How to design more secure online payments systems: the lesson learned from the analysis of security incidents

Marco Morana

Venezia, 27 settembre 2013
How to design more secure online payments systems: the lesson learned from the analysis of security incidents
Soluzioni e sicurezza per applicazioni mobile e payments

Consorzio Triveneto, azienda leader nei sistemi di pagamento a livello italiano da sempre all'avanguardia nello studio e nella sperimentazione di nuove tecnologie nell'ambito dei pagamenti, è una realtà del Gruppo Bassilichi che opera prevalentemente nei campi della Monetica – con la gestione dei servizi POS e di Commercio Elettronico – e del Corporate Banking a supporto delle imprese.

SPONSOR DELL’EVENTO

Sponsor e sostenitori di ISACA VENICE Chapter

Con il patrocinio di
About Me and This Talk

1. What is my role today? I lead a global team of security architects and analysts whose responsibility is to secure engineer mobile applications used by millions of private clients in several countries in the world. These applications bear the highest financial and security risks.

2. What is learnt in my career as security technologist? Today cyber-security risks are business risks, for risk managers, security auditors, security consultants it is imperative to be able to analyze threats and translate technical impact risks to business impacts.

3. What are the goals of this talk? Provide the rationale for factoring threats and risk analysis in the risk strategy for mitigation of the security risks of online banking and payments. Provide a process and a tool for modeling and managing the technical and business risks caused by insecure design and lack of adequate countermeasures for emerging cyber threats.
What I hope you can learn from my talk..

1. **How the cyber-threat landscape has evolved** in attack sophistication and the evolution of the cyber threat actors

2. **The lessons CISOs can learn from the security incident’s post-mortem** from publicly disclosed security incidents, open source intelligence as well as from their own sources

3. **The risk mitigation strategy can be adopted** by security managers to effectively mitigate the risk of cyber threats and mitigate the technical and business impacts of payment fraud

4. **The tactical risk processes and tools** that can be used to analyze threats, model attacks and design countermeasures against cyber attacks against online payment systems
Cyber Threats Evolution in Attack
Sophistication and Threat Agents
Motives and Capabilities
The Evolution of Cyber Threat Actors

Threats: Basic Intrusions and Viruses
Motives: Testing and Probing Systems and Data Communications
Attacks: Exploiting Absence of Security Controls, Sniffing Data Traffic, Defacing

Threats: Script Kiddies, Viruses, Worms
Motives: Notoriety and Fame, Profit from renting Botnet for spamming
Attacks: DoS, Buffer Overflow Exploits, Spamming, Sniffing Network Traffic, Phishing emails with viruses

Threats: Fraudsters, Malware, Trojans
Motives: Identity Theft, Online and Credit/Debit Card Fraud
Attacks: SQLi, Sniffing Wireless Traffic, Session Hijacking, Phishing, Vishing, Drive by Download

Threats: Hacktivists, Cyber crime, Cyber Espionage, Fraudsters, Malware
Motives: Political, Stealing Company Secrets and Clients Confidential and Credit Card Information for Fraud
Attacks: DDoS, Defacing, Account Take Over/Session Hijacking, SQLi, Spear Phishing, APT, RAT

WHAT NEXT?
The evolution of attack techniques and technologies
Technology evolution of online payments and banking applications/technologies

Welcome to Internet Banking

To log on, enter your User ID and Password.

Log on details

User ID
Password
Remember my User ID for this computer

Unable to log on? Continue

How to design more secure online payments systems: the lesson learned from the analysis of security incidents
Mobile wallets and security design flaws

Google Wallet hacked again; new exploit doesn’t need root access [video]

By Zach Epstein on Feb 10, 2012 at 8:10 AM

http://youtu.be/Rh1ytHrhj2E
Which lessons we can learn from security incidents?
Cyber-attacks against traditional financial systems: ATMs processing prepaid cards

Global cyber, ATM heist nets thieves $45 million from 26 counties

Eight people have been arrested in New York for participating in a global scheme that stole ATM PINs and siphoned millions from banks and other financial institutions around the world.

Card Payments and Online Fraud Schemes

- **Account takeover**: hijacking authenticated session for transferring money to a fraudulent account or making fraudulent purchases.

- **Card application fraud**: using stolen personal data for opening bank account and for applying for new credit/debit cards.

- **Card non present fraud**: online payments and purchases with stolen credit cards and personal data.

- **Card present fraud**: criminal approaches a merchant and uses fraudulent means to pay for it, such as a stolen or counterfeit card made with credit/debit card data and personal information stolen online.

- **Card counterfeiting fraud**: validation of stolen credit card data (PANs, CVVs, PINs) using online banking web sites for the sake of counterfeit cards.

- **Identity theft fraud**: someone assume your identity through social engineering, phishing for PII with malware/keylogger and man in the browser to perform a fraud or other criminal act.

- **Internet fraud**: non-delivery of items ordered online and credit and debit card scams.
Fraud and Mobile Risks, Food for Thought

- U.K. Identity fraud totalled £3.3 billion in 2012 and affected 27% of the UK adult population (source National Fraud Authority, June 2013)
- Mobile malware increased by 400% in 2012 and Mobile related data breaches are expected to grow (source Verizon DBIR 2013)
- Payment card fraud, phishing attacks and check fraud are the top three fraud threats financial institutions face in 2013 (source Security Media Group, faces of Fraud Survey, 2013)
- Wire and ACH fraud is on the rise despite the investment anti-fraud technologies, IP reputation based tools, dual-customer authorization and customer education (source Security Media Group, faces of Fraud Survey, 2013)
- 45% of service providers, 40% of card issuers use device identification for mobile fraud prevention but 55% of merchants can’t detect a transaction from mobile device (source Kount 2013)
- 60% mobile apps don’t have a privacy policy notifying consumers which of their data the apps access (Source: InfoWorld March 2012)
Risk mitigation security strategy for online and mobile payment systems
Cyber risks mitigation strategy for online payments

1. Meet technology security standards and regulations
   - Payment Card Industry Data Security Standard (PCI-DSS)
   - Guidelines for authentication (FFIEC-OCC)
   - Recommendation for the security of online payments (ECB)
   - General data protection regulation (EU)

2. Conduct a risk assessment
   - Analyze internet security threats against online payments systems
   - Assess impacts of online payment fraud (card non present fraud, phishing attacks, check fraud, mobile payment fraud, internet fraud)

3. Implement security measures
   - Strong authentication for customers
   - Transaction monitoring to identify abnormal customer payment patterns
   - Operational process for authorizing transactions
   - Customer awareness and education
Payment Security Standards (ECB, PCI)

How to design more secure online payments systems: the lesson learned from the analysis of security incidents

Payment Security Standards (ECB, PCI)


https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf
Mobile Security Technology Standards (NIST)

Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)

Recommendations of the National Institute of Standards and Technology

Lily Chen
Joshua Franklin
Andrew Regenscheid

Figure 2: BYOD Scenario


How to design more secure online payments systems: the lesson learned from the analysis of security incidents
Threat analysis and attack modelling processes and tools
The Process for Attack Simulation and Threat Analysis (PASTA™)

STAGE I - Definition of the Objectives (DO) for the Treatment of Risks

STAGE II - Definition of the Technical Scope (DTS)

STAGE III - Application Decomposition & Assertion (ADA)

STAGE IV - Threat Analysis (TA)

STAGE V - Weakness & Vulnerability Analysis (WVA)

STAGE VI - Attack Modeling & Simulation (AMS)

STAGE VII - Risk Analysis & Management (RAM)
How to design more secure online payments systems: the lesson learned from the analysis of security incidents
# Bank Trojan Threat Analysis

<table>
<thead>
<tr>
<th>Trojan</th>
<th>Infection Method</th>
<th>Attack Capabilities</th>
<th>Timing</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MB-MitB</td>
<td></td>
<td>MB MM D D B B D O O O O</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MM-MitM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B-Both</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O-Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zeus</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>SpyEye</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>InfoStealer</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>SilentBanker</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>URLZone</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Clampi/Bagat/Gozl</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Haxdoor</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Limbo</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>
How to design more secure online payments systems: the lesson learned from the analysis of security incidents

Attack Modeling

Fraudster

Upload Malware on Vulnerable Site

Drive-by Download/Malicious Ads

Steal Digital Certificates For Authentication

Delete Cookies Forcing to Login To Steal Logins

Fraudster

Attack Victim's Vulnerable Browser

Upload Banking Malware on Customer's PC

Man In The Browser

Modifies UI Rendered By The Browser

Harvest Confidential Data/Credentials From Victim

Phishing Email, FaceBook Social Engineering

Phish User To Click Link With Malware

Steals Keystrokes with Key-logger

Redirect Users To Malicious Sites

Sends Stolen Data to Fraudster's Collection Server

Use Stolen Banking Credentials/Challenge C/Q

Remote Access To Compromised PC Through Proxy

Logs into Victim's Online Bank Account

Perform Unauthorized Money Transfer to Mule

Money Transferred From Mule to Fraudster

Money Transferred From Mule to Fraudster
Risk Analysis & Management

Risk = \[ \frac{(\text{Threats} \times \text{Attack} \times \text{Vulnerabilities} \times \text{Assets})}{\text{Controls}} \times \text{Impacts} \]

How to design more secure online payments systems: the lesson learned from the analysis of security incidents
Mobile Wallet Functional Component Analysis

How to design more secure online payments systems: the lesson learned from the analysis of security incidents
## Secure Design And Application Risk Analysis

### ThreatModeler

<table>
<thead>
<tr>
<th>Design Item</th>
<th>Risk</th>
<th>NA</th>
<th>No</th>
<th>Yes</th>
<th>Except</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are you segregating the authentication logic from the requested resource?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you using standard, tested authentication services?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is Authentication required for all pages and resources except the ones designated as public?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are Authentication controls enforced on a trusted system?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you using a centralized authentication control?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Should the authentication control fail, is it failing securely?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are stored credentials stored in the form of strong one way salted hashes?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the storage table/file writeable only by the application?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is validation of authentication data taking place only after completion of all data input?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are your Authentication Failure responses generic without giving information on which part of authentication was incorrect?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For connections to external systems that involve sensitive information or functions, are you using authentication?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are you using POST requests for transmitting credentials to the server?</td>
<td>Very High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
How to design more secure online payments systems: the lesson learned from the analysis of security incidents

Threat Analysis using Threat Libraries
Component Level Threat Analysis

How to design more secure online payments systems: the lesson learned from the analysis of security incidents
How to design more secure online payments systems: the lesson learned from the analysis of security incidents
Risk Management

How to design more secure online payments systems: the lesson learned from the analysis of security incidents
Conclusions

1. The threat agents have evolved in motives and capabilities from ego-driven to value-driven and from isolate actors to organized crime.

2. The attack tools used by threat agents have increased in sophistication and effectiveness.

3. Security incidents today involve compromises of millions of credit card data records per incident, payment fraud and online fraud.

4. New technology for mobile banking and payments brings new security challenges for security and risk managers and increases the opportunity for attackers to exploit security holes and design flaws.

5. To protect customers, merchants, credit card processors and banks it is important to adopt a new risk mitigation strategy, focus on mitigating risks of cyber-threats and technical and business impacts.

6. The process for attack simulation and threat analysis PASTA™ and the tool ThreatModeler™ allow to identify design flaws in architecture exploited by threat agents, derive security requirements, prioritize tests and remediate vulnerabilities before these become liabilities.
How to design more secure online payments systems: the lesson learned from the analysis of security incidents
Grazie per l’ attenzione!

Email me:
Marco (dot) M (dot) Morana (at) Citi (dot) com

Follow me on twitter:@threatmodeling

Preorder the book “Application Threat Modeling Book, Wiley-Blackwell” on Amazon
http://www.amazon.co.uk/Application-Threat-Modeling-Marco-Morana/dp/0470500964

Download free ThreatModeler™ too at
http://myappsecurity.com/threatmodeler/