PCI: The Dark Side

May 2012
Roanoke, VA
Agenda

- The problem
- Who are they?
- Why?
- What do they steal?
- How do they do it?
- What can they do with it?
- How can you stop it?
CampusGuard is an information security firm

- Working exclusively with colleges and universities
- All things PCI: PCI DSS, PA-DSS, QSA, ASV
- Also Red Flags, GLB, HIPAA

Help schools become PCI compliant
A short story…
PCI 101

- PCI DSS: Payment Card Industry Data Security Standard
- Goal is to protect Cardholder Data
  - And to keep you out of the headlines
- PCI does not make you secure
- If you take plastic, PCI applies to you
- Under contract law, not a state or federal regulation
- PCI scope includes
  - “Store, process, or transmit” cardholder data
  - Paper, too
- PCI is a program, not a project
- Two things you need to accept about PCI:
  - Your costs have gone up
  - You will change the way you do business
PCI Relationships

Bank
Communicates and educates merchants on PCI DSS and reports compliance status to Card Associations

Responsible for managing the PCI DSS and certifying QSAs and ASVs

CREDIT CARD SECURITY

Responsible for enforcing and monitoring merchant compliance with the PCI DSS

Merchant
Responsible for safeguarding credit card data and complying with the PCI DSS

Responsible for helping merchants with PCI DSS compliance.
## PCI DSS: 6 Goals, 12 Requirements

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Build and maintain a secure network</td>
<td>1. Install and maintain a firewall configuration to protect data</td>
</tr>
<tr>
<td></td>
<td>2. Change vendor-supplied defaults for system passwords and other</td>
</tr>
<tr>
<td></td>
<td>security parameters</td>
</tr>
<tr>
<td>2. Protect cardholder data</td>
<td>3. Protect stored data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder magnetic-stripe data and</td>
</tr>
<tr>
<td></td>
<td>sensitive information across public networks</td>
</tr>
<tr>
<td>3. Maintain a vulnerability management program</td>
<td>5. Use and regularly update antivirus software</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>4. Implement strong access control measures</td>
<td>7. Restrict access to data to a need-to-know basis</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>5. Regularly monitor and test networks</td>
<td>10. Track and monitor all access to network resources and</td>
</tr>
<tr>
<td></td>
<td>cardholder data</td>
</tr>
<tr>
<td></td>
<td>12. Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>
## Merchant Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Visa/MC Transactions</th>
<th>American Express Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&gt; 6 million txns/yr</td>
<td>&gt; 2.5 million transactions/yr</td>
</tr>
<tr>
<td>2</td>
<td>1 to 6 million txns/yr</td>
<td>50,000 to 2.5 million txns/yr</td>
</tr>
<tr>
<td>3</td>
<td>20,000 to 1 million txns/yr</td>
<td>All other Amex Merchants</td>
</tr>
<tr>
<td>4</td>
<td>All other Visa/MC merchants</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Validation Requirements

<table>
<thead>
<tr>
<th>Level</th>
<th>VISA</th>
<th>MasterCard</th>
<th>American Express</th>
</tr>
</thead>
</table>
| 1     | • Annual on-site assessment (QSA)  
       | • Quarterly network scan (ASV)  
       | • Annual penetration test (ASV)  | • Annual on-site assessment (QSA)  
       | • Quarterly network scan (ASV)  
       | • Annual penetration test (ASV)  |
| 2     | • Annual on-site assessment (QSA)  
       | • Quarterly network scan (ASV)  
       | • Annual penetration test (ASV)  | • Quarterly network scan (ASV)  
       | • Annual penetration test (ASV)  |
| 3     | • Annual Self-Assessment Questionnaire (SAQ)  
       | • Quarterly network scan (ASV)  
       | • Annual penetration test (ASV)  | • Quarterly network scan (ASV)  
       | • Annual penetration test (ASV)  |
| 4     | • At discretion of acquirer  
       | • Annual SAQ  
       | • Quarterly network scan (ASV)  
       | • Annual penetration test (ASV)  | ▪ N/A |
Higher Ed Is Vulnerable

Past 3 Years

Higher Education

- Government: 33%
- Healthcare: 14%
- Financial Services: 22%
- Retailers: 17%
- Other: 6%
- Past 3 Years: 8%

Source: Privacy Rights Clearinghouse
Colleges and Universities are like Cities...
Looking something like this...

- Athletics
- Student Accounts
- Parking Services
- Library
- Theatre
- Events
- Foundation
- Continuing Ed

- Radio Station
- Hotel
- Residential Life
- Book Store
- Student Life
- Reprographics
- More...
Compared with...
Higher Education Challenges

Many groups, organizations and departments want to offer credit card payments, but they all have:

- Different needs
- Resource limitations
- Lack of payment processing knowledge

This poses challenges for IT:

- Open networks and systems
- Little or no monitoring of traffic
- Overloaded IT staff
- Fiscal constraints
Some Data Breach Stats

Who is Behind Data Breaches?
92% from external sources
17% caused by insiders
<1% implicated business partners
9% involved multiple parties

How Do Breaches Occur?
11% aided by significant errors
50% resulted from hacking
49% utilized malware
17% involved privilege misuse
29% occurred via physical attacks

What Commonalities Exist?
86% discovered by a third party
89% of victims were not PCI compliant
96% considered avoidable through simple or intermediate controls
83% of victims were targets of opportunity
92% of attacks were not highly difficult

Source: Verizon 2011 Data Breach Investigations Report
Penalties can be Huge

- In the event of a breach the bank can make the merchant responsible for:
  - Fines from card associations
    - Up to $500,000
  - Cost to notify victims
  - Cost to replace cards
  - Cost for any fraudulent transactions
  - Forensics
  - Level 1 certification

*Bad Publicity – Priceless!*
Who are they?

- 1970’s – Phone Phreakers
  - “Blue Box”
- Stages
  - Curiosity, bragging rights
  - Control
  - Criminal intent
- Now
  - Organized Crime (e.g. RBN)
  - Terrorist Groups (to fund their operations)
What do they Steal?

What’s in your wallet?

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Magnetic Stripe
- Card Verification Value (CVV)
How do they do it?

Google

Yourschool.edu intitle:index of apache
How do they do it?

Google

Yourschool.edu intitle:index of apache

packet storm

Search files: apache

Red Hat Security Advisory 2012-0570-01

Red Hat Security Advisory 2012-0570-01 - PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server. A flaw was found in the way the php-cgi executable processed command line arguments when running in CGI mode. A remote attacker could send a specially-crafted request to a PHP script that would result in...
How do they do it?

- SQL injection
- Cross-site scripting

Cell Phones

Printers

Laptops

Payment Server

Dept PCs

Internet
What can they do with it?
What can they do with it?
What can they do with it?
What can they do with it?
What can they do with it?
What can they do with it?
What can they do with it?
What can they do with it?

FARGO HDP600 LAMINATING ENCODING PRINTER

Item Code: PRRF-HDP600L-02
Model: 88026
Manufacturers: Fargo Electronics
Categories: HDP SERIES
Weight: 70.00 LB

Fargo HDP600L Double-Sided HD Printer with Lamination and Mag. Encoder - REFURBISHED (GREEN)

Manual PVC Card Embosser, Embossing Machine, Card Embosser
by Dinwood

Be the first to review this item | 0

Price: $398.00

In Stock.
Ships from and sold by MIN Super Outlet.

Only 9 left in stock—order soon.

2 new from $398.00
What can they do with it?

[Images of various items being added together to equal a stack of dollar signs with the eBay logo]
Skimming
Phishing

Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.
## How can you prevent it?

### PCI DSS: 6 Objectives and 12 Requirements

<table>
<thead>
<tr>
<th>Control Objective</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| 1. Build and maintain a secure network | 1. Install and maintain a firewall configuration to protect data  
2. Change vendor-supplied defaults for system passwords and other security parameters |
| 2. Protect cardholder data | 3. Protect stored data  
4. Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks |
| 3. Maintain a vulnerability management program | 5. Use and regularly update antivirus software  
6. Develop and maintain secure systems and applications |
| 4. Implement strong access control measures | 7. Restrict access to data to a need-to-know basis  
8. Assign a unique ID to each person with computer access  
9. Restrict physical access to cardholder data |
| 5. Regularly monitor and test networks | 10. Track and monitor all access to network resources and cardholder data  
11. Regularly test security systems and processes |
| 6. Maintain an information security policy | 12. Maintain a policy that addresses information security |
# Self-Assessment Questionnaires

<table>
<thead>
<tr>
<th>Method</th>
<th>SAQ A (11 questions)</th>
<th>SAQ B (29 questions)</th>
<th>SAQ B (29 questions)</th>
<th>SAQ C / VT (80/51 questions)</th>
<th>SAQ D (286 questions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card-Not Present, All Cardholder Data Functions Outsourced</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Imprint Only, No Cardholder Data Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standalone Dial Out Terminal, No Cardholder Data Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payment Application Systems Connected to the Internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All other methods</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Move as far to the left as possible!
How can you prevent it?

- Strategic Scope
- Only payment systems are in scope
- Better all around
PCI Compliance

Discovery and Assessment

- Payments Analysis
- Merchant Discovery
- Documentation
- Preliminary Scanning
- Gap Analysis

Remediation

- Correct Problems
- Compensating Controls

Validation

- ROC or SAQ Submission

Quarterly Scanning
- Penetration Testing

Re-Validate every 12 mos
Test Your Institution

Use these questions to test the PCI readiness for your institution:

- Are we PCI Compliant?
- What level merchant is our institution?
- Can I see the SAQ?
- Did we have any NO answers? N/A?
- Which credit cards do we accept?
- Can I see copies of our policies/procedures?
Summary

- The problem is real
- You are probably doing a lot of things right today
- Your bank will soon be requiring proof
- Prevention is key
- Not a one-time project
- Help is available
Resources

"I found it as entertaining as I did enlightening."
—Tony Brulhy, CISSP, CSSLP

THE ART OF INTRUSION
KEVIN D. MITNICK
& William L. Simon
The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers

STEAL THIS COMPUTER BOOK 4.0
WALLACE WANG
What They Won’t Tell You About the Internet