Protect 2013

ATM Cash-out Attacks

Susan Langford, Ph.D.

Atalla Sr. Cryptographer

About HP Atalla Security Products

Founded 1972, HP 2002, HP Enterprise Security Products 2012

Trusted security partner in the Financial Services industry

Customers are the largest financial institutions and retailers worldwide

35 years experience in data protection, key management, cryptographic performance

250 Million card transactions protected daily by Atalla

Technology leader in Host Security Modules and banking standards

Leading HSM vendor serving Americas and APJ card payments markets

Banks, payments processors, retailers, oil and gas firms, and more…

Solutions the support highest government and industry standards

ATM, POS, and EFT payments applications and transactions (ANSI X9F, PCI-DSS, PCI-PTS-HSM)

Serve/protect/manage encryption keys for broad range of encryption devices/solutions

Cash-out attacks

Coordinated raids on ATMs using cloned cards & stolen PINs

2008 – RBS WorldPay - $9.5 Million

Cash withdrawn in less than 12 hours using 2100 ATMs worldwide - United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada.

- Used just 44 cards – Payroll Debit
- Hackers manipulated the bank's database to change balances, limits, and delete transaction data
- Watched the attack in real time from within WorldPay's network.

2013 – $45 Million

December: $5 million, National Bank of Ras Al-Khaimah in the United Arab Emirates, known as RAKBANK, 4500 ATM transactions in 20 countries.

February: $40 million, Bank of Muscat in Oman, 24 countries.

- RAKBANK's processor is based in India, and Bank of Muscat's processor is based in the U.S
- In New York City: $2.4 million via 3,000 ATM withdrawals over the course of about 13 hours

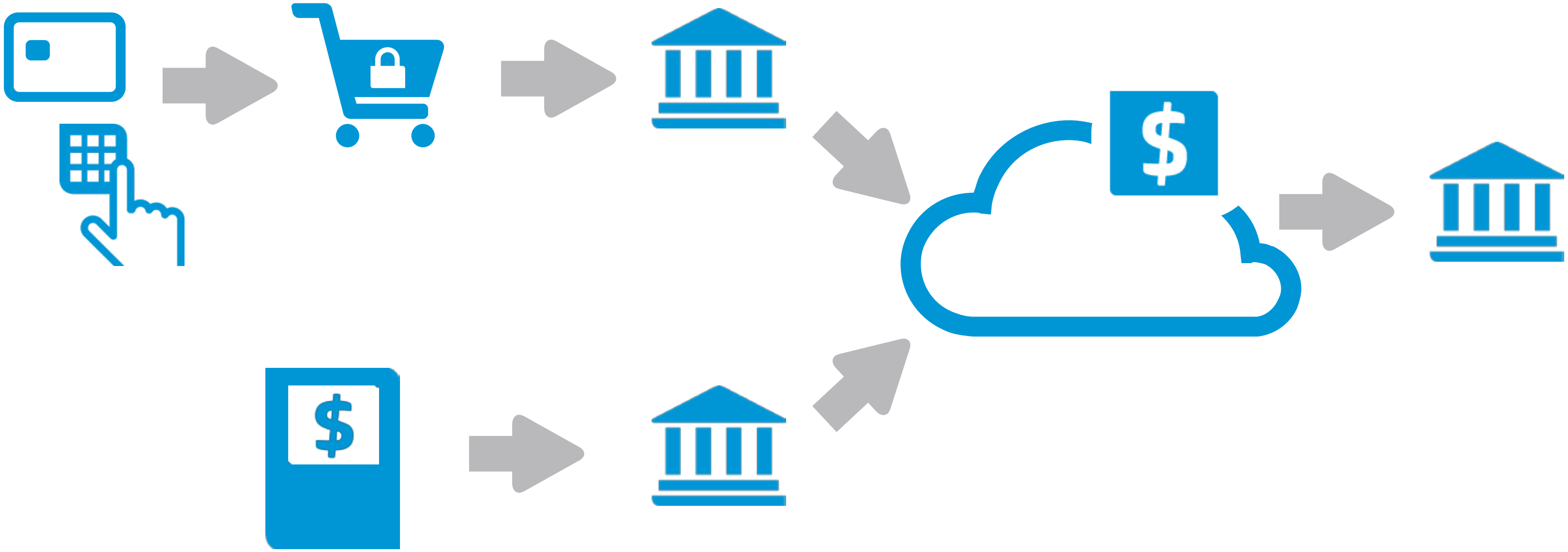
Process of a cash-out attack

How banks are robbed in the 21st century

1. Steal debit card numbers. (These can be bought or snooped in bulk).
2. Infiltrate financial institution(s) to find matching PINs. (This **should** be hard.)
3. Hack bank payment apps to inflate/replenish account balances and remove transaction limits.
4. Clone the cards.
5. Send a bunch of runners out with cards/PINs in an orchestrated attack window.
6. Erase the logs.

The payments network

PIN is encrypted at point of entry and never in the clear outside of secure hardware



Why worry about this type of attack?

Attackers are getting better it targeted intrusions

Attack is appealing because it's cash

US lags in EMV implementation

- Cloning mag stripe cards is easier than cloning chips
- The world's organized crime is being herded in US direction.
- EMV is **not** a "silver bullet".

PINs over the Internet

- WorldPay attackers apparently finessed the HSM (the hard way).
- Internet allows compromise at user
- DDoS become distributed PIN cracking
- You may not know where a transaction comes from.

PINs

The good, the bad, and the ugly

The good: a PIN isn’t just a numeric password

If it is handled correctly

Security model can make 4 digits “good enough”

PIN only entered via secure PIN pad

- Bound with single account number
- Entry can’t be automated

PINs only processed and verified in secure hardware

- Never accessible to even root user of system
- Keys change as it passes through different systems, but still bound to same account
- Always a function of account + PIN + key
- Can’t do offline checking
- Can’t compare your PIN to other accounts

Velocity checking works if PIN only comes from known entry points.

The bad: encrypting PIN blocks

Lots of legacy issues

PIN blocks without the account number

Older PIN Pads and some smartcards

- No randomness: if your PIN = my PIN, can easily tell by monitoring line.
- With randomness: Easy for insider (malware) to run my known PIN against every account.
- Attacks get interesting when server supports changes in format.

Insider attack against even the “good” formats

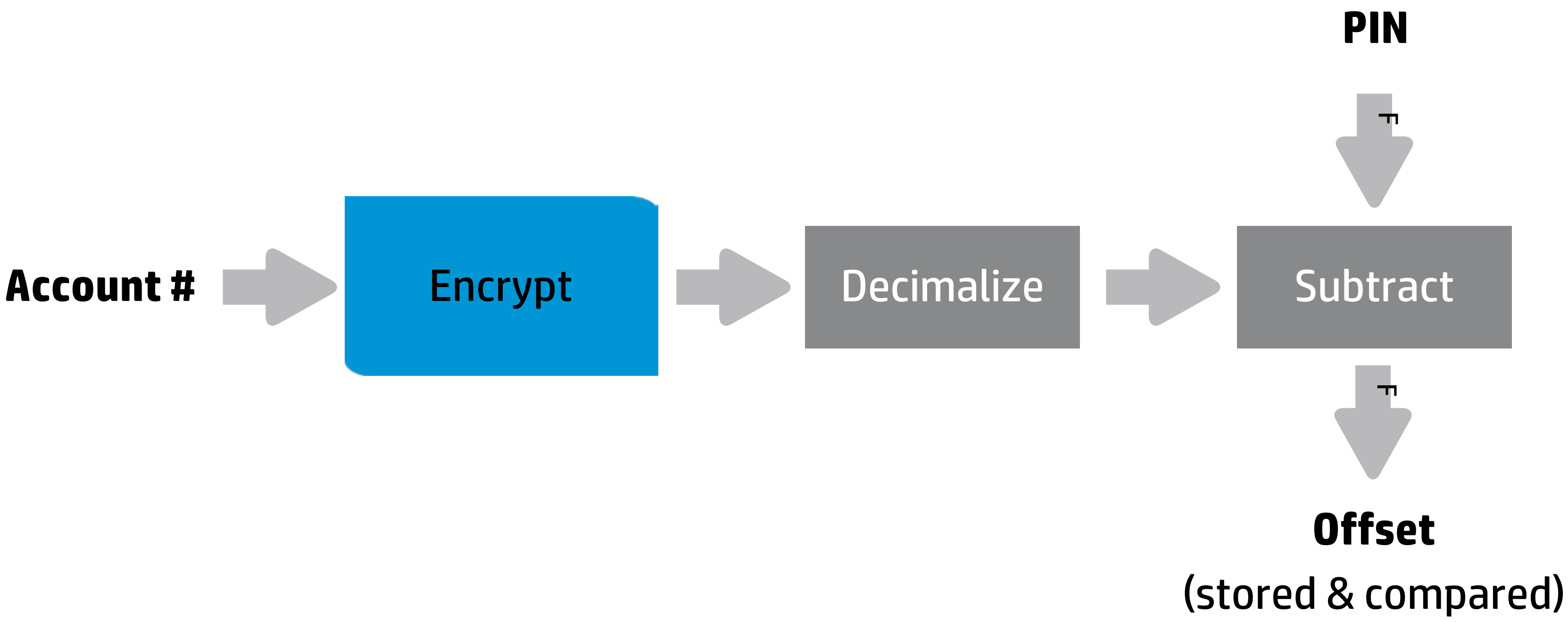
ANSI PIN block (aka ISO-0) and ISO-3

- Combine account number and PIN via XOR
- Account number is an input to the function
- Putting in the wrong account number returns different errors depending on value of PIN digit.

There are implementation fixes but generally not enabled by default.

The bad (continued): verifying PINs

IBM 3624



Account #

Encrypt

Decimalize

Subtract

PIN

Offset

(stored & compared)

The ugly: distributed PIN search

Or, other things to do with a botnet…

Compromise a few thousand PCs

Each PC tries 2 different account numbers with 2 PINs

- Most user PINs are 4 digits
  - And those 4 digits are badly chosen
- Two wrong tries aren't going to raise flags
- WorldPay attack only took 44 PINs.

Home banking PINs often limited to IP address

- Harder limitation to enforce for eCommerce
- If the attacker is on your network, user-side security doesn't help.

PIN	Frequency
1234	10.713%
1111	6.016%
0000	1.881%
1212	1.197%
7777	0.745%
1004	0.616%
2000	0.613%
4444	0.526%

Defenses

Dual-control/split knowledge

A compromised computer looks like an insider

So protect against insiders

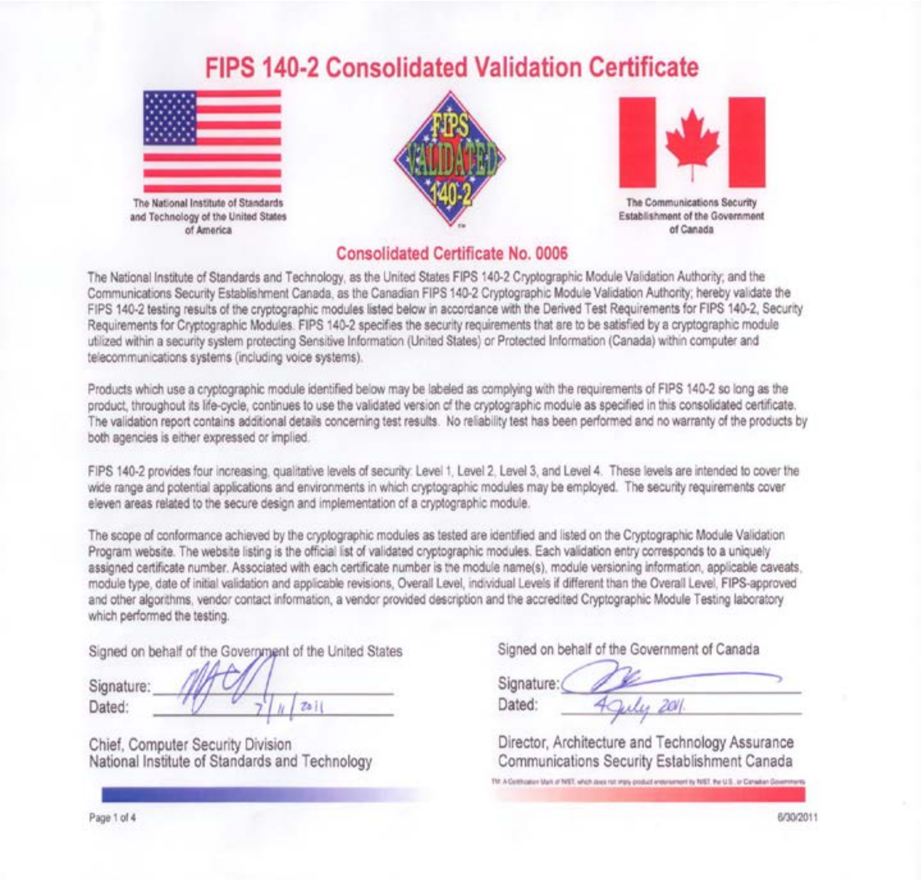
Dual control: It takes at least two people to approve any security-relevant action

- Needs “enough” ease of use
- Remote management and policy setting

Split knowledge: No single person knows any key or other secret

- PINs should never be accessible by any employee

FIPS 140-2 validation


FIPS
VALIDATED
140-2
TM

FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0006

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature:
Dated: 7/11/2011

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature:
Dated: 4 July 2011

Director, Architecture and Technology Assurance
Communications Security Establishment Canada

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S., or Canadian Governments

Page 1 of 4

6/30/2011

Why Atalla?

35+ years of experience in data protection, security and cryptographic performance.

- Physical & Logical Security
  - Tamper-reactive security
  - FIPS 140-2 level 3 + active zeroization
  - PCI-HSM validated
  - FIPS 140-2 level 3 smartcard based management
  - Industry leading key protection – AKB
- Ease of use
  - GUI-based Secure Configuration Assistant (SCA) makes setup easier and faster
  - Secure remote management and upgrades
- Flexibility with customer defined security policy and software upgrades
- Support backed by the power of HP.

HP Atalla Ax160 NSP products

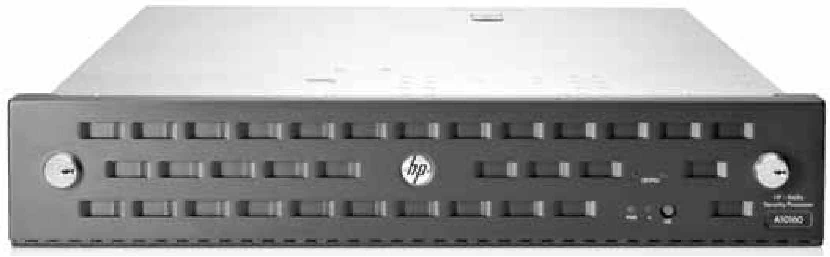
Hardware Security Module (HSM)

Highly secure cryptographic processor

Functionality is aimed financial payments

- ATM /EFT/POS
- Credit cards and EMV
- Stored Value, loyalty cards and funds transfer

May be of use for other high-security applications



Hardware

Active zeroization

- State-of-the-art, 2U rack-mountable form factor
- Locking bezel with two Medeco locks
- Auto-sensing 10/100/1000 Base-T Ethernet TCP/IP
- Dual power supply

Atalla HSMs

Hardware appliance

A8160

- Entry level hardware
- 66 PIN translates/second

A9160

- Mid Range
- 200 PIN translates/second

A10160

- High End
- 1080 PIN translates/second

+ Firmware image

Basic Software

- Included in module price
- Different key management techniques
  - AKB – more secure: A1.30
  - Variant – legacy key management: V1.30

Premium Software

- Additional charge, sold separately
- More Features
  - AKB – A2.10
  - Variant –V2.10
- Uses newer, stronger smartcards

“Why did I rob banks? Because I enjoyed it. I loved it ...

Go where the money is...and go there often.”

Willie Sutton, bank robber

Thank you

Protect 2013

Security for the new reality