até US$ 8 bilhões com crime cibernético, 2014. Disponível em: < http://www1.folha.uol.com.br/mercado/2014/06/1467110-brasil-perde-ate-us-8-bilhoes-com-crime-cibernetico.shtml> Acesso em 25/10/2015.

TONETTO, M. Fraudes virtuais crescem 500% em um ano no Brasil; saiba como se defender. Disponível em: <http://zh.clicrbs.com.br/rs/noticias/noticia/2015/07/fraudes-virtuais-crescem-500-em-um-ano-no-brasil-saiba-como-se-defender-4792272.html> Acesso em 25/10/2015.

MERRITT, M. Roubo de identidade: Introdução. Disponível em: <http://br.norton.com/identity-theft-primer/article> Acesso em 26/01/2016.

JUNQUEIRA, R. Biometria: prós e contras. Disponível em:<http://www.abrep.com.br/site/pros-e-contras-do-sistema-biometrico/> Acesso em 26/01/2016.