CS7053/CS7453/CS7NS5/CS4407

Security & privacy

Stephen Farrell

stephen.farrell@cs.tcd.ie
x2354, Room WR3.4

Course materials:
https://down.dsg.cs.tcd.ie/cs7053/
https://github.com/sftcd/cs7053

Slideware + some papers
Administrivia

• Lectures:
  – Mon 1600-1800, LB04
  – Thur 0900-1000, LB01

• Dates:
  – Term: Today -> April 6\textsuperscript{th}
  – Reading week: Feb 26\textsuperscript{th} – Mar 2\textsuperscript{nd}
  – Me away: week of Mar 19\textsuperscript{th}
    • Will let you know what’s on closer to time
Examination

- 80%/20% exam/assignments marking split
  - Old exam questions/solutions:
    - https://down.dsg.cs.tcd.ie/old-exams/index.html
- Assignment 1 (15%) “security considerations”
- Assignment 2 (5%) “security incident” or PR
- Due dates:
  - Due: any time up to the last day I'm marking exam papers, April 1\textsuperscript{st} if you prefer a date
  - Submit via blackboard – Module CS4407
    - Email me if any issues
Assignment Tasks

• Security Considerations:
  - 3-4 pages usually; use in dissertation/FYP
  - Discuss the security issues for your dissertation topic
  - See RFCs 3552, 6973 and W3C tech report on sec/privacy considerations
    https://www.w3.org/TR/security-privacy-questionnaire/

• Security Incident:
  - 1 page describing a significant incident that happens during the course saying why its significant
  - Or, a github PR that's accepted
Course Outline

• Introduction
• Security and privacy concepts
• (Enough) cryptography (AES, RSA, ...)
• (To grok) core security standards (TLS,...)
• Stuff that's interesting for the last few weeks
  – Ethics of disclosures
  – Snowdonia and consequences
  – More advanced crypto (ECC, FHE)
  – Firewalls/IDS, Spam, DNSSEC etc.
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
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

• 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
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 (0–310kHz), 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: a hijacked ISP router, a compromised SIM card factory, etc.
Possible Bad Actors

• Disgruntled employees (*plenty*)
• Crackers (*hackers*)
• Script-Kiddies (*cracker wannabes*)
• Spies (*industrial and military*)
• Criminals (*thieves, organized crime*)
• Terrorists
• Governments
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
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
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
Other terms not yet mentioned

• Snowdonia/pervasive monitoring
• Usable Security
• Trusted computing
• Digital rights management
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
Puzzle

(If you know the answer already, please STFU/stay quiet!)

How do you send a secret message via courier (when you don't trust the courier)?