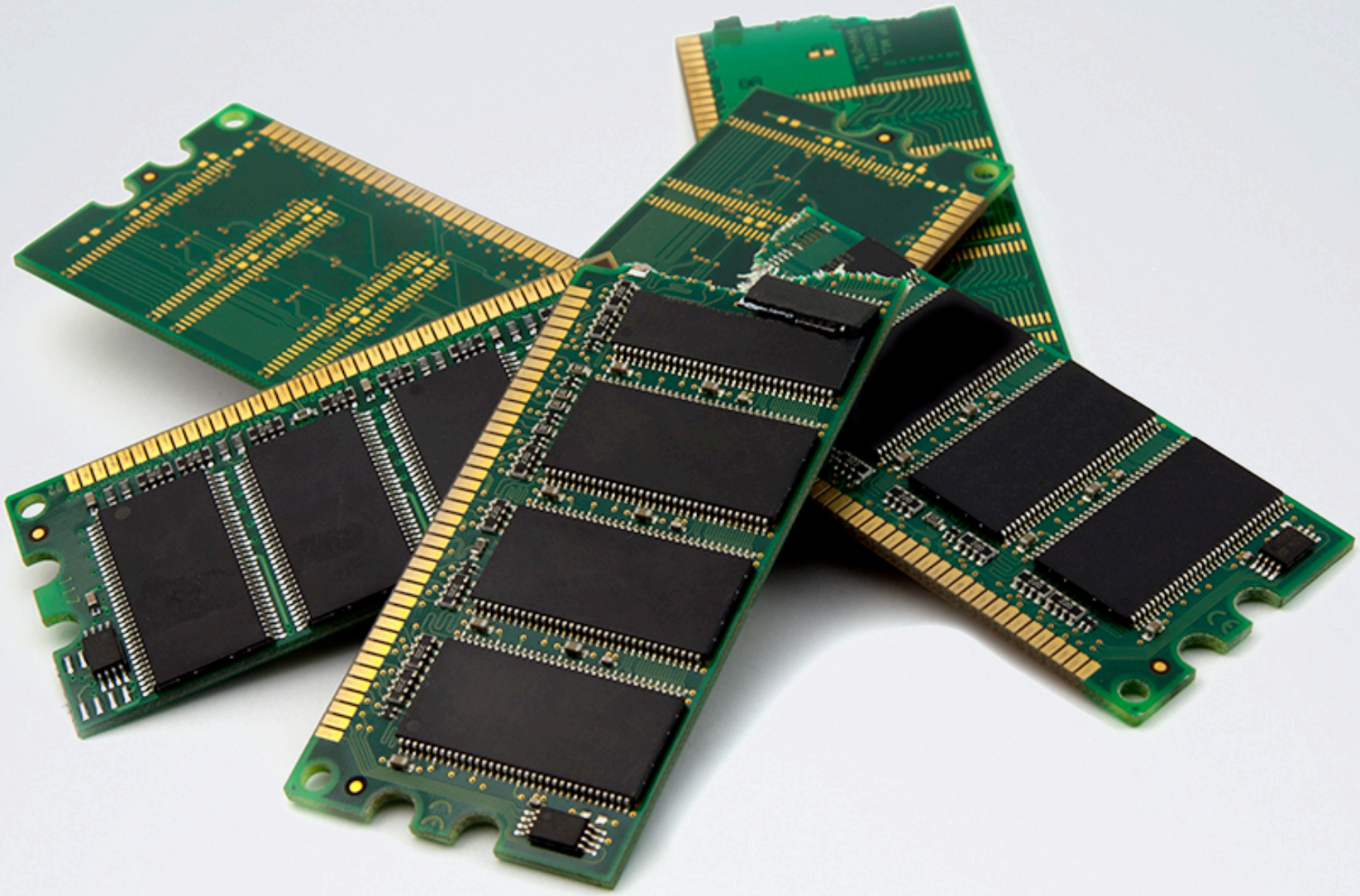


HARDWARE HACKS

OWASP NYC Chapter May 17th 2012

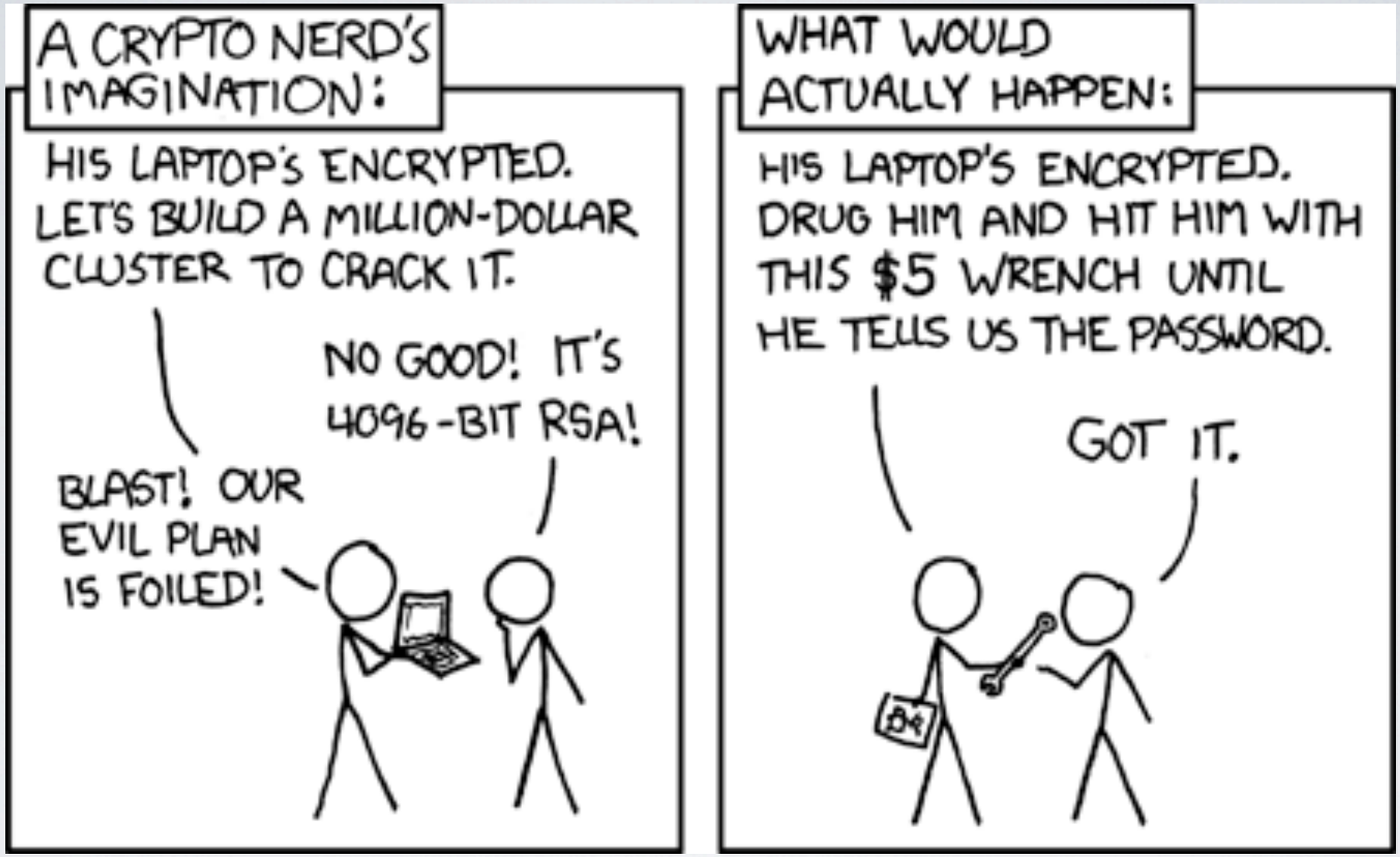
Carsten Maartmann-Moe @breaknenter

MOBILE UNITS PRESENT A VARIETY OF ATTACK VECTORS

- Small and valuable - and prone to be forgotten at Starbucks
- Simple to steal - compared to a desktop or server
- Perhaps you lend your mobile unit to your friends
- Ever-expanding storage
- Always on
- Access all [your, your company's] data, anytime, anywhere

SECURITY KNEE-JERK RESPONSE: ENCRYPTION

- AES 256
- "Military-grade"
- Done and done - "where's my bonus?"



* Source: XKCD.com

ENTER RUBBER-HOSE CRYPTANALYSIS

HOW TO DEFEAT REAL-LIFE CRYPTO SYSTEMS

- The implementation matters as much as the key length and algorithm design!
- Don’t attack the crypto; focus on the security of underlying components
  - Avoid cryptanalysis - time consuming and difficult
  - Exploit false assumptions about the environment

HARDWARE SECURITY - A FALSE ASSUMPTION

- If hardware security is present at all, it usually not well understood by developers
- Hardware is:
  - Built to interoperate in a trusted environment
  - Built to be hot-plug capable
  - Built for speed and stability, not security

THE REALITY GAP

- Modern users expect:
  - Always on
  - Secure
- Security practitioners have long ignored physical security

What do you mean "my password doesn't protect my computer"?

- my mother (and every other user I know)

Haha, physical access = 0wnage, kthxbai

- security "experts"

DEMONSTRATION TIME

Teensy | Inception | Cold Boot

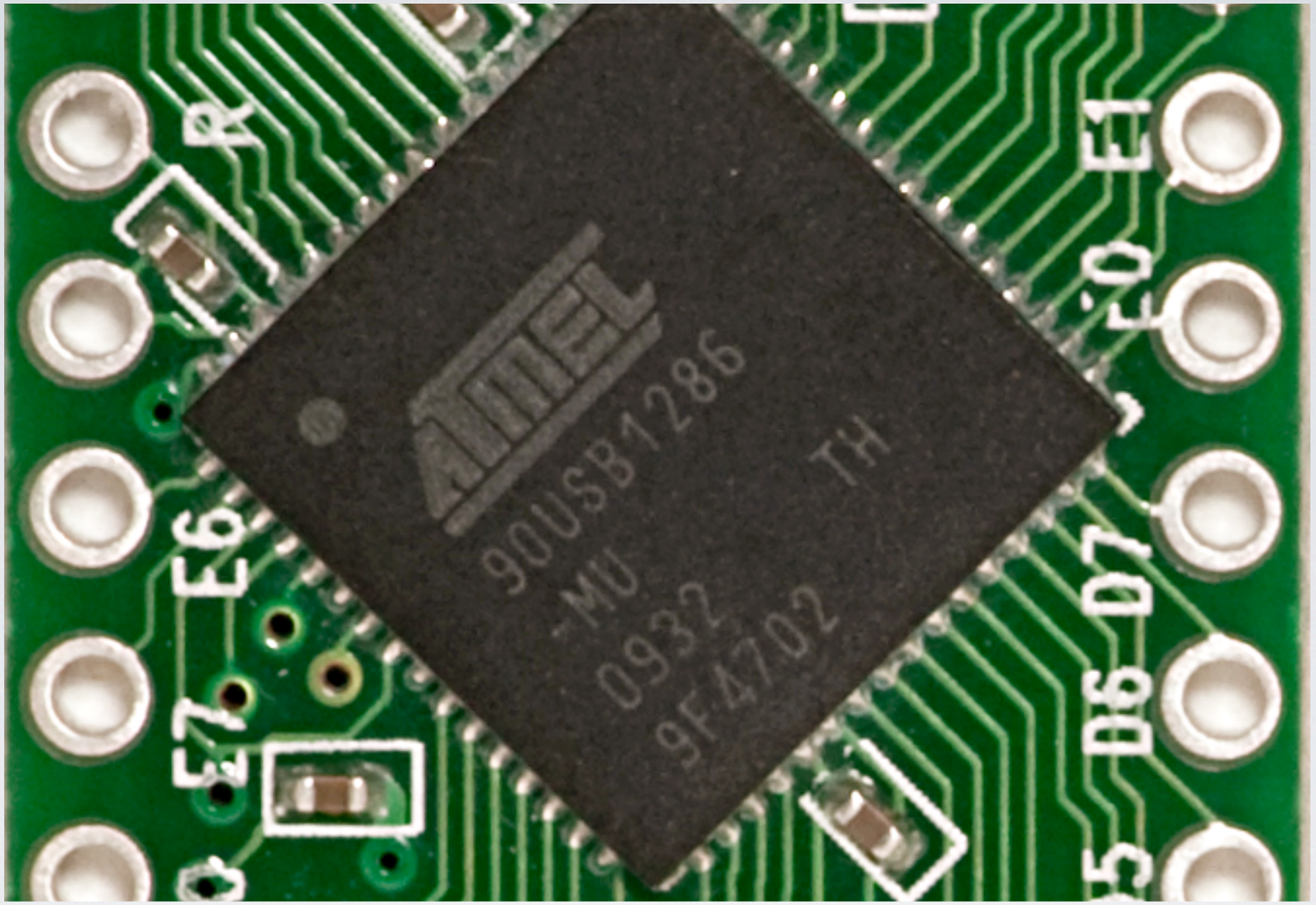
TEENSY

- Human Interface Devices are usually bound by few security restrictions

- **Teensy** is a programmable HID simulator with storage capacity

- Simulates a keyboard with a speedy hacker (@16Hz)

- Social Engineering Toolkit integrates with Metasploit and is able to generate Teensy payloads



DEMONSTRATION

INCEPTION

- The SBP-2 protocol of FireWire has by design Direct Memory Access (DMA) to the lower 4 GiB of RAM
- You can **read** and **write** to arbitrary memory locations
- Operating systems are hot-plug capable, even in a locked state
- Patching live memory without the OS is suddenly an option
- **Inception** places the idea that all passwords are correct into the memory of the machine

DEMONSTRATION

COLD BOOT

- Physical RAM retains its state for a period after power loss
  - The period is directly related to the heat of the transistors
- Software crypto systems needs to keep the encryption key in-memory at all times
- AES key schedules have error-correcting code behavior
- The **Cold Boot** attack exploits all of the above

DEMONSTRATION

MITIGATION

- Inform your employees - use the firm's information security policy
- Be aware of hardware security when designing software!
- Disable hibernate and standby functionality on mobile units
- Lock down and password protect BIOS
- Physically shut down FireWire-ports
- Remove FireWire drivers or set driver installation restrictions at OS level
- Switch to hardware-based encryption
- End point protection software

QUESTIONS?

Carsten Maartmann-Moe

@breaknenter

http://www.breaknenter.org/projects/inception

http://github.com/carmaa