

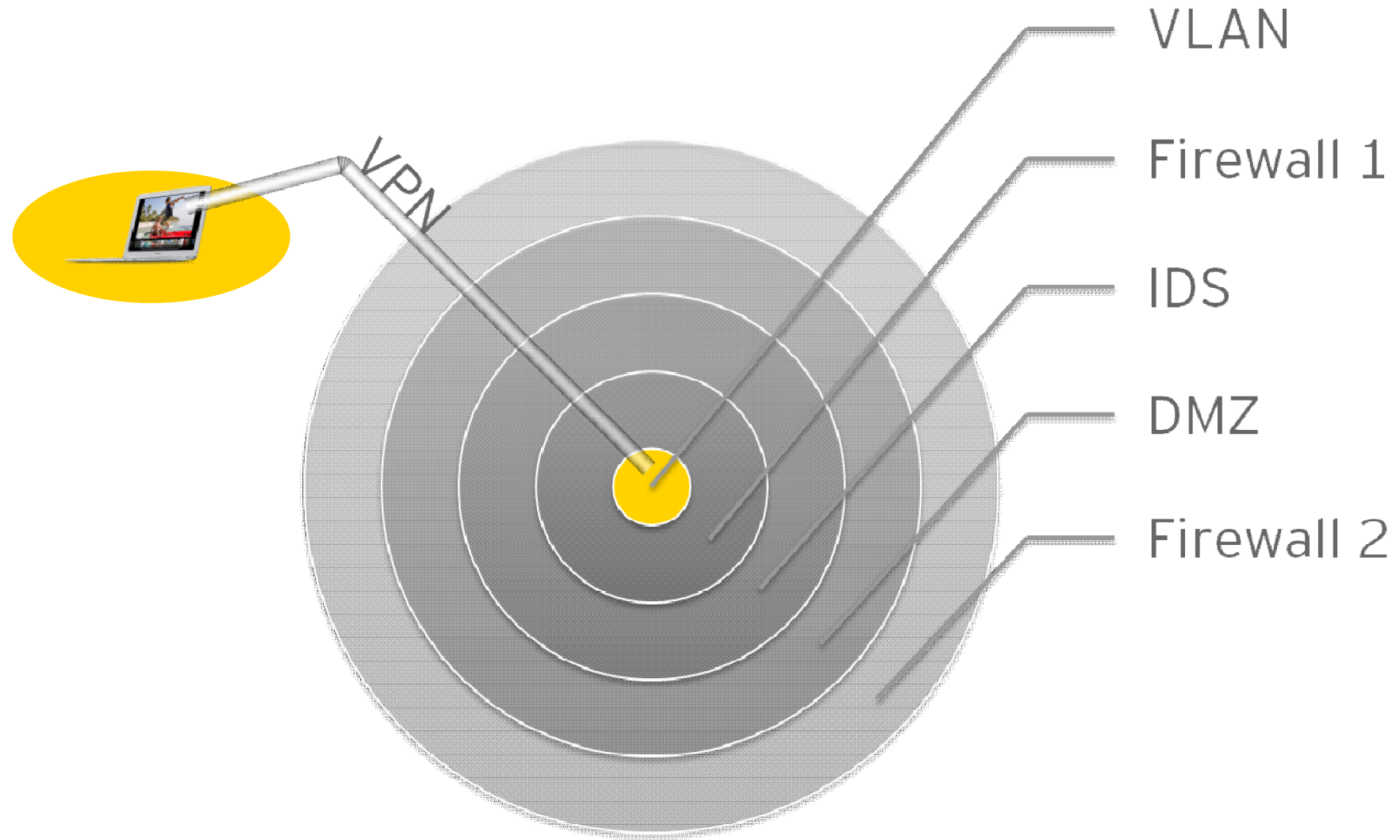
Endpoint security & mobility

AFSecurity, 20. May 2011



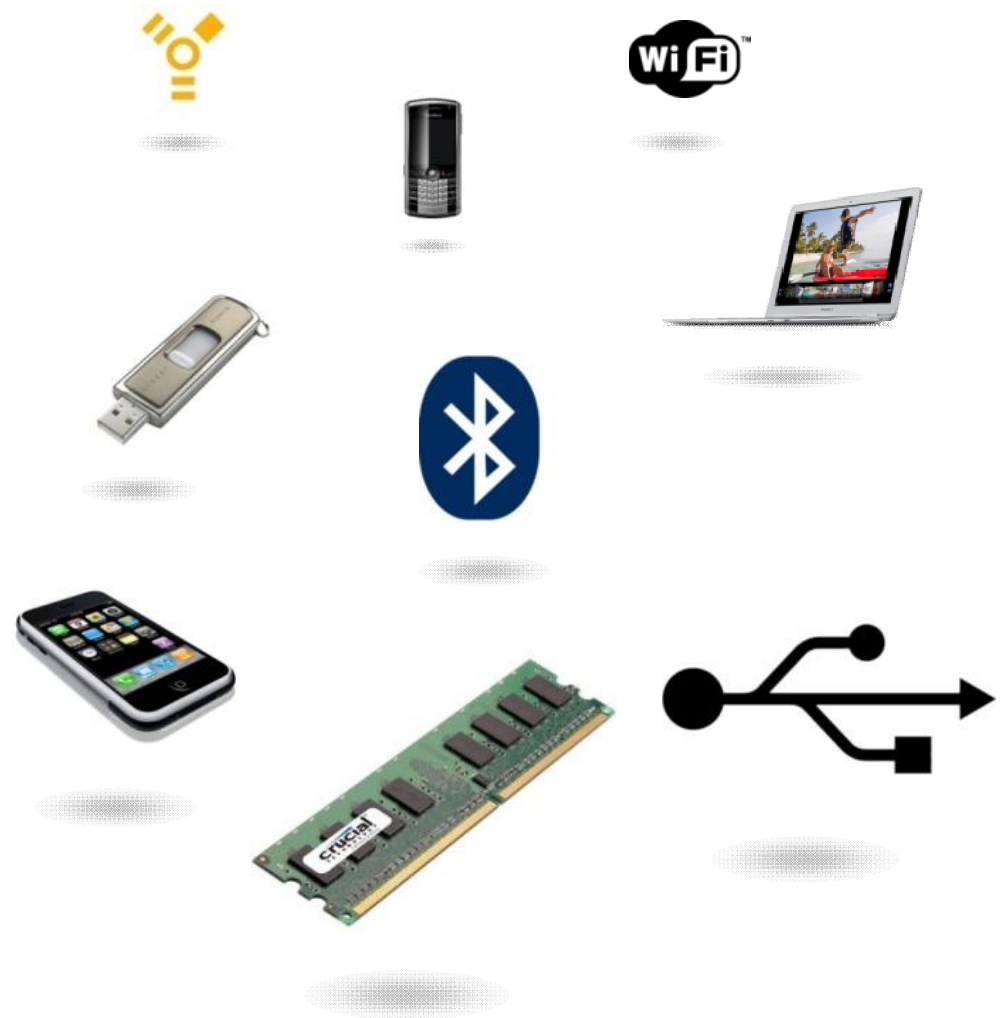
INTRODUCTION

Layered protection is all good, but what about the endpoint?



Mobile units presents a variety of attack vectors

- ▶ Mobile units
 - Small
 - Prone to be lost
 - Easy to forget at a café, etc.
 - “Simple” to steal
 - You lend it to a friend
 - Lots of storage
 - “Always on”
 - Plenty of physical and logical access routes
- ▶ How certain are you that your hardware is secure?



So what has happened? *Encryption* has become common in order to protect some endpoints

Private data lost

Consulting firm Inuit contacts 22 000 individuals after laptop theft
(pogowasright.org 15.12.2008)

Forced disclosure

Retail-firm TJX in the US forced to disclose data leakage
(searchsecurity.com 18.01.2007)

Banking data on eBay

Royal Bank of Scotland hard drives sold on eBay
(BBC, 26.08.2008)

Encryption demands

Loss of customer data forces encryption of all laptops in Virgin Group
(Full Disclosure, 30.09.2008)

512 331 180

The number of leaked identities based on publicly disclosed incidents
(privacyrights.org, 25.01.2011)

600 000

The number of lost laptops on airports in 2008... In the US alone!
(Dell Ponemon Lost and Found Study)

Encryption algorithms are designed to withstand attacks from adversaries with unlimited resources

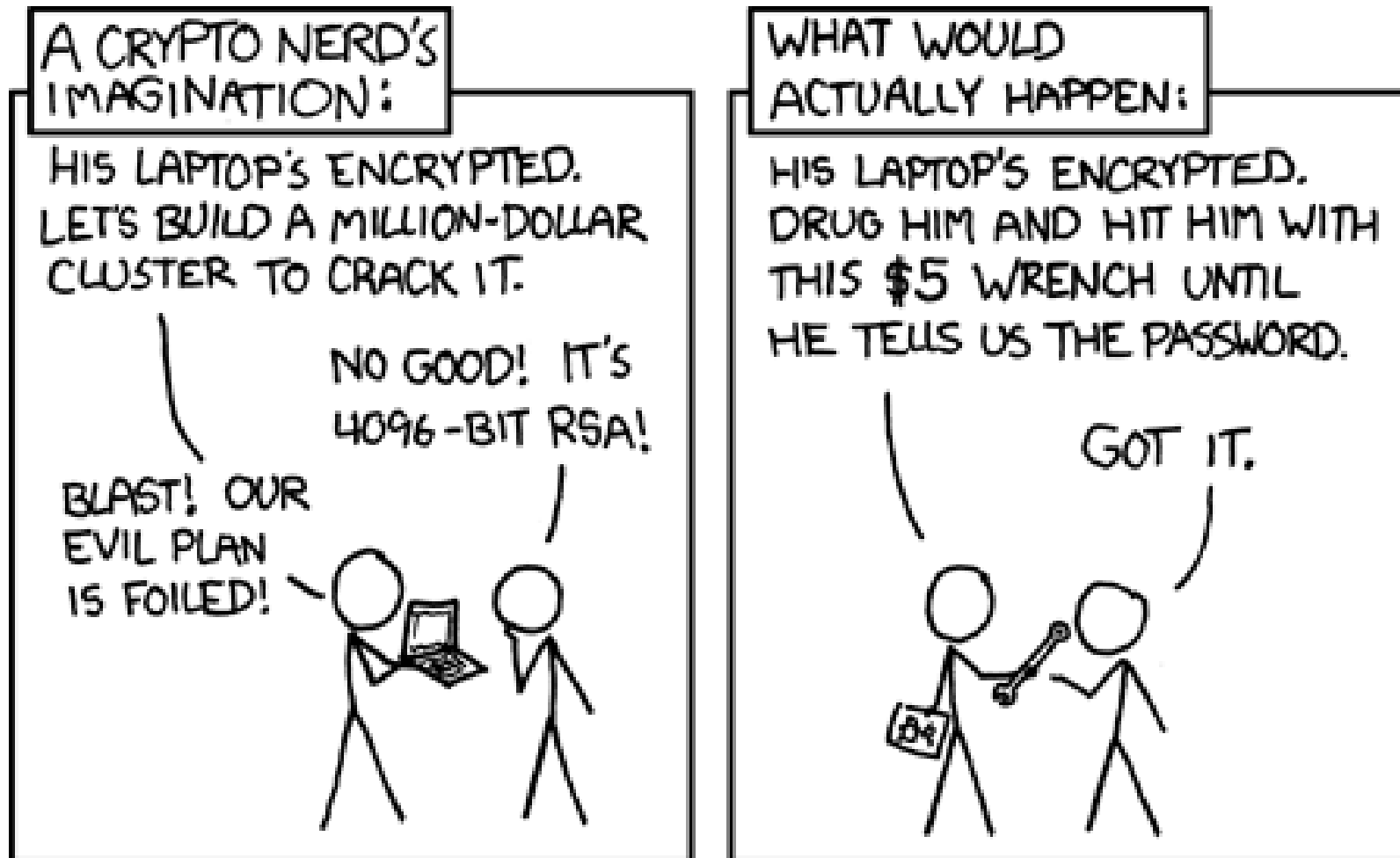
- ▶ The security lies in the secrecy of the key, not the secrecy of the encryption algorithm¹
 - Assumption: An adversary has full knowledge of the algorithm
 - The encryption key must be kept secret
 - Given a good algorithm, the best attack is brute force
 - An adversary is therefore dependent on huge resources to crack the encryption
- ▶ To put key bit lengths in perspective:

Reference	Size expressed as power of 2 (bits)
One million (10^6)	2^{20}
Seconds in a year	2^{25}
Number of humans on earth	2^{32}
Age of the Universe	2^{34} year
1 MIPS ² Year	2^{45} operations
1 Sony PS 3 Year (230400 MIPS)	2^{63} operations
Estimated number of protons in the Universe	2^{256}

1) Kirchhoff's principle

2) Million Instructions Per Second

Back to reality...



Physical memory (RAM) on mobile units contain interesting information while powered on

- ▶ Passwords
- ▶ Process-structures
- ▶ Open network connections
- ▶ Open documents, images, etc.
- ▶ Cached data from your server
- ▶ Open DLLs
- ▶ Registry
- ▶ Function calls, binary applications
- ▶ **Encryption keys**





ATTACKING USING IPOD

FireWire is a potential attack vector to gain access to memory without asking the OS



- ▶ FireWire (IEEE1394) - specification specifies Direct Memory Access (DMA) for certain units
- ▶ These units (like the Apple iPod) has write access to memory (RAM)
- ▶ Yes, **write access**
- ▶ [insert evil plan here]

Demonstration scenario: Whole-disk encrypted corporate laptop

- ▶ Powered on, locked
 - Or in Standby
- ▶ Truecrypt whole-disk encryption
 - 256 bit AES
- ▶ Adversary has unlimited physical access (e.g., stolen laptop)
- ▶ No FireWire-port (oops)



Demonstration: Winlockpwn



+



+





ATTACKING USING MEMORY DUMPING

In 2008 a team of Princeton-scientists discovered that we can find AES-keys in RAM even after reboot

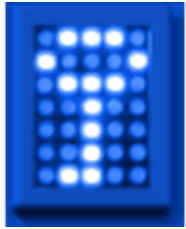
▶ "Coldboot"

- DRAM maintains its state several seconds after loss of power
 - ▶ Timeframe can be extended to several hours given proper cooling
- The team publicized code that automates attacks on BitLocker and TrueCrypt

▶ Method:

Cool down memory ▶ Hard reboot ▶ Boot from network or USB-disk ▶
Dump memory ▶ Search for encryption keys in memory dump ▶ Decrypt

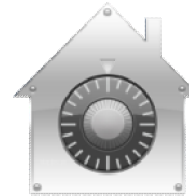
Almost all (software) whole-disk encryption products are vulnerable



TrueCrypt



Vista BitLocker



OS X FileVault



PGP Desktop



ProtectDrive



DriveCrypt



BestCrypt

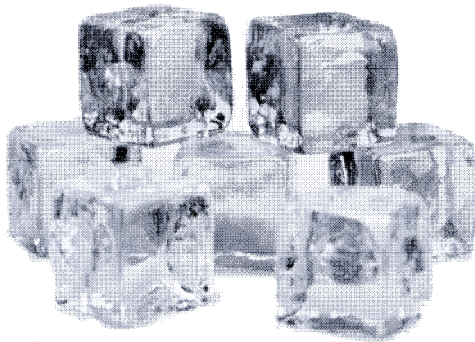


Dm-crypt/LUKS

Demonstration: Coldboot



+



+



+





PROTECTION

A memory dumper's attack kit: Less than 3 000 NOK + laptop

- ▶ PC (laptop)
- ▶ Crossover CAT. 5 cable
- ▶ Toolbox
- ▶ USB-stick 4 GB+
- ▶ iPod
- ▶ FireWire-disk
- ▶ CRC Dust Off
- ▶ Glad-pack
- ▶ Universal charger unit for mobile devices
- ▶ Software
 - Interrogate
 - Coldboot
 - PTFinder
 - Volatility

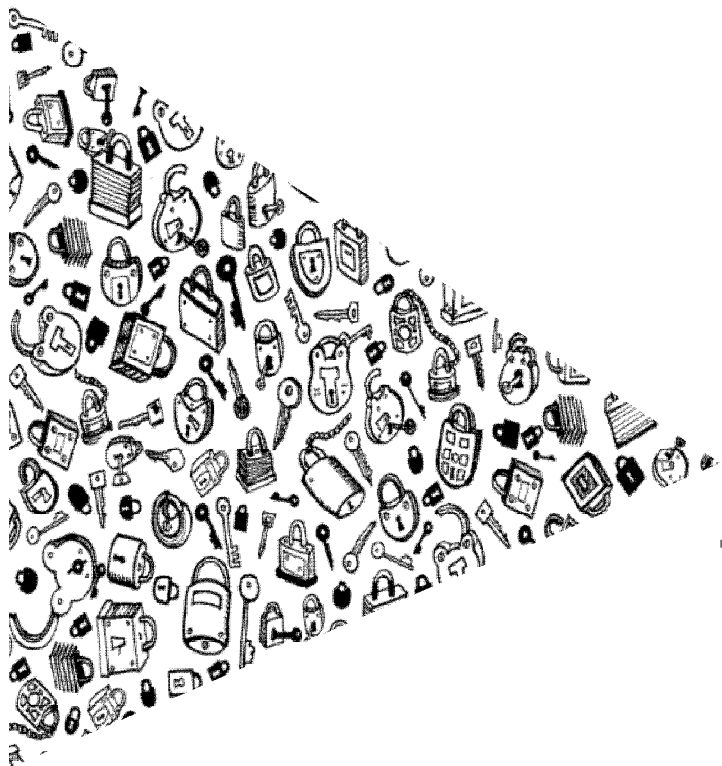


The simplest protection is to lessen the window of opportunity for an attack

- ▶ Disable hibernate and standby functionality on mobile units
- ▶ Lock and password protect BIOS
 - Makes it difficult to boot an alternative OS
- ▶ Physically shut down FireWire-ports or remove FW drivers
 - I've seen glue-guns been utilized for the former:-)
- ▶ Inform your employees
 - Use the firm's information security policy
- ▶ Use HW-based encryption
- ▶ Get some end point protection

Summary

- ▶ Hardware can be utilized as a side channel to perform exotic attacks
 - FireWire, USB, COM-port, Ethernet, Motherboard, insert rigged hardware, dump memory, PCMCIA, flash memory cards, LTP, electromagnetic radiation, keyboard sounds, vibrations in laptop screens, +++
- ▶ It is hard to build security on an unsecure fundament
 - E.g., open hardware
- ▶ Don't become paranoid
 - Unless you're hired to be so
- ▶ The information security policy is there for a reason
 - Power off your laptop!



Thank you for your attention

Questions?

carsten.maartmann-moe@no.ey.com

<http://www.carmaa.com>

<http://www.breaknenter.org>

ERNST & YOUNG
Quality In Everything We Do