Metodologia de Identificação de Vulnerabilidades em Aplicações de Pagamento

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 Tecnologia da Informação Renato Archer (CTI)
Rodovia Dom Pedro I, km 143,6 - Amarais - CEP: 13069-901
Campinas - SP

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

Abstract. *Shopping with payment cards has been increasing. Such transactions allow cardholders to buy without cash and moreover, nowadays, even without necessity of going to stores. The e-commerce surfaces comforts and financial advantages to customers. However, it may also bring information disclosure risks, mainly because, due to some payment authentication data it is possible to perform purchases. Based on this security necessity, this work is presenting a metodology to identify vulnerabilities to reduce the risks of payment application being exploited by crime.*

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, principalmente porque, com certos dados de autenticação de pagamento é possível realizar compras. Com base nesta necessidade de segurança, este trabalho tem por objetivo apresentar uma metodologia para identificação vulnerabilidades com intuito de diminuir os riscos de exploração em aplicações de pagamento por criminosos.*

1. Introdução

A utilização de cartões de pagamento trouxe outros benefícios, além da praticidade e crédito, 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 específica para esta finalidade. Quando essas aplicações recebem os dados de 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 cartões de crédito e saldos no caso de débito.

Em todos os casos de utilização de aplicações de pagamento, 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.

Com base nas fragilidades existentes e no alto impacto do comprometimento de dados de cartão, este artigo tem como objetivo principal apresentar uma metodologia para identificação de vulnerabilidades em aplicações de pagamento antes que estas sejam exploradas por criminosos.

2. Metodologia de Identificação de Vulnerabilidades em Aplicações de Pagamento

O mapeamento correto de uma aplicação pode dar uma visão bem profunda às pessoas que estão a analisando. Uma verificação que antes poderia ser considerada como cega, pode 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 uma aplicação 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.

Para auxiliar na organização do processo de avaliação de segurança visando identificar vulnerabilidades [OWASP 2007] e atingir partes profundas da aplicação não cobertas pelos procedimentos de teste de segurança convencionais, como os do PCI DSS[PCI SSC 2008] por exemplo, a seguinte metodologia foi desenvolvida. Esta é basicamente dividida em cinco grandes etapas onde é possível identificar as todas as vulnerabilidades conhecidas que normalmente são encontradas em aplicações de pagamento. As etapas são: recepção de dados, processamento de dados, armazenamento de dados, distribuição de dados e gerenciamento de acessos. Essas etapas são aplicadas em três fases fundamentais onde em cada uma delas o nível de aprofundamento e técnico da análise vai aumento.

A primeira fase é a avaliação de segurança, onde são realizadas entrevistas com base na utilização da aplicação como um usuário final. A segunda é a verificação de segurança, que trata a utilização da aplicação com o objetivo de tentar driblar regras de

negócio e medidas de segurança. Já a terceira aborda a revisão de segurança para permitir que as origens das vulnerabilidades sejam encontradas, assim como, identificar outras, que por ventura, não foram diagnosticadas anteriormente, com base na leitura do código fonte.

Em cada fase são aplicadas as cinco etapas mencionadas porém com abordagens e focos diferentes. Essas etapas são importantíssimas na condução da execução das três fases devido ao fato delas dividirem uma aplicação em partes onde concentram-se as vulnerabilidades em aplicações de pagamento. A seguir serão apresentadas as cinco grandes etapas e logo após as três fases fundamentais.

As Cinco Grandes Etapas

1)Recepção de Dados

Esta etapa visa mapear as formas como as aplicações de pagamento recebem dados externos assim como os protocolos utilizados neste processo.

a.Transmissão de dados para a aplicação de pagamento

O primeiro passo é pensar na aplicação sob perspectiva externa como um poliedro onde cada uma de suas faces fosse uma possível fonte de dados.

b.Recebimento de dados pela aplicação de pagamento

Depois de analisar a manipulação de dados sob uma perspectiva externa, agora é a vez de averiguar como estes entram dentro da aplicação.

2)Processamento de Dados

Esta etapa visa mapear as formas como as aplicações de pagamento processam os dados internamente, incluindo, regras de negócio e comunicação entre módulos internos.

a.Utilização de dados pela aplicação

O primeiro passo é identificar as tecnologias envolvidas na arquitetura da aplicação com intuito de mapear as possíveis formas de utilização de dados internamente.

b.Transferência de dados dentro da aplicação

Logo após a identificação das possíveis tecnologias envolvidas na implementação das regras de negócio, é importante mapear os módulos e as formas de comunicação inter-processos.

3)Armazenamento de Dados

Esta etapa visa mapear as formas de armazenamento e manipulação dos dados pelas aplicações de pagamento com o objetivo de identificar possíveis pontos de vazamento, fragilidades na retenção e maneiras de capturá-los.

a.Armazenamento de dados pela aplicação

O primeiro passo é identificar os locais onde os dados podem estar armazenados com intuito de mapear as possíveis formas de acesso.

b.Manipulação de Dados

Uma vez armazenados, os dados podem ser requisitados para serem utilizados e este processo precisa ser verificado visando identificar possíveis fragilidades que possibilitam a captura indevida.

4)Distribuição de Dados

Esta etapa visa mapear as formas como os dados são tratados e distribuídos para entidades externas a solução da aplicação de pagamento, como por exemplo, para o usuário final e outros sistemas em geral.

a.Tratamento de dados

O primeiro passo é tentar levantar os tipos de dados que saem da aplicação e como eles são apresentados com intuito de identificar formas de saída de dados indevidos.

b.Distribuição de dados

Após a identificação dos dados e formas como são preparados, é a vez levantar como eles são entregues às entidades solicitantes visando encontrar fragilidades na distribuição.

5)Gerenciamento de Acessos

Esta etapa visa mapear as formas como os acessos são controlados, as permissões são concedidas, as sessão são gerenciadas e as requisições são controladas.

a.Autorização de Entidades.

O primeiro passo é mapear os perfis de acesso para que depois seja possível identificar formas de driblar permissões de acesso.

b.Controle de Sessão

Uma outra atividade importante que precisa ser investigada é o controle de sessão com intuito de identificar formas de seqüestrá-la e executar comandos se passando por usuário da aplicação.

A tabela a seguir apresenta as principais perguntas para auxiliar na identificação de vulnerabilidades em cada uma das etapas apresentadas.

Tabela 1. Principais perguntas para identificação de vulnerabilidades

1. Recepção de Dados	**2. Processamento de Dados**
Por onde os dados entram na aplicação?	Quais as tecnologias envolvidas na aplicação?
Quais protocolos são utilizados na recepção?	Como os dados são utilizados dentro da aplicação?
Quais proteções são utilizadas na recepção?	Como as regras de negócio são implementadas?
Quais dados são recebidos?	Quais são os módulos internos?
Que tipos de dados a aplicação trabalha?	Quais são as formas de comunicação inter-processos?
Como a aplicação valida uma entrada?	Como os dados são trocados dentro da aplicação?
3. Armazenamento de Dados	**4. Distribuição de Dados**
Quais dados são armazenados?	Quais dados são distribuídos?
Como os dados são armazenados?	Como os dados são preparados para distribuição?
Como os dados são protegidos no armazenamento?	Como os dados são validados antes da distribuição?
Como os dados são manipulados dentro da aplicação?	Como os dados são distribuídos?
Como os dados são requisitados?	Quais protocolos são utilizados na distribuição?
Como os dados são removidos?	Quais as proteções na distribuição?
5. Gerenciamento de Acessos	
Quais são os perfis de acesso?	
Como são controlados os acessos?	
Quais as permissões de acesso?	
Como a sessão é gerenciada?	
Como os identificadores de sessão são criados?	
Como as equisições são controladas?	

As Três Fases Fundamentais

1)Avaliação de Segurança

A primeira fase é destinada a entrevistas com os fabricantes da aplicação e a utilização da aplicação para conhecimento do alvo da avaliação. O entendimento correto da aplicabilidade e funcionamento da aplicação de pagamento é fundamental para o mapeamento de possíveis pontos de comprometimento e identificação de supostas vulnerabilidades. Conversas com desenvolvedores podem também ser bastante esclarecedoras porque além de entender algumas possíveis implementações, em algumas situações, eles mesmos podem apresentar problemas existentes. As entrevistas e conversas são conduzidas pelas cinco grandes etapas com intuito de abordar todo ciclo de vida de um dado e formas de acesso. As perguntas apresentadas servem como guia durante a entrevista.

2)Verificação de Segurança

A segunda fase tem por finalidade identificar vulnerabilidades durante a utilização da aplicação assim como maneiras de driblar a lógica de negócio e medidas de segurança. Algumas supostas vulnerabilidades encontradas na fase

anterior podem ser comprovadas com a verificação de segurança. Analisar uma aplicação por outras perspectivas é a base para a identificação de vulnerabilidades que por ventura podem não ser encontradas através de testes de segurança convencionais. Nesta fase, comunicações são interceptadas, parâmetros de entrada são alterados, dados em memória são modificados, dentre outras formas de verificação. As cinco grandes fases apresentam locais de averiguação e utilização de possíveis ferramentas caso seja necessário. Nesta fase, as perguntas servem para ser respondidas através das verificações realizadas.

3)Revisão de Segurança

A terceira fase visa revisar a aplicação de pagamento sob uma perspectiva interna, ou seja, através de seu código fonte. Esta fase, além de ser fundamental para encontrar a origem de uma vulnerabilidade e propor soluções de correção, é extremamente importante na identificação de vulnerabilidades não encontradas pelas fases anteriores, como as que dependem de certas condições para serem exploradas. Durante a revisão é possível saber exatamente quais são essas condições e preparar formas de comprovação prática da existência das vulnerabilidades. As cinco grandes fases servem como um guia durante uma leitura de código fonte pois apresentam exatamente os locais onde deve-se ser revisado. E as perguntas deixam mais claros os pontos de possíveis vulnerabilidades.

4. Considerações Finais

Analisando a forma como 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 extremamente 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 possível 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 driblar as regras de negócio e controles de segurança antes que pessoas mal intencionadas façam.

5. Referências

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

PCI SSC (2008), “Payment Card Industry - Data Security Stantard”. https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf

PCI SSC (2008), “Payment Card Industry – Payment Application - Data Security Standard”. https://www.pcisecuritystandards.org/pdfs/pci_pa_dss.pdf