



Payment Card Theft, an overview of the latest trends and threats

June 2009

Malcolm Bradly



Agenda



- Introduction
- Compromises in VE
- The hackers targets
- The value of card data
- Compromise example
- Compromise trends
- Myths and facts
- Common vulnerabilities
- Compliance, the right approach

Data compromise introduction



- Data compromise is high on the risk agenda for payment schemes, issuers and acquirers
- The way that fraudsters obtain data is becoming more complex and more innovative
- More touch points (e.g. processors) in the transaction flow, each one of them representing a potential risk
- Criminals are no longer stealing data on a card-by-card basis (skimming), today it is the wholesale stealing of data which is causing issues for the payment card industry

Visa Europe based compromises



How many individual data compromises took place within VE during 2008?

248 (170 in 5 months in 2009)

How many Visa Europe cards were deemed to be 'at risk' during 2008, due to a data compromise?

9.9 million

Today's Targets



Hackers are attacking:

- Brick-and-mortar merchants
- Issuers & acquirers
- E-commerce merchants
- Third Party Processors

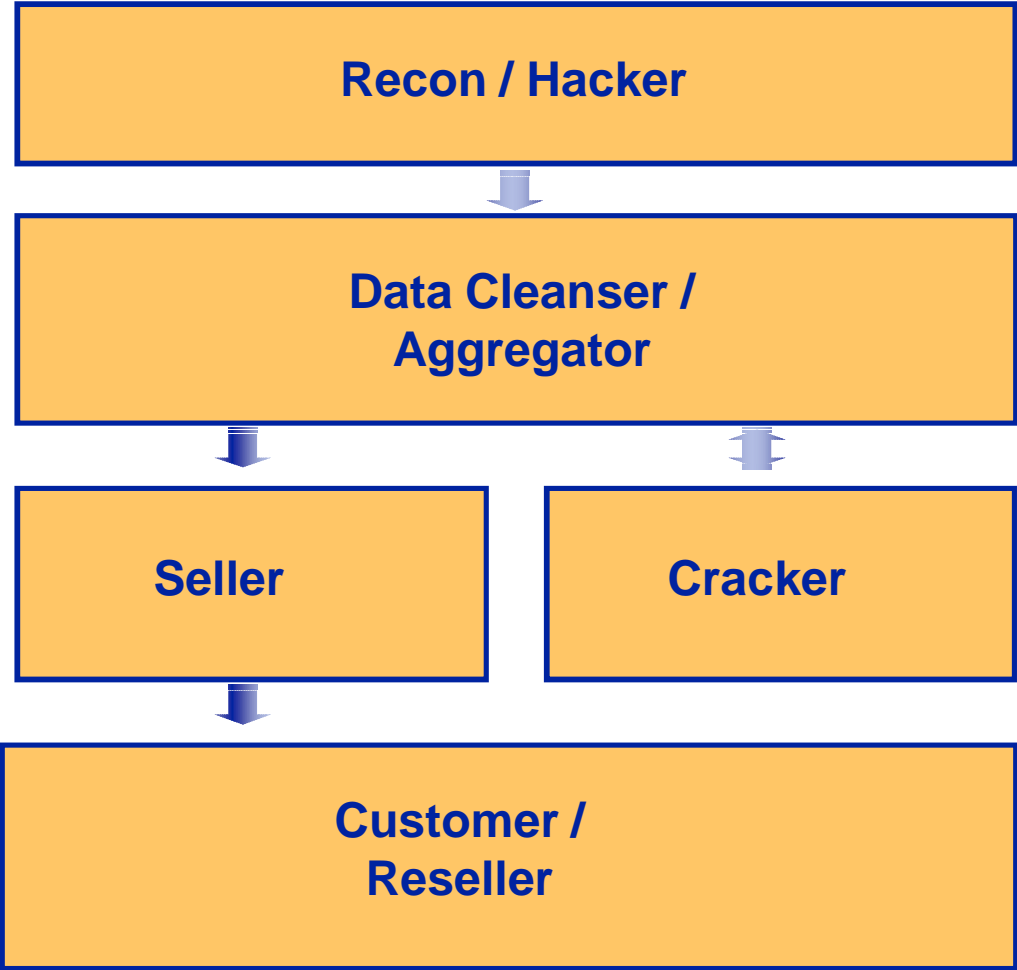


Hackers are looking for:

- Networks that store sensitive cardholder data
- Track data
- CVV2 & passwords
- PINs
- Malware injection opportunities



Criminals are Sophisticated & Organized



The value of compromised data



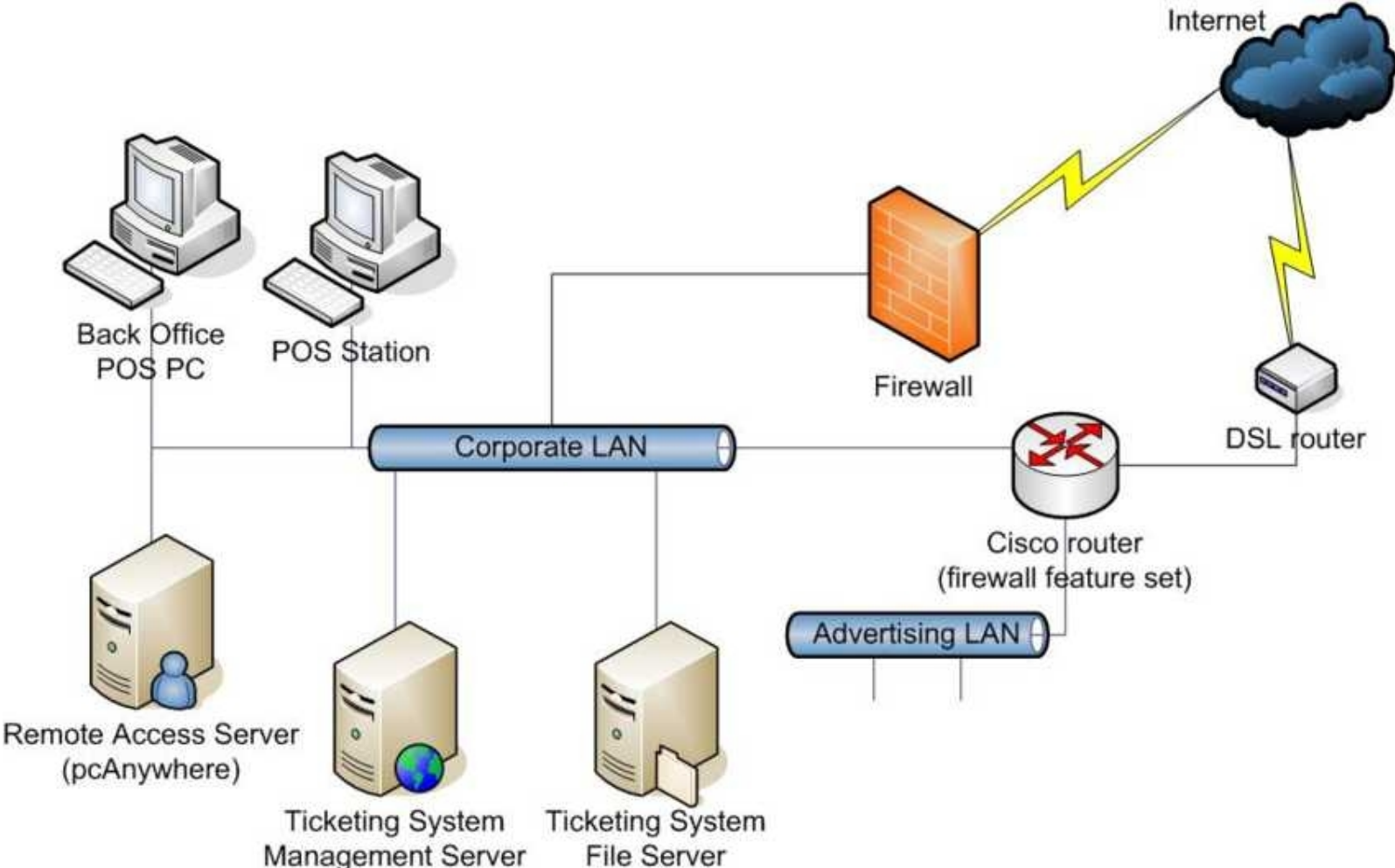
Estimated market value of compromised accounts*

<p>Account number and CVV2</p>  <p>No Plastic \$1 - \$5</p> <p>Semi-finished blank plastic</p>  <p>White-Plastic \$80 - \$100</p>	<p>Classic track data</p>  <p>No Plastic \$15</p> <p>Complete counterfeit Gold plastic</p>  <p>Finished \$250</p>	<p>Gold/Plat/Corp track data</p>  <p>No Plastic \$30</p> <p>Track data and PIN</p>  <p>Finished \$1,000**</p>
--	--	--

* Source: Symantec Internet Security Threat Report Volume XI: March 2007

**Typically track data and PIN not for sale; profit share arrangement amongst criminals; estimated criminal profit per card

Compromise Example – Internet Facing POS



PCI Data Security Standard



PCI Data Security Standard

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

Security Environment



»» As PCI DSS compliance rates rise, new compromise trends emerge

Compliance Milestone

- PCI DSS compliance is adopted by acquiring participants in the U.S.
- Merchants and service providers reduce historical storage of cardholder data
- PCI DSS compliance improves among large merchants
- E-commerce and payment channel websites better secured



Compromise Trend

- Issuers and processors increasingly targeted; non-U.S. compromises increasing rapidly
- Data criminals seek capture of cardholder data in transit through sniffer attacks
- Compromises of small and medium size merchants increase
- SQL injection attacks on non-payment sites to gain access to payment environment



Compromises in the Media

Myths and Facts



Myths

- PCI DSS compliant entities have been breached
- PCI DSS does not address sniffer* attacks
- Encryption of data transmission can prevent compromises



Facts

- As of today, no compromised entity has been found to be compliant at the time of the breach
- PCI DSS should prevent and detect unauthorized network access and installation of sniffers
- Encryption does not eliminate the risk of data being compromised if data is decrypted at any point




PCI DSS continues to serve as a robust foundation to protect cardholder data in a static data environment

*Sniffers are used by hackers to monitor and capture data in transit over an internal network

Common Compromise Vulnerabilities



PCI DSS compliance should mitigate common vulnerabilities found to contribute to data breaches

PCI Data Security Standard	Common Compromise Vulnerabilities	
Build and Maintain a Secure Network	Failure to secure and monitor connected non-payment environment Improperly segmented networks Insufficient egress and ingress filtering and firewall monitoring Insecure database configuration Failure to update or change default passwords	PREVENTION  DETECTION
Protect Cardholder Data	Storage of sensitive data	
Maintain a Vulnerability Management Program	Unprotected systems vulnerable to SQL injection attacks Corporate websites targeted to gain access to network Malware installed to capture passwords and cardholder data	
Implement Strong Access Control Measures	Failure to limit user access to critical system	
Regularly Monitor and Test Networks	No monitoring of privileged user access No implementation or monitoring of intrusion detection or anti-virus	
Maintain an Information Security Policy		

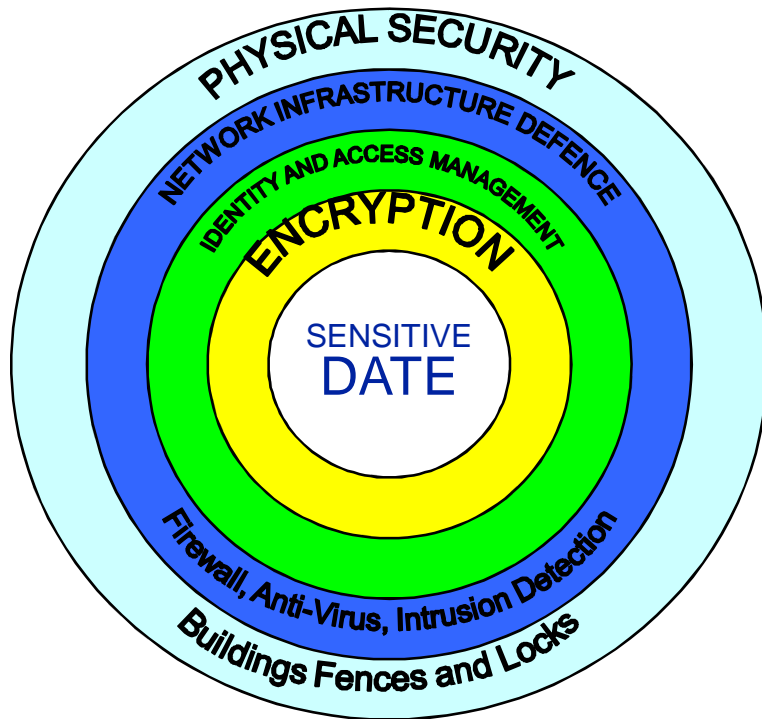


Suspected Data compromise



- Suspected Data compromise identified by Issuers noting a Common Point of Purchase (CPP)
- The Visa Europe rules require the acquiring member to investigate
- A Qualified Forensic Investigator is appointed
- Accounts at risk are sent to Visa Europe who will then distribute them to the issuers
- The forensic report is sent to Visa Europe
- The compliance council assesses fees and penalties against the Visa Europe member.

Compliance: The right approach



Philosophy

- Trust no one
- Assume bad guys are already in
- Assume no control over data location and use (web, Mobile devices)
- Security must follow the data

Typical Threat

- Privacy breach, data leakage, IP theft, identity theft, insider attacks



Compliance is not an end point



Too much emphasis on PCI DSS validation finish line rather than ongoing security and compliance leaves compromise risk

- PCI DSS controls, when implemented properly, can prevent network intrusions
 - If the network is compromised, impact should be mitigated via timely detection
- In all compromise cases, forensic investigations have found significant gaps in the compromised entity's PCI DSS controls to be major contributors to the breach
- Validating compliance is a snapshot, point-in-time review of a business' systems, and is limited in scope to a sample of systems
 - Entities must not rely solely on a Qualified Security Assessor to determine their PCI DSS compliance and overall information security programs
 - A PCI DSS assessment can no more account for every eventuality than a financial audit can review all the financial transactions of a company
- Maintaining good security requires an ongoing commitment
 - PCI DSS compliance is a 24 hour a day, 7 day a week, 365 day a year job
 - Businesses must build ongoing compliance monitoring into their internal auditing processes



PCI DSS mandated for everybody



PCI DSS is mandated for all merchants and other entities with access to card holder data

PCI DSS was created to protect card data

No access to data = no need for compliance validation

In the future, more companies may consider not handling data directly, rather than going through the cost and risk of securing them



VISA

