Anatomy of a Credit Card Stealing POS Malware

Amol Sarwate
Director of Vulnerability Labs, Qualys Inc.
@amolsarwate

QUALYS®
CONTINUOUS SECURITY

Agenda

POS systems and Credit Cards

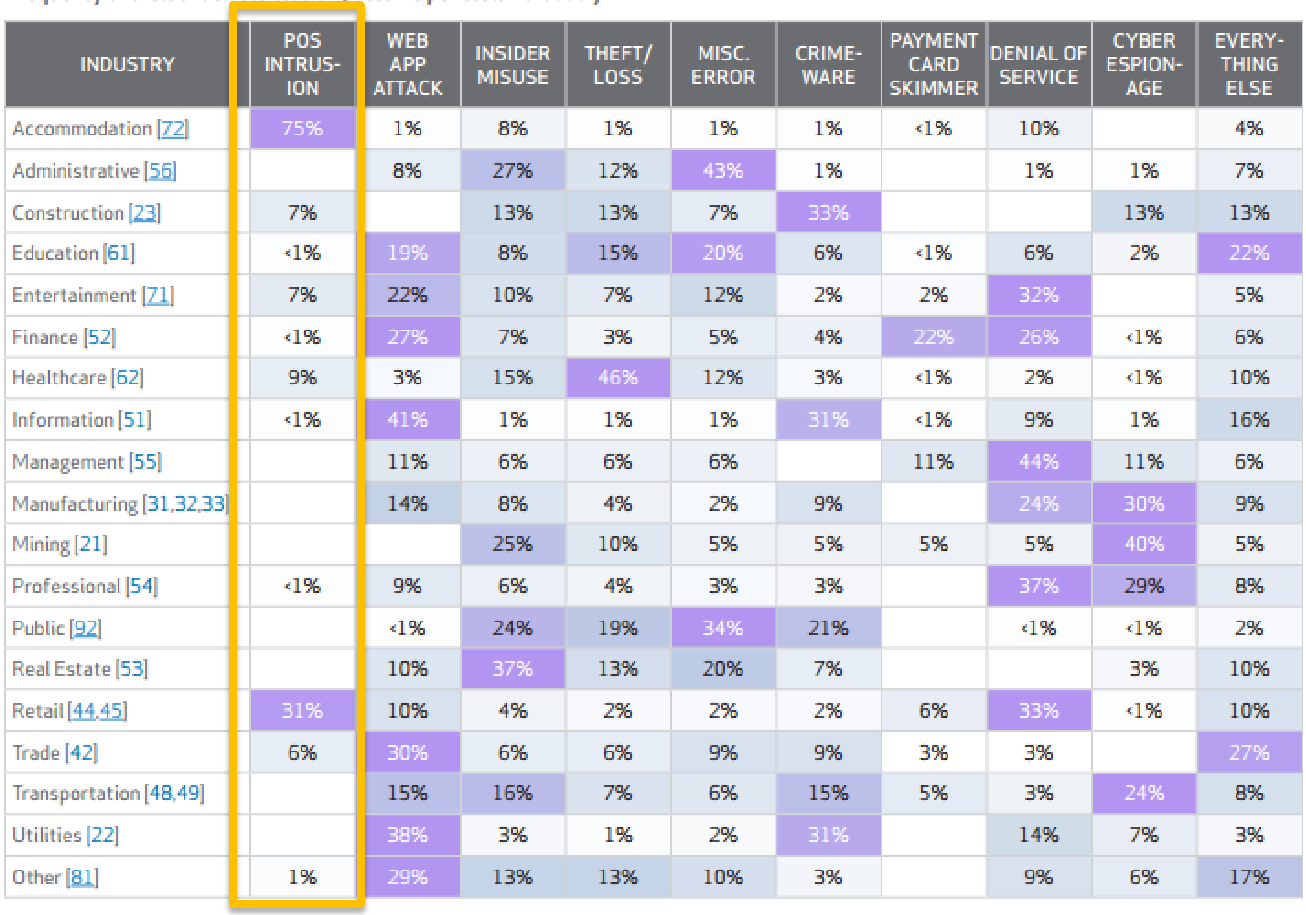
Attack working

Demo !

Countermeasures

2014 Verizon Data Breach Report

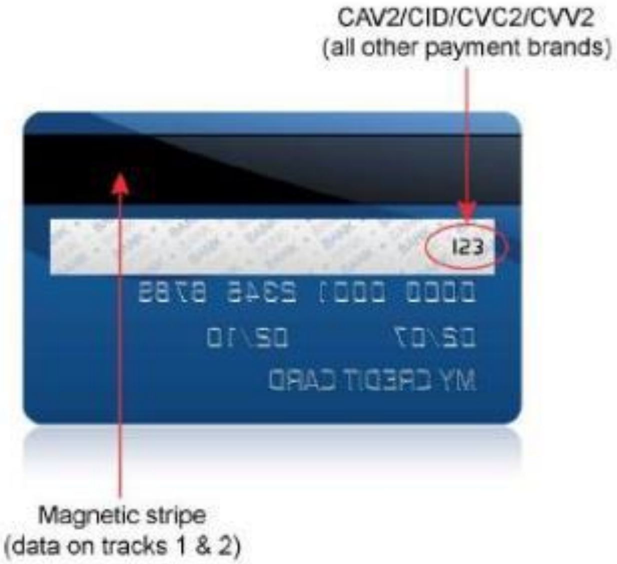
Figure 19.
Frequency of incident classification patterns per victim industry



INDUSTRY	POS INTRUSION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIMEWARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPIONAGE	EVERYTHING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

For more information on the NAICS codes [shown above] visit: https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012

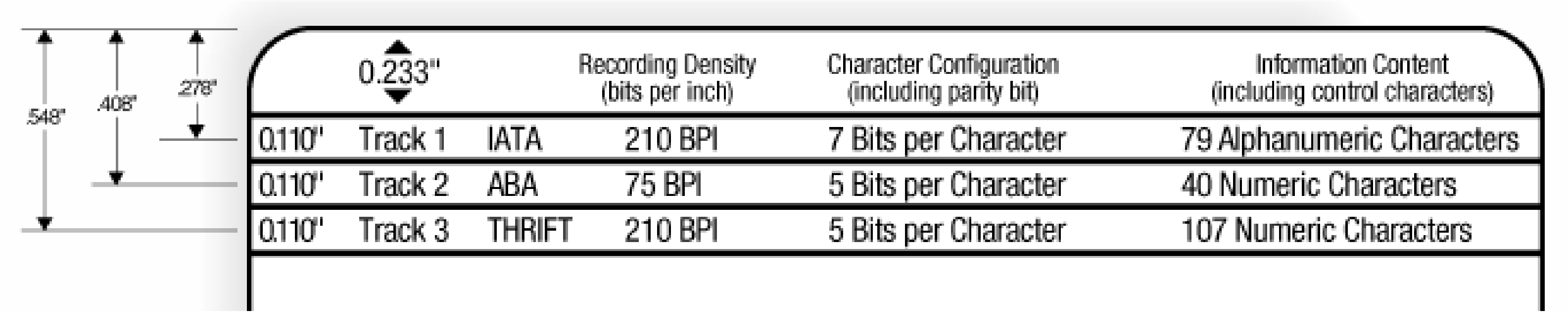
Credit Cards


CAV2/CID/CVC2/CVV2 (all other payment brands)

Magnetic stripe (data on tracks 1 & 2)

POS Components

Magnetic Stripe

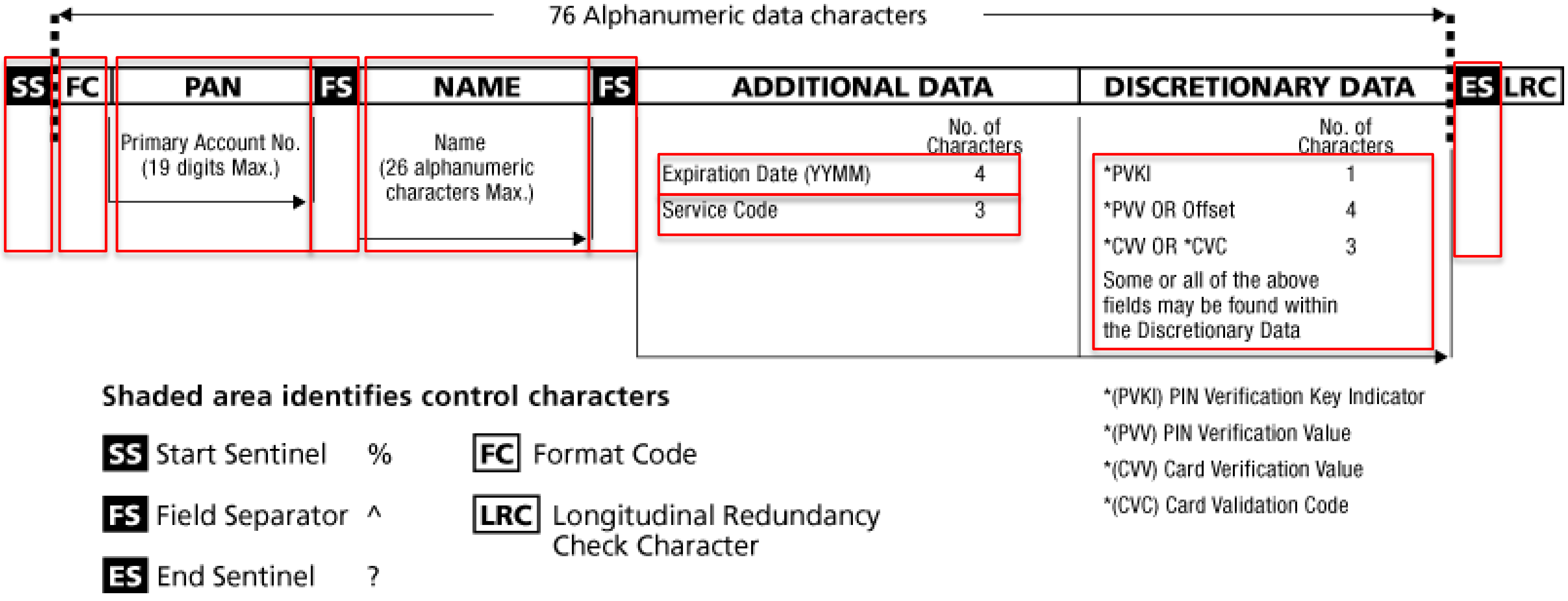


			Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110'	Track 1	IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110'	Track 2	ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110'	Track 3	THRIFT	210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

Image: http://www.q-card.com/support/magnetic-stripe-card-standards.asp

Magnetic Stripe: Track 1

%B4074410291410104^Doe/John^1409101000000182?



76 Alphanumeric data characters

SS | FC | PAN | FS | NAME | FS | ADDITIONAL DATA | DISCRETIONARY DATA | ES | LRC

PAN: Primary Account No. (19 digits Max.)

NAME: Name (26 alphanumeric characters Max.)

ADDITIONAL DATA:

	No. of Characters
Expiration Date (YYMM)	4
Service Code	3

DISCRETIONARY DATA:

	No. of Characters
*PVKI	1
*PVV OR Offset	4
*CVV OR *CVC	3

Some or all of the above fields may be found within the Discretionary Data

Shaded area identifies control characters

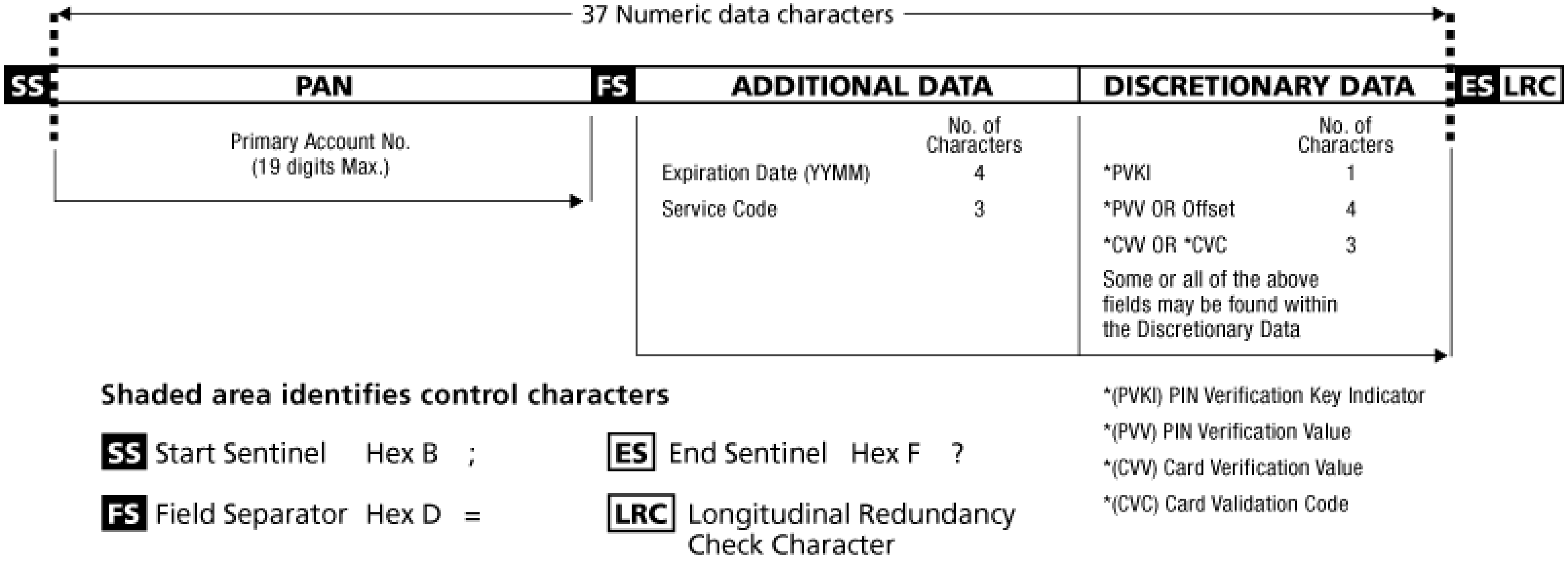
SS	Start Sentinel	%
FS	Field Separator	^
ES	End Sentinel	?
FC	Format Code	
LRC	Longitudinal Redundancy Check Character	

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

Image: http://www.q-card.com/support/magnetic-stripe-card-standards.asp

Magnetic Stripe: Track 2

;4074410291410104=14091010000182?



37 Numeric data characters

SS | PAN | FS | ADDITIONAL DATA | DISCRETIONARY DATA | ES | LRC

Primary Account No.
(19 digits Max.)

ADDITIONAL DATA	No. of Characters
Expiration Date (YYMM)	4
Service Code	3

DISCRETIONARY DATA	No. of Characters
*PVKI	1
*PVV OR Offset	4
*CVV OR *CVC	3

Some or all of the above fields may be found within the Discretionary Data

Shaded area identifies control characters

SS	Start Sentinel	Hex B	;
FS	Field Separator	Hex D	=
ES	End Sentinel	Hex F	?
LRC	Longitudinal Redundancy Check Character		

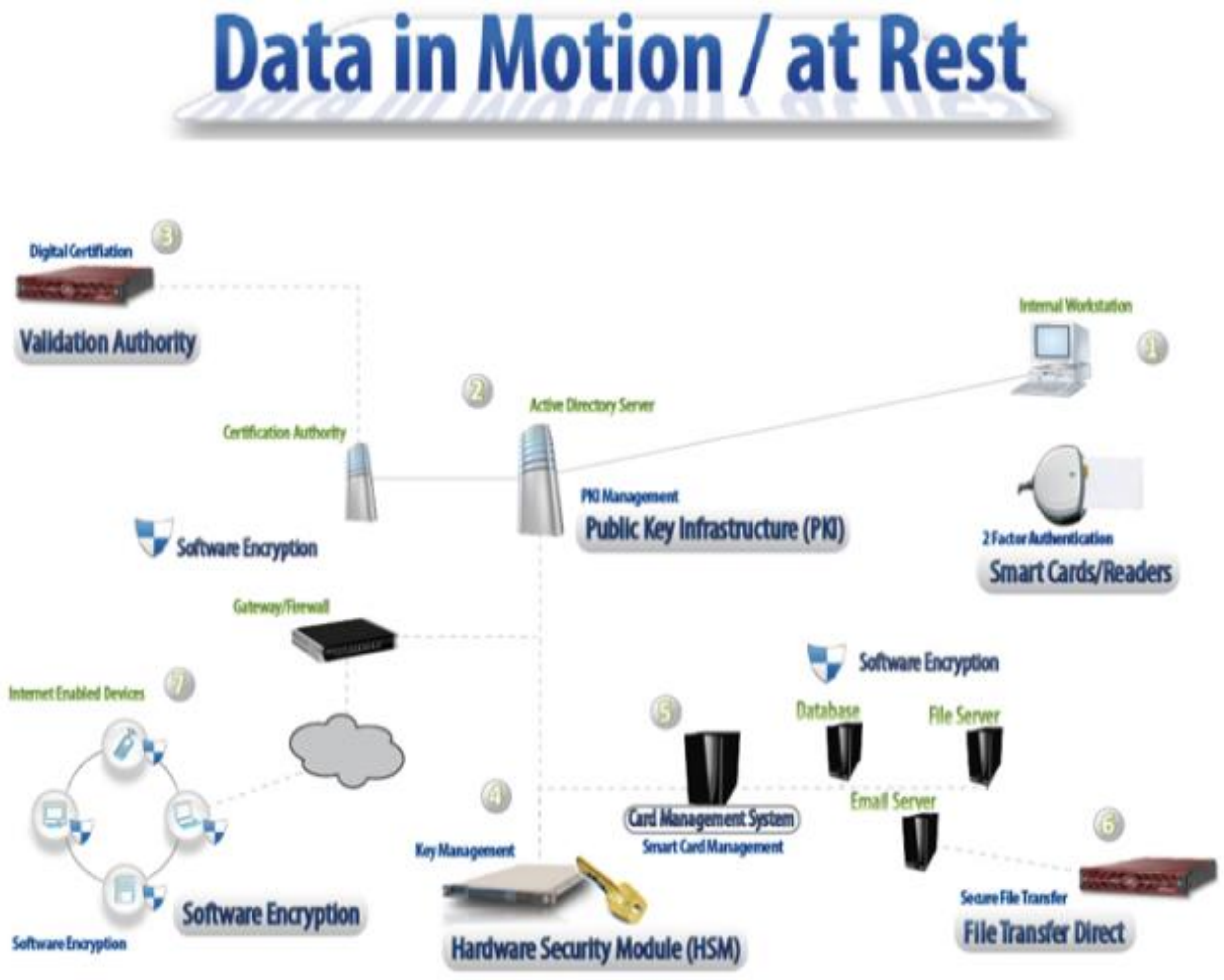
*(PVKI) PIN Verification Key Indicator
*(PVV) PIN Verification Value
*(CVV) Card Verification Value
*(CVC) Card Validation Code

Image: http://www.q-card.com/support/magnetic-stripe-card-standards.asp

Major Transition Types

1. Card swipe

2. Card not present



Data Encryption

Data in Motion / at Rest

Data in RAM

Attack Scenario

RAM Scraper Attack Working

Step 1: Find POS process with credit card data

EnumProcesses
OpenProcess
EnumProcessModules
GetModuleBaseName

RAM Scraper Attack Working

Step 1:
Find POS process
with credit card data

Step 2:
Elevate privilege to
SE_DEBUG_NAME

OpenProcessToken
LookupPrivilegeValue
AdjustTokenPrivileges

RAM Scraper Attack Working

Step 1:
Find POS process
with credit card data

Step 2:
Elevate privilege to
SE_DEBUG_NAME

Step 3:
Open
POS process

OpenProcess

RAM Scraper Attack Working

Step 1:
Find POS process
with credit card data

Step 2:
Elevate privilege to
SE_DEBUG_NAME

Step 3:
Open
POS process

Step 4:
RAM
scraping

VirtualQueryEx
ReadProcessMemory

RAM Scraper Attack Working

Look only for committed memory (MEM_COMMIT)

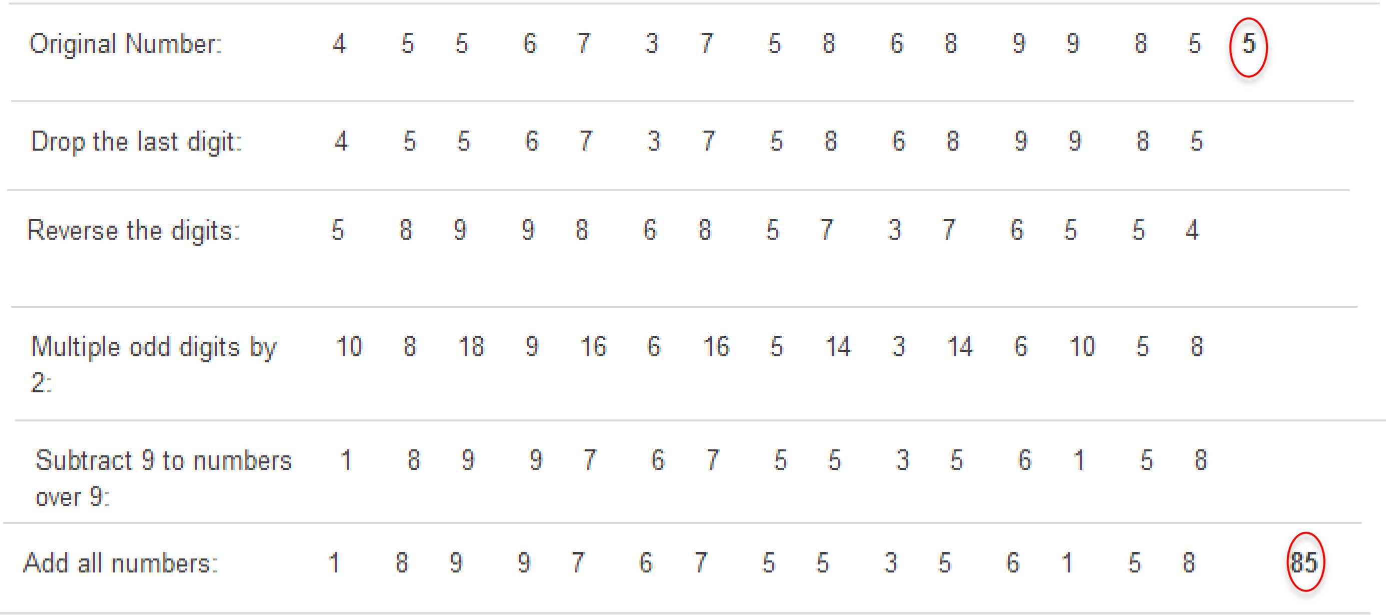
Ignore memory that is part of the executable image (MEM_IMAGE)

Remember memory addresses for next scrape

Pattern match on Track 1 or Track 2 data

%B4074410291410104^Doe/John^14091010000182?

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

Luhn algorithm – Quick and dirty C++ code

```
// returns 0 if credit card number is valid

int luhn(const char* cc) {

    int val,total=0,len = strlen(cc);
        int last = cc[len-1] - '0';
        bool flag = true;

        for(int i = (len-2); i >= 0;--i){
            val = (cc[i] - '0');
            if(flag)
                val *= 2;

            if(val > 9) val -= 9;
            flag = !flag;
            total += val;
        }
        return ((total + last) % 10);
}
```

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