A Journey To Protect Points Of Sale

Nir Valtman, CISSP
w : www.valtman.org
: @ValtmaNir
Introduction
I'm an architect
Zombies!!!
Defacement
OPEN SOURCE

AntiDef

Secure TDD

Memory Scraper
Why Points Of Sale Targeted?
CC's are delivered like this:

IBAN | CVV/CVV2 | EXP DATE | NAME | ADDRESS | CITY | STATE (USA) | ZIP | COUNTRY | MMN | DOB | SSN (USA) | PHONE | EMAIL |

USA CC Fullz + tutorial

Choose one or leave blank
- 5 Full info CC USA - $40 / 0.08BTC
- 10 Full info CC USA - $80 / 0.14BTC
- 20 Full info CC USA - $145 / 0.25BTC
- Dumps USA + PIN - $100 / 0.17BTC

Your Email (You will receive CC by email)

BUY (no javascript)
Deployment
Point Of Sale IS NOT Payment Application
Where Are My Credit Cards?

Rest
Transit
Memory

Store

Payment Processor's Data Center

Payment Processing Host

Rest
Transit
Memory
Where Are My Credit Cards?

- **Rest**
- **Transit**
- **Memory**

**Mobile App** → **Presentation Server** → **Application & Payment Server** → **Payment Processor’s Data Center**
Keys to the Kingdom

Matthew 16:19
Retail Environment Assumptions

100% PCI Compliant
Retail Environment Assumptions
Retail Environment Assumptions
Retail Environment Assumptions

Not vulnerable
Retail Environment Assumptions
Retail Environment Assumptions

Cashier ≠ hacker
Retail Environment Assumptions

Big Brother
RATS

Achilles Tendon
Remote Administration Tools

Achilles Tendon
Routing

Achilles
Tendon
Threats
Payment Stages - Authorization

Transmit Track1/2

PA

POI

Route Track1/2

Difficult
Exploitation

Transmit Track1/2

Issuer

Processor

Acquirer
Payment Stages - Authorization
Payment Stages - Settlement

Store & Send PANs

PA Server

Difficult Exploitation

Credit Merchant’s Account

Processor

Acquirer

Settlement

Issuer

Gateway

Transmit
Payment Stages - Settlement
Memory Scraping
Demo by Idan Geula
http://securitytools.github.io/MemoryScraper/
PRIVACY
Bypassed Solutions
SecureString Class Demo
Next Generation Firewall
ANTI *
Data loss
Correct Solutions
Cyber Intelligence
I have access to POS terminals in the US, what is the best malware I should use?
You need to infect the firmware of the terminal. By doing that, you can get full track 1 + 2, but the PIN will be hashed.
Selling malicious firmware for Verifone’s POS terminals. Leaks dumps + PINs through GPRS. Price: Only 700$
Business Development Offer
Owner of a fake POS sells his terminal. Price: 50% from revenue sharing.
RFI: Change terminal configuration to require PIN for all cards. Cause: Get only 101 data, but wants PINs

Proposed Solution: Thermal Imager
Network-based Anomaly Detection
Operating System
Anomaly Detection
Runtime Obfuscation
Not only products required!
Security

Architecture
Security Architecture

Performance

Security
Assembly Signing
Assembly Obfuscation
PROCESS ISOLATION
What Next
What Would You Steal?

BIP BIP

[Image of a cartoon bird saying "BIP BIP"]

[Image of a cartoon character in discomfort]
Memory Scraping
Cashier = hacker
Summary
Security by Obscurity
Simple Exploitation
Hard to Protect
You’re Insured