SECURITY AND PCI

TIM RAY

DEPARTMENT OF INFORMATION RESOURCES, STATE OF TEXAS

Bio

- Security Analyst for the Network/Security Operations Center (NSOC) Department of Information Resources, State of Texas
- IT full time since 1996
- Origin Systems 1990-1992
- Wing Commander III, Strike Commander, etc.
- MCSE, CISSP (2008), IAM/IEM, CAN

Disclaimer

The views expressed here are my own, and not necessarily held by the State of Texas nor the Department of Information Resources.

Three Things for Today:

- Current Threat Landscape (for background)
- PCI History and Issues
- PCI DSS Specifics Pertaining to Online Games

Threats 2010

- What I see:
  - At the state level, I see attacks from overseas.
  - They are targeted at financial assets and political rivals
  - There is much spear phishing
  - Botnets delivered by drive-by or e-mail are an every day thing
  - Many old attack signatures are present, just blocked.
  - Many new attacks don't have signatures yet.
  - SQL injection remains the most common single form of attack from the outside.

Stuxnet

- Malware directed against Siemans software and controls
- Such controls are found in Iranian nuclear facilities
- Spreads on infected USB drives
- No less than four unpublished exploits
- Weird ‘Myrtus’ reference in code, reported 10/1/10.
- Called the first cyberweapon in DoD circles.

Reading the Entrails

- Stuxnet copycats
- Low hanging fruit will be plucked
- Bad guys will go for volume targets
- Cloud computing applications will have to be secured better
- Graphics card malware will experience a large increase.

Industry Information

- No good source of information on breaches in the game industry exists.
- We rely on anecdotal accounts, hearsay and rumor.
- However, we know who plays games, and they are a juicy target for criminals.
- The ESA report on gamer demographics, for 2010:

http://www.theesa.com/facts/pdfs/ESA_Essential_Facts_2010.PDF

esa entertainment software association

Follow the Money

- Criminals go where the money is.
- Over 26% of gamers are 50 years old or older.
- The average age of a game buyer is 40.
- 67% of American households have a console for games, or use a dedicated PC for games.
- These groups are also the most targeted in bank fraud.
- Your customers are giving you their data for subscriptions and micro-transactions.
- Much of that data falls under the PCI umbrella.

Overview of PCI

- Payment Card Industry Data Security Standard
- PCI DSS is a financial industry regulatory standard, NOT a law.
- PCI DSS is an example of industry self-regulation
- PCI DSS is reviewed and changed every two years.
- PCI compliance does not come in a box!
- PCI DSS is hotly debated at all levels of IT security

PCI Definition Wall of Text!

- PCI: Payment Card Industry
- DSS: Data Security Standard
- QSA: Qualified Security Advisor
- ASV: Approved Scanning Vendor
- SAQ: Self-Assessment Questionnaire
- 'Merchant': Any entity that accepts payment cards from the five PCI founders (more on that below)
- 'Service Provider': Any entity that stores, processes or transmits cardholder data.
- 'Cardholder Data': Any personally identifiable data associated with a cardholder. Name, address, etc.

Penalties, We Haz Dem!

- The Big Five (in a sec, I promise) don't penalize you.
- They charge your bank if you're found non-compliant, and the *bank* charges you.
- Check your merchant agreement.
- Typical amounts are $5,000-$100,000 per **month** of non-compliance.

PCI History and Issues

- Officially adopted December 15th, 2004.
- Developed by the big five:

History Cont.

- PCI DSS was developed so that the industry could self-regulate rather than face Congressional regulation because…

Yet More History!

- It was developed as a minimum standard.
- Immediately after it was introduced, complaints started and no one adopted it.
- It was only a matter of time…

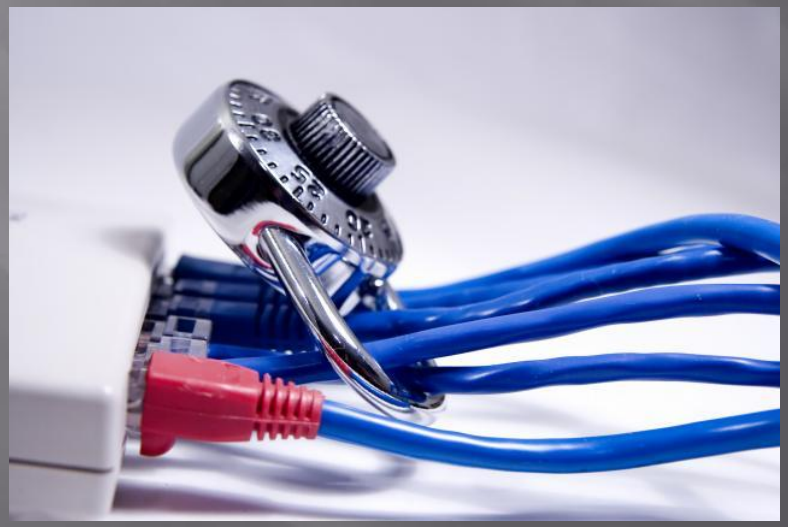
CARD SYSTEMS
INCORPORATED

Throwing the Book

- In 2005, CardSystems Solutions, Inc. revealed that they had been hacked for 40 million records.
- They were contractually obligated to delete cardholder data. They did not.
- They were storing it unencrypted.
- They were not PCI compliant.
- The Big Five cut them off. Forever.
- CardSystems Solutions was bought, then scuttled.
- Even so, PCI adoption was slow.

But it was just the beginning…

- 2007 – TJX revealed 100 million records compromised.
- Also not PCI compliant.
- This was the impetus for widespread acceptance of PCI regulations.



One More Time!

- In 2009, 

reveals they were hacked.
- We'll never know how many records were compromised.
- Likely over 130 million.
- They were PCI compliant, **the day before** they announced the breach.
- It cost Heartland $12.5 million and six months to regain compliance, on top of the lost business revenue.

The Debate

- PCI is Security Theater. It makes money for the Big Five and is fundamentally a protection racket.

On the Other Hand

- PCI is the beginning of a good security posture, and is meant to address the lowest fraction of the non-compliant while being relatively easy for the rest of the business world to follow.

Apologies and credit to Joshua Corman

But Does It Work?

- The Verizon PCI report is an interesting read.
- http://www.verizonbusiness.com/resources/reports/rp_2010-payment-card-industry-compliance-report_en_xg.pdf
- One of the only reports that has a large enough statistical sample to matter.
- Biased, because Verizon is a QSA
- The data indicates that compliant firms are much less likely to suffer a breach.

At Last, Substance!

- So what does PCI DSS actually say?
- https://www.pcisecuritystandards.org/index.shtml

PCI Security Standards Council™

- And a cool license plate

TL;DR!

- 12 areas of security you must cover if you want to take credit cards.
- You can transfer your PCI responsibilities to a service provider.
- You still have to fill out the SAQ and a few other documents.
- Hire a consultant to help you through this!

Twelve Areas

- **Build and Maintain a Secure Network**
- *Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
  Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
- *Requirement 3:* Protect stored cardholder data
  Requirement 4: Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
- *Requirement 5:* Use and regularly update anti-virus software
  Requirement 6: Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
- *Requirement 7:* Restrict access to cardholder data by business need-to-know
  Requirement 8: Assign a unique ID to each person with computer access
  Requirement 9: Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
- *Requirement 10:* Track and monitor all access to network resources and cardholder data
  Requirement 11: Regularly test security systems and processes
- **Maintain an Information Security Policy**
- *Requirement 12:* Maintain a policy that addresses information security

Twelve Areas, Cont.

- Each of the requirements above is exhaustively covered in the PCI standard.
- Remember it's a minimum standard and a starting place.
- Compliance is checked by a QSA and ASV of your choice!

So How Do We Do It?

- The simple answer is to use a third party provider.
- The system benefits companies that can make the commitment to handle large numbers of transactions securely.
- It's to your benefit to distance your firm from potential breach liability.
- There are several third party providers that would be ideal for the games industry.

Best-Case for a Game Company

SAQ Validation Type 1 in th*e PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises. Such merchants must validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that**:**

- Your company handles only card-not-present (e-commerce or mail/telephone-order) transactions;
- Your company does not store, process, or transmit any cardholder data on your premises, but relies entirely on third party service provider(s) to handle these functions;
- Your company has confirmed that the third party service provider(s) handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant;
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically; **and**
- Your company does not store any cardholder data in electronic format.

Last Example

- The closest example to a game company I could find was:

- They suffered a data breach in 2004.
- They rolled their own card reader software
- It stored mag track data (violating PCI)
- Total cost to sort out the breach: $5.5 million.

Resources and Links

- https://www.pcisecuritystandards.org/index.shtml
- http://www.pcicomplianceguide.org/
- http://www.451group.com/about/bio_detail.php?eid=407 (Josh Corman)
- http://vimeo.com/15108149 (PCI panel at DEFCON 18)
- http://www.schneier.com/ (Because any discussion about IT security needs a little Schneier)
- http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf (latest Verizon data breach report)
- http://www.verizonbusiness.com/resources/reports/rp_2010-payment-card-industry-compliance-report_en_xg.pdf (Verizon's PCI report)

Thank you!

Please contact me for security or IT questions!

timothy.ray@dir.texas.gov

@securitytim on Twitter