The Failings of PCI DSS as a Security Strategy

Chris Mark,  CPISA/M, CISSP, CIPP
Founder,
Society of Payment Security Professionals
Agenda

• About the Society of Payment Security Professionals
  • About Chris
• Rational Actor Model (RAM)
• Snipers & Snake Eaters
  • Understanding the Adversary
• Data Compromise Information
• Doctrine, Strategy, and Tactics
• PCI DSS Limitations
About SPSP

Organization dedicated to providing Payment Security Professionals with a resources to access information, education, and certifications

Forums, Blogs, Newsletters, Magazine

CPISA and CPISM Certifications – designed for individuals with responsibility for Payment Security

• Certified Payment Card Industry Security Auditor
• Certified Payment Card Industry Security Manager
About Chris

• I am a payment card industry “Insider”.
  • On original team that wrote CISP in 2001 (predecessor to PCI DSS)
  • First QSA in 2002 (before there were QSAs)
  • Founded a QSA firm in 2003
  • Conducted over 100 PCI DSS assessments
  • Worked at MasterCard Worldwide on SDP team
  • Original member of PCI SSC
  • On team that created PCI DSS from CISP
  • Contracted with major card brands to train merchants, banks, and service providers on PCI DSS.
    • Personally trained over 8,000 people
  • Original QSA Trainer
    • Personally trained over 1,000 QSAs
  • Published numerous articles on PCI DSS, CISP, Risk Management
Preface:
This presentation is not about the failings of PCI DSS as a standard.

Like any tool the PCI DSS is very good for what it was intended. Building a house using only a chainsaw is a very bad idea.

The focus of this presentation is on the application of the Tool.
Rational Actor Model (RAM)
Rational Actor Model

• Based upon Rational Choice Theory

  • Framework for understanding and modeling behavior

  • Used in economics and political science to understand past actions.

  • Limited value as prescriptive or predictive model.

  “...assumes individuals choose the best actions according to stable preference functions and constraints facing them.”

• “If the reward is big enough relative to the risk, I will choose to focus upon hacking into company A” (Macro Level, I choose life of crime over hard work)

• “If the company is protecting their stored data using encryption, I will focus on intercepting unencrypted data in transit” (Micro level)
Limitations of RAM

• Limitations on trying to predict behavior or actions

• Requires knowledge of the adversary’s beliefs, values, motivations, and resources.

• Assumes a consistent value system and consistent definition of “Rational”
  
  • *Rationality is predicated upon perspective*

• Danger is to project onto your adversary the same beliefs, values, and motivations that you possess.

• “If a company is compliant with the PCI DSS, they will not be compromised.” Makes assumptions about the resources, motivations, and values of the data thieves.
“BootStrapping”

- Basing a hypothesis upon pre-existing results.
- Results in spurious, unreliable findings (not statistically valid)
  - “If I had been a more strict parent, my teenager would not have died her hair blue and orange.”
  - Is this an accurate assessment?
- “If the company had been truly PCI DSS compliant, they would not have been compromised.”
  - This discounts the adversaries’ creativity, motivation, and resources and ignores the differences in values and mores.
Snake Eaters & Snipers;
Understanding the adversary
The Soldier’s Perspective

- It is 3am.
- You have been awake for almost 24 hours and have seen and heard little.
- It is 35 degrees and you pray it doesn’t rain again.
- You miss your family and are thinking about payday and going to Disneyland next week.
- It starts raining.
- You think that you don’t get paid enough for this job.
- You are hungry, tired, and cold.

Are you alert?
The Sniper’s Perspective

• It is 3am.
• I have been awake for almost 48 hours, lying in the cold mud and watching you since yesterday......waiting for an opportunity or mistake.
• It is 35 degrees and I pray it starts to rain again.
• I live in the cold, and the mud. I move silently in rain.
• I am driven by a single purpose.

Are you alert?
The Difference

• The difference between the two scenarios?

• Training/Experience;
  • “you fight like you train”
  • Sniper is highly trained, Solder is well-trained

• Motivation/Ideology;
  • “Visceral thrill of the hunt vs. tedium”

• Resources/Capabilities;
  • Better equipped, better trained
Understanding the Adversary

• We have a tendency to view “hackers” and “data thieves” abstractly (out of sight out of mind)

• They are real. They are sophisticated, organized, and motivated.
  • Russian Business Network, Boa Factory, Shadow Crew, ICA, 76Service.

• There is a lack of respect for the skills of the adversary.
  • Do we really believe that a simple firewall or AV will prevent a former KGB or Stasi computer expert from penetrating the network?
Quick Facts About Breaches

• In spite of data protection efforts, data breaches have increased 47% from 2007-2008.[4]

• Approximately 70% of Internet related breaches are caused, at least in part, by SQL injection.

• In over 500 Investigations, Verizon Business found that Payment Card Data was involved in 84% of cases.[5]
Views on Last Slide

• If the last slide were a boxing match, we would say we were “losing the fight”.

• Why do we continue to insist that we are “winning”?

• More importantly, why do we keep employing the same ‘strategy’?

Insanity: Doing the same thing repeatedly and expecting a different result.
Data Compromises

Surviving in the jungle
Timeline of Major Breaches

2003
Major credit card processor compromised because lack of adherence to security processes (Network Layer Attack)

2005
Customer information aggregator failed to verify identity of hacker posing as a customer (Social Engineering Attack)

2005
Major service provider listed as compliant but later hacked resulting in the loss of 40+ million credit cards (Malicious Software)

2006
Government organization looses laptop with records for 28+ million records (Loss)

2005-2007
Hackers place wiretaps on bank lines to capture transaction data being sent for authorization (Physical Wiretapping)

2007
Major retailer compromised and disclosed over 100 million credit card accounts (Network Sniffer, Trojan)

2008
Attackers build custom malware to capture magnetic track data off the network of large grocery chain (Malware)

2008
Attackers build custom malware to capture magnetic track data off major processor (Malware)

2008
Attackers build custom malware to capture magnetic track data off a major processor (Malware)
Who is behind the theft?

An International Web

The Justice Department has charged 11 people with operating an international identity theft ring that stole millions of credit card account numbers. According to the indictments, here is who was involved and how most of the crimes were carried out.

TRAFFICKING EASTERN EUROPE
Stored stolen identity information and used it to make and distribute fake credit cards.

IDENTITY THEFT MIAMI
Hacked into wireless computer networks of national chains in the Miami area and stole credit card information.

MAKING CREDIT CARDS CHINA AND UNKNOWN
Sold plastic blanks and equipment used to make fake credit cards.

Source: Justice Department

©2008 Society of Payment Security Professionals. All rights reserved
Who leads the groups

- Dmitry Ivanovich Golubov “Script”
  - Founder of CarderPlanet
  - Running for Ukrainian Senate

Roman Vega “Boa”

- Founder of BoaFactory
- Linked to 5 major hacks

Russian Business Network (RBN)

- Group of hosted sites that specialize in theft of information.
- Creators of Sinowal Trojan & Pinch
Russian Business Network

• Founded by computer science graduates
• Hire top grads and pay 2 x 10 western salaries
• Provide “BulletProof” Hosting
  • Child Pornography, Id Theft, DOS attacks
• Responsible (directly or indirectly) for up to 60% of worldwide cybercrime.
• Hosts (ed) 76Service.com
76Service.com

- Discovered by SecureWorks researcher Don Jackson
- “Malware As A Service (MaaS)” hosted at RBN
- Allows people to “rent” bot infected systems to monitor personal information
- Employs form grabbing trojans to capture bank logins, credit card info, etc.
Boa Factory

Dumps (tracks)
Credit card dumps from $0.89 per workable dump with both tracks

Travelers checks
Thomas Cook's MC & Visa, AmEx checks. $20 per $100 check

Passports
Passports from eighteen countries for a choose from

Real plastic
Banking quality unembossed blank Visa, MC, AmEx & Diners cards

Services
Clearing of money, reception of wire transfers, etc.

Merchant's board
Board of verified suppliers of the goods & services

What's new today
Fresh arrivals - a thousands of Gold, Platinum, Business, Corporate dumps from Europe, Caribbean, Japan, Asia, Australia. You can select it by Bank, country, type from here

SOLD OUT
The special offer. Only one lot always is offered. Do not miss.

Lot of 100 of Visa Credit Platinum (USA). Just are taken off from the processing centre. Cardholders shopped for Christmas. Fresh. All dumps are workable. Only one batch for special price 1399.00 $
## Carder Planet

### International Carder's Alliance -> Forum for English Speaking Carders

Welcome back; your last visit was on Aug 1 2004, 05:09

<table>
<thead>
<tr>
<th>Forum</th>
<th>Topics</th>
<th>Replies</th>
<th>Last Post Info</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Carders Work</strong>&lt;br&gt;CC, DNS, dump, cashing, online Shops Carding, Buying/Selling goods from online shops. Mail drops.</td>
<td>2302</td>
<td>8350</td>
<td>Aug 1 2004, 00:01&lt;br&gt;In: 400$ for only...&lt;br&gt;By: FastCarder</td>
</tr>
<tr>
<td><strong>ID</strong>&lt;br&gt;Real passports, ID, etc. on desired name and also all that with it is connected - scans of ID's, sale, manufacturing.&lt;br&gt;Forum Led by: xxx</td>
<td>1040</td>
<td>4516</td>
<td>Jul 31 2004, 14:30&lt;br&gt;In: Canadian ID&lt;br&gt;By: Expert2004107</td>
</tr>
<tr>
<td><strong>Programming, Hacking, Soft.</strong>&lt;br&gt;This section is for programmers and hackers, and also for people who requires their services. A software for carders.</td>
<td>280</td>
<td>1077</td>
<td>Jul 28 2004, 09:24&lt;br&gt;In: anyone can track mini22.re...&lt;br&gt;By: 5C0r302</td>
</tr>
<tr>
<td><strong>Anonymity &amp; Security</strong>&lt;br&gt;All about anonymity in the net. Anonymous proxies, soft for better anonymity etc.</td>
<td>216</td>
<td>1021</td>
<td>Jul 29 2004, 00:28&lt;br&gt;In: The perfect browser?&lt;br&gt;By: Demonstrator</td>
</tr>
<tr>
<td><strong>Questions of beginners, Search of employers.</strong>&lt;br&gt;Here beginners can post their questions and get answers. Search of employers.</td>
<td>590</td>
<td>2247</td>
<td>Jul 29 2004, 17:15&lt;br&gt;In: need tester in any state USA&lt;br&gt;By: Quentin</td>
</tr>
<tr>
<td><strong>Idle talk, Humor, Histories of carders' life.</strong>&lt;br&gt;Idle talk, Humor. Histories of carders' life. All themes from carders are welcome. :)</td>
<td>280</td>
<td>1898</td>
<td>Jul 6 2004, 10:16&lt;br&gt;In: tipping cards tutorial for...&lt;br&gt;By: not_so_pulpitude</td>
</tr>
<tr>
<td><strong>Scammers/Bippers activity reports</strong>&lt;br&gt;Discovered scammers. Place for activity of scammers, reports and resolution of problems.&lt;br&gt;Forum Led by: xxx</td>
<td>245</td>
<td>1303</td>
<td>Aug 1 2004, 04:59&lt;br&gt;In:不甘是你...&lt;br&gt;By: shatat</td>
</tr>
</tbody>
</table>

### Board Statistics

121 user(s) active in the past 15 minutes

102 guests, 18 members 1 anonymous members

- Hacker, Virtubi, shatan, ducky, Sinposer, knowledges, XX, cc-trader, slony, l0st0ther, l0w3b00zz, Russland, winchezc08, [M]SAn, BullD0zer, S3ver, Fuz0zz, Scre3n

©2008 Society of Payment Security Professionals. All rights reserved
Trojan Sniffers

• **2005 Payment Processor Compromise**

• “More details emerged Monday on the cyberbreak-in at a payment processing company that exposed more than 40 million credit card accounts to fraud.

• The data security breach, possibly the largest to date, happened because intruders were able to exploit software security vulnerabilities to install a rogue program on the network of (Company), MasterCard International spokeswoman Jessica Antle said. The program captured credit card data, she said.”

Creating your own Trojan

• Building a Trojan is relatively easy:
  • *Pinch 2.0* allows people to create their own trojans
  • Most will be undetectable by AV
  • Result of work by RBN
More Trojan Creators

“...these “beginners” in creating malware use different antivirus scanners with which they test their creations until they are undetectable.” - Pandalabs

Turkojan can be purchased online for $99US and $249US for ‘Gold’ support. The warranty states:

• 6 months (unlimited) or 9 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
Still a Hot Market!

Discussions 1 - 10 of about 1,279 about credit card detail dumps (0.000 seconds)

Ads by Google
Chase MasterCard ®
www.Chase.com/Platinum Get 0% Intro APR, No Annual Fee. Apply Now!

Apply For Credit Cards

Fresh Cards, Selling Dumps, Cvv's, Fullz... - [05 Oct 2008]
Hello. We selling fresh dumps with original Track1 and Track2. There are normal cc's with cvv code
dumps from USA, large bases. Visa Classic, MC Standart - $20. Visa Gold, Platinum, Business, Signature - Preview...
www.dnp.in/showthread.php?t=55324&mode=linear - At least 6 Posts and 6 Authors - Only this forum

Www.dumpshop.ch = Your Best Legit Source For Dumps & Carding !!! Try Us Out... - [08 Nov 2008]
! We dont sell dumps for any person. We dont sell money for money! We check dumps before provide you
whit my pos terminal, we buy cigarettes and dumps is 1000% working. We send you dumps via e-mail whit - Preview...
www.dnp.in/showthread.php?t=5542&mode=linear - At least 8 Posts and 6 Authors - Only this forum

Selling dumps! We sell fresh skimmed dumps from all over the world! - [29 Jun 2008]
Hello. We are happy to present you our service. USA, CANADA, EU, LATIN, ASIA, EXOTIC dumps
! From all over the world. Big end HOT fresh base! Don't loose your chance! *ALL DUMPS TRACK1 TRACK 2 (some - Preview...
www.webmasterforum.cc/showthread.php?t=27662&m... - At least 8 Posts and 6 Authors - Only this forum

Sell Dumps (org tr1 and tr2) - [16 May 2008]
Hello all. I am glad to present u friends service of selling fresh dumps. I sell only best dumps
that u can buy around. My dumps has extremely low decline rate. I have perfect checker which give me - Preview...
forums.lamusica.com/showthread.php?t=29073&mot... - At least 15 Posts and 11 Authors - Only this forum

©2008 Society of Payment Security Professionals. All rights reserved
Doctrine, Strategy, & Tactics
Doctrine, Strategy, Tactics

• Doctrine:
  • “... principle, or position, or the body of principles in a branch of knowledge or system of belief.”

• Tactics:
  • “How resources are employed in support of a defined strategic objective.”

• Strategy
  • “the practical adaptation of the means placed at a general’s disposal to the attainment of the object in view.”
  
    Carl VonClauswitz
How they relate

Doctrine

Strategy

Tactics

Tactics

Tactics

Objectives
PCI DSS as Doctrine

• PCI DSS or any other ‘static’ standard is much like doctrine.
  • Static principles
  • Prescriptive

• Limitations:
  • “To the degree that doctrine becomes overly prescriptive, it becomes irrelevant. Worse, it instills a penchant for proceeding by the book whether warranted by the circumstances or not.”
  • “Those who expect doctrine, and tactics, techniques, and procedures, to provide solutions and checklists for action are soon disabused of that notion during actual operations.”
The short story

• Following Doctrine is **NOT** the same as applying strategy.

• The current environment is focusing upon using the standard as the foundation of risk management.

• The standard is very useful but has limitation.

• We are using a conventional, outdated doctrine as a strategy for fighting an organized, motivated, sophisticated, adaptable adversary.

• *World War II tactics for a post Cold War Battle*
Seatbelts

• We all are required by law to wear seatbelts.
  • Compliance with the law

• It is difficult to dispute that seatbelts save lives.
  • Demonstrated minimum level of protection

• We all likely know people who have been killed while wearing seatbelts.
  • There is no guaranteed security

• Does this mean that seatbelts are ineffective?

• Would it be appropriate to tell a Nascar driver that simply wearing a seatbelt would be sufficient protection?
Is Compliance Security....or not?

- “The PCI SSC believes that the best way to protect cardholder data that is stored, transmitted, and processed is by implementing the PCI DSS and remaining in full compliance.”

Myth 4 – PCI will make us secure

Successful completion of a system scan or assessment for PCI is but a snapshot in time. Security exploits are non-stop and get stronger every day, which is why PCI compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data.

- “The DSS does clearly address protecting systems and networks from these new threats.”

- “Standards aren't the same as security.”
# Visa Security Alerts

**Visa Inc. Data Security Alert**  
Malicious Software and IP Addresses  
Updated February 20, 2009

## Table 1

<table>
<thead>
<tr>
<th>File Name</th>
<th>Purpose</th>
<th>File Size</th>
<th>MD5 Hash(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>bp0.exe</td>
<td>Backdoor</td>
<td>49,152</td>
<td>7997A3B118DDEFE1930FD48C0698CD3FA; d1e7183284a55db71a0e3eb949a5a19</td>
</tr>
<tr>
<td>wiadbyis.dll</td>
<td>Password Collector</td>
<td>23,552</td>
<td>080AC4794A3E257146406EF791AC60F4; 50E5D2D106ADB5D7087E6094E61DEF</td>
</tr>
<tr>
<td>wladel.dll</td>
<td>User Enumeration</td>
<td>57,856</td>
<td>8D049435C66ED6793517801B3F54414E6; 9D479C8BEE257A3B7119CC1B75D45013</td>
</tr>
<tr>
<td>sp.exe</td>
<td>Process Injection</td>
<td>69,632</td>
<td>EF7839780A08F100F8495D84DFEBA6; 5D1623B8E9DA5A70C15ECAD7DE375377</td>
</tr>
<tr>
<td>service_torun.exe</td>
<td>Malware Installer</td>
<td>16,896</td>
<td>cc1602121bb990a786527a2086300</td>
</tr>
<tr>
<td>Project1.exe</td>
<td>Downloader</td>
<td>398,848</td>
<td>FD5E73A822F4A118FF7C4F17B73FC80A</td>
</tr>
<tr>
<td>hider.exe</td>
<td>Process Injection</td>
<td>104,448</td>
<td></td>
</tr>
<tr>
<td>d.bat</td>
<td>Deletes hider.exe and itself.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>key.exe</td>
<td>Keystroke Logger</td>
<td>40,960</td>
<td></td>
</tr>
<tr>
<td>keylogger.exe/</td>
<td>Keystroke Logger</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rundll32.exe</td>
<td>Keystroke Logger</td>
<td>415,232</td>
<td>46E644182909D3011130A125BDEBCD76</td>
</tr>
<tr>
<td>lgr.exe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ca_setup.exe</td>
<td>Contains Cain &amp; Abel</td>
<td>6,282,200</td>
<td>3c882f3edc758e538528a0b06c748</td>
</tr>
<tr>
<td>cain.exe</td>
<td>Redirect ARP</td>
<td>not available</td>
<td>931C763C04B8F8F85200B3EE07</td>
</tr>
<tr>
<td>abel.exe</td>
<td>Redirect ARP</td>
<td>not available</td>
<td>06685B89AE3372E32774AC5F52C5679</td>
</tr>
<tr>
<td>src.rar</td>
<td>Stealth Malware</td>
<td>not available</td>
<td>46e411629093011130a125bdebc576</td>
</tr>
<tr>
<td>rar.exe</td>
<td>Packing Utility</td>
<td>not available</td>
<td>541CCA44C5590E43791D5984B8A262D13</td>
</tr>
<tr>
<td>wput.exe</td>
<td>Utility to conduct FTP Puts</td>
<td>not available</td>
<td>B41014C25719624D1E50B81BE02DA</td>
</tr>
<tr>
<td>Netmon.exe</td>
<td>Backdoor</td>
<td>97,280</td>
<td>91fbaf2de6525d8da6e4b9a689f84987;</td>
</tr>
<tr>
<td>GSJ352JY,TMP</td>
<td>Backdoor</td>
<td>not available</td>
<td>7a7c4551981db07b3366d7bb8c5b82c0</td>
</tr>
<tr>
<td>cmdex.dll</td>
<td>See <code>netmon.exe</code>.</td>
<td>23,040</td>
<td>83B3EB73FC86127D5FC455609AA0A343</td>
</tr>
<tr>
<td>OracleSniffert.exe</td>
<td>Sniffing Tool</td>
<td>not available</td>
<td>83b3eb73fc86127d5fc455609aa0a343</td>
</tr>
<tr>
<td>atmdes.exe</td>
<td>ATM Encryption Tool</td>
<td>1,755,487</td>
<td></td>
</tr>
<tr>
<td>req_all2.sql</td>
<td>SQL statement to modify account balance reset tool.</td>
<td>not available</td>
<td>48546ca4ec1249e680a21048dd88d70</td>
</tr>
<tr>
<td>hsm.exe</td>
<td>HSM Query</td>
<td>732,388</td>
<td>b0cb0cb7497a6147c0033124ef3ee0ad</td>
</tr>
</tbody>
</table>
• “There is no fate worse than being continuously under guard, for it means you are always afraid.”
If you cannot remove the princess

• Ensure you are in compliance with the PCI DSS

• More importantly.....DO NOT have a data compromise. You will likely be found non-compliant.

  • *Has anyone ever hired a new QSA? Did they find issues the other QSA had “missed”. The standard is subjective.*

  • *Conduct a risk analysis and protect the data first....not the network. In this world you should operate under the assumption that the hackers have penetrated the perimeter of the network.*

  • *Consider internal encryption of data*

  • *Consider egress controls to prevent data from leaving the network*