U.PORTO
FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

Segurança em Sistemas Informáticos

User authentication in E-commerce

Rúben Pinto Aguiar, ei09062
Vítor Hugo Coelho Santos, ei09060

Indíce

Introdução

Dados recentes indicam que o recurso ao comércio online (e-commerce) em Portugal está em crescimento, prevendo-se um amento na ordem dos 40% até 2017. Do mesmo modo, a nível mundial se verifica esta tendência, uma vez que em 2012 pela primeira vez foi passado o bilião de dólares em transações online. Com este aumento, aumentou também a quantidade de dinheiro perdido pelas companhias e utilizadores devido a fraudes ou quebras de segurança nos sistemas. E é precisamente por isto que são necessários sistemas que permitam aumentar a segurança no e-commerce. Para este projeto, o grupo decide responder à pergunta: “como é que eu, empresa no ramo do e-commerce, posso ter a certeza que estou a vender à pessoa certa?”. Para isto foi pensado um processo de autenticação de utilizadores que lhes permitirá ter um maior controlo sobre o acesso que é feito às suas contas, respondendo ao mesmo tempo à pergunta acima colocada.

Case Studies

Para avaliar em mais detalhe a problemática em causa, o grupo analisou dois casos de empresas de venda online: em primeiro lugar a Amazon, líder mundial da área que conta com um sistema patenteado para reduzir o processo de compra ao mínimo de cliques possível, e a Caliroots, empresa sueca que utiliza o seu website como suporte ao negócio de venda em loja.

Amazon

Uma das mais antigas companhias na área do e-commerce, implementa várias medidas para aumentar a segurança dos utilizadores. O uso de SSL e HTTPS é bem-vindo, no entanto, medidas simples podiam, logo à partida, melhorar a segurança, como um indicador da força de uma password ou a proibição de uso de passwords antigas. Para além disto, o número de telemóvel de um utilizador é apenas usado para tracking de encomendas, algo que o grupo tenta alterar com a sua proposta de alteração. Uma das particularidades desta empresa é o seu sistema 1 Click que, permitindo que os dados de um utilizador fiquem registados, como a morada e o cartão de crédito, o processo de compra fica reduzido ao menor número de passos possível, tendo o utilizador apenas que confirmar a compra, não poucas vezes sem rever os dados de pagamento e envio.

Caliroots

Ainda que muito menor que o exemplo acima, a Caliroots possui de qualquer maneira um volume de negócios considerável, fruto do seu envio para todo o Mundo. No entanto, as medidas de segurança implementadas não são consentâneas com a dimensão da mesma. Logo no processo de registo existe uma falha muito grave: quando um utilizador insere a password desejada, ela é exibida em plaintext, tornando o utilizador um alvo perfeito para shoulder surfers. Como se isto não bastasse, a mesma password é enviada, novamente em plaintext, para o email do utilizador, levando a que alguém com o acesso ao mesmo tenha acesso imediato à conta criada no site. Para finalizar, em nenhuma parte deste processo é utilizado HTTPS, algo que devia ser standard.

Porque é que uma password não chega?

Apesar de ter sido desde há muito tempo o método preferencial para validação de um utilizador, o simples uso de uma password já não é tido como adequado. Roubos, colocação das mesmas ao alcance de outros ou ataques como os que são descritos de seguida levam à necessidade de um método alternativo mais eficaz.

Social Engineering

Apesar de não ser exclusiva da área dos sistemas informáticos, Social Engineering é uma prática bastante eficaz quando usada em sistemas cujos utilizadores não têm qualquer formação que os alerte para a existência desta prática, tal como é a área do *e-commerce*. Esta prática consiste no uso de técnicas de manipulação psicológica que levem os alvos a divulgarem informações confidenciais, como passwords ou respostas a perguntas de segurança, após conseguir ganhar a confiança da vítima. Existem várias técnicas que podem ser utilizadas para este fim, sendo provavelmente o Pretexting ou Phishing os mais relevantes neste caso:

- **Pretexting**, que envolve a criação de um cenário, ou uma mentira elaborada, que leve o utilizador a divulgar a informação que pretendemos. Para isto, é comum os atacantes fazerem uma investigação prévia sobre a pessoa em causa para encontrar informações verdadeiras que sirvam de ponto de partida para obter as informações que são realmente desejadas. Isto torna-se mais fácil com o advento das redes sociais, onde é muito fácil, por exemplo, obter o nome completo e data de nascimento de alguém e assim tentar, a partir de perguntas aparentemente inócuas, obter dados mais sensíveis como o NIF ,BI, etc.
- O **Phishing**, mais utilizado num ambiente eletrónico, envolve o disfarce numa entidade legítima para assim conseguir informações privadas de um utilizador. O método mais comum para isto é a difusão de emails por emails aparentemente pertencentes a entidades conhecidas, mas que redireccionam o utilizador para páginas, não raras vezes clones de páginas legítimas, controladas pelo atacante. Isto torna-se extremamente fácil através do uso de protocolos como o SMTP original, que não previa autenticação de utilizadores.

Existem outras práticas associadas a social engineering, como a difusão de falsas mensagens de infecção por vírus que levam a instalação de malware mas que não implicam o ganho da confiança da vítima, usando o medo como método.

Shoulder Surfing

Shoulder Surfing é uma técnica de observação directa para obter dados confidenciais como passwords. Como o próprio nome indica é, basicamente, olhar sobre o ombro de alguém e ver o que essa pessoa escreve. É particularmente eficaz em locais com bastantes pessoas, como cafés ou transportes públicos. Não há muitas soluções para este problema, pelo que apenas mudanças na postura do utilizador, como tapar com uma mão o que a outra escreve, ou ter o serviço, como um website, a esconder automaticamente as informações confidenciais (passwords com **** por exemplo) mitigam este problema.

Autenticação

Autenticação é o processo de estabelecer uma ligação entre um utilizador e um identificador, ou seja, certificação de que alguém é de fato quem diz ser. Existem vários tipos de prova que um utilizador pode fornecer para comprovar a sua identidade. Isto está explicado em maior pormenor na secção seguinte.

Provas em Autenticação

Para que um sistema saiba que um utilizador é quem diz ser, ou por outras palavras, para **validar** um utilizador, é necessário receber alguma informação do mesmo que só a si diz respeito. Esta informação pode ser enquadrada em três categorias, os Knowledge Factors, Possession Factors ou ainda Inherence Factors:

Knowledge Factors (Prova por conhecimento) - Comumente designado por "algo que o utilizador sabe", ou jocosamente "algo que o utilizador esquece", é a forma mais comum de autenticação, e manifesta-se na forma de passwords, respostas a perguntas específicas, PIN's ou padrões. É o principal alvo da Social Engineering, mas também pode sofrer com ataques de tentativa e erro ou ataques de dicionário.
Possession Factors (Prova por posse)- "Algo que o utilizador possui", tem como exemplo mais familiar o uso de uma chave numa porta, e prevê a posse de algo, que pode variar desde um token eletrónico para geração de códigos de acesso a smartcards ou um smartphone. No entanto, são métodos vulneráveis a roubo ou clonagem, e ainda a ataques do tipo *man in the middle (fig.1)* , em que o atacante se intromete entre o processo de autenticação e o utilizador, interceptando as mensagens e inserindo também as suas próprias mensagens para obter informações e as usar indevidamente.
Inherence Factors (Prova por propriedade)- "Algo que o utilizador é ou faz". Está associado a características específicas de um utilizador ou classe de utilizadores, como a espécie humana, e prendem-se com a utilização de identificadores biométricos como uma sequência de DNA, impressões digitais, retina, voz, etc. para autenticação de um utilizador. O problema com este tipo de autenticação prende-se com a quantidade de falsos negativos (e falsos positivos!) que tornam este tipo de sistemas pouco fiáveis. Para além disso exigem hardware adicional pelo que são apenas usados em contextos muito específicos.

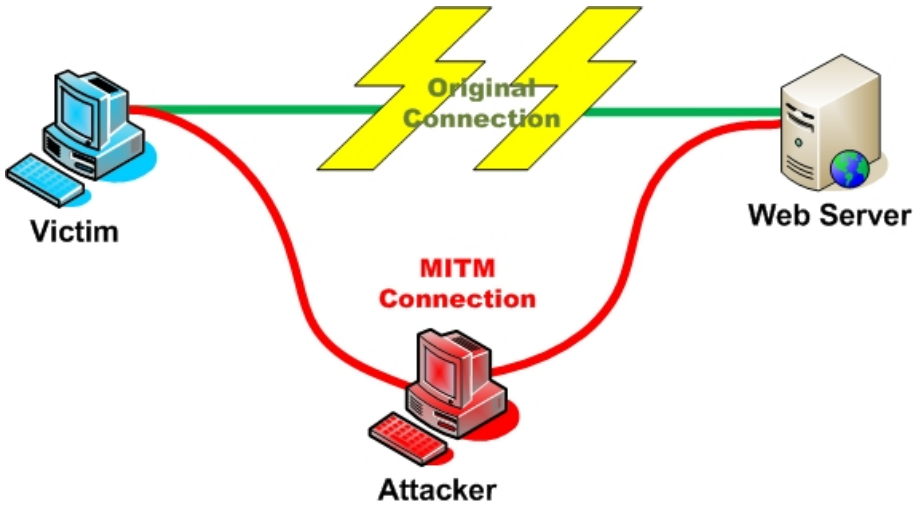

Fig. 1 - Man in the Middle Attack

Para além do uso deste tipo de fatores, existem outos tipos de prova que podem auxiliar em processos de autenticação, como a **prova por origem**, que contempla a autenticação feita a partir de máquinas específicas ou a partir de um lugar geográfico em específico.

Existem basicamente dois tipos de processo de autenticação, Single Factor Authentication, que usa apenas um dos fatores de autenticação descritos acima, sendo que o mais comum é a password, e Multi Factor Authentication, que, por ser mais relevante para o tema em causa, é descrito em mais detalhe de seguida.

Multi Factor Authentication

Como descrito anteriormente, as três categorias de Authentication Factors possuem vulnerabilidades ao nível da segurança, por isso, o passo lógico seria a combinação de mais do que um desses factores por forma a aumentar a segurança dos sistemas. A estas soluções dá-se o nome de Multi Factor Authentication. Um exemplo disto são as caixas Multibanco, que necessitam que um utilizador apresente o cartão (Possession Factor) e também o PIN respectivo (Knowledge Factor). Ao nível informático, existem inúmeros sistemas de Multi Factor Authentication, especialmente na sua forma Two-Step, onde são utilizados dois tipos de prova. Exemplo disto é a autenticação no Gmail, a qual, após validada a password de um utilizador, envia uma SMS para um número de telemóvel predifinido com um código, que pode em alternativa ser gerado numa aplicação disponível nos diversos Market, que deverá ser introduzido no Browser. A

Amazon é outra das empresas que disponibiliza uma solução deste tipo. Infelizmente, esta opção só está disponível para utilizadores da Amazon Web Services e não para utilizadores da Amazon E-Commerce.

A Solução

Para aumentar a segurança nas transações on-line, o grupo propõe um protótipo de um sistema de autenticação seguindo a filosofia do Two-Step Authentication, contando com algumas modificações para que este se torne menos intrusivo e especialmente mais adaptado à realidade das compras online, tentando mitigar a possibilidade de ocorrerem ataques do tipo *man in the middle*.

Um dos requisitos que existem ao pensar um sistema destes para uma área como o e-commerce, é que se deve evitar ao máximo a criação de custos adicionais para o utilizador. Caso isto não aconteça, o mais provável é que este irá optar por uma empresa concorrente. Paralelamente, a utilização de hardware adicional deve estar restringida a aparelhos que façam parte do quotidiano da maioria dos utilizadores. Na solução que foi desenvolvida, o grupo teve estes cuidados, pelo que soluções baseadas em Inherence Factors, ou seja, em parâmetros biométricos, acabaram postas de lado. São apenas necessários 2 dispositivos (assumindo que as compras são feitas num **computador**) ou mesmo 1 caso as compras sejam feitas por **smartphone/telemóvel**. O diagrama de sequência do funcionamento básico encontra-se na Fig. 2:

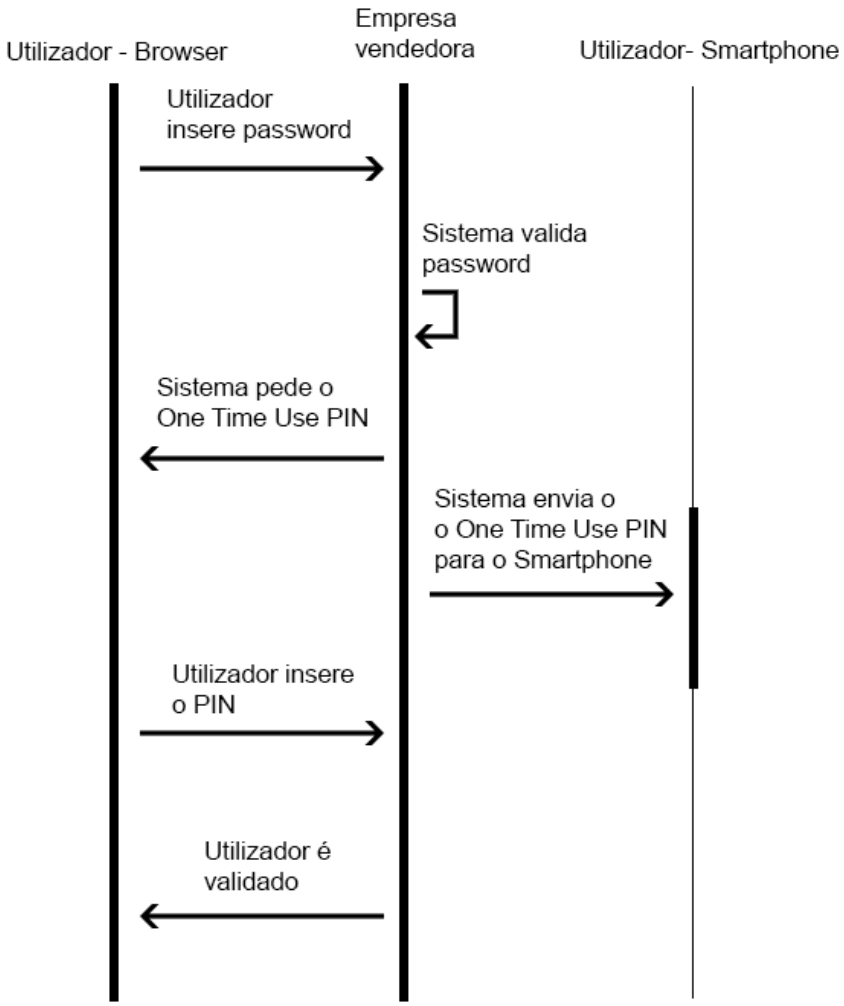

Fig 2: Funcionamento básico de autenticação (Google Authenticator)

Este funcionamento básico, à semelhança do que acontece com o **Google 2-Step Verification**, introduz o conceito de *Trusted Machines* (proof by location). Isto significa que um utilizador pode adicionar uma máquina específica como confiável, através da criação de uma *cookie* no computador do utilizador, e assim, sempre que o utilizador iniciar sessão nessa máquina não será enviado o código para o smartphone. Isto deve-se à necessidade de tornar o sistema o menos intrusivo possível e também baixar custos de implementação do sistema (envio de mensagens).

Por outro lado, este sistema por si só não só não é perfeitamente adequado à área do e-commerce como ainda é vulnerável a ataques do tipo *man in the middle* ou *cookie hijacking* (ver Riley et al). Para adaptar a solução a esta realidade e mitigar possíveis problemas, são implementadas novas medidas de segurança noutra fase do

processo de compras: a fase do checkout. Aquando do registo no site, um utilizador define um endereço pré-definido para o qual deverão ser enviadas as suas encomendas. No entanto, a grande maioria dos sites de venda online permitem que um utilizador defina uma nova morada de envio. O que o grupo decidiu como sendo uma alternativa que permite à empresa vendedora saber com um maior grau de certeza que está a enviar o produto para o utilizador legítimo e não alguém a fazer-se passar por ele é, feita a análise da distância entre as moradas de referência (a que tinha sido definida no registo e a que é definida no ato de compra) recorrendo à API do Google Maps, se esta passar um determinado limite, o utilizador recebe mais uma vez uma mensagem no seu smartphone/telemóvel, mas desta vez com dois PINS: um para confirmar a compra e outro para a anular imediatamente. Desta forma, a probabilidade de um ataque do tipo *man in the middle* tem uma probabilidade de sucesso bastante menor, pois a não ser que esteja em controlo das duas ligações da empresa ao utilizador (via sms e via browser), não há maneira de saber qual dos PIN's corresponde a que operação, e, de qualquer das maneiras, o utilizador fica a saber que alguém está a tentar realizar uma operação ilegal à sua custa. Obviamente que num sistema deste tipo o uso de HTTPS devia ser praticamente obrigatório, no entanto, com a possibilidade de haver certificados comprometidos ou a CA não ser de confiança, a solução proposta oferece mais uma barreira de segurança. Num protótipo mais avançado, poder-se-ia introduzir o conceito de livro de endereços, em que novas moradas seriam adicionadas quando fossem confirmadas via PIN.

Outra das opções pensadas, mas que cai um pouco fora do âmbito deste projeto, devido à dificuldade de implementação e necessidade de conhecimento prévio, é um sistema de alerta ao utilizador, em tudo semelhante ao que é utilizador na análise de moradas, mas aplicado ao tipo de itens que é comprado. Isto implica que o sistema "aprenda" os gostos do utilizador e decida quando deve agir. Seria uma solução interessante a aplicar num site como a Amazon que possui um excelente mecanismo de recomendação de artigos baseado no histórico de pesquisas dos utilizadores.

Desvantagens desta solução

Apesar de o grupo ser da opinião que esta é uma solução sólida para o problema apresentado, existem problemas que vêm associados com a mesma. O primeiro é uma questão de custos: podem ser enviadas várias mensagens para um utilizador, que possuem sempre um custo associado. Esse custo terá que ser assumido pelo fornecedor de serviço, que terá que abdicar de parte do seu lucro, ainda que seja uma fracção. Em segundo lugar, quanto mais camadas de segurança são adicionadas a um sistema, mais intrusivo ele se torna. O conceito de 1-Click Ordering introduzido pela Amazon acabaria por ter que sofrer ligeiras alterações com a introdução de uma solução como aquela que

é proposta pelo grupo, mas que o grupo acha que não seriam extensas o suficiente para quebrar as vantagens presentes no sistema.

Conclusões

Neste trabalho, o grupo propôs uma solução para um problema já importante a nível mundial, e com potencial para se tornar cada vez mais importante. Nesta solução, foram aproveitados elementos já em uso noutras áreas, fazendo alterações para que o mesmo se possa adequar melhor à área do e-commerce. O protótipo implementado pretende apenas funcionar como prova de conceito e não como algo funcional (os serviços de sms implicam custos e não estão disponíveis para o nosso país tendo por isso o grupo simulado o seu envio com envio de emails), e no mesmo foram feitas algumas concessões mesmo ao nível de segurança que nunca poderiam ser feitos num sistema em produção. Ainda assim, o grupo acredita que cumpriu os objetivos.

Bibliografia

1 - Authentication: An Overview, its types and Integration with Web and Mobile Applications, Basavala et al., 2012

2 - A Multi Factor Security Protocol For Wireless Payment - Secure Web Authentication Using Mobile Devices

3 - Empowering Users Against SideJacking Attacks, Riley et al.

4 - Improving Security of E- Commerce Application by using Multifactor Authentication, Yeole, Meshram, 2011

5 - http://en.wikipedia.org/wiki/Multi-factor_authentication (acedido em Dezembro 2013)

6 - www.amazon.co.uk (acedido em Dezembro 2013)

7- http://en.wikipedia.org/wiki/Man-in-the-middle_attack (Acedido em Dezembro 2013)

8 - http://web.fe.up.pt/~jmcruz/ssi/ (Acedido em Novembro 2013)

9 - http://www.social-engineer.org/ (Acedido em Dezembro 2013)