Segurança em Aplicações de Pagamento: Antecipando as Ocorrências

Luiz Gustavo C. Barbato[1], Nandamudi Vijaykumar[1], Antonio Montes[2]

[1]Laboratório Associado de Computação e Matemática Aplicada (LAC)
Instituto Nacional de Pesquisas Espaciais (INPE)
Avenida dos Astronautas, 1.758 - Jd. Granja - CEP: 12227-010
São José dos Campos – SP

[2]Divisão de Segurança de Sistemas de Informação (DSSI)
Centro de Pesquisas Renato Archer (CenPRA)
Rodovia Dom Pedro I, km 143,6 - Amarais - CEP: 13069-901
Campinas - SP

{lgbarbato,vijay}@lac.inpe.br, antonio.montes@cenpra.gov.br

Abstract. *Purchase with payment cards has been increasing. Such transactions allow cardholders to buy without cash and without necessity of going to stores. The e-commerce surfaces comforts and financial advantages to customers as well as information disclosure risks, mainly because, with some payment authentication data it is possible to perform purchases. Based on this security necessity, this paper is presenting an event anticipating approach to reduce the risks of payment application being exploited by bad guys.*

Resumo*. As compras com cartões de pagamento vêm aumentando com o tempo. Essa forma de efetuar transações possibilita que os usuários destes recursos realizem compras sem a necessidade de dinheiro em espécie e até mesmo sem estar fisicamente em uma loja. O comércio eletrônico traz comodidades e vantagens financeiras aos consumidores e ao mesmo tempo riscos de vazamento de informações, principamente porque, com certos dados de autenticação de pagamento é possível realizar compras. Com base nesta necessidade de segurança, este trabalho tem por objetivo apresentar a abordagem de antecipar as ocorrências com intuito de dimimuir os riscos de exploração em aplicações de pagamento por criminosos.*

1. Introdução

Há muito tempo atrás o comércio era puramente a base de trocas. No início as pessoas trocavam seus pertences por necessidade. Já houve um tempo onde tribos primitivas trocavam seus objetos excedentes com outras tribos. Membros de uma tribo deixavam seus pertences em locais considerados neutros e depois recolhiam os pertencem deixados pela outra tribo. E assim começava o comércio a base de trocas.

Mais tarde, grupos de pessoas se organizavam para praticar atividades específicas como agricultura, pecuária e artesanato. Nesta época todos eram produtores e consumidores ao mesmo tempo pois trocavam seus produtos entre estes grupos. Inicialmente as pessoas trocavam por necessidade e posteriormente virou-se profissão. Com esta profissionalização, as pessoas começaram a pensar em ter vantagens em cima das coisas que produziam, surgindo assim a noção de lucro. Produzir com pouco esforço e trocar por coisas mais valiosas. Esta maneira de pensar e trabalhar foi aprimorando-se ao ponto de criar um mecanismo para valorizar o que era produzido: o dinheiro.

O acumulo de dinheiro em espécie, por motivos de segurança, motivou a criação de um outro mecanismo para se comprar e vender: o cheque. Esta preocupação com segurança nos bens acumulados vem desde o início do comércio devido ao fato que grupos de pessoas não se preocupavam em produzir e sim em saquear. Ao mesmo tempo em que dinheiro era roubado, atacantes também eram mortos por pessoas que protegiam os bens dos terceiros. Baseado neste risco de morte, as técnicas de obtenção destes bens evoluiram a partir da identificação de fragilidades no processo de compra e venda utilizando cheques, dando origem às fraudes.

Assim como as técnicas de ataque, as medidas de segurança também evoluíram. Sempre que um processo era quebrado, um outro surgia para suprir as deficiências: os cartões de pagamento. Ao invés de utilizar de papéis para manipulação do dinheiro, cartões plastificados foram criados. Todo o pagamento pôde ser realizado através de cartões cujos dados eram lidos através de sistemas de alta tecnologia: os papéis carbono.Esta nova tecnologia criada facilitou ainda mais as fraudes. Pessoas descobriram que os papéis carbonos eram descartados nos lixos pelos comerciantes sem utilização de mecanismos de destruição adequados. E através destes papéis era possível clonar um cartão de pagamento pois todas as informações necessárias estavam no carbono.

Para corrigir este problema, sistemas computacionais foram desenvolvidos para permitir a leitura de dados diretamente do cartão, através de tarjas magnéticas, e submissão diretamente para os bancos. Fraudadores então, quebraram o processo de leitura e escrita nos cartões desenvolvendo leitores de tarjas magnéticas minúsculos, que podiam ser colocados próximos aos leitores originais. Novas medidas de segurança foram criadas assim como, já foram quebradas e novas estão sendo criadas mas um dia poderão ser quebradas.

Da mesma maneira que há formas de driblar o hardware também há para o software. O interessante com o software é que mesmo que as tecnologias e metodologias de desenvolvimento tenham evoluído com tempo, as vulnerabilidades são praticamente as mesmas. Os mesmos problemas de codificação que foram explorados pelo Morris Worm na década de 80 [Spafford 2004], por exemplo, continuam sendo até hoje. Fragilidades de codificação, técnicas de programação segura, vulnerabilidades conhecidas, estudos de casos podem ser encontrados em vários livros, artigos, revistas, cursos, assim como páginas públicas na Internet. Mesmo com essa grande diversidade de divulgação de problemas, as aplicações não evoluíram, do ponto de vista de programação segura, nestes últimos 20 anos.

Com base nesta fragilidade no processo de desenvolvimento de software e da constante briga entre medidas de segurança e quebras de processo, este artigo tem como

objetivo principal discutir a abordagem de antecipação das ocorrências com intuito de identificar vulnerabilidades em aplicações de pagamento antes que estas sejam exploradas por criminosos.

2. Aplicações de Pagamento

A utilização de cartões de pagamento trouxe outros benefícios para os usuários como a possibilidade de realizar compras a distância, ou seja, sem a necessidade de estar presente fisicamente em uma loja. A tele-venda permite o usuário ligar para o número do tele-atendimento escolher o produto e passar os números do cartão necessários para a autorização da transação. Já o processo de venda via Internet, conhecido como comércio eletrônico, é bem semelhante mas neste caso o usuário precisa acessar a página Web da loja, escolher os produtos e preencher um formulário com os dados do cartão. E em ambos os casos, os produtos podem ser entregues à domicílio.

Para que as empresas trabalhem com cartão, seja por Internet, televenda ou loja física é necessário possuir uma aplicação de pagamento que pode ser instalada em um computador ou utilizar uma máquina, conhecida como POS (*Point of Sale*), específica para esta finalidade. Quando essas aplicações leêm o cartão, elas se comunicam com as operadoras para solicitar a autorização da compra. Neste processo, são verificadas várias informações dos usuários, como por exemplo, limites no caso de cartão de crédito e saldos no caso de cartões de débito.

A comunicação com as operadoras pode ser realizada através de várias formas dependendo da bandeira ou marca do cartão do usuário. Geralmente quando o cartão é lido por uma aplicação de pagamento, esta se comunica com o banco adquirente que é a entidade responsável por tratar as transações de determinada bandeira de cartão e permitir ou não as transações.

Cada estabelecimento comercial pode possuir arquiteturas de rede diferentes. Há estabelecimentos que centralizam todas as transações de suas lojas, através da interconexão de redes, em um único servidor e este fica responsável pela comunicação com as operadoras. Outros preferem que cada loja possua comunicação independente. Em ambos os casos é necessária uma aplicação de pagamento que irá receber os dados de equipamentos que leêm os dados do cartão e se comunique com as operadoras. Seja comunicação direta ou através de servidores centralizados.

Os equipamentos POS se comunicam diretamente com as operadoras através de linhas discadas (*dial-up*) ou celulares (GPRS). Já os sistemas que são instalados nos computadores se comunicam internamente nas lojas através de redes IP e com as operadoras através de canais privados como X.25. As aplicações de comércio eletrônico podem trabalhar de várias formas. A maneira mais comum é redirecionar automaticamente os usuários para as páginas Web das operadoras quando estes selecionam opções de pagamento por cartão de crédito. Assim, os estabelecimentos nunca recebem os dados de cartão dos usuários. Uma outra maneira é o próprio estabelecimento receber os dados e transacionar com as operadoras através de aplicações de pagamento internas.

Os tele-vendas podem receber os dados manualmente, ou seja, os usuários falam os números do cartão para os atendentes e estes acessam as aplicações de pagamento, ou

quando a opção de pagamento por cartão é escolhida, o usuário pode ser automaticamente redirecionado para uma URA (Unidade de Reconhecimento Auditiva). E uma terceira forma é os usuários passarem os dados e os atendentes acessarem o próprio sistema de comércio eletrônico da empresa, da mesma forma que o usuário poderia fazer.

Em todos os casos há fragilidades nos processos que podem colocar em risco os dados dos usuários. Algumas fragilidades são inerentes ao processo manual e humano de realizar as operações e outras são baseadas no desenvolvimento inseguro de aplicações de pagamento. Os problemas de projeto e implementação dos sistemas podem ser explorados tanto localmente quanto remotamente por criminosos. E uma vez que estas pessoas consigam acessos aos sistemas, os dados de cartão dos usuários podem ser capturados e utilizados para realização de transações.

3. Antecipando as Ocorrências

Levando em consideração a fragilidade em geral dos sistemas desenvolvidos devido a não preocupação com o desenvolvimento seguro, a melhor alternativa para garantir a segurança das aplicações de pagamento é colocá-las a prova de testes profundos e técnicos conhecidos como testes de penetração ou invasão. Se os atacantes possuem conhecimento para explorar vulnerabilidades em sistemas, esse mesmo conhecimento deve ser utilizado no processo de testes visando única e exclusivamente a identificação das brechas antes que estas sejam exploradas.

Utilizando esta abordagem é possível verificar todas as partes ou interfaces externas do sistema da mesma forma que um atacante faria. Estas verificações são consideradas cegas porque quem analisará o sistema não possuirá conhecimento profundo sobre a arquitetura e desenvolvimento. Algumas informações sobre o sistema que está sendo testado podem ser obtidas perguntando para próprio sistema através de requisições do protocolo utilizado. Toda essa interação entre o testador e o sistema é conhecida tecnicamente como testes de caixa preta. E é através dessa constante interação que é possível mapear todo o sistema do ponto de vista externo e assim encontrar possíveis locais onde os testes deveriam ser realizados com mais profundidade.

O mapeamento do sistema pode dar uma visão bem profunda ao testador dependendo da forma como é realizado. Uma verificação que antes era conhecida como cega, pode agora se tornar bem clara e com visão abrangente. Tão abrangente que pode mostrar possibilidades de entrada que não foram encontradas antes nem mesmo pelos próprios desenvolvedores. Olhar para um sistema sem pensar em impossibilidades de acontecimentos é a melhor forma de se encontrar vulnerabilidades. E é assim que criminosos pensam quando atacam sistemas. Portanto esta maneira pensar e agir deve ser trazida para o lado da segurança de sistemas e principalmente para o ciclo de desenvolvimento de software.

Todas as etapas do ciclo de desenvolvimento de software podem ser tratadas do ponto de vista de segurança, desde o levantamento inicial dos requisitos até a etapa de entrega do software ao cliente, ou seja, desde o mal entendimento dos ativos principais do sistema que devem ser protegidos até a entrega de software modificado com códigos maliciosos embutidos. O projeto do sistema é uma etapa extremamente importante pois

é nesta etapa que a arquitetura é discutida. E mais fundamental ainda é a implementação ou codificação, onde diagramas e desenhos são convertidos em linhas de código. Linhas estas, que podem conter defeitos de programação insegura e possibilitando assim a injeção de códigos maliosos que exploram as fragilidades e permitem acesso, que por projeto não era permitido, aos sistemas.

Tendo como base as preocupações com programação insegura, desenvolvedores adotam certas medidas de segurança para impossibilitar que seus sistemas sejam comprometidos. Algumas implementações são feitas com base no mal entendimento das técnicas de ataque aumentando assim, a falsa sensação de segurança. Se as técnicas de ataque não forem bem conhecidas pela equipe de desenvolvimento, os códigos podem ser inocentemente criados. Para cada vulnerabilidade conhecida há formas de escrever códigos para corrigí-la corretamente ou não permitir pelo menos que sejam exploradas. Um código pode até ter problemas internos mas se não houver uma maneira externa de acessá-lo, a vulnerabilidade pode não ser explorada e consequentemente o sistema pode não ser comprometido.

Há medidas de segurança que são verificadas com mais profundidade pelos atacantes, que é caso da validação de entrada por exemplo. Dependendo da forma com que esta validação é realizada, é possível driblá-la utilizando caracteres e funções de controle inerentes da própria plataforma utilizada para o desenvolvimento. Neste caso, o que está sendo explorado é a implementação insegura de uma medida de segurança que se não for verificada com atenção, a aplicação pode estar sendo protegida através da falsa sensação de segurança. O mesmo acontece com outras partes que podem exploradas, tais como, comunicação, controle de sessão, configuração, autenticação, autorização, etc [OWASP 2007].

Sistema que ainda não foi comprometido não pode ser considerado seguro devido ao fato do sistema ainda não ter sido atacado por criminosos motivados. Alguns ataques são realizados de forma aleatória mas outros são realizados direcionalmente. Neste último caso, essas pessoas estariam procurando brechas nos sistemas pois são motivadas por alguma razão. Em aplicações de pagamento a motivação primordial é financeira pois o resultado do ataque é a obtenção de dados de cartão com intuito de realização de fraudes.

Analisando a forma apresentada que aplicações de pagamento trabalham, é possível identificar várias partes que precisam ser verificadas com certa atenção. Tomando como base as aplicações de comércio eletrônico, é extremente importante analisar as possíveis entradas de dados com intuito de encontrar maneiras de chegar até o banco de dados que contem cartões, se a aplicação permite o redirecionamento de páginas para uma outra aplicação falsa clonada, se os usuários são corretamente autenticados ou se é possível driblar este processo, quais operações um usuário pode executar e se é possivel aumentar o privilégio, a possibilidade de acessar recursos teoricamente ocultos ou desconhecidos pelos próprios desenvolvedores, se é possível fazer com que a aplicação mostre mais informações que inicialmente não era permitido, etc. Enfim, o importante é entender como a aplicação trabalha, quais são as regras de negócio e tentar encontrar maneiras de domesticar a aplicação, em outras palavras, fazer com ela trabalhe da forma que o testador queira e não da forma como foi projetada.

O mesmo acontece com aplicações de pagamento internas. A comunicação com os leitores de cartão visando identificar maneiras de interceptá-la, o recebimento de dados pelo sistema operacional, a alocação de memória da aplicação, as chamadas a bibliotecas dinâmicas, a comunicação inter-processo, a criação de arquivos temporários, as formas de armazenamento de dados, o protocolo de comunicação entre a aplicação cliente e servidora, são exemplos de pontos que precisam ser verificados. Os mesmos pontos se estendem às outras partes da arquitetura como as aplicações servidoras. O mais importante na hora de testar é pensar em pontos onde a aplicação pode ser quebrada e principalmente esquecer da impossibilidade dos acontecimentos pois é nesta impossibilidade que os sistemas são explorados, comprometidos e dados são capturados.

4. Considerações Finais

Dados comprovam que, atualmente cada vez mais pessoas aderem ao pagamento por meio de cartões no Brasil. Este número vem crescendo espantosamente. Segundo a Folha em uma matéria publicada no dia 10 de setembro de 2007 *O uso de cartões para o pagamento de contas no varejo fez o cheque perder a posição de liderança entre os meios mais utilizados pelos consumidores brasileiros. O papel ficou em primeiro lugar entre 2001 e 2005, mas perdeu a posição no ano passado, quando foram feitas 1,737 bilhão de operações com cartão de crédito, contra 1,622 bilhão de cheques compensados*[Ribeiro (2007)]. Um outro dado interessante publicado no dia 13 de setembro do mesmo ano na Gazeta Mercantil mostra que *o mercado brasileiro de cartões de crédito deve registrar ao final de setembro faturamento de R$ 15 bilhões, crescimento de 19,8% em relação ao registrado em setembro de 2006*[Gazeta Mercantil (2007)].

Já que a tendência é utilizar cartões cada vez mais, antecipar as ocorrências é a melhor abordagem de verificação da segurança das aplicações de pagamento antes que sejam colocadas em produção. Identificar maneiras de quebrar a lógica de negócio em laboratório pode diminuir muito o impacto de um comprometimento. Investir nesta etapa pode evitar grandes prejuízos financeiros tais como perdas de clientes e multas por vazamento de dados de cartão. Contratar pessoas qualificadas para realizar tais testes é uma atividade que será muito mais comum em futuro mais próximo. De qualquer forma, o importante é encontrar os problemas dentro de casa e antes que criminosos façam.

7. Referências

OWASP (2007), TOP Ten 2007. http://www.owasp.org/index.php/Top_10_2007.

Ribeiro, A. P. (2007), Cartão toma lugar do cheque como meio de pagamento mais usado. Folha de São Paulo. http://www1.folha.uol.com.br/folha/dinheiro/ult91u327219.shtml.

Gazeta Mercantil (2007), Cartões de crédito devem movimentar R$ 15 bi. http://www.gazetamercantil.com.br/integraNoticia.aspx?Param=3%2C0%2C+%2C829559%2CUIOU

Spafford, Eugene H (2004). The Internet Worm Program: An Analysis. http://homes.cerias.purdue.edu/~spaf/tech-reps/823.pdf