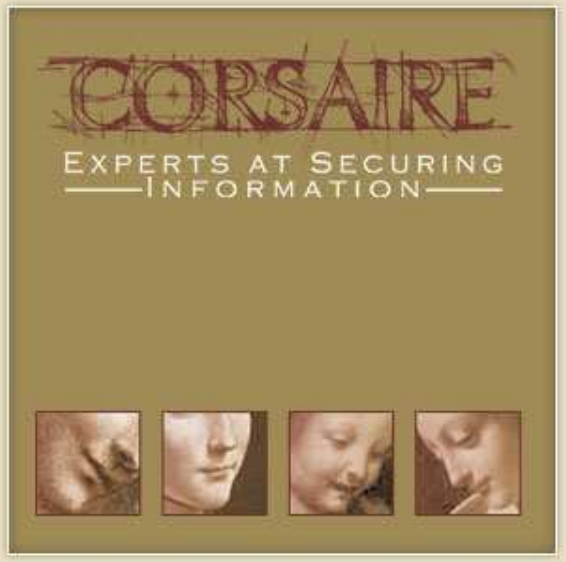


A Pentester's Guide to Credit Card Theft Techniques

by Adrian Pastor
adrian.pastor@corsaire.com

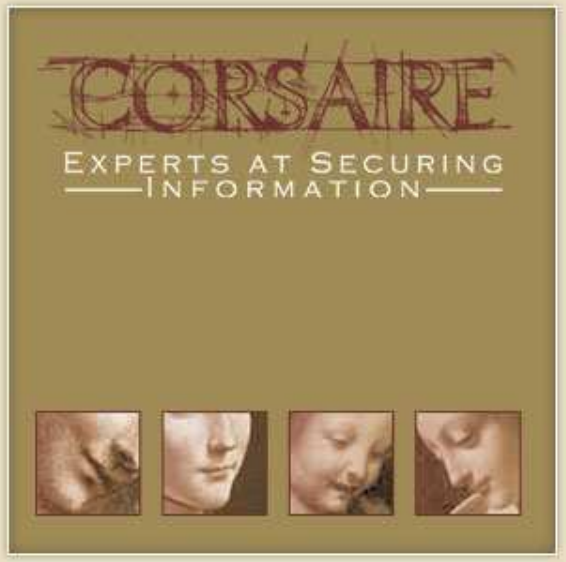
About me

- Principal Security Consultant @ Corsaire.com
- Independent Security Researcher @ GNUCITIZEN.org
  - AKA pagvac
  - Google “hacking linksys ip cameras” for last project
- I love what I do like most of you!
- Particularly interested in:
  - **Web** hacking
  - **Embedded** devices
  - **Credit card** security
  - Old school technologies such as **magstripes**
  - Meeting **people** with similar interests

Disclaimer

- Everything in this presentation is based on **personal opinion** and based on **personal experience**
- My views do *not* necessarily represent those of my employer
- I'm not here to persuade you or sell you anything, but rather to share my experience and exchange ideas and different points of view
- I don't expect you to agree with me
- I do not consider myself a PCI DSS expert, so do your homework

CORSAIRE

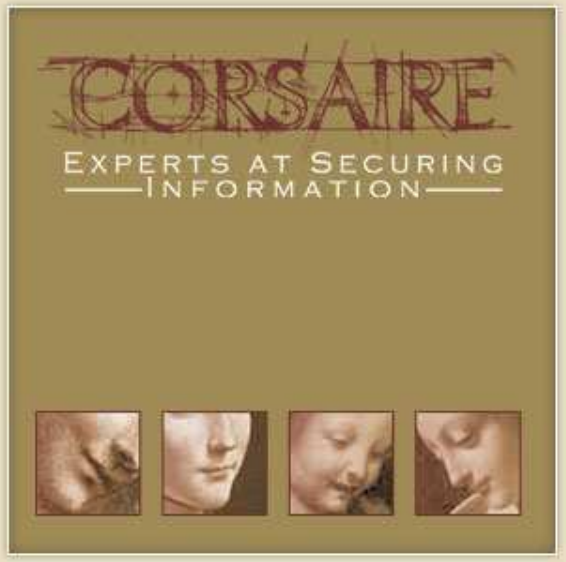


Agenda

What the heck does this presentation cover?

Agenda

- What made me choose this presentation topic?
- PCI DSS
- Common techniques used to compromise CC data



What made me choose this presentation topic?

Because there is always a reason for everything

What made me choose this presentation topic?

- Was trained to become a QSA
- Didn't know what to expect
  - my speciality had always been pentesting
- Eventually learned that QSA is about auditing and **checklists** rather than really **testing** if systems are secure

What made me choose this presentation topic? (pt 2)

- Was disappointed: most merchants wanted to hire a QSA to simply **shift responsibility** to third-party companies*
  - *Usually Payment Service Providers (PSPs)
- Felt I was acting as a lawyer rather than an IT security professional! ☹
- Gave up doing QSA work and kept focusing on pentesting and research

lawyer mouse 8-) →

CC-licensed content from
http://www.flickr.com/photos/thehouseofmouse/2798732003/

CORSAIRE

EXPERTS AT SECURING INFORMATION

PCI DSS 101

PC what?

PCI DSS 101

- Set of standards to protect **CC and personal data**
- Created to protect consumers and merchants, or just a global business scheme created by CC companies (jointly known as PCI SSC)?
- **12 requirements** in total
- Bored yet? ☺

CORSAIRE

CC-licensed content from http://www.flickr.com/photos/id-iom/3471057884/

PCI DSS 101 (pt 2)

- Juicy CC data
  - Full name
  - **PAN** (the actual CC number)
  - From/**Issuing** and **Expiry** date
  - **CVV2** (security code on back of card). NOT to be confused with CVV

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name	Yes	Yes	No
	Service Code	Yes	Yes	No
	Expiration Date	Yes	Yes	No
Sensitive Authentication Data [2]	Full Magnetic Stripe Data	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

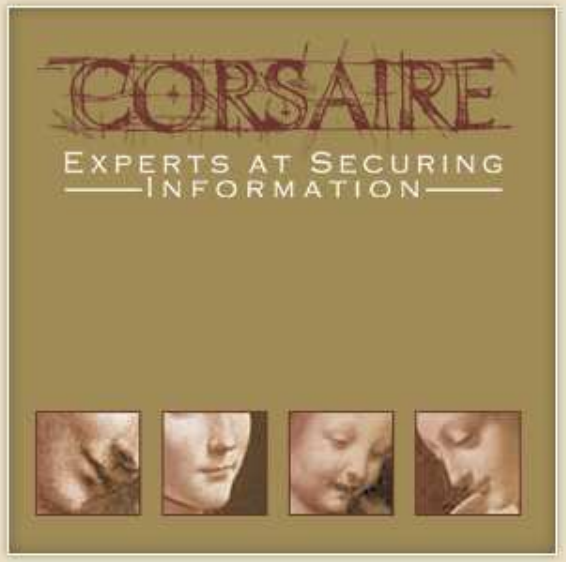
CORSAIRE

Chart from "PCI DSS Requirements and Security Assessment Procedures"

PCI DSS 101 (pt 3)

- Common architecture:
  Card Holder (Consumer)→ Merchant/Service Provider → Acquirer → Issuer

Diagram from “PCI Quick Reference Guide”



Interview with QSAs

QSAs wished to remain anonymous

Interview with QSAs

- Q. As a QSA, do you feel your certified status would be removed for openly sharing negative opinions as a QSA?
- A. *"If I was vocal enough with my negative views, I think my [QSA] status would be removed or at least 'threatened'"*
  - Anonymous QSA

CC-licensed content from http://www.flickr.com/photos/jacobdavis/

Interview with QSAs (pt 2)

- Q. What do you think of the PCI DSS standards overall?
- A. "*The standard is incredibly vague in some areas and strangely in depth in others. There is very little balance to it. Some elements you HAVE to enforce, others are open to interpretation.*"
  - *Anonymous QSA*

CC-licensed content from http://www.flickr.com/photos/jacobdavis/

Interview with QSAs (pt 3)

- Q. What would you say are the main reasons why credit cards are stolen from merchants?
- *A. "Money == Happiness?"*
  - Anonymous QSA

CC-licensed content from http://www.flickr.com/photos/jacobdavis/

CORSAIRE

EXPERTS AT SECURING INFORMATION

PCI DSS 1.2 weaknesses

Loopholes and limitations

PCI DSS 1.2 weaknesses

- WEP still allowed until June 2010!
  - *"For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. For current wireless implementations, it is prohibited to use WEP after* ***June 30, 2010****."* PCI DSS Requirement 4.1.1
  - Good post on the subject: http://snipurl.com/hz5wl

PCI DSS 1.2 weaknesses (pt 2)

- Level 4 merchants not required to be assessed? Weakest link?
  - Merchants with less than 20,000 e-commerce transactions and up to 1,000,000 in-store POS transactions
  - *"Quarterly Scan by an Approved Scanning Vendor (may be **recommended or required**, depending on acquirer compliance criteria)"*
    - http://snipurl.com/hz5zz
  - *"In addition to adhering to the PCI DSS, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and **may be required** for Level 4 merchants."*
    - http://snipurl.com/hz652
  - *"More than 80% of compromises identified since 2005 are Level 4 merchants"*
    - http://snipurl.com/i267c

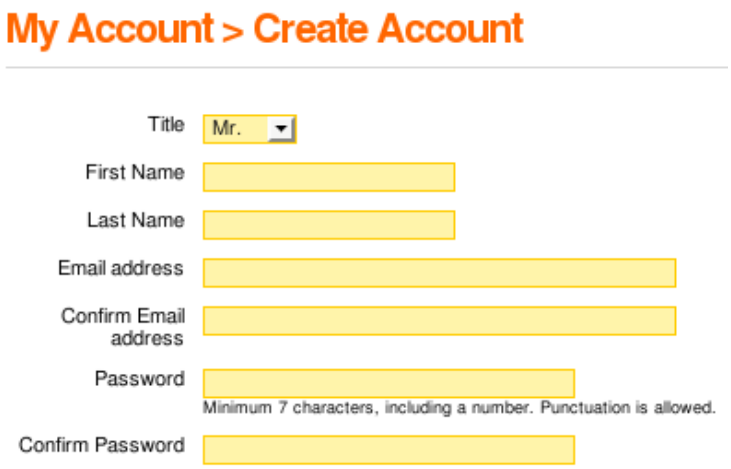
CORSAIRE

PCI DSS 1.2 weaknesses (pt 3)

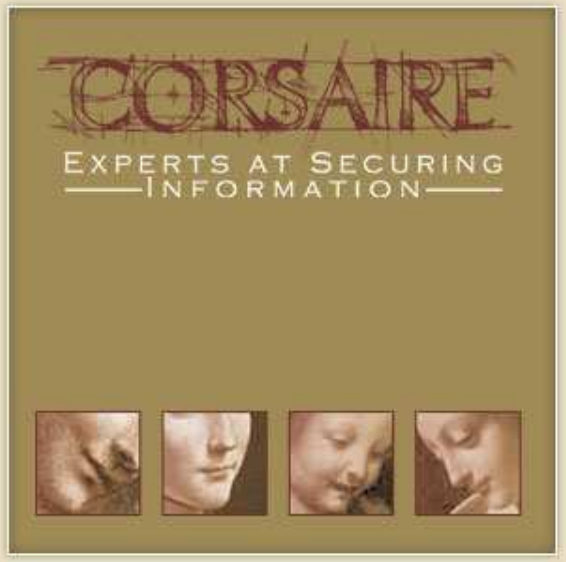
- PCI SCC attempting to compile full list of merchants
- CC data allowed to travel unencrypted within internal networks!
  - Large batch files sometimes not encrypted when sent between the merchants and processors
  - Only traffic sent over “public” networks should be encrypted (requirement 4.1)

PCI DSS 1.2 weaknesses (pt 4)

- Language can be vague! i.e.
  - Requirement 10.2.7: "creation and deletion of system-level objects“
- No details on whether authenticated testing (after login) is required for web application pentests
  - On a merchant site, any attacker can login by design, by simply registering a user account
  - It would be absurd to not cover this attack vector during a pentest



Screenshot shows account signup screen of anonymous merchant



Common techniques used to compromise CC data

Where the fun is happening

Techniques used to compromise CC data

- Wi-Fi hacks. i.e. WEP cracking, WPA Personal Edition dict attacks
  - POS terminals directly communicating with back-end data centres
  - Lack of segmentation
- SQLi
  - Classic error-based SQLi remains the most popular type to compromise CC data
- Lack of PAN masking + user traversal
- Unauthorised CNP transactions without CC data

Techniques used to compromise CC data (pt 2)

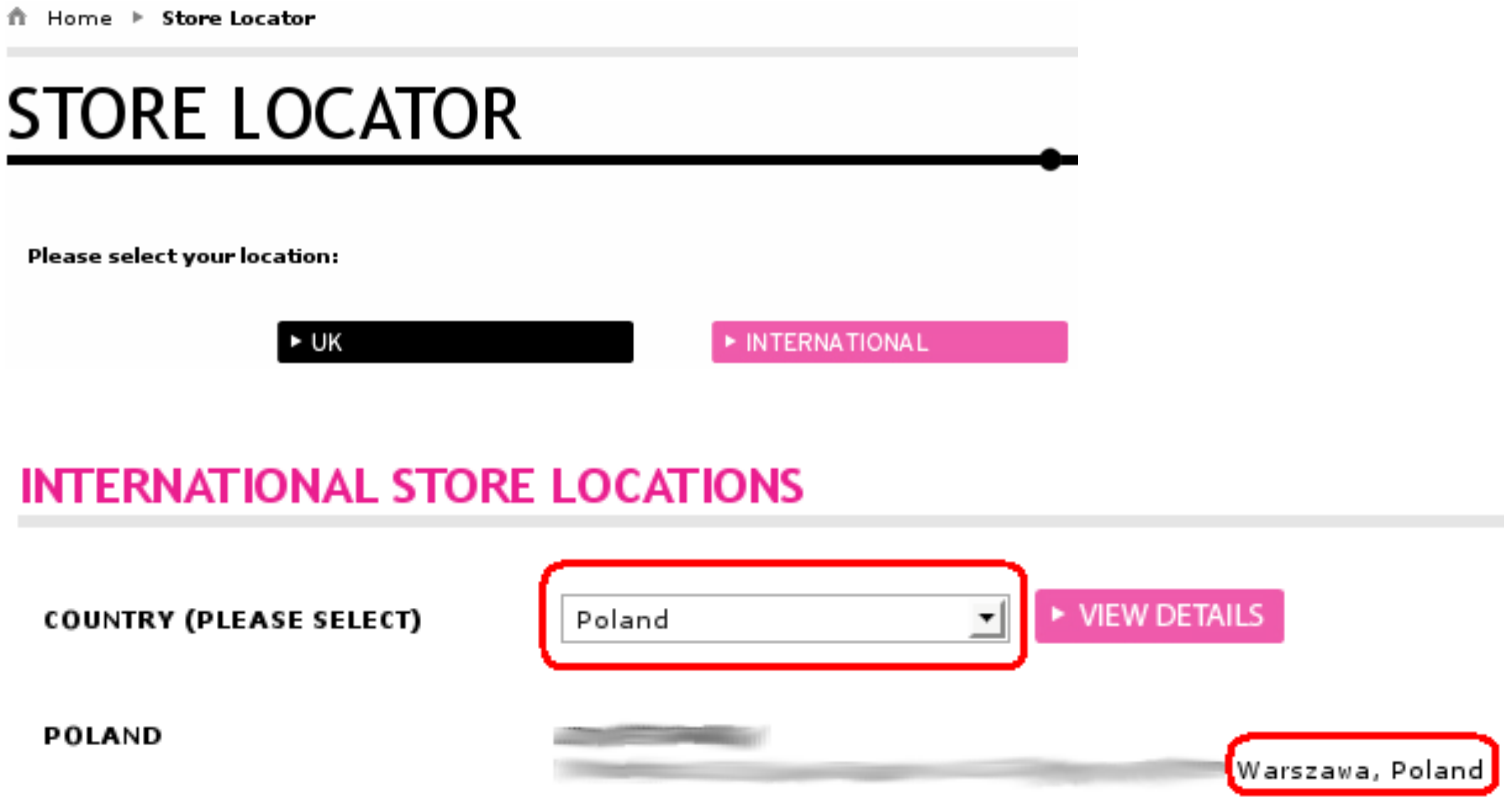
- Skimming
- Phishing
- Botnets-based malware. i.e.: Torpig
  - http://snipurl.com/hz4k7

Techniques used to compromise CC data (pt 3)

- We'll focus on attacks relevant to **pentesters**

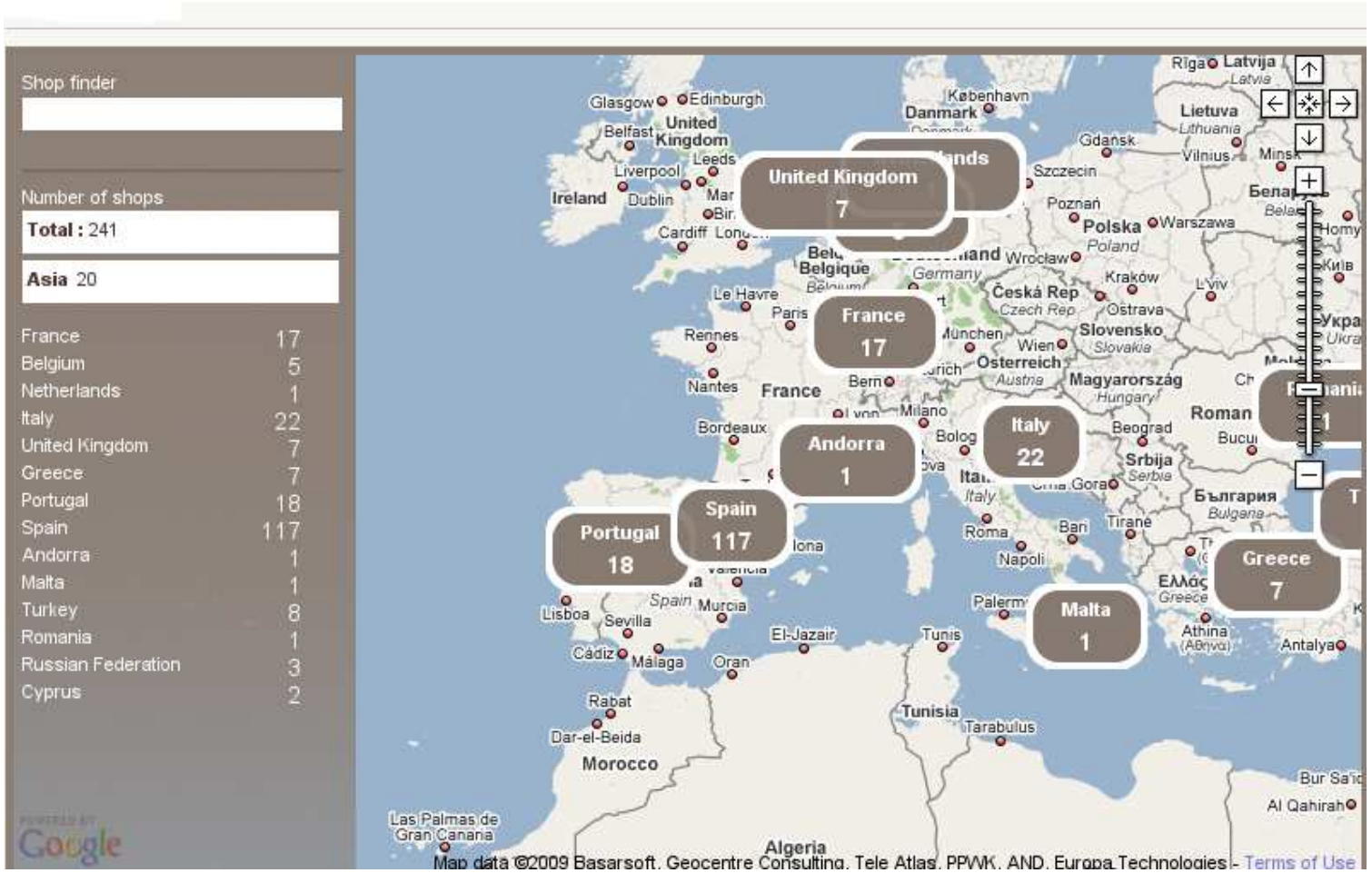
CC theft over Wi-Fi: the easy way

- Find stores: store locator / shop finder are your friends



Screenshot shows “store locator” screen of anonymous merchant

CC theft over Wi-Fi: the easy way (pt 2)



Screenshot shows “shop finder” screen of anonymous merchant

CC theft over Wi-Fi: the easy way (pt 3)

- Low-hanging fruit discovery: **open** and **WEP**-enabled APs
  - $ sudo airodump-ng -t **OPN** -t **WEP** -w test eth1

```
CH  5 ][ BAT: 1 hour 17 mins ][ Elapsed: 11 mins ][ 2009-05-11 18:36

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:14:1C:[redacted]  219     1170       51    0   6  54. OPN              tmobile
00:1A:30:[redacted]  187       29        1    0  11  54. OPN              BTOpenzone
00:11:50:[redacted]  190      111       14    0  11  54  WEP  WEP         BEcauseLan
00:17:3F:[redacted]  188       59        0    0  11  54. WEP  WEP         Belkin54g
00:17:3F:[redacted]  186       12        0    0   8  54. WEP  WEP         EK_SALES01
00:19:E4:[redacted]  187        5        0    0  11  54. WEP  WEP         Daily-Exchange
00:14:7F:[redacted]  186       49        0    0  11  48  WEP  WEP         SpeedTouch[redacted]
00:14:7F:[redacted]  183       31        0    0   7  48  WEP  WEP    SKA  BTHomeHub-[redacted]
00:16:C8:[redacted]  183       47       71    0   6  11. OPN              BTOpenzone
00:1B:2F:[redacted]  183        5        0    0  11  54  WEP  WEP         BEcausePublicWAN
00:17:3F:[redacted]  181       32        0    0   6  54. WEP  WEP         EK_SALES01
00:1F:9F:[redacted]  180      173        2    0   6  48  WEP  WEP         O2wireless[redacted]
00:0A:B8:[redacted]  181       36       11    0   6  11. WEP  WEP40       <length: 11>
00:0A:B8:[redacted]  182       39        0    0  13  11. WEP  WEP         <length: 11>
00:15:70:[redacted]  179       23        0    0   6  54. OPN              Gloucester WiFi
00:0D:65:[redacted]  179      147       23    0   1  11. OPN              tmobile
00:02:2D:[redacted]  178       20        3    0   1  11  OPN              VDAPL
00:15:70:[redacted]  178        3        0    0   6  54. OPN              Gloucester WiFi
00:15:70:[redacted]  178        2        0    0  11  54. OPN              Gloucester WiFi
00:1B:11:[redacted]  178        5       13    0   6  54. OPN              DLINK WIRELESS
```

CORSAIRE

Screenshot shows output of aforementioned “airodump-ng” command

CC theft over Wi-Fi: the easy way (pt 4)

- **Crack key** (if encryption is enabled at all)
  - aireplay-ng is your friend
- Save pcap file unencrypted
  - $ airdecap-ng -w 11A3E229084349BC25D97E2939 goodies.cap

CC theft over Wi-Fi: the easy way (pt 5)

- **Parsing** the juicy **CC data** from .cap files. ie: PANs
  1. Grab printable **strings** from .cap file
  2. Parse **numbers**
  3. Does the number follow **Luhn**'s algorithm?
  4. Is **length** of number correct? i.e.: 14-19 digits number
  5. We could also lookup the Issuer Identification Number (**IIN**) from up-to-date database in order to reduce false positives
     - http://snipurl.com/hz7jc
     - http://snipurl.com/i0jxo

CORSAIRE

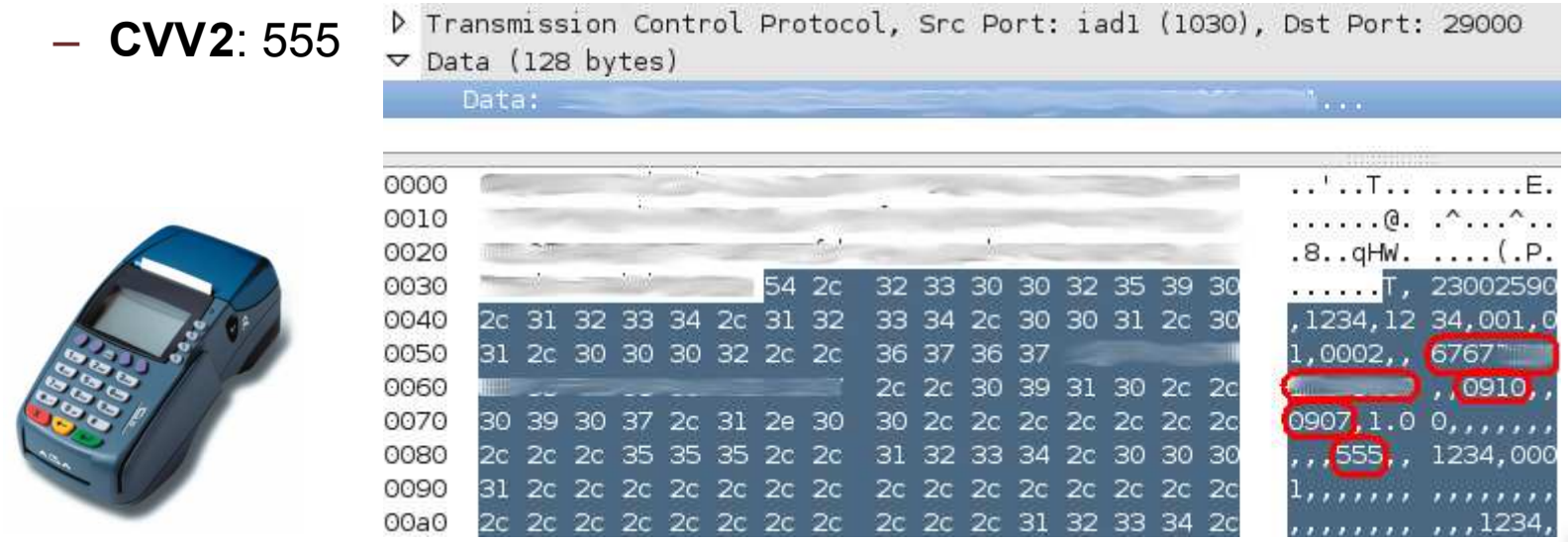
CC theft over Wi-Fi: the easy way (pt 6)

- $ ./**getPANs** ~/CONFidence_2009/caps/**goodies.cap** | head

  5522542365339919
  5522542365339927
  5522542365339935
  5522542365339943
  5522542365339950
  5522542365339968
  5522542365339976
  5522542365339984
  5522542365339992

CC theft over Wi-Fi: the easy way (pt 7)

- On the wire: Card Not Present (CNP) transaction
  - POS terminal ID (TID): 23002590
  - Terminal login and password: 1234/1234
  - **PAN**: 6767 XXXX XXXX XXXX
  - **Expiry** and **Issuing** date: 0910 0907
  - Transaction amount: 1.00
  - **CVV2**: 555



.pcap file kindly provided by researcher Bruno Kovacs

CC theft over Wi-Fi: the easy way (pt 8)

- Probe **back-end DB** servers directly if sniffing doesn't take anywhere
  - i.e.: common default credentials in Oracle server such as 'SYSTEM' account, MSSQL 'sa' account, etc

SQL injection

- Despite cutting-edge blind SQLi attacks in the vulnerability research realm, most CC compromises due to SQLi are based on vanilla **error-based SQL injection** attacks

Lack of PAN masking + user traversal

- Two types of vulnerabilities required for a successful attack
  - Unmasked PAN + expiry date returned
  - User traversal vulnerability

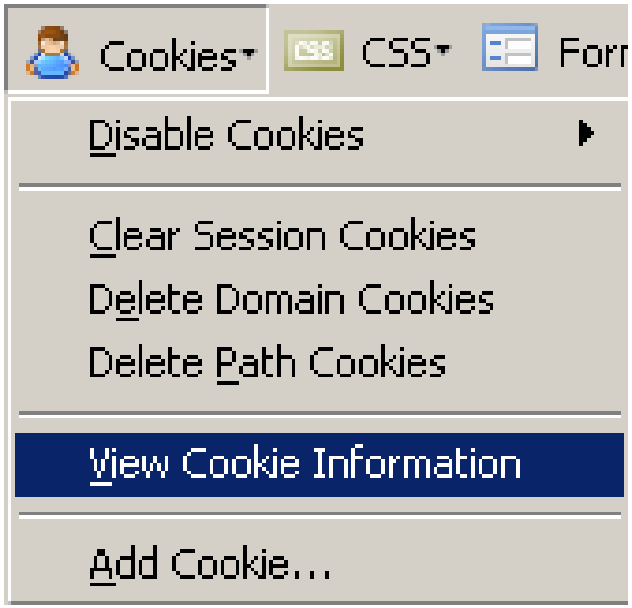
Lack of PAN masking + user traversal (pt 2)

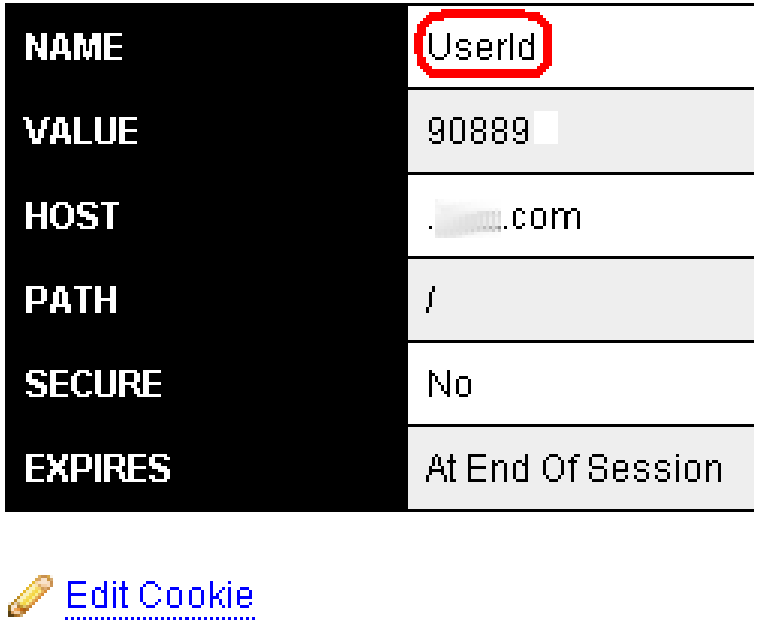
- All digits of PAN fully returned when accessing “update payment details” page
- Yes, we’re talking about real crappy shopping cart/basket software
- Spot the difference!

Screenshots show original and modified version of anonymous merchant’s “update payment details” screen

Lack of PAN masking + user traversal (pt 3)

- User traversal. i.e. via URL parameter manipulation or cookie poisoning
- https://www.shoppingsite.foo/view_payment_details.jsp?**uid**=90889





Screenshots show Firefox Web Developer extension

Unauthorised online transactions without CC data

- Account compromised
- **No access** to CC **details**
- Attacker still able to **buy goods** on target site and deliver to his address
  - Victim uses “remember my payment details” feature

Q&A

- No, I don't expect you to have listened to everything I've talked about!

Picture from http://icanhascheezburger.com/

Thank you / Dziękuję bardzo

- To the audience for attending
- To the CONFidence crew for inviting me
- To Corsaire for sponsoring this presentation
- To everyone who helped me preparing for my presentation, including but not limited to, pavlovs_dog, Bruno Kovacs, Jan Fry, Amir Azam, and Monsy Carlo