JÖNKÖPING UNIVERSITY
School of Engineering

Seminars – 2.5 ECTS

Information Security, 7.5 ECTS

Erik Bergström
erik.bergstrom@ju.se

Overview

- ILO
- Seminars

Intended learning outcomes

Intended learning outcomes	Examined elements	Learning activities
Display knowledge of basic concepts, principles, laws, models, and standards within the area of information security	Written examination	Lectures
Display knowledge of recent cases of **data breaches** and/or information leakage, and **show an understanding of the underlying reasons**	Written examination, seminar	Lectures, seminars
Display knowledge of how information security is practiced in an organization	Written examination	Lectures
Display knowledge of technical and administrative security mechanisms	Written examination	Lectures
Demonstrate the ability to **search for and present relevant research** results **related to current events and/or trends** within the field of information security	Seminar	Lectures, seminars
Demonstrate the ability to **analyze and reflect over current events and/or trends** within the area of information security	Seminar	Lectures, seminars
Demonstrate the ability to **reflect over how vulnerabilities** in information systems **affect organizations and society**	Written examination, seminar	Lectures, seminars

What will we do?

- Three parts/assignments
  - Seminar 1 - Ethics in cybersecurity research and practice
  - Seminar 2 - Encryption
  - Seminar 3 - Threats and vulnerabilities

- 1-3 also reflect the workload (1 least)

Gah – theoretical?!

- Many ideas
  - Our lab
  - Virtual machines
  - Install on your computers
  - Hacking challenges
  - …
- Too much risk with different hw/sw
- Many topics require a background in OS/dcom/math/…
  - Course is G1N
- Corona limits attendance
- Supervision is harder online

- Want more practical → network security, wireless networks,…

Seminar 1 – Ethics in cybersecurity research and practice

- Aims at introducing more about ethics in our field.
- Seminar on a paper by Macnish and van der Ham (2020)
  - Ethical issues in two case studies
    - University-based development
    - In the community of practising cybersecurity experts

Macnish, K. and van der Ham, J. (2020), "Ethics in cybersecurity research and practice", *Technology in Society*, Vol. 63, p. 101382.

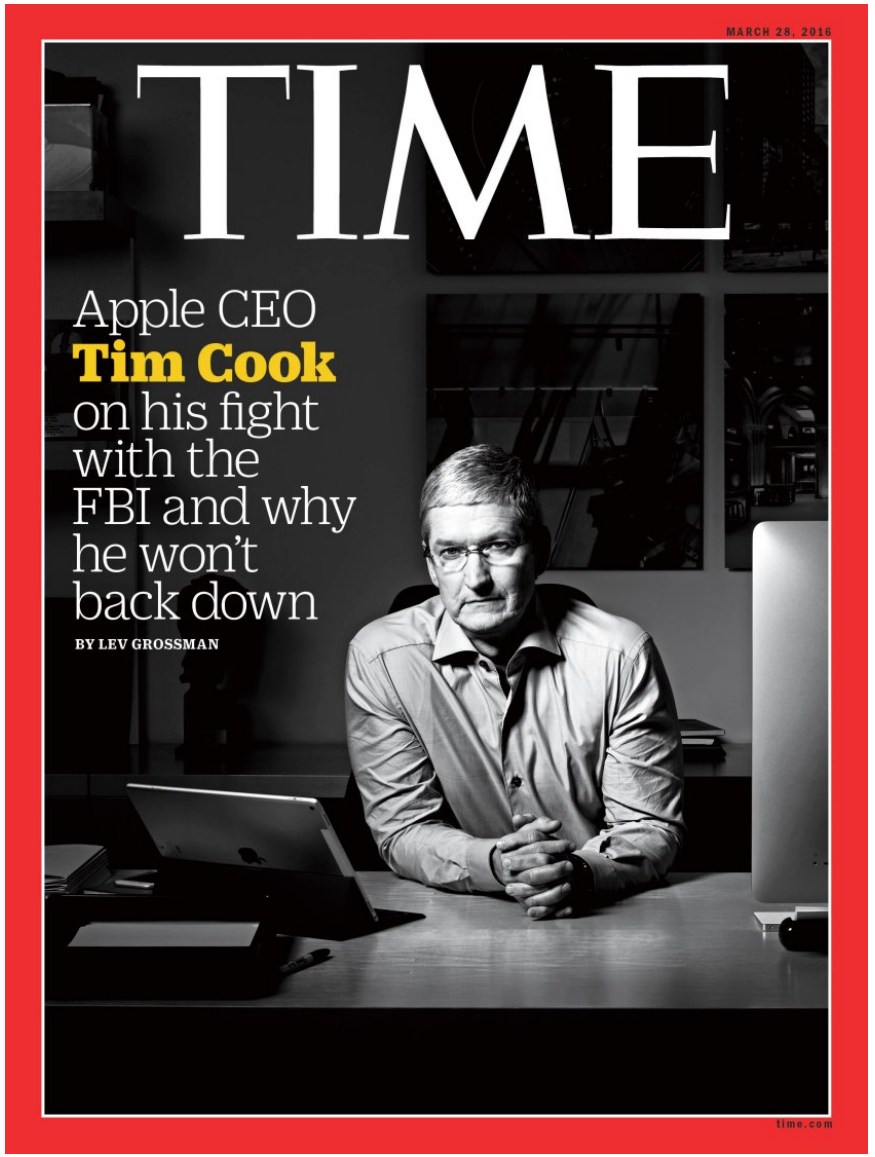
Seminar 1 - Assignment

- Individual assignment.
- Submit a summary with key learnings from each case, from *your* perspective.
  - Deadline before the seminar.
  - ~500 words summary.
- Include two questions for the seminar.
- Active participation in the seminar is required.

Seminar 2 - Encryption

- Ethics on the use of encryption has been discussed for decades.
- Can courts order manufacturers to help out unlocking cryptographically protected devices?

- FBI–Apple encryption dispute is most well known
- https://en.wikipedia.org/wiki/FBI%E2%80%93Apple_encryption_dispute



Seminar 2 - Encryption

- Generally believed that the police and intelligence agencies must be allowed to snoop
- Should we be allowed access to strong encryption that render lawful interception impossible?

- John Sawers, former head of the Secret Intelligence Service (aka MI6) said in November 2014:
  - *"There is a dilemma because the general public, politicians and technology companies, to some extent, want us to be able to monitor the activities of terrorists and other evil-doers but they don't want their own activities to be open to any such monitoring."*

https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11356645/Ex-MI6-chief-Sir-John-Sawers-We-cannot-stop-terrorism-unless-we-spy-on-innocent-people.html

Seminar 2 - Encryption

THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT | OUR AGENCY | PRIORITIES | NEWS | RESOURCES | CAREE

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice
Office of Public Affairs

FOR IMMEDIATE RELEASE — Sunday, October 11, 2020

International Statement: End-To-End Encryption and Public Safety

We, the undersigned, support strong encryption, which plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security. It also serves a vital purpose in repressive states to protect journalists, human rights defenders and other vulnerable people, as stated in the 2017 resolution of the UN Human Rights Council[1]. Encryption is an existential anchor of trust in the digital world and we do not support counter-productive and dangerous approaches that would materially weaken or limit security systems.

https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Facebook behind 94% of child abuse image reports by US tech firms last year

Metro Tech Reporter Monday 12 Oct 2020 10:57 am

Facebook is responsible for a lot of the online child abuse that gets posted (Credits: Dan Kitwood)

Facebook was responsible for 94% of the 69 million child sex abuse images reported by American technology companies last year.

The figures emerged as seven countries, including the UK, published a statement on Sunday warning of the impact of end-to-end encryption on public safety online.

https://metro.co.uk/2020/10/12/facebook-behind-94-of-child-abuse-image-reports-by-us-tech-firms-last-year-13407633/

THE Sun — THE SUN, A NEWS UK COMPANY

WS | MONEY | DEAR DEIDRE | TECH | TRAVEL | MOTORS | PUZZLES

All News | UK News | World News | Brexit | Politics | Opinion

PRITI PATEL Facebook's changes to encryption will only help terrorists and paedophiles

COMMENT

Priti Patel, Secretary of State for the Home Department
10 Oct 2020, 23:34 | Updated: 10 Oct 2020, 23:34

19 Comments

A YEAR ago, I asked Facebook founder Mark Zuckerberg not to risk lives with the company's plan to bring in end-to-end encryption.

Today, I am leading international action to amplify that call and to ask all tech companies to put the safety of children first.

https://www.thesun.co.uk/news/12899271/priti-patel-facebook-help-terrorists-paedophiles/

Seminar 2 - Encryption

- Should companies be able to read stored encrypted user data?
- Should companies answer legal law enforcement requests?
  - Or only for certain types of threats, such as terrorists?
- Should we have backdoors?
- Should we limit automatic encryption?
- If we don’t encrypt, how can we safely store and transmit sensitive information?
- Is it not my individual right to protect my (sensitive) information?

Seminar 2 - Assignment

- Individual assignment.
- Prepare a one-page report (excl. references) taking a stance on either:
  - 1) Limiting the use of encryption for companies and individuals so that law enforcement and intelligence agencies can get access to information.
  - 2) Allowing companies and individuals to use any encryption they wish, regardless of the consequences.
- Need to join seminar group.
  - For or against ultimately depends on timing (equal number for/against).
  - You decide what group you want to belong to.
- Use at least five scientific references supporting your claims.
- Should use proper referencing.
- Submit report one day before the seminar.
- Active participation in the seminar is required.

Seminar 3 - Threats and vulnerabilities

- Select a recent security breach featured in the national or international press.
- Based on the breach, identify:
  - What type of breach was it?
    - Describe the general type of attack.
  - What was the vulnerability?
    - Describe the general type of vulnerability.
  - Describe the threat?
  - What can/could be done?
    - Both in general and specific.

Example – Ransomware @ University Hospital Düsseldorf

- September 10th, 2020 the UKD suffered a ransomware attack.
- 30 servers were invaded and caused crashing systems
- Forced the hospital to turn away emergency patients.
- A woman in a life-threatening condition died because she was forced to go to a more distant hospital.

The New York Times

Cyber Attack Suspected in German Woman's Death

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.

The ransomware attack involved servers at the University Hospital Düsseldorf on Sept. 10. Roland Weihrauch/dpa, via ZUMA Press

https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html

Example – Ransomware @ University Hospital Düsseldorf

- The ransom note left on the encrypted servers were incorrectly addressed to Heinrich Heine University.
- Police contacted the threat actors to explain that they encrypted a hospital.
  - The ransomware operators withdrew the demand and provided a decryption key.
- German prosecutors are now investigating possible manslaughter charges.
- Highly unlikely arrests will be made.

Example – Ransomware @ University Hospital Düsseldorf

- Someone compromised their network using a software vulnerability in *"a commercial add-on software that is common in the market and used worldwide."*
- Citrix VPN products suffer from the ADC CVE-2019-19781 vulnerability.
  - The vulnerability allows unauthenticated users to utilize directory traversal to perform arbitrary code execution
- Patches were available in January 2020.
- Hospitals are prime targets of ransomware attacks from some operators.
  - Increased likelihood that victims will pay their extortionists.

Seminar 3 - Assignment

- Work two-and-two (self-organized)
  - But contact me if you need help to team up.

- Submit a two-page report (excl. references) one day before the seminar.
- Use scientific references supporting your claims.
- Use proper referencing.

- Presentation + questions = 10 min (~7+3)
  - Use slides.
  - Both group members need to present.

Time plan

	Seminar 1 (Ethics in cybersecurity research and practice)	Seminar 2 (Encryption)	Seminar 3 (Threats and vulnerabilities)
Week 43			
Week 44	Supervision		
Week 45	Seminar 1, and hand in entry ticket		Supervision
Week 46		Supervision	Supervision
Week 47		Supervision	Supervision / Mandatory check with supervisor / Registration in Canvas
Week 48		Seminar 2, and hand in the report	
Week 49			Supervision
Week 50			Seminar 3, presentation, and hand in the report
Week 51	Reserve	Reserve	Reserve

JÖNKÖPING UNIVERSITY

School of Engineering