Security evaluation of Intel's Active Management Technology

Vassilios Ververis
ververis{at}kth.se

March 11, 2010

Under the supervision of:

- Professor Gerald Q. Maguire Jr., KTH Stockholm
- Professor Dr. Jean-Pierre Seifert, TU Berlin

Outline

Addressing the Problem

Fundamental security vulnerabilities in:

- Authentication schema
- Remote provisioning mechanism
- Mobile version

Create a powerful **backdoor** *even* while the PC is turned off

What others have done

Timmers and Zee: limitations and capabilities of Intel AMT

- *Cover a* **limited** *fraction of AMT capabilities*

Tereshkin and Wojtczuk introduce ring -3 rootkit: code injection executed into AMT

- *Assumes* **local access** *being locally in order to be successful.*

Why is this thesis important

- Uncovers **fundamental** security vulnerabilities of Intel's AMT
- Sketches implications of vulnerabilities in critical operations
- Our attacks can be *accomplished* **remotely**

What is Intel AMT

Highly available out-of-band remote management

- Remote management capabilities in all system states
- Embedded in Intel based platforms

OS independent

- Runs outside the context of the OS
- Protected from OS configuration alternations

Persistence

- Nonvolatile storage of state
- Survives power outages and system rebuilds

Architecture Components

Management engine:

- Embedded micro-controller (ARC4)
- Lightweight micro-kernel OS

Nonvolatile flash memory:

- Protected/hidden partition from host OS.

Network controller:

- Direct access to network interfaces.

Examples of Use Cases

Discovery

- Remote hardware/software inventories
- Configuration via the network independent of the system state

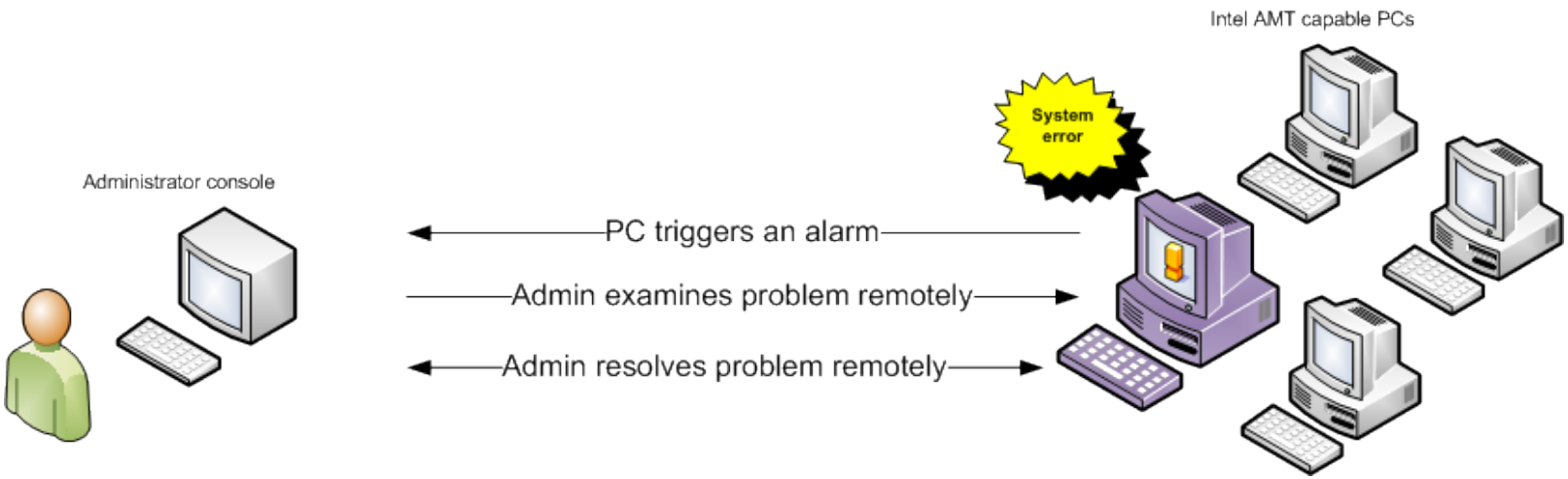
Remote wake/update

- Remote troubleshooting and recovery
- Power off, power on, reboot, or wake up the PC

Detect and block anomalous network behavior

- Network packet filtering for inbound/outbound traffic

Primary Use Case



Provision 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

Authentication Scheme

HTTP digest access authentication scheme (RFC 2617):

- Applied when TLS is not available
- Old authentication mechanism
- Vulnerable to man-in-the-middle attack
- Off-line brute force password attack

Results I

We implemented a patch on JtR password cracker
Benchmarks based on:

- GNU/Linux Ubuntu 9.10 distribution
- GNU C compiler version 4.4.1
- mpich2 version 1.2

Vendor	**Baseboard**	**CPU**	**Cores**
Gigabyte	GA-MA74GM-S2H	AMD Athlon 64 X2 5200+	2
Intel	MFS5520VI	Intel Xeon E5530 2,40GHz	8(16 HT)

HT: Hyper-threaded

Results II

CPU	Time	Combinations/s	Total c/s
AMD Athlon 64 X2 2.7Ghz	200 s	1,421,000	2,842,000
Intel Xeon E5530 2.4GHz	200 s	1,380,000	22,080,000

C/S: Password combinations / second

Zero touch Remote Provisioning

Intel AMT platform provides a remote provisioning feature:

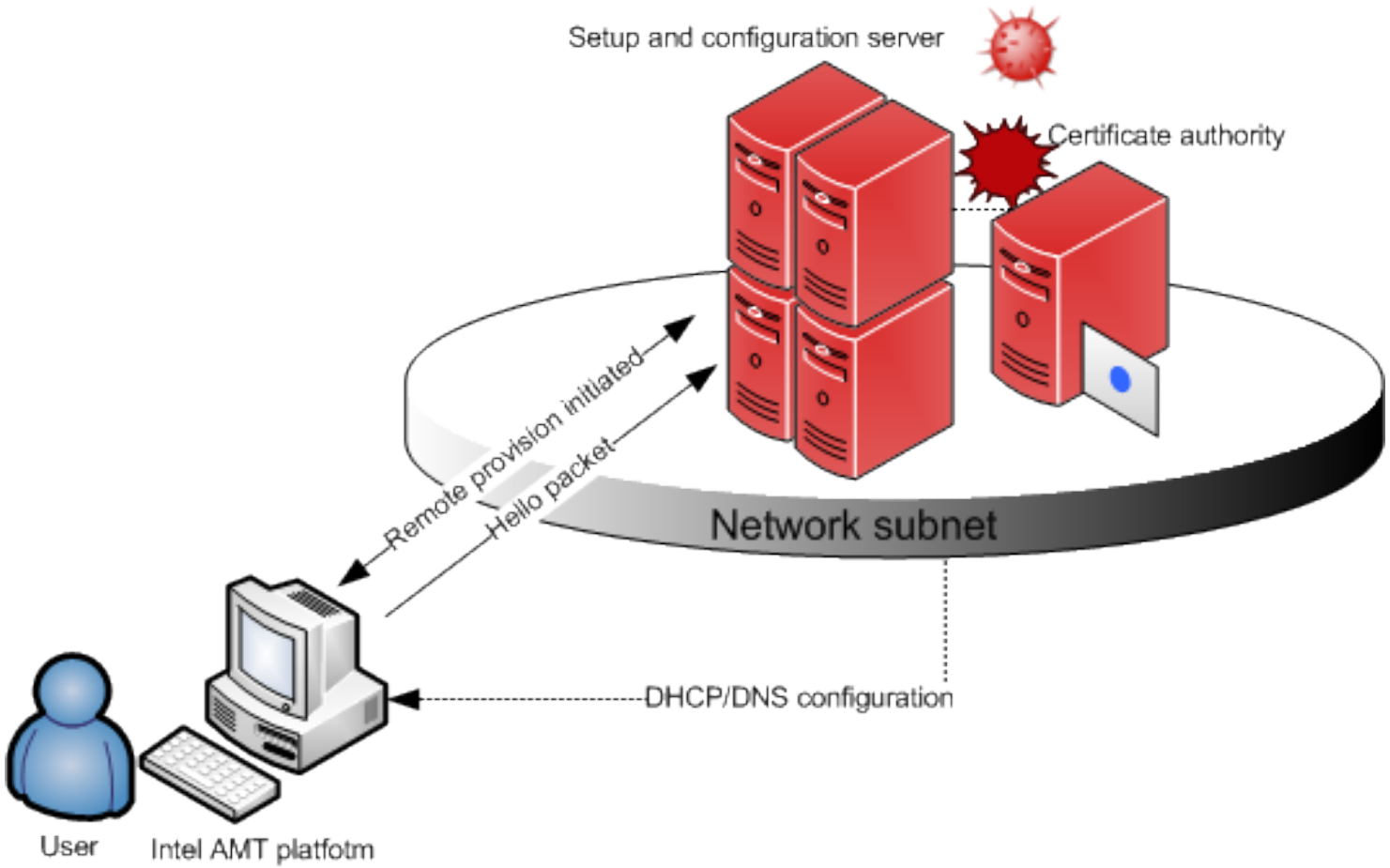
- Workstation(s) managed remotely from the network
- **No** physical attendance required
- **No** extra software on the workstation side required

Zero touch Remote Provisioning Requirements

Zero touch Remote Provisioning requirements:

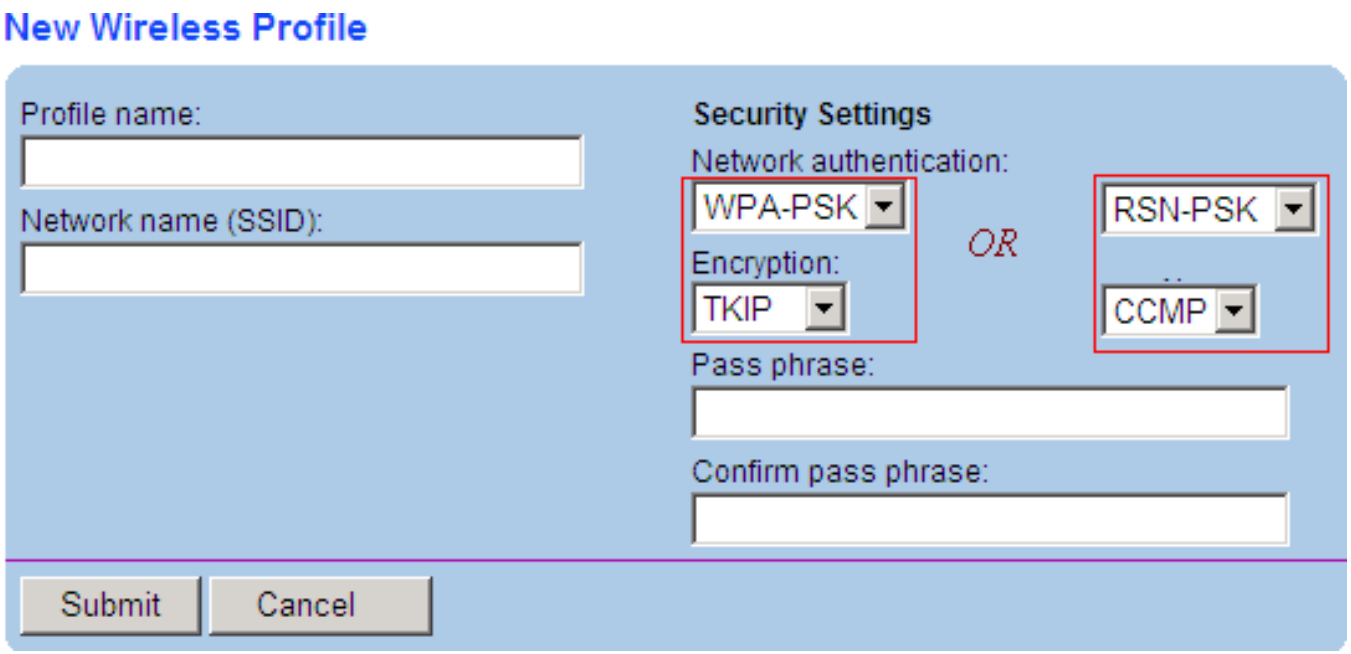
- AMT device is pre-programmed with 4 certificate hashes
- Provisioning SSL certificate
- DHCP and DNS server
- Setup and configuration server

Zero touch Remote Provisioning Schema



Wireless Profiles

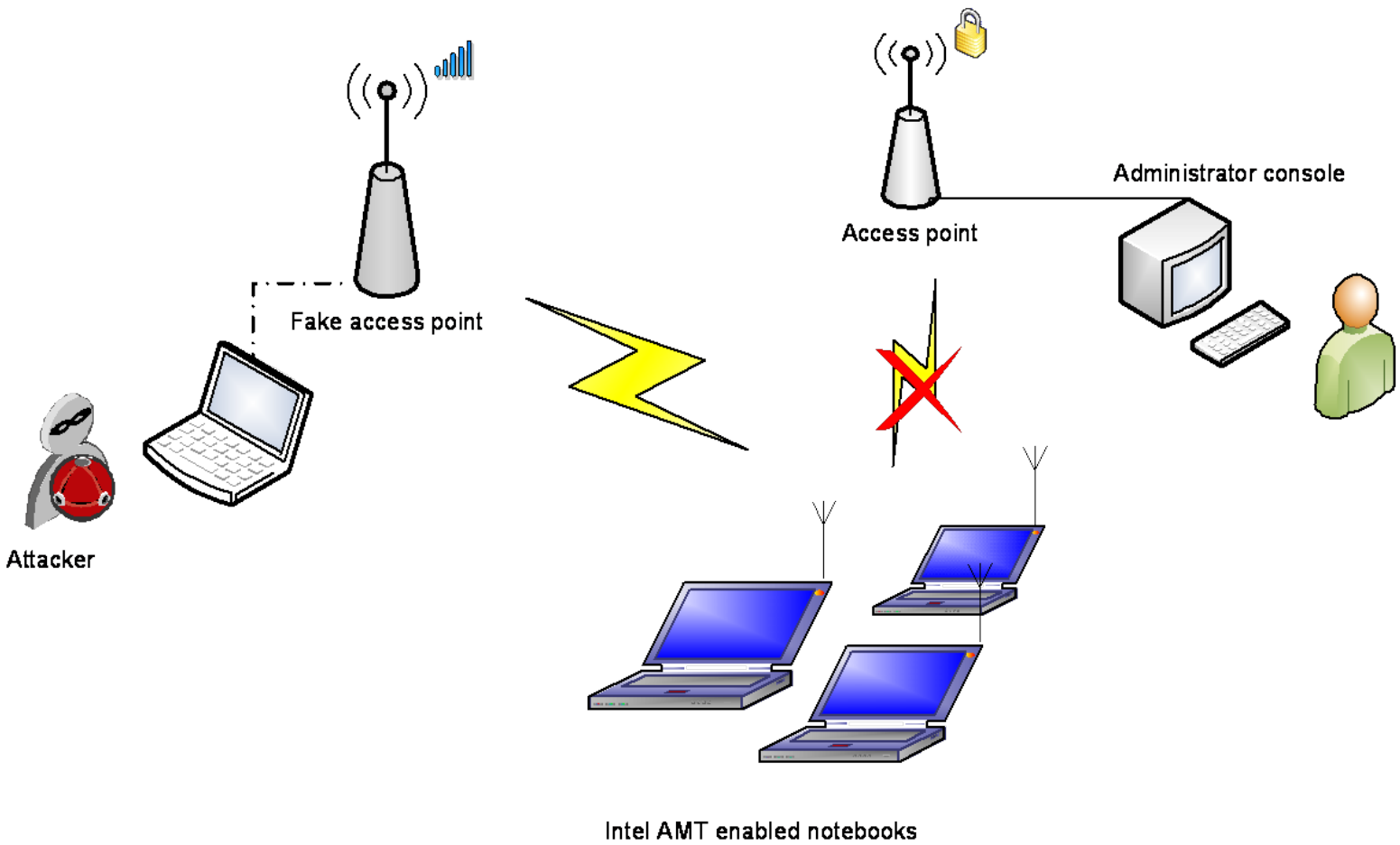
- No built in wireless security support
- Depends upon AP security



Wireless (In)security

- Highly dependent upon access point security scheme
- Falls into a variety of wireless attacks
  - Access control – Fake access points, *ad hoc* associations, MAC spoofing
  - Confidentiality – Man-in-the-middle, access point phishing
  - Availability – De-authentication flood, RF jamming
- Attacker can deploy attacks with limited resources

Wireless Attack Scenario



Conclusions I

- Embedded HTTP and XML server gives a clear advantage for malicious activities and exploits
- Remote BIOS updates and serial-over-LAN functionalities over the network $\Rightarrow$ *a powerful exponentially spreading worm*
- End-user has no knowledge whether a device is being managed and monitored by the AMT

Conclusions II

Intel made a very bad choice in choosing protocols which are known to be vulnerable for a critical application: remote management

Free hardware based rootkit

- AMT included in: desktop, notebooks, servers, POS, embedded systems, ATMs
- Provides the basis for secretly realizing a hardware based rootkit
- Provides a covert communication channel:
  - Allows malicious parties to perform: surveillance, monitoring, espionage, and to fully (remotely) control a system

Suggested Recommendations

- Enforce TLS/SSL implementation in all provisioning models
- Enhance security features in mobile version
- Careful design and implementation with respect to network centric attacks is needed
- Redesign of remote configuration (specifically ZTC)

Suggested Future Work

- Implementing attack vectors for SSL/TLS implementation of AMT
- Security evaluation of AMT platform at the hardware layer
- Evaluation of Intel's AMT certificate based protection

Thank you for your attention

Questions ?

Acknowledgements

SECT Security IN TELECOMMUNICATIONS

http://www.sec.t-labs.tu-berlin.de/