CS7NS5/CSU44032

Security & privacy

Stephen Farrell

stephen.farrell@cs.tcd.ie
(still in the spare room;-)

Course materials:

https://down.dsg.cs.tcd.ie/cs7053/

https://github.com/sftcd/cs7053

Slideware + some papers

Course Outline

- Introduction
- Security and privacy concepts
- (Enough) cryptography (AES, RSA, ...)
- (To grok) core security standards (DNS, TLS,...)
    - ...and where those are headed
- Stuff that's interesting for the last few weeks (liable to change)
    - Centralisation
    - Maybe COVID tracking apps?

Computer and Network Security is…

- …a good thing to study (“one born every minute”, and some of those are programmers!)
- …something with more and more impact (scaling factor is about the same as the Internet)
- …a part of risk management

Privacy is…

- …nowhere near as well understood
- …an issue for people and not companies
- …not clearly a part of risk management, but related
  - I’m unsure if risk analysis is a good approach to address privacy
  - I’m pretty sure “consent” is an awful model that pretends to address privacy
    - Good presentation on the problem, with IMO less good (but worth exploring) ideas on HOWTO fix https://datatracker.ietf.org/meeting/105/materials/slides-105-ietf-sesse-privacy-modern-concerns-steven-m-bellovin-00.pdf

Risk Management

- Risks (bad things)
  - Disclosure of trade secrets
  - Sabotage (information or hardware)
  - Denial of service
  - Accidents (fire, flooding, earth quakes, …)
- Solutions (not always good things)
  - Security policies and mechanisms
  - Physical security (locks, guards, CCTV, …)
  - Formal specification/verification of software
  - Halon, UPS, off-site backups

Vulnerabilities

- Many risks arise due to the existence of vulnerabilities in computer systems
- All systems have vulnerabilities, our goal is not to remove absolutely all of them, but to control their impact
  - Reducing numbers is good
  - Can also isolate parts of the system (e.g. Firewalling)

Vulnerabilities

- Most common:
  - Scripting user agents
  - Buffer overruns
  - XSS & Injection (e.g. SQL injection)
  - Insecure default settings
- Uncommon, but interesting:
  - Acoustic side-channel key extraction,
    - Genkin, Shamir & Tromer
  - https://eprint.iacr.org/2013/857.pdf

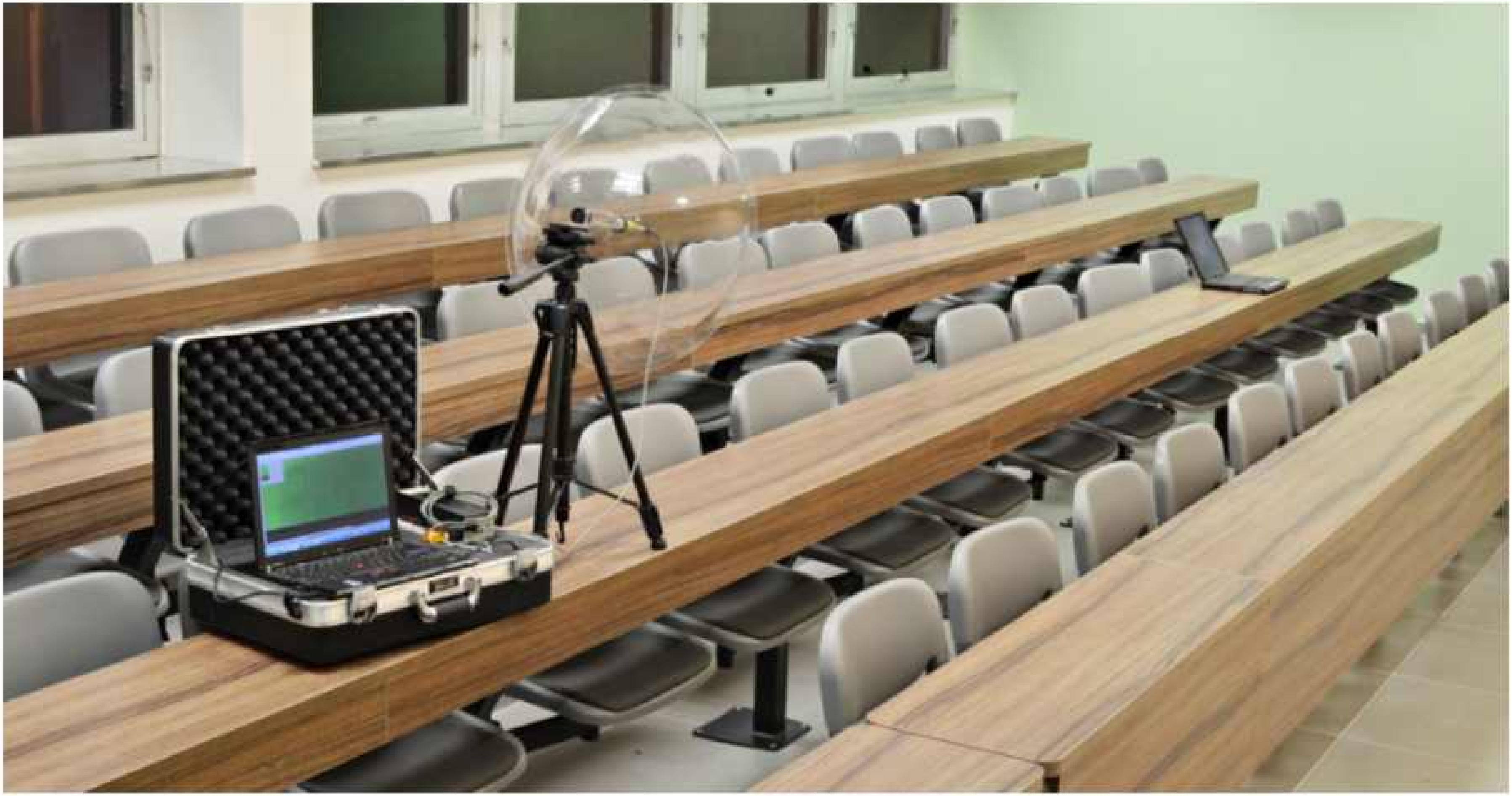

Figure 6: Parabolic microphone (same as in Figure 5), attached to the portable measurement setup (in a padded briefcase), attacking a target laptop from a distance of 4 meters. Full key extraction is possible in this configuration and distance (see Section 5.4).

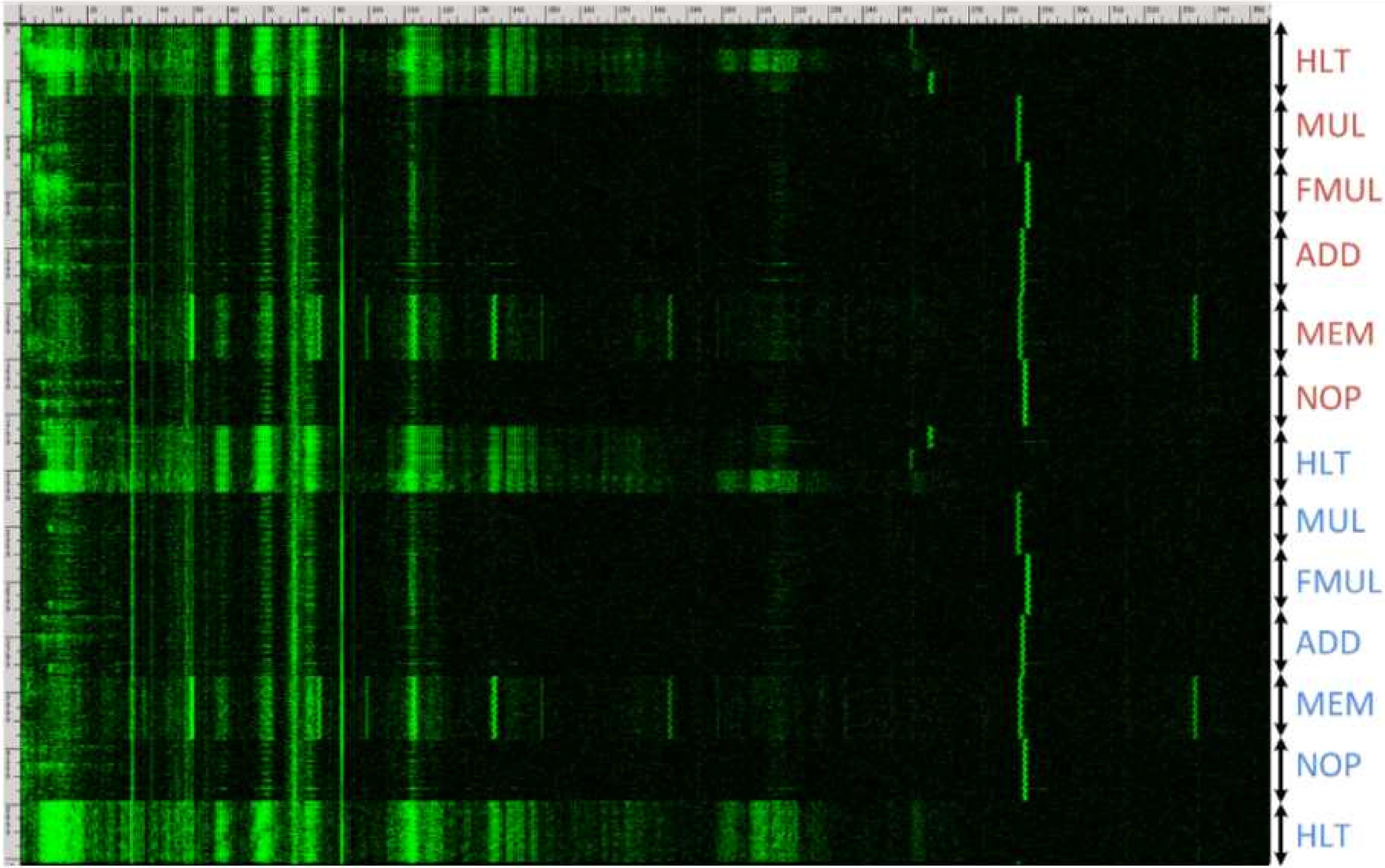

Figure 7: Acoustic measurement frequency spectrogram of a recording of different CPU operations using the Brüel&Kjær 4939 microphone capsule. The horizontal axis is frequency (0–310 kHz), the vertical axis is time (3.7 sec), and intensity is proportional to the instantaneous energy in that frequency band.

Good/Bad Actors

- Systems have users
  - Normal, administrative, “root”
- Networks have nodes
  - “Inside”, “outside”, trusted...
- Attackers
  - Can be one of the above, or not...
  - Hijacked ISP router, compromised SIM card factory, bot etc.

Possible Bad Actors

- Disgruntled employees (*plenty*)
- Crackers (*hackers*)
- Script-Kiddies (*cracker wannabes*)
- Spies (*industrial and military*)
- Criminals (*thieves, organized crime*)
- Terrorists
- Governments
- Bait’n’switchers

Possible Exploits

- Force legitimate user to reveal passwords
- Social engineering
- Recruit legitimate user
- Sabotage (*fire, electricity, …*)
- Sifting through garbage
- Attacking the network (*network threats*)
- Install malware

Active/Passive Attacks

- Active attacks
  - Fabrication, modification, deletion, replay of messages
- Passive attacks
  - eavesdropping/traffic analysis
  - can be off-line (e.g. weak encryption)
- Different protocol mechanisms are used to counter these

Risk Analysis Process

Many variations exist, mostly they resemble:

- Identify assets
- Identify risks and vulnerabilities
- Consider probabilities
- Consider consequent costs/losses
- Rank risks
- Develop mitigation(s) for highest ranked risk(s)
- Iterate, until effort exhausted or time up
  - All the time recording what you’ve done

Summing up risk

- Risk is a function of the cost of threats and their probability of occurrence
  - Which function can be debated
  - High/Medium/Low
    - For both costs and probabilities
- Threats occur when a vulnerability is exploited

A cyber-warning

- With few exceptions people who say cyber-blah have little or no clue
  - Or feel forced to succumb to “the market”
- Cyber-foo is a marketing term for almost all foo
  - Avoid using it
  - When you hear it, be suspicious

Privacy

- Less well understood than security
- Who cares? About what?
  - Governments, marketers and large corporates do “care deeply” about your (lack of) privacy
- How to protect that?
  - Encrypt things in transit and storage
  - Short-lived dynamic identifiers are better than long-lived static identifiers
  - Just don't (require) identification