BREAKING THE PAYMENT POINTS OF INTERACTION (POI)

Nir Valtman @ValtmaNir & Patrick Watson @PatrickTheDev
THE CHALLENGE

Introduce 2 chatterboxes in 1 slide!
<?xml version="1.0" encoding="WTF-8"?>
<speakers>
  <identity username="Nir Valtman" twitter="@ValtmaNir">
    <org title="Head">NCR Application Security</org>
    <motto>If security is expensive, try to ignore it!</motto>
    <presented>Black Hat, DEF CON, OWASP etc.</presented>
    <opensource>SAPIA, Cloudefigo, Secure TDD, AntiDef</opensource>
  </identity>
  <identity username="Patrick Watson" twitter="@PatrickTheDev">
    <org title="Architect">NCR Application Security</org>
    <motto>If I shouldn't tell you how my system works, it isn't secure</motto>
    <presented firstTimeSpeaker="F***K YEAAAH" />
    <opensource>Who cares? I develop better than Nir!</opensource>
  </identity>
</speakers>
THE RESEARCH

Nir: "Can’t we just change this damn flow in the POI?"
Patrick: “LOL, see what happens! We’re going to Vegas this year!”
The result – high fived our product to research anarchy!

I did not slap you, I high fived your face!
Various Business Flows

What would you say if I told you that the Retail industry is the most secure?
LOL, good one!
INTRO TO PAYMENTS & POI

Payments POI, meet Nir & Patrick. We hack stuff for fun!
Segregated store architecture
All-in-one store architecture
Fuel station architecture
Typical Payment Flow
WEAK AUTHENTICATION TO POI

Knock-knock. Who’s there? It’s YOU!
How fuel pumps authenticate to the L2 adaptor?
How shim software works?

Point of Sale → Payment App → POI

Shim Software (TCP/IP, Serial, Binary)
A shim software demo using a Pi
Encryption strength limitations

Sometimes NOT even SSLv3!

Business justification: “we have old hardware (POS or POI)”
Hackers’ justification: “it wasn’t encrypted, I had to steal it”
Showing off with a demo
Unclear API documentation
FORGET ABOUT SWIPIING!
WHAT ABOUT EMV?

It’s obviously secure as hell, isn’t it?
EMV DOES

Prevent duplication of card

Chip & PIN prevents using a stolen card
EMV DOES NOT

- Prevent using card number elsewhere
- Prevent using modified Track 2 in offline mode
- Prevent unmodified Track 2 w/ EMV after tricking into technical fallback to swipe
Passive MITM Track 2 Compromise
I’m all ears! Where’s the demo?
The Basics of EMV

On Sale Now: Track Data!
Which info you need to make a purchase online?

- Personal Account Number (aka PAN)
- Expiration Date
- Cardholder’s Name
- CVV2

I love ordering things online because when they arrive, It’s like a present from me to me...
BYPASSING THE EMV FLOWS

It’s obviously secure as hell, isn’t it?
Active MITM
Track 2 &
CVV2
Compromise
Active MITM
Track 2 & PIN Compromise
DEMO: Let’s steal few PINs
WHAT IF CVV2/PAN ARE RESTRICTED BY A WHITE LIST?

We leverage other white listed functionality!
Bypassing the prompt white list

Please Reenter

Enter Phone
Enter User ID
Enter Card Number
Enter SSN
Enter CVV
Form/Screen Injection

Remember that there is NO authentication to POI?

Photo

Enter PIN

Signed

May be required by several vendors though

Masked 4-digit control
It’s an illusion
ANY OTHER ATTACK VECTORS?

Let me think about it for a day or two … YES!
Skimmers
Exploit POI’s Operating System
MITIGATIONS

Enough complaining about problems!
Point-to-Point Encryption (P2PE)

Use ONLY hardware-based message encryption

Preferably SRED enabled
Point-to-Point Encryption (P2PE)

Leverage strong crypto algorithms

AES/3DES DUKPT
RSA
Point-to-Point Encryption (P2PE)

Prevent remote firmware downgrades to software-based encryption

Firmware must be signed anyway
Point-to-Point Encryption (P2PE)

Allow ONLY signed white list updates by vendor

Credit card bin ranges
Trusted Certificate Authorities
Point-to-Point Encryption (P2PE)

Encrypt offline transaction data on payment applications
What if the POI or Payment Application doesn’t support P2PE?

WE'RE SCREWED?
What can merchants/vendors do?

TLS it!

Sign all requests to POI
WHAT CAN A CONSUMER DO?

Except paying with cash...
Never re-enter PIN

Be cautious of unusual prompts

App-based payment systems MAY be preferred

No PAN transmission - tokenization
Unique Track2 per transaction
Summary

- Relatively easy to exploit common POI deployments.
  - The lack of authentication poses the POI to major risks.
  - EMV can be bypassed by easily tricking the POI.

- Points of interaction can be secure.
  - P2PE solution
  - Added authentication mechanisms