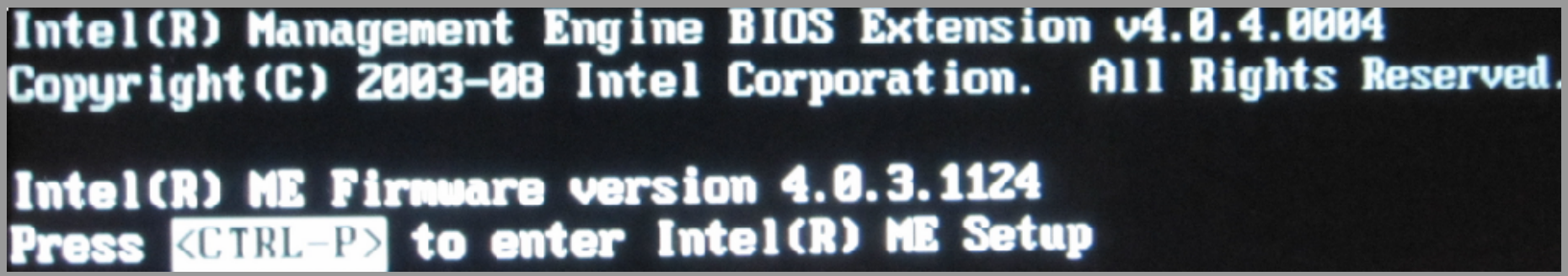
Intel AMT/ME
Meet Intel's hardware backdoor

"csk" casek@uberwall.org

LaCon

September 21st-22nd, 2012

UH? booting a brand new laptop



One day I pressed Ctrl+p

WTF?

disklamer

- Part of vpro blah, sorry I am not working for Intel
- It's a work in progress, simply driven by curiosity
- I stole most of this stuff

WTF - Intel Active Management Technology

- Intel's native remote support feature, part of Management Engine
- Introduced by Intel in 2005 as key vpro feature
- Implemented as another chipset on vpro enabled mother boards
- Pretty much independent of the installed OS
- Able to work even when the machine's OS is in S3 state
- Ownz your NIC

Features at a glance

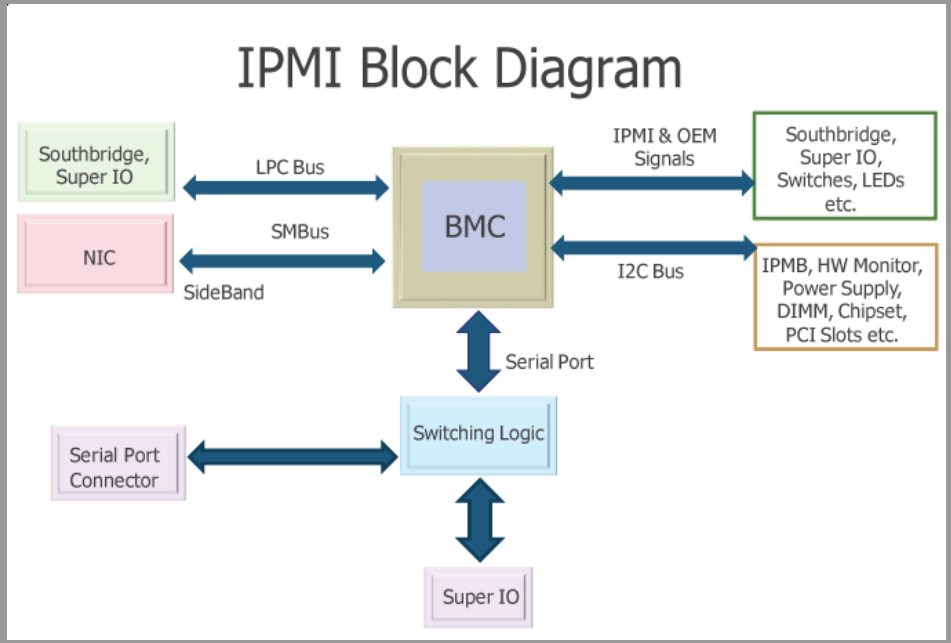
Features

- Out of band remote access to remotely diagnose, control and repair
- Three configuration mode, manual, one touch and zero touch
- Two provision modes, each enabling different level of security
- Support IDE-Redirection and Serial-Over-Lan capabilities

Use cases

- Software/Hardware discovery and invertory
- Remote diagnosis and repair, helpdesk work
- Hardware based isolation and recovery
- Agent Presence Checking (read AV)
- Network Access Controls

Anything new?



Not really, see IPMI for instance

- Intelligent Platform Management Interface - IPMI
- v1.0 introduced in 1998 on the lead of Intel (+200 vendors)
- OS independent, pre-boot OOB (read no SSH) management platform
- Based on a Baseboard Management Controler, BMC

Anything new?

Main diffs

- Not a server technology, more desktop oriented
- Not supported byt any other vendor than Intel, marketing takeover
- Real full featured remote management plateform, with L4 stack
- The major third party software management vendors including Altiris, Cisco, CA, LANDesk and Microsoft have all integrated AMT support

Any other similar stuff so far?

- HP iLO, Integrated Lights-Out. HP's own IPMI implementation
- Dell Remote Access Controller, DRAC. Also based on IPMI
- IBM Remote Supervisor Adapter, RSA. Optional interface card
- Sun System Service Processor, SSP
- And more.. DMTF(will speak about it latter)

Nothing new, even for IT Sec industry

BH 2009 - prez Alexander Tereshkin and Rafal Wojtczuk

"We show how malware can bypass the AMT's dedicated memory protection, and consequently compromise the AMT code executing on the chipset. Additionally we discuss tricks we used for reverse engineering the AMT code, that were needed in order to create meaningful rootkits that can have access to the host memory"

2009 - Vassilios Ververis's thesis - SECT research at Berlin's TU

"At the Black Hat conference in USA, Alexander Tereshkin and Rafal Wojtczuk presented a ring -3 rootkit[10]. They describe ring -3 rootkit as a backdoor that abuses the Intel AMT technology and could potentially bypass the dedicated memory protection of AMT and compromise the AMT code executed on the chipset. They introduced an attack vector that assumes to be performed locally in order to be successful; whereas in this thesis our attack vectors can be accomplished remotely."

The academic side as well is looking at it

University of Cambridge 2011-2012 research suggestions
http://www.cl.cam.ac.uk/ fms27/part2/2011-2012/

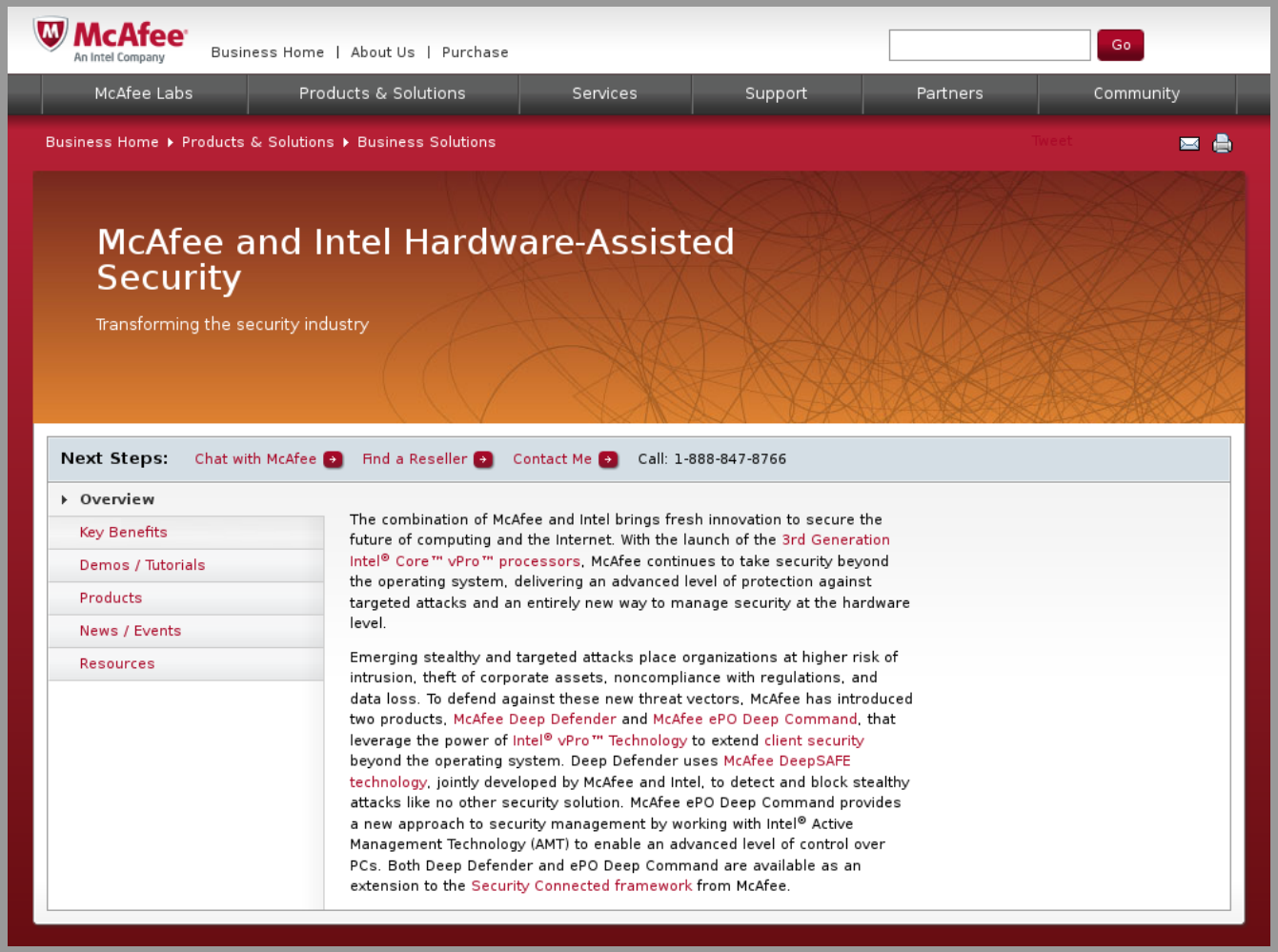
"But what if a bad guy could impersonate the security administrator and 0wn your computer at a distance?"

"have recently started looking at the security of this control connection with some US colleagues and we already have a few ideas about where to look. You will be involved in probing for vulnerabilities and possible attacks. The work may involve fuzzying and reverse engineering."

"A high risk / high reward project for a low level hacker. High risk because you might not find any vulnerability worth exploiting; high reward because, if you do a great job, you might end up as coauthor on our paper."

Past future.. was about time (and Intel to aquire McAfee)

[http://www.mcafee.com/us/solutions/mcafee-intel-hardware-assisted-security/hardware-assisted-security.aspx]



Configuration modes

local

- Pretty much physical configuration
- Weak initial password "admin"

one touch

- Same as local but booting from a USB stick
- Still the weak initial password

zero touch

- Remote config, no hands
- BIOS contains at least 1+ trusted cert fp
- Need a Setup and Configuration Service, SCS
- Requires a special type of cert for remote config

ZeroCool.. Touch / Bare Metal remote provisioning

Limitations

- Available at boot, limited by a timer (1h.. to 255h)
- Requires DHCP
- Not limited to ethernet, WLAN works as well (with a few prior steps)

How does it work

- First DHCP, then AMT "HELLO" (2b header + fp)
- Configuration server lookup for and send config params

Certificates?

- 1+, usually 4 hashed root certificate, fp, from various vendors
- Stored in flash memory
- All what you need is a cert and an SCS
- The best is it works even when AMT is set disabled in BIOS

Provisioning models

Feature	**Basic** (no encryption)	**Standard** (no encryption)	**Advanced** (encryption)
Firmware setting	SMB Mode	Enterprise mode (no TLS)	Enterprise mode (TLS)
Provision model	Manual, One touch	Manual, One touch, Remote	Manual, One touch, Remote
Network infrastructure	DHCP or Static IP	DNS and DHCP	DNS and DHCP, CA, AD (opt.)
Client authentication	HTTP digest	HTTP digest	HTTP digest, Kerberos (opt.)
Management traffic encryption	n/a	n/a	TLS using certificates
Secure network authentication	n/a	802.1X, NAC, NAP (opt.)	802.1X, NAC, NAP (opt.)
Client configuration maintenance	One-to-one	One-to-many	One-to-many

Models

- Small Medium Business, SMB, no transport (should be default)
- Enterprise no-TLS, probably the most interesting from remote
- Enterprise TLS, still remotely interesting but a bit more locked up

The password story (as always)

Beside the initial password "admin"

- Must contain a number
- Must contain a non alphanumerical character
- Must contain a lower case Latin letter
- Must contain an upper case Latin letter

But...

- Password is shared accross every services
- IDE-R/SoL protocol transmits it in clear text
- HTTP services use MD5 digest auth but..
  - Intel only comformed to default rfc2617 (+10y old)
  - Offline bruteforce attack is possible (JtR's HDAA-MD5)

Connecting people

Then?

- AMT hardware is linked to the NIC
- If a WLAN NIC is built in, it uses it as well
- It intercepts DHCP traffic to get the IP @
- It works with IPv6 natively as well

Once again

- Everything is done on hardware level
- It works even if the OS is in S3 state

Client Initiated Remote Access, CIRA

- "Initiate remote connection"
- AMT Port Forwarding protocol, APF
- Similar to SSH, multiplexed tunneling

Scanning for AMT

Ports in use

```
amt-soap-http    16992/tcp    Intel AMT SOAP/HTTP
amt-soap-https   16993/tcp    Intel AMT SOAP/HTTPS
amt-redir-tcp    16994/tcp    Intel AMT Redirection/TCP
amt-redir-tls    16995/tcp    Intel AMT Redirection/TLS
```

And sometimes

"Default Port (5900) VNC Clients that do not include support for Intel AMT can use this port. This is a less secure option." (RFB 3.8 & 4.0)

Passively

You always can wait for AMT "HELLO" packets

Let's scan the thing

Small enterprise provision model

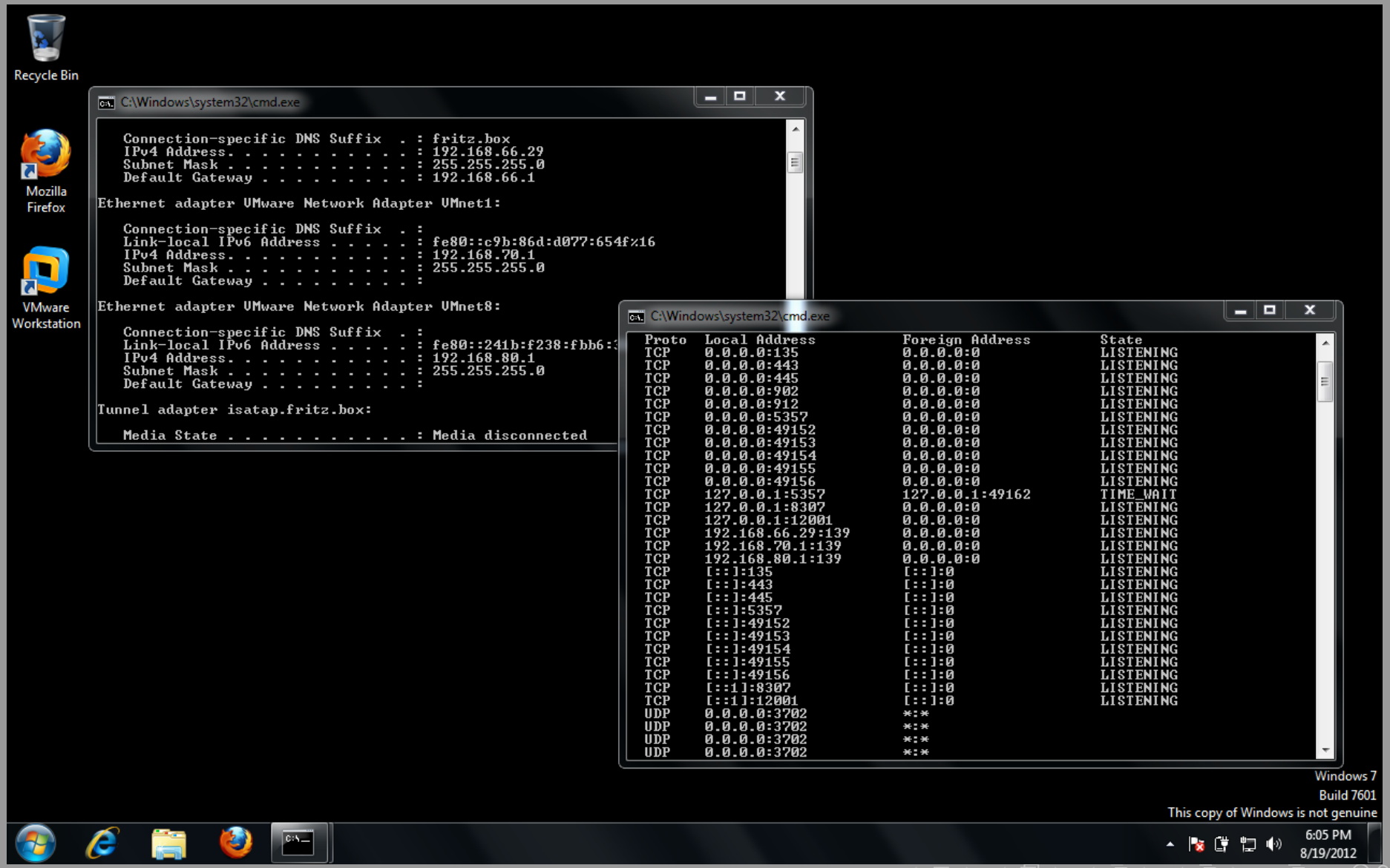
```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-08-19 13:54 EDT
Nmap scan report for USER-7.fritz.box (192.168.66.29)
Host is up (0.020s latency).
Not shown: 65525 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
623/tcp   open  oob-ws-http
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
5357/tcp  open  wsdapi
16992/tcp open  amt-soap-http
16994/tcp open  unknown
MAC Address: 00:1F:16:0C:46:1C (Wistron)
```

Let's scan the thing

Enterprise provision model

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-08-19 13:08 EDT
Nmap scan report for USER-7.fritz.box (192.168.66.29)
Host is up (0.014s latency).
Not shown: 65525 filtered ports
PORT      STATE  SERVICE
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
443/tcp   open   https
445/tcp   open   microsoft-ds
623/tcp   closed oob-ws-http
664/tcp   open   secure-aux-bus
902/tcp   open   iss-realsecure
912/tcp   open   apex-mesh
5357/tcp  open   wsdapi
16993/tcp open   amt-soap-https
MAC Address: 00:1F:16:0C:46:1C (Wistron)
```

From inside, as expected



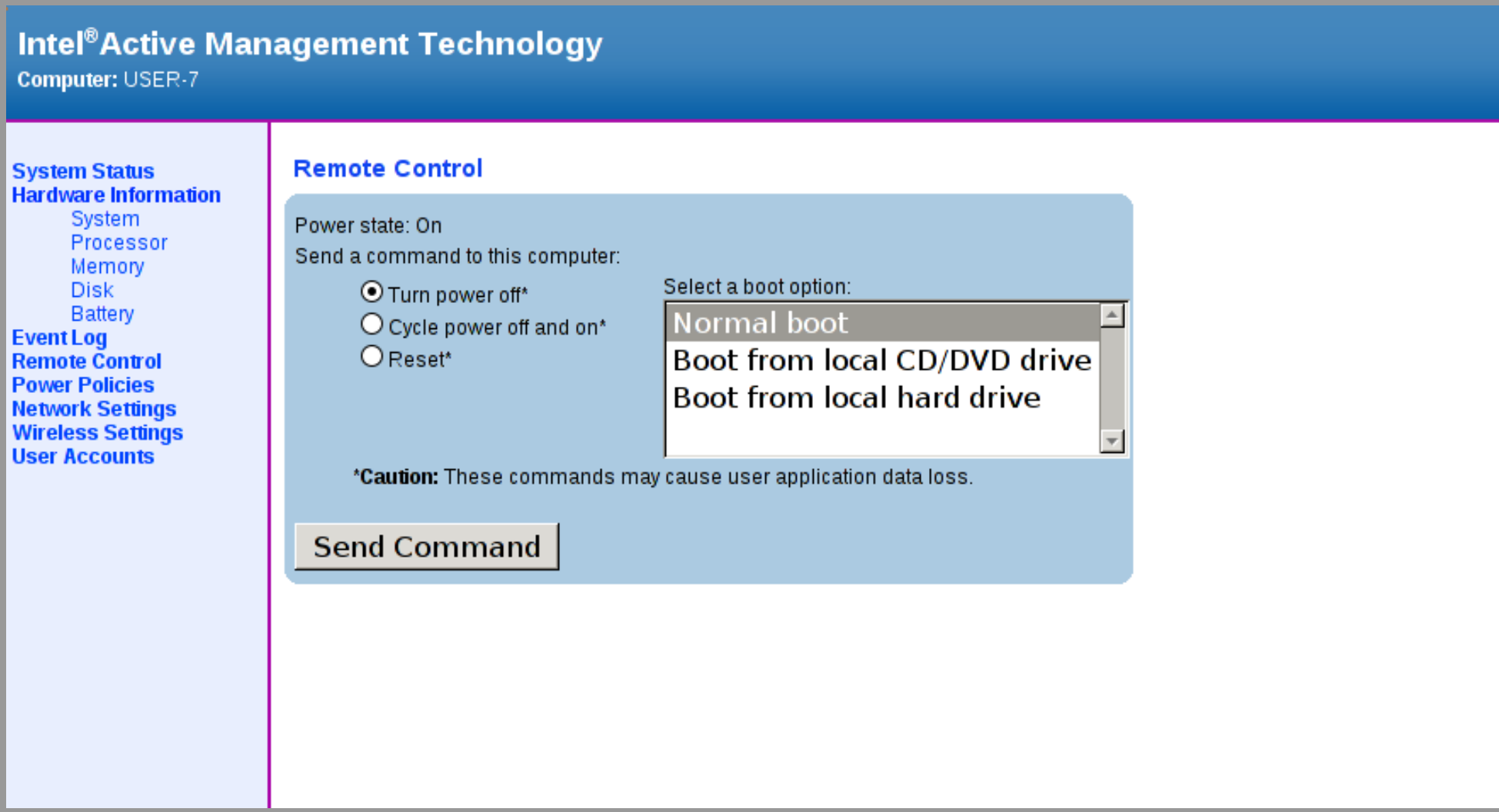
Manual monkeys

AMT Web UI

```
$ nc -v 192.168.66.29 16992
USER-7.fritz.box [192.168.66.29] 16992 (?) open
HEAD / HTTP/1.0

HTTP/1.1 302 Found
Location: http:///logon.htm
Content-Length: 0
Server: Intel(R) Active Management Technology 4.0.3
```

The ugly thing - SOAP opera



Manual monkeys

AMT Redirection service

```
$ amtterm 192.168.66.29
AMT password for host 192.168.66.29:
amtterm: NONE -> CONNECT (connection to host)
ipv4 192.168.66.29 [192.168.66.29] 16994 open
amtterm: CONNECT -> INIT (redirection initialization)
amtterm: INIT -> AUTH (session authentication)
amtterm: AUTH -> INIT_SOL (serial-over-lan initialization)
amtterm: INIT_SOL -> RUN_SOL (serial-over-lan active)
serial-over-lan redirection ok
connected now, use ^] to escape
```

A bit more on IDE-R & SoL

Shortly

- Multiplexed protocol over TCP 16994/16995
- Serial over LAN is the simplest mode
- IDE-R Pretty much allows to boot remotely a local media

Obvious use

- Remote access on local console
- Remote install of new OS
- Remote run of diagnostic software
- Remote forensic, booting on your favorite Linux distro

Scanning bonus - RMCP

RMCP... DMTF

DMTF, Distributed Management Task Force, is a not-for-profit association of industry members dedicated to promoting enterprise and systems management and interoperability.

RMCP as in Remote Management and Control Protocol

The Desktop and Mobile Architecture for System Hardware, DASH, implementation requirements (DSP 0232) specifies that a DASH-compliant platform should respond to a Remote Management and Control Protocol (RMCP) ping with an indication that the platform supports DASH.

The ping message format and response are defined in the Alert Standard Format (ASF) Specification. Starting with Release 4.0, Intel AMT responds to an RMCP ping.

RMCP

Why do we care about RMCP "ping"

- In Releases 4.x through 5.0, Intel AMT responds to an RMCP ping with bit 5 of byte 9 set to true
- In Release 5.1 and later, Intel AMT responds with bit 5 of byte 10 set to true
- Release 6.0 adds additional information such as firmware version, open ports and so on
- Release 7.0 enable the ping feature also for shared static address
- Release 8.0 disable the ping feature for Small Business
- Even better, we can discover platforms which haven't been yet configured (only works with dynamic address)

RMCP

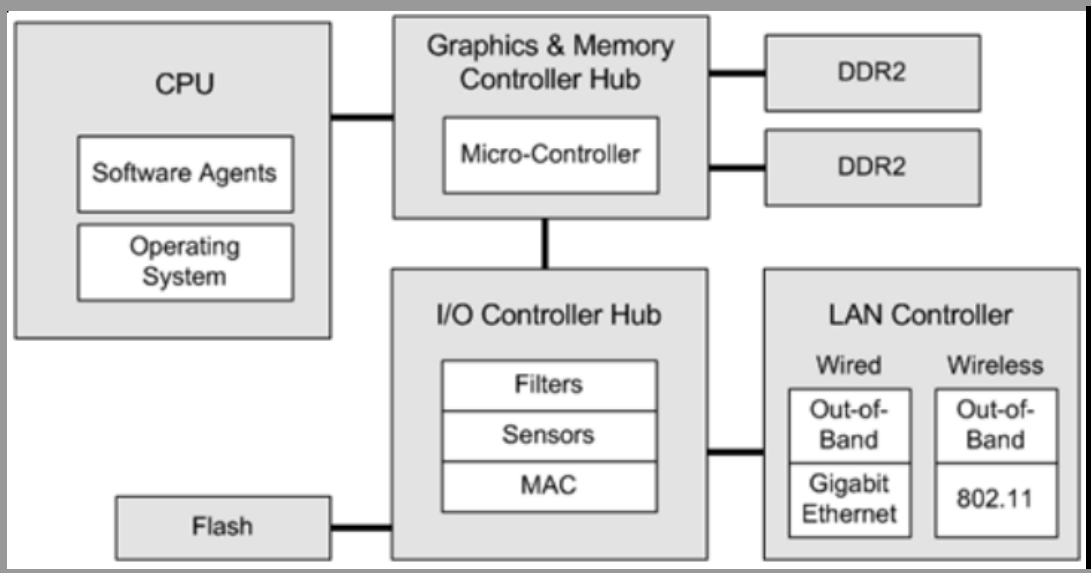
Network footprint, remember the slides before?

oob-ws	623/tcp	DMTF WS-Management
rcmp	623/udp	RMCP ASF
oob-ws	664/tcp	DMTF Secure WS-Management
rcmp	644/udp	RMCP Secure ASF

Sounds a lot of fun, RCMP "ASF" messages types

- Reset (10h), Power-up (11h), and Power Cycle Reset (13h)
- Unconditional Power-Down (12h)
- Presence Pong (40h) / Presence Ping (80h)
- Capabilities Response (41h) / Capabilities Request (81h)
- System State Response (42h) / System State Request (82h)
- Open Session Response (43h) / Open Session Request (83h)
- Close Session Response (44h) / Close Session Request (84h)

Hardware - Architechture




```
st r28, [sp,120]
st r31, [sp,132]
add r1, sp, 8
mov fp, sp
jl stage3
mov sp, fp
ld r0, [sp,8]
ld r1, [sp,12]
```

Basically

- Embeded ARC4 micro-controller
- Located in chipset's graphics and memory controler hub
- Management Engine's (ME) firmware into Flash (same as BIOS's)
- Protected memory space accesible even in S3 state
- Directly connected to the NIC

Hardware - ARC4

[http://en.wikipedia.org/wiki/ARC_International]

ARC International plc was a developer of configurable microprocessor technology and is now owned by Synopsys. ARC developed synthesisable IP and licensed it to semiconductor companies.

The configurability of the ARC happens at design time (as opposed to run time) using the ARChitect processor configurator.

The core was created in such a way that it is extensible. Unlike most embedded microprocessors you can add extra instructions, registers and functionality as if they were made from Lego.

Hardware - ARC4

In short

- Real name "ARCtangente-A4"
- 32 bits RISC code
- 36x32 bits code register
- Can work in little and big endian mode
- Most known models are ARC600 and ARC700
- Specs are not public

Coding for ARC4

- Before Synopsys, contributed to elf-32-arc support in gcc/binutils
- With a bit of effort you still can build a tool chain
- IDA doesn't have a cpu module for it

Hardware - chipsets

From Vassilios Ververis's thesis (2010)

Version	South Bridge	Chipset
1.0	ICH7	Intel 82573LM/LC
2.0	ICH8	Intel Q963/Q965
2.5	ICH8M	Intel GM965/PM965
3.0	ICH9	Intel Q35
4.0	ICH9M	Intel GM45 or 47/PM45
4.1	ICH9M	Intel GM45
5.0	ICH10	Intel Q45
6.0	PCHM	Calpella, Piketon

Hardware - desktops and notebooks

Again stolen from Vassilios Ververis's thesis (2010)

D	Lenovo ThinkCentre M55p	Intel Q965 Expres	2.1
D	Lenovo ThinkCentre M57p	Intel Q35 Express	3
D	Lenovo ThinkCentre M58p	Intel Q45 Express	5
N	Lenovo M58pX200/X200s,X301	Mobile Intel GS45 Express	4
N	Lenovo T400,T500	Mobile Intel GM45 Express	4.x
N	Lenovo W700	Mobile Intel PM45 Express	4
N	Lenovo X61, X61S	Mobile Intel GM965 Express	2.x
N	Lenovo T61/T61P	Mobile Intel PM965 Express	2.x
N	Lenovo X61	Mobile Intel GM965 Express	2.x

I was just interested by Lenovo's, but have a look at Vassilios's paper for:

- Acer TravelMate, Veriton
- Dell OptiPlex, Latitude, Lifebook, Esprimo, Celcius
- Fujitsu LifeBook, Esprimo
- HP Compaq, EliteBook
- Panasonic, LG, Samsung.. Intel boards DQ35JO or DQ45CB/EK

Bonus Hardware - POS

Thanks again Vassilios

Type	Brand/Model	Chipset	Version
POS	Fujitsu TeamPoS 3624	Intel Q35 Express	3.2
POS	Fujitsu TeamPoS	Intel Q35 Express	3.2
POS	NCR RealPOS 70XRT	Intel GM45 Express	4.1
Kiosk	NCR SelfServ 60	Intel GM45 Express	4.1
POS	NCR RealPOS 80XRT	Intel Q965 Express	2.2
SC	NCR SelfServ Checkout	Intel Q965 Express	2.2
ATM	NCR SelfServ 22,25,26,32,34,38	Intel Q965 Express	2.2
POS	Radiant P1760	Intel GME965 Express	2.6
POS	Radiant P1560	Intel GME965 Express	2.6
POS	Wincor Nixdorf Beetle /S-II plus	Intel Q35 Express	3.2
POS	Wincor Nixdorf Beetle /M-II plus	Intel Q35 Express	3.2

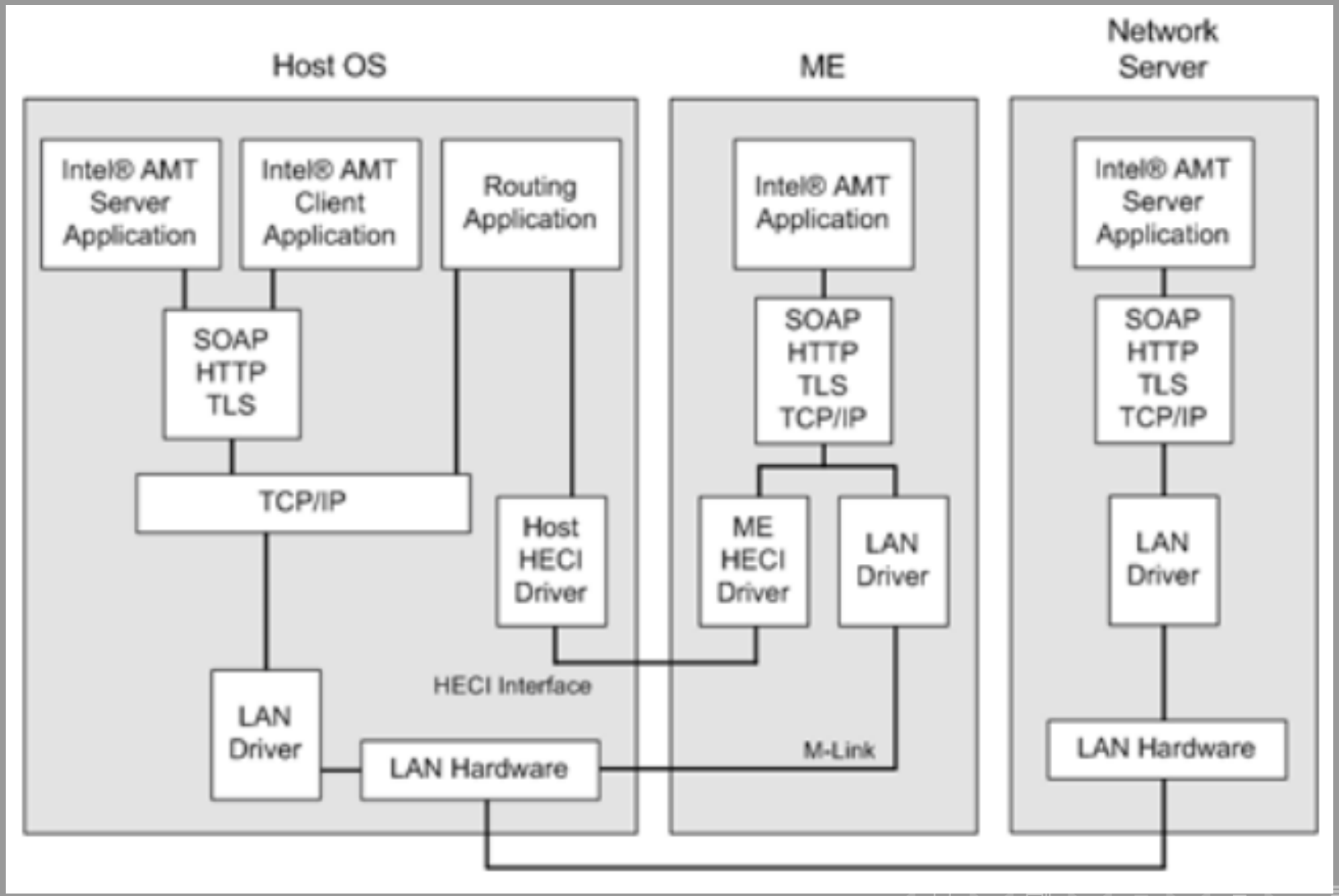
Something scary from Intel's doc

Firmware update

- Intel provides an interface for updating the Intel Management Engine (ME) firmware.
- A firmware image is sent to the ME using either the Intel ME Interface (MEI) or via HTTP, replacing the original firmware image.
- The Firmware Update interface is used only by OEMs via Intel-supplied tools and is not intended for use in ISV applications.
- The HTTP interface for sending the firmware image, and the WS-Management interface for retrieving the firmware update status are enabled only for local access.
- This feature was removed from Intel AMT starting with Release 7.0.
- The Firmware Update realm is deprecated in Release 7.0 and will be removed in a future release.

Integration with OSs

Pretty much all about Host Embeded Controller Interface - HECI



Food for thoughts, what could be possibly done with it

First steps

- Can zero touch deployment be used to our advantage?
- Easy ownage? KVM over SOL, passing kernel options
- As for AVs or TR069, attacking the manager means mass ownage
- From OS upgrade sounds possible via HECI

Maintaining access

- Use SoL for backdoor communication, bypassing local FW/AV
- Probably the best place for MitM, traffic mirorring and interception

Conclusions?

- Still many things to look into
  - AMT's internals
  - Other methods to access/update (remotely?)
  - Obviously developing reliable code for it
  - Many unexplored/undocumented features
  - AMT/OS communication and interaction
- Good points for Intel
  - Very well documented, at least for the basics
  - SDK, DTK and AMT emulator are freely downloadable
- From our perspective
  - Obviously a wet dream for backdoor/malware
  - Would it be more reliable than SMM?
  - How much compmanies are now deploying it (mass takeover?)
  - More third parties using it means more vulnerability?
  - LARGE fuzzable surface, probably funny things to find