DRESSER
Wayne

SIGMA
Annual Meeting
2007
Boston, MA

Payment Card Industry (PCI) Compliance at the Dispenser: Are You Prepared?

Tim Weston, Dresser Wayne

October 12th, 2007

PCI Data Security Standards

Data Security …

- Payment Card Industry Security Standards Council (SSC)
  - *An open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection*
  - *Founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International*
- PCI Data Security Standard (DSS)
  - *PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures*
  - *Commonly referred to as "The Digital Dozen" by those in the industry*
  - *Relative to all retailers handling cardholder account information wherever it is stored, processed, or transmitted*

More info available at www.pcisecuritystandards.org

PCI PIN Security Standards

… and now PIN Security

- PCI PIN Security Standards
  - *PIN Entry Device (PED) Security Requirements were recently added to the standards administered by the PCI Security Standards Council*
  - *Designed to secure Personal Identification Number (PIN)-based transactions globally and applies to devices that accept PIN entry for all PIN based transactions*
  - *Previously administered under the auspices of JCB, MasterCard International and Visa International*
- Involves both device security and device management
  - *Resist attacks on the device with physical and logical security protections*
  - *Protect from unauthorized modifications during manufacturing and key loading*
- Similar to ANSI X9 PIN standards that have been in place for many years

More info available at www.pcisecuritystandards.org

PCI PIN Security Standards

PCI Security Standards Council

Device Classifications

PIN Entry Device (PCI PED)	Encrypting PIN Pad (PCI EPP)	Unattended Payment Terminal (PCI UPT)

- Preserve integrity of payment card network and consumer confidence through:
  - *Increased physical security of PIN entry devices (PEDs)*
  - *Improved management of devices through their lifecycle*
  - *Migration to Triple-DES encryption algorithm (TDES)*
- Current device classifications include:
  - *PIN Entry Devices (PED) – traditional counter-top style card reader/pin pads*
  - *Encrypting PIN Pads (EPP) – commonly found in Automated Teller Machines*
- Newest classification is for Unattended Payment Terminals (UPT)
  - *Includes Kiosks, Vending Machines,* ***Automated Fuel Dispensers (AFDs)****, etc.*
  - *Currently in draft version being circulated to industry providers for review*

PCI PIN Security Standards

Visa has taken the lead in specifying compliance mandates

Mandates Summary

- Visa Mandates
  - *January 2009 for dispensers in the US, October 2007 outside the US –*

    All newly deployed unattended POS PIN acceptance devices must contain an EPP that has passed testing by a PCI recognized laboratory and is approved by Visa for new deployments

    Impact – TDES-capable PCI certified keypads required on <u>new dispensers</u> accepting PIN debit transactions
  - *July 2010 globally –*

    All transactions originating at POS PEDs must be encrypting PINs using TDES from the point of transaction to the Issuer (end-to-end).

    Impact – TDES-capable PCI certified keypads required on <u>all dispensers</u> accepting PIN debit transactions
- Additional association mandates are expected once the Unattended Payment Terminal (UPT) requirements have been published

PCI PIN Security Standards

Canadian marketplace is seeing similar mandates

Mandates Summary

- Interac Association
  - *January 2008 – 3rd party certification required for all new units deployed*
    - *Must also be chip capable, although not initially chip enabled*
  - *December 2012 – AFD Chip migration 25% operational milestone*
  - *December 2015 – Chip migration 100% complete*
    - *All non-chip devices removed from the network*

  Impact – Interac certified hardware required on <u>all dispensers</u> accepting PIN debit transactions
- Visa Canada
  - *October 2007 – All newly deployed unattended POS PIN acceptance devices must contain an EPP that has passed testing by a PCI recognized laboratory and is approved by Visa for new deployments*
  - *October 2010 – Chip & PIN migration liability shift*

  Impact – TDES-capable PCI certified keypads required on <u>new dispensers</u> accepting PIN debit transactions

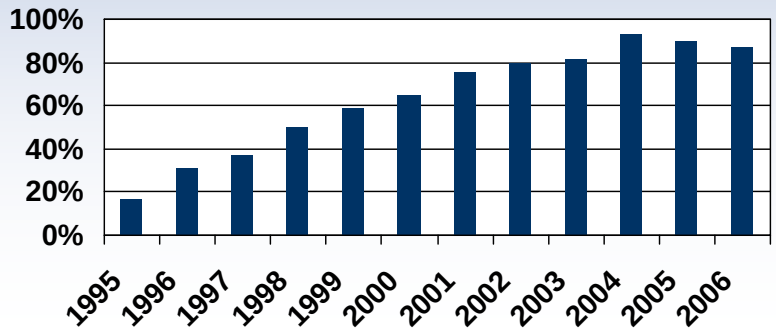
Why New Standards and Why Now?

Significant growth in card use at retail petroleum sites

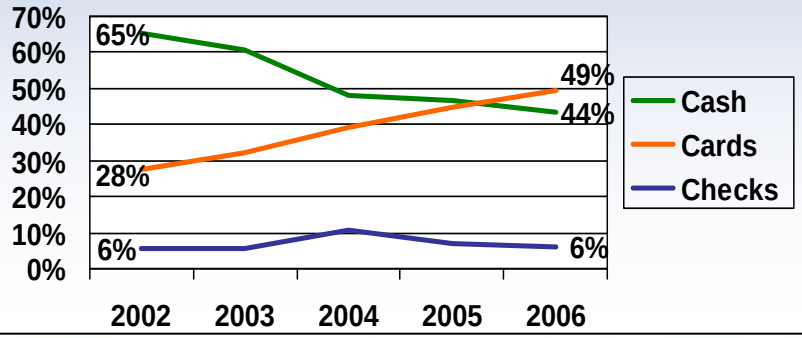
Retail Petroleum Card Usage

- Pay at the Pump availability has seen steady growth nearing market saturation
  - *87% of sites offer Pay at the Pump*
  - *56% of sites also accept PIN Debit at the Pump*
- Estimates indicate the industry has reached *more than a million fueling points* in North America (~600K dispensers)
- Cards have surpassed cash as dominant payment form at convenience stores

Sites Offering Pay at Pump



Site Payment Type Mixture



Data Courtesy NACS State of the Industry Report

Why New Standards and Why Now?

Fraud incidents at the dispenser are on the rise

Organized Crime Involvement

- Dispenser market size identified as significant opportunity
- Already proficient at skimming in ATM and POS environments
- Technology advances making device components smaller, and easier to obtain
  - *Able to operate in high-temp conditions inside electronics cabinet*
- Obtaining skills to overcome technology challenges
  - *Specialized knowledge (interface protocols, electronics)*
- Sophistication of new attack methods are finding ways to circumvent existing defenses

Fraud Growth Contributors

- Potential to skim many cards without detection
  - *No externally-visible indication skimmers are installed*
- Card remains with consumer
  - *Unlike card being out of sight as with restaurants*
- Station operators not diligent in routine inspections
  - *Need education and best practices information*
- Easy access to dispensers
  - *Common keys readily available for some models*
- Past fraud focus has been on in-store skimming

Payment Card Fraud in the News

CSP
CONVENIENCE STORE / PETROLEUM

Issue Date: CSP Daily News, June 28, 2007

'Path of Least Resistance'

Gartner says gas station POS terminals are major threat to data security

STAMFORD, Conn. – Using a credit card at a gas station could pose more of a risk for data theft than shopping online, as point-of-sale (POS) terminals have emerged as a weak link in the security chain, said the IDG News Service, citing a Gartner Inc. analyst.

When a card is swiped, POS terminals often collect and store the data held in the magnetic stripe on the back of a credit card, said Avivah Litan, a Gartner vice president and analyst. Retailers are often unaware that their POS applications collect so much information, said the report.

In the hands of sophisticated hackers and counterfeiters, the data collected from the magnetic stripe is enough to create a replica card. "It's almost more dangerous to go to the gas station than it is online," Litan said at Gartner's Identity & Access Management Summit in London on Monday. "The data is just sitting there. No one even thought about what data is on a POS controller."

Retailers' network configurations are partly to blame. Many are using the Internet to transmit data in place of dialup networks, and many have incorporated wireless access points into their networks using WEP (Wired Equivalent Privacy), Litan said, which is not considered a strong form of encryption.

Hackers lurk in parking lots looking for weak networks to penetrate. Since the POS terminals are linked via IP, once a hacker has accessed a network they can try out neighboring IP addresses until they locate a store of data, Litan said.

Data breaches that occur offline are common, the report said. Of 160 breaches investigated for one major credit card brand, 128 took place in the brick and mortar world where the card was physically present for the transaction, rather than being used online or over the telephone, according to Gartner.

To strengthen security, card brands such as Visa and MasterCard are pressuring retailers to comply with the Payment Card Industry (PCI) Data Security Standard, a code of best practices created by the card industry. The standard forbids the storing of magnetic stripe data on POS terminals, and Visa plans to start fining retailers in the coming months if they do not comply, Gartner said.

Implementing security is cheaper in the long run than having a data breach, which can be expensive and hurt a company's reputation, said the report. Gartner calculates that a data breach costs companies around $300 per exposed account because of investigations, fines and lawsuits. On the other hand, beefing up security costs around $16 per account for the first year, and that cost falls over time, according to Litan.

The short-term forecast for POS security does not look great, however, said the news service. Gartner predicts that by next year, most attacks against retailers will be directed at their POS terminals, and only 30% of POS software will be compliant with the prevailing security standards by 2009. "The thieves always find the path of least resistance," Litan said.

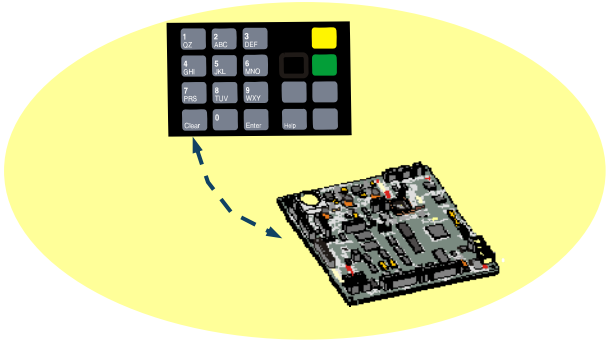
Meanwhile, pay-at-the-pump technology ranked No. 9 on *USA Today*'s list of "25 Eureka Moments" that have changed the lives of American since 1982. The list was topped by cell phones, followed by laptop computers, the BlackBerry, debit cards, caller ID, DVDs, lithium rechargeable batteries, iPods and pay at the pump. Lettuce in a bag rounded out the top 10. Click here to view the complete list.

For an in-depth look at how identity theft is affecting retailers, watch for the July issue of CSP magazine.

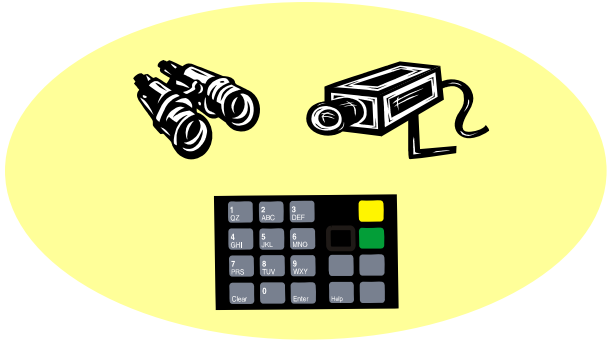
Areas of Concern at the Dispenser

Example attack scenarios – Skimming PINs and Card Data

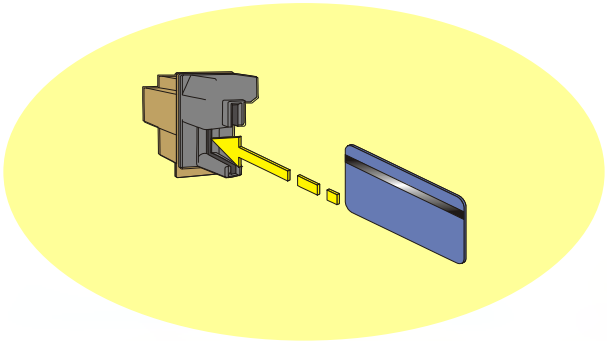
Keypad Cables



PIN Entry Observation



Card Readers & Cables



Attack Scenarios

Keypad Cables

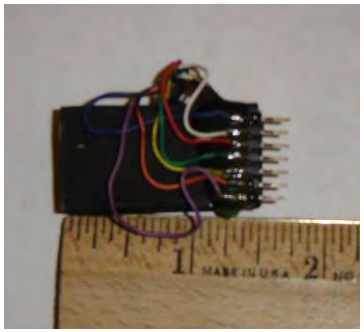
Scenario Details

- Installed skimmer devices “in-line” on data cable between keypad and dispenser electronics
- Easily prevented by replacing with encrypting pin pad

Scenario Attributes

- Access to dispenser electronics
- Unobserved installation or collusion with site personnel
- Undiscovered equipment
- Specialized knowledge of keypad electronics and interfaces

Example Devices



Attack Scenarios

PIN Entry Observation Cameras

Scenario Details

- Used in combination with skimmer devices for card data
- Known incidents of both remote distance and in-dispenser camera

Scenario Attributes

- Extensive access to dispenser electronics for on-site modifications
- Collusion with site personnel
- Specialized knowledge of electrical interface
- Substantial investment in devices and technology

Example Devices

Attack Scenarios

Card Reader Cables and Electronics

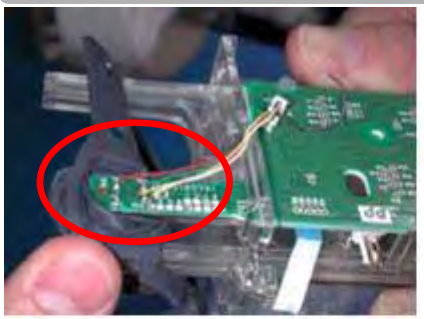
Scenario Details

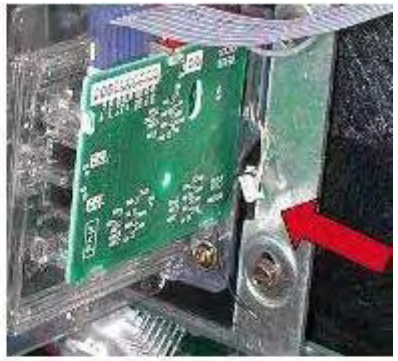
- Replaced existing card reader with skimmer modified version
- Installed devices “in-line” on data cable between card reader and dispenser electronics

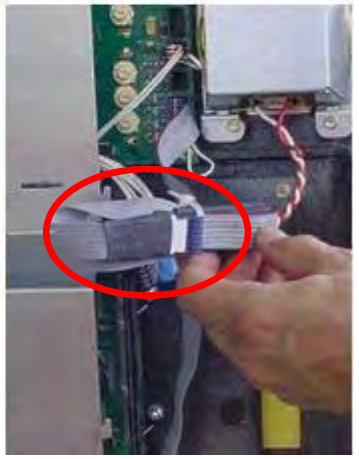
Scenario Attributes

- Access to dispenser electronics
- Unobserved installation or collusion with site personnel
- Undiscovered equipment
- Specialized knowledge of card reader electronics and interfaces

Example Devices







Current Market Situation

The marketplace is vulnerable to these new types of attacks

Multiple Generations of Equipment

- Security levels vary widely for existing equipment in the marketplace
  - *Age of the dispenser is a direct factor as numerous security improvements have taken place on dispensers since the introduction of pay at the pump*
- Given the extended lifespan of dispensers, many early generations of pay at the pump equipment are still in operation today
  - *Access to sensitive electronics easier on older models*
  - *Some have tamper-resistant encrypting pin pads as standard offering, others do not*
- Use of non-encrypting keypads with standard mag-stripe card readers is of particular concern as it provides thieves with access to both sensitive card and PIN data with little chance of detection by the cardholder
  - *Some industry insiders estimate the number of these vulnerable dispensers still in operation to be more than half of the current market population*

Increasing Defensive Measures

New product introductions raising the level of equipment security

- Dispenser manufacturers are responding to the increasing threat levels
  - *Introducing new hardware solutions to meet increased security requirements*
  - *Similar to efforts being undertaken by pin pad and ATM manufacturers*
- Dresser Wayne's latest secure payment offering has been designed for new security standards including PCI EPP/UPT, ANSI X9, ISO, EMV, APACS, and Interac
  - *Soon to be available on new dispensers and as a retrofit for many existing models currently in the market*
  - *Enhanced Security to Meet Increasing Demands of Security Regulations*
    - *Increased resistance to PIN disclosing bugs and track data skimming*
    - *Card Reader Protection/Secure Communications*
    - *Deterring visual observations of cardholder's PIN entry*
    - *Protections against unauthorized removal of the devices from the terminal*

How can I be prepared?

Protect your customers and your reputation today

- Assess the threat potential at your sites - are you in a skimming hotspot?
  - *Inquire with local authorities and your payment processor*
- Assess the vulnerabilities of your existing equipment
  - *Ensure your dispensers have all available security features installed*
  - *Become familiar with your equipment so skimming devices are more easily detected*
  - *Reduce access to sensitive payment electronics by replacing standard locks with site specific versions*
- Put defensive measures in place improve security of your forecourt
  - *Educate staff to increase awareness of fraud potential*
  - *Establish periodic/frequent inspections of equipment for evidence of tampering*
  - *Security cameras should be trained on AFDs whenever feasible to discourage unauthorized access*
  - *Develop a comprehensive mitigation strategy to reduce fraud potential at your sites*

Preparing for PCI Compliance

How can I be prepared?

Protect your customers and your reputation tomorrow

- Monitor status of evolving standards and required implementation dates
  - *Identify security standards applicable to your sites*
    - *Including PCI EPP, UPT, ANSI X9, ISO, EMV, APACS, and Interac*
  - *Pay special attention to new dispenser and existing dispenser mandates*
- Understand merchant responsibilities for maintaining compliance
- Determine equipment migration strategy with your equipment providers
  - *Perform an inventory of your existing equipment population*
  - *Implement a combination of dispenser upgrades and replacements depending on age of existing equipment and upgrade/retrofit kit availability*
- Consider deployment of certified pay at the pump hardware as soon as it becomes available - even if ahead of scheduled mandates
  - *Deploy configurations that protect both PINs and sensitive cardholder data*
  - *Choose configurable solutions that provide flexibility for future requirements*

Summary of Key Messages

- New PIN security requirements are approaching for automated fuel dispensers
  - *PCI PED now being administered by the PCI Security Standards Council*
  - *Separate from more commonly known Data Security Standards*
  - *Require certified equipment deployments to begin in the US by January 2009*
  - *Similar requirements coming into effect for Canadian market*
- Security mandates are timely considering:
  - *The industry has seen significant growth in card use at retail petroleum sites*
  - *Fraud incidents at the dispenser are on the rise*
- Security levels vary widely for existing equipment in the marketplace
  - *Dresser Wayne is bringing compliant product to market ahead of deadlines*
- Defensive measures today will help protect your sites while preparing for PCI compliance tomorrow
  - *Deploy certified hardware as soon as it becomes available*

Thank You!

Payment Card Industry (PCI) Compliance at the Dispenser: Are You Prepared?

Tim Weston, Dresser Wayne
October 12th, 2007