ANATOMY OF POINT-OF-SALE MALWARE

Amol Sarwate, Director of Vulnerability Labs, Qualys

October 21, 2014 | Toronto

QUALYS®
CONTINUOUS SECURITY
QUALYS®

Agenda

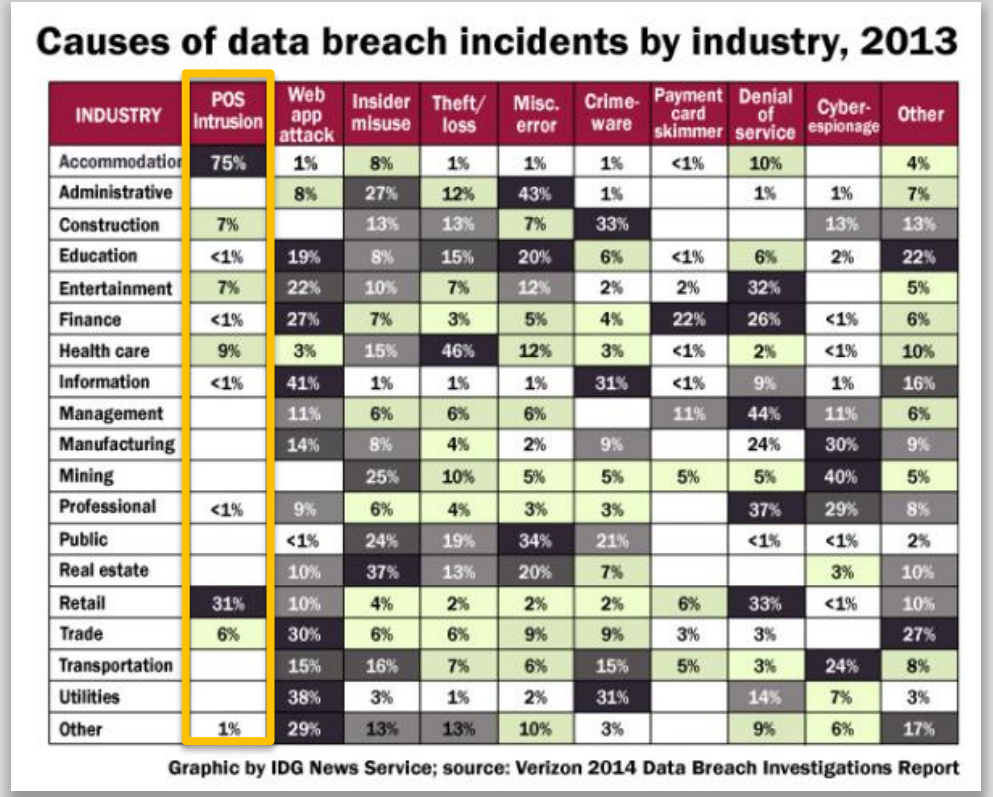
Credit Cards and PoS systems

Malware Attack working

Demo !

Qualys VM for detection

PoS Data Breaches



Causes of data breach incidents by industry, 2013

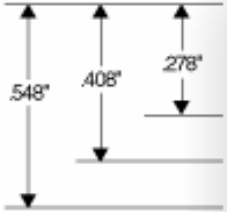
INDUSTRY	POS intrusion	Web app attack	Insider misuse	Theft/ loss	Misc. error	Crime-ware	Payment card skimmer	Denial of service	Cyber-espionage	Other
Accommodation	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative		8%	27%	12%	43%	1%		1%	1%	7%
Construction	7%		13%	13%	7%	33%			13%	13%
Education	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Health care	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing		14%	8%	4%	2%	9%		24%	30%	9%
Mining			25%	10%	5%	5%	5%	5%	40%	5%
Professional	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real estate		10%	37%	13%	20%	7%			3%	10%
Retail	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities		38%	3%	1%	2%	31%		14%	7%	3%
Other	1%	29%	13%	13%	10%	3%		9%	6%	17%

Graphic by IDG News Service; source: Verizon 2014 Data Breach Investigations Report

Credit Cards

PoS Components

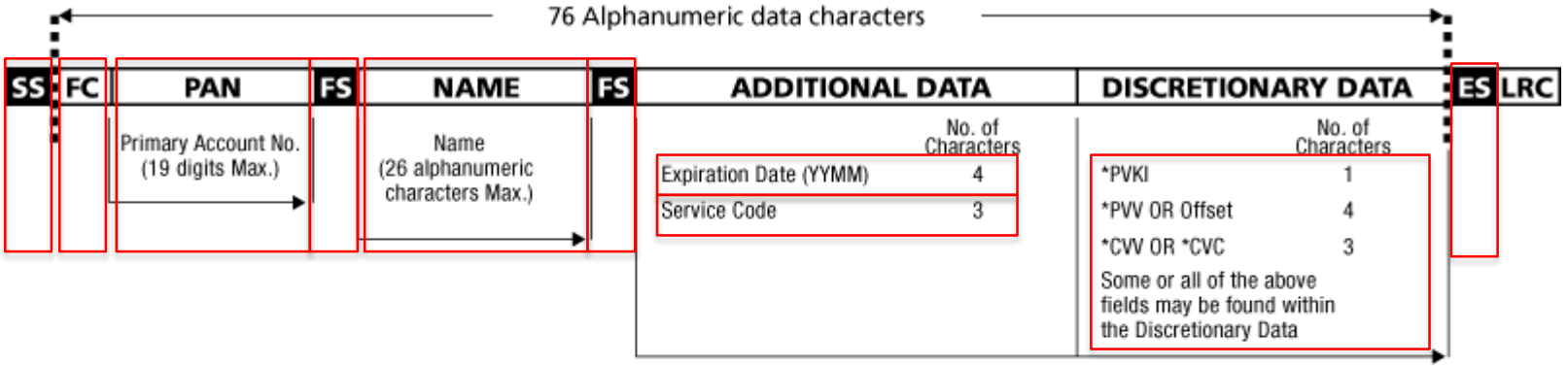
Magnetic Stripe



0.233"			Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	Track 1	IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110"	Track 2	ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110"	Track 3	THRIFT	210 BPI	5 Bits per Character	107 Numeric Characters

Magnetic Stripe: Track 1

%B4074410291410104^Doe/John^1409101000001822
?



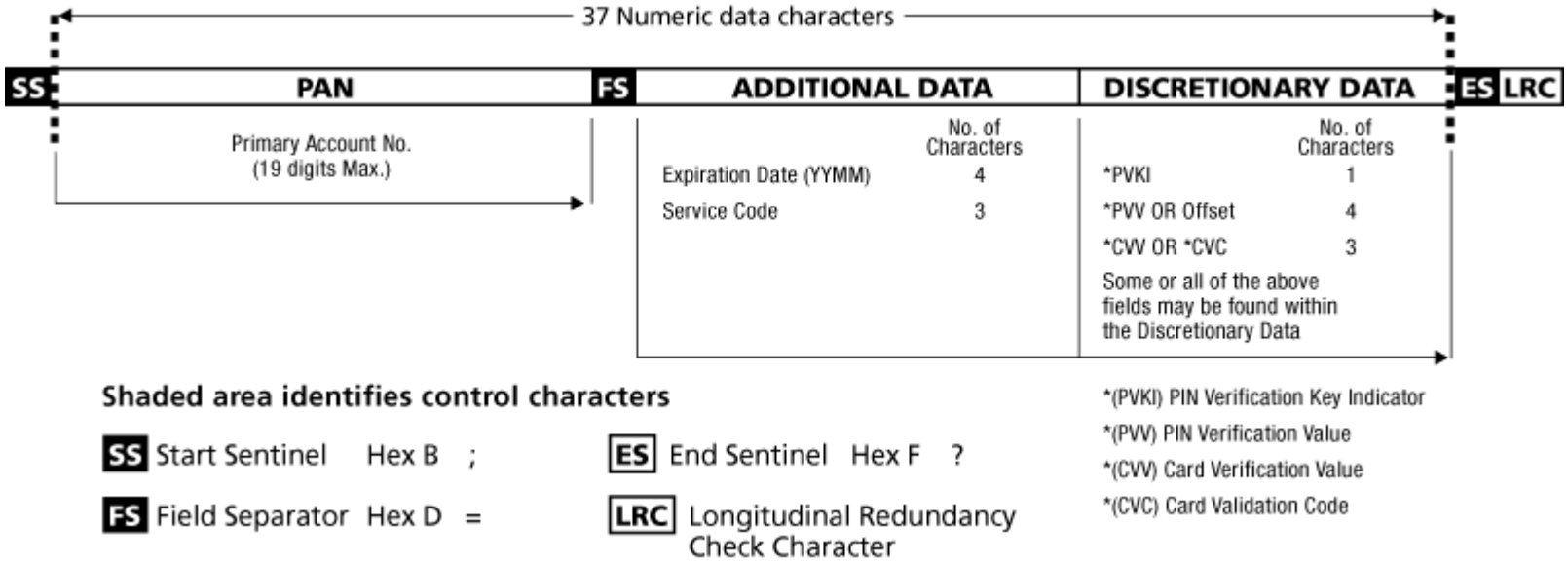
Shaded area identifies control characters

- SS Start Sentinel %
- FS Field Separator ^
- ES End Sentinel ?
- FC Format Code
- LRC Longitudinal Redundancy Check Character

*(PVKI) PIN Verification Key Indicator
*(PVV) PIN Verification Value
*(CVV) Card Verification Value
*(CVC) Card Validation Code

Magnetic Stripe: Track 2

;4074410291410104=14091010000182?



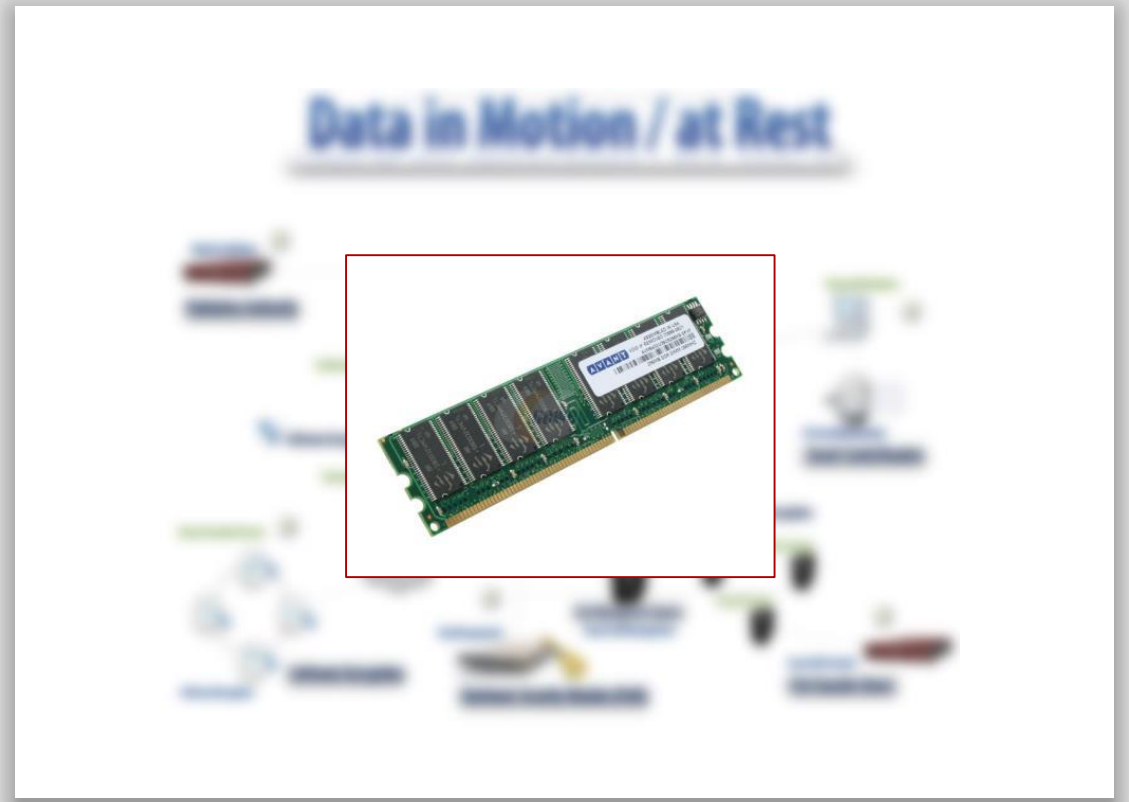
Major Transition Types

1. Card swipe

2. Card not present

Data Encryption

Data Encryption in RAM?



Attack Scenario

RAM Scraper Attack

Step 1: Find POS process
with credit card data

EnumProcesses
OpenProcess
EnumProcessModules
GetModuleBaseName

RAM Scraper Attack

Step 1: Find POS process with credit card data

Step 2: Elevate privilege to SE_DEBUG

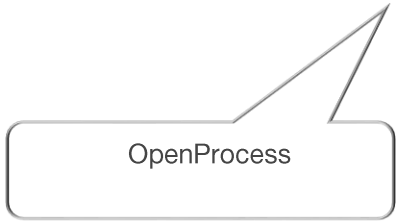
OpenProcessToken
LookupPrivilegeValue
AdjustTokenPrivileges

RAM Scraper Attack

Step 1: Find POS process with credit card data

Step 2: Elevate privilege to SE_DEBUG

Step 3: Open POS process



RAM Scraper Attack

Step 1: Find POS process with credit card data

Step 2: Elevate privilege to SE_DEBUG

Step 3: Open POS process

Step 4: RAM scraping

VirtualQueryEx
ReadProcessMemory

Verify Card Number: Luhn algorithm

Original Number:	4	5	5	6	7	3	7	5	8	6	8	9	9	8	5	5
Drop the last digit:	4	5	5	6	7	3	7	5	8	6	8	9	9	8	5	
Reverse the digits:	5	8	9	9	8	6	8	5	7	3	7	6	5	5	4	
Multiple odd digits by 2:	10	8	18	9	16	6	16	5	14	3	14	6	10	5	8	
Subtract 9 to numbers over 9:	1	8	9	9	7	6	7	5	5	3	5	6	1	5	8	
Add all numbers:	1	8	9	9	7	6	7	5	5	3	5	6	1	5	8	85

(85 + 5) mod 10 = 0

Optimizations

Look only for committed memory (MEM_COMMIT)

Ignore memory that is part of the executable image (MEM_IMAGE)

Remember memory addresses for next scrape

Pattern match on Track 1 or Track 2 data

Regular expressions
%B4074410291410104^Doe/John^140910100000182?

Demo !

Mitigation

POS Business Owners

Use POS only for its intended purpose
Secure remote management software (RDP, VNC and others)
Measures to protect against insider threats (11% in 2013 idtheftcenter.org)
Best practices (RunAs, Patching, EOL, Access Control, Vuln scan & Auditing)
Enable end-to-end encryption hardware/software
Deploy smartcard (aka chip-card) enabled POS terminals.

POS Software Vendors

Restrict un-encrypted sensitive data in memory
Use built-in encryption support from application frameworks

What can credit card users do? (audience participation)

Thank YOU !

@amolsarwate

QUALYS®
CONTINUOUS SECURITY
QUALYS®