
TOM CRUISE
MISSION: MPOSSIBLE

Mission MPOSsible

Mobile Card Payment Security

Black Hat US - 7th August 2014

Agenda

MPOS Introduction

Attack Surface

Demos

Conclusion / Further Work

Introduction

Nils

- Security researcher at MWR
- Research
  - Mobile (Android)
  - Payment system security
    - Terminals
    - ATM

Jon

- Heading up MWR's research in the UK
- Vuln dev / reverse engineering
- Browser security / sandboxing technologies

MPOS Introduction

- POS: Point-of-Sale
- MPOS: Mobile Point of Sale
    - Because, mobile …
- Usually aimed at small businesses
    - Because it’s cheap
    - Sometimes used by larger companies


スキャン

MPOS - Small Business Example (Contrived)

- Selling “creative execution software”
- Sick of carrying bags of cash
- MPOS to the rescue!
- Example:
  - No recurring fees
  - 1.5% per transaction
  - XP 0day: $50k ~ 750 USD

US Devices

US Devices

- “Mobile skimming devices”
- No Chip&Pin
- Swipe your CC into any mobile device
- This model has obvious flaws

US Devices - Next Gen

- Announced by Square last week:
- EMV
  - However still signature based.

MPOS in Developed Countries

- Meanwhile, in the 1st world…
  - Widespread Chip&Pin adoption
- Works well with standalone terminal
  - Use case
- We found many different providers, however

75%

Use the same platform

Popular Brands

Popular Brands

Popular Brands

Public

EXTERNAL

Popular Brands

Popular Brands

Popular Brands

Miura Shuttle

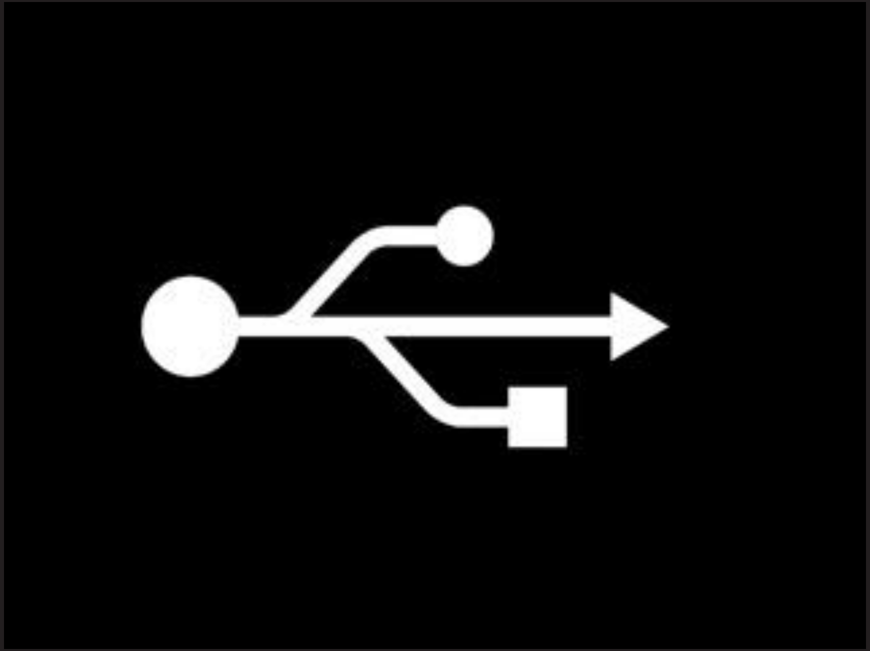
- Different looks, same device
- Small embedded Linux device
  - ARMv5 CPU, generic hardware
- Multiple interfaces

Attack Surface - EMV

Attack Surface - Magnetic Swipe

Attack Surface - Bluetooth

Attack Surface - Micro USB



USB Attack Surface

- Only meant for charging
  - Oops…

```
[ 2860.309364] usb 3-2: Product: File-backed Storage Gadget
[ 2860.309368] usb 3-2: Manufacturer: Linux 2.6.31-506-g30df573M000-OS-V5-10 with fsl-usb2-udc
[ 2860.309372] usb 3-2: SerialNumber: 3230204E6F76
[ 2860.326260] usb-storage 3-2:1.0: USB Mass Storage device detected
..
[ 2861.335842] sd 6:0:0:0: [sdb] Attached SCSI removable disk
[ 2871.864367] sd 6:0:0:0: [sdb] 65536 512-byte logical blocks: (33.5 MB/32.0 MiB)
[ 2871.872502] sd 6:0:0:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
```

USB Attack Surface

```
jon@elixir:~$ ls /media/jon/MIURA/
jon@elixir:~$
```

☹

USB Attack Surface

- dd & binwalk to the rescue!

```
jon@elixir:~/Research/mPOS$ tar -tzvf Install.tar.gz
...
-rw-rw-r--   998      2013-03-28 10:43 Install/EMV-Config/emv.cfg
-rwxrwxr-x  1501664   2013-03-28 10:43 Install/libcrypto.so.1.0.0
-rwxrwxr-x  77512     2013-03-28 10:43 Install/libhlbluetooth.so
-rwxrwxr-x  332828    2013-03-28 10:43 Install/libssl.so.1.0.0
-rwxrwxr-x  545168    2013-03-28 10:43 Install/Retail-API
drwxrwxr-x 0          2013-03-28 10:43 Install/SecureConfig/
-rw-rw-r--  567       2013-03-28 10:43 Install/SecureConfig/emv-pinbypass.cfg
-rwxrwxr-x 2943       2013-03-28 10:43 Install/start
...
```

USB Attack Surface

- Able to analyse device software
- Software images signed
  - No easy win there
- Or is there?

USB Demo

Tl;dr – shells

USB Demo 2

Tl;dr – r00t shells

Bluetooth Attack Surface

- Some security features for free
  - Let’s see what a paired device can do…
- File upload!
  - Possibly to enable software updates?

Bluetooth Demo

EMV

- Standard for payment card interaction
- Interoperability between cards and terminals
- Implementation? Security?
  - Not so much...

EMV Testing Methodology

- Programmable smart card
- Initiate part of EMV transaction
- Return malformed values at key points
  - Watch for terminal errors

EMV Attack Surface

- Standard tags
  - Good list at www.emvlab.org
- TLV
  - Tag, Length, Value
- Parsed by the EMV Kernel
  - Usually C/C++
  - Susceptible to memory corruption

EMV Attack Surface

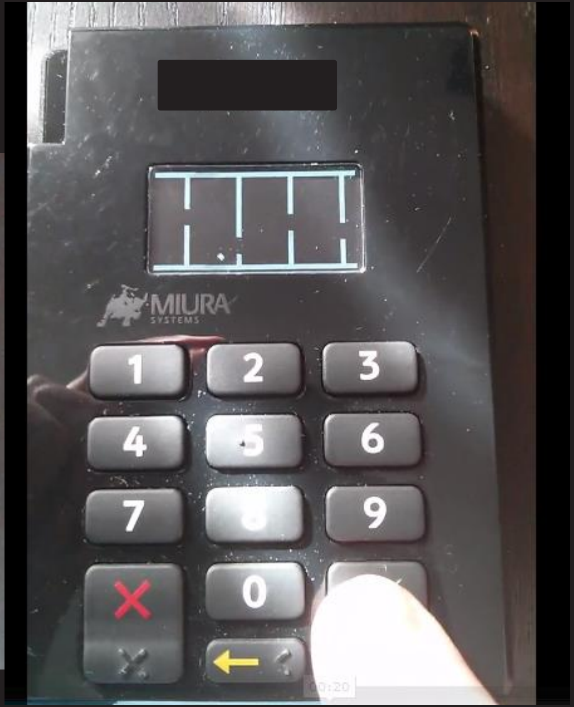
- Found stack-based buffer overflow in EMV parsing
  - No NX / ASLR
- Actually very similar to bugs we presented in 2012
  - On traditional POS terminals

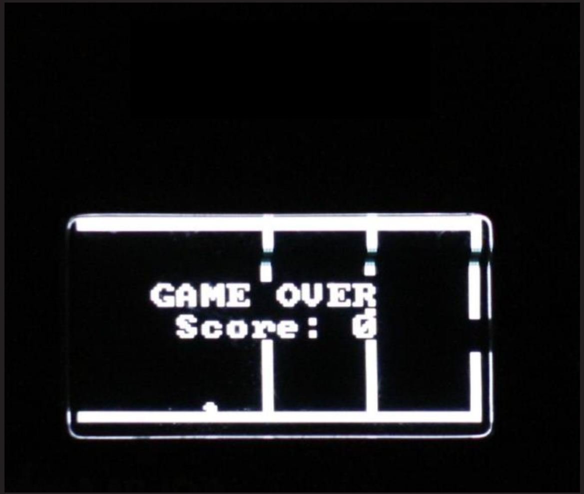
EMV Demo

- You may remember PinPadRacer
- Nowadays exploits have to be entertaining…
    - Shells? Yawn. Where’s my flappy bird clone?!

EMV Demo - Chippy Pin

EMV Demo - Chippy Pin





The Exploit

- Stack-based buffer overflow
- Only static address in ld-2.5.so (jump to code on stack)
  - Same across all tested devices, always loaded @0x40000000
- 180 byte shellcode:
  - Retrieves a .tar.gz archive from the smartcard (~4k)
  - Writes archive to /tmp
  - Exploits setuid vuln to "mount –o remount,exec /tmp"
  - Extracts archive and runs 2nd stage from archive

What would an attacker do?

- Probably not interested in games…
  - Cash monies!
- Pin pad in “secure” state
  - 1 ioctl away from “insecure”
- Full control over screen

What would an attacker do?

- Display “try again” message
- Switch pin pad into insecure mode
- Capture the pin when entered

- Bonus points!
  - Display fallback to swipe message
  - Read /dev/mag-swipe
  - Pass go, collect track 2 data

What would an attacker do?

- Accept with malicious card
- Yes Terminal
  - Accept stolen credit cards

Attacking the mobile device

- Fully compromised terminal
- “Trusted” connection to mobile device
- Terminal could compromise mobile device
  - Internet connection (C&C)
  - Control of Merchants View
- Requires vulnerability in BT protocol handling

Attacking the mobile device

- We looked at 6 Terminals
  - Standard Protocol: 4, Custom: 2
- Implementations:
  - Android:
    - 5 Java, 1 Native. All different.
    - 1 Potentially vulnerable (Hard to verify)
  - Java:
    - All different. Obj-C with varying degrees of plain C
    - Varying quality of implementations.

Vendor response

- Very cooperative
- Worked with MWR team on a full code review
- Hardend software to protect against similar issues
- New OS, Application and EMV library released to third party vendors in April 2014

Conclusion

- Separate terminals
  - Promising approach
- Implementations lacking
- Lessons learnt from desktop/server computing
  - Need to be applied across POS industry
- Important to get it right early
- EMV and other standard not adapted to address security issues in a timely manner

Questions?