Forging the USB armory

Andrea Barisani
<andrea@inversepath.com>
2007: Unusual Car Navigation Tricks
    Injecting RDS-TMC Traffic Information Signals

2009: Sniff Keystrokes With Lasers/Voltmeters
    Side Channel Attacks Using Optical Sampling Of
    Mechanical Energy And Power Line Leakage

2011: Chip & PIN is definitely broken
    Credit card skimming and PIN harvesting in an EMV world

2013: Fully arbitrary 802.3 packet injection
    Maximizing the Ethernet attack surface
Designed for personal security applications

- mass storage device with advanced features such as automatic encryption, virus scanning, host authentication and data self-destruct
- OpenSSH client and agent for untrusted hosts (kiosk)
- router for end-to-end VPN tunneling, Tor
- password manager with integrated web server
- electronic wallet (e.g. pocket Bitcoin wallet)
- authentication token
- portable penetration testing platform
- low level USB security testing
enhanced mass storage
enhanced mass storage

Host

webapp

clamav

gnupg

Internet

copy secret.txt to folder Bob/

please scan

passed

tcp/ip over cdc ethernet

usb armory

Google Drive ajax for secret.txt.jpg

share secret.txt.jpg with Bob

secret.txt.jpg

Host

webapp

clamav

gnupg

Internet
enhanced mass storage

Chuck

show me the secret files
of course

nothing to see here ^_^

Alice

mass storage gadget

open secretfoldergamma

failsafe word detected!

wipe command

data self-destruct

USB armory

mass storage gadget

microSD

Copyright 2014 Inverse Path S.r.l.
Forging the USB armory
SSH proxy

SSH

Alice → Kiosk → Server
Password
Kiosk has password/key!

SSH proxy

Alice → Kiosk → USB armory → Server
Input/Output
TCP/IP over CDC Ethernet
SSH/telnet/whatever

Kiosk never sees the key

Copyright 2014 Inverse Path S.r.l.
Forging the USB armory

**Password Manager**

Host → USB armory

TCP/IP over CDC Ethernet

password for my banking site?

what's your PIN?

1234

seriously?

yep

ok, password is ***********

cut & paste *********** to banking site

Host → webapp → Bank

*trivial example, better options planned*
USB device authenticates host
Design goals

Compact USB powered device
Fast CPU and generous RAM
Secure boot
Standard connectivity over USB
Familiar developing/execution environment
Open design
Selecting the System on Chip (SoC)

Freescale i.MX53

- ARM® Cortex™-A8 800-1200 Mhz
- almost all datasheets/manuals are public (no NDA required)
- Freescale datasheets are “ok” (far better than other vendors)
- ARM® TrustZone®, secure boot + storage + RAM
- detailed power consumption guide available
- excellent native support (Android, Debian, Ubuntu, FreeBSD)
- good stock and production support guarantee
ARM® TrustZone®

http://genode.org/documentation/articles/trustzone
ARM® TrustZone®

http://genode.org/documentation/articles/trustzone
Development time-line

2014/01: first concept idea (based on Atmel SoCs)
2014/03: schematics development begins (Freescale chosen)
2014/04: PCB layout for breakout/prototyping board
2014/08: alpha board order
2014/09: USB armory alpha board delivery & evaluation
2014/10: project announcement
2014/10: order for 7 optimized beta revisions
2014/11: beta boards delivery & evaluation
2014/11: design finalization, Mk I production candidate order
2014/12: Mk I delivery
2015/01: first batch production
USB armory - Open source flash-drive-sized computer

- Freescale i.MX53 ARM® Cortex™-A8 800Mhz, 512MB DDR3 RAM
- USB host powered (<500 mA) device with compact form factor (65 x 19 x 6 mm)
- ARM® TrustZone®, secure boot + storage + RAM
- microSD card slot
- 5-pin breakout header with GPIOs and UART
- customizable LED, including secure mode detection
- excellent native support (Android, Debian, Ubuntu, FreeBSD)
- USB device emulation (CDC Ethernet, mass storage, HID, etc.)
- Open Hardware & Software
device mode
host mode
(stand-alone)
custom host adapter
*we actually measure consumption with better equipment ^_^
Forging the USB armory

Copyright 2014 Inverse Path S.r.l.

α
8L-NOUSBH, 8L, 8L-DDR-LDO, 8L-DDR-NCP
6L, 6L-DDR-LDO, 6L-DDR-NCP

βs

Mk I

Forging the USB armory
lessons learned #1
tiny inductors are fragile
Lessons learned #2 (the five-second rule)
gold plating traces cause under-voltage on hot swap
Thank you!

Q & A

Andrea Barisani
<andrea@inversepath.com>