TDDE61 Ethical hacking Lecture 2: Laws and regulations

Mikael Asplund

LINKÖPING UNIVERSITY

Disclaimer:

I am not a lawyer and I have no legal training

Swedish law

Brottsbalken 4 kapitlet 8 §

Den som olovligen bereder sig tillgång till ett meddelande, som ett post- eller telebefordringsföretag förmedlar som postförsändelse eller i ett elektroniskt kommunikationsnät, döms för brytande av post- eller telehemlighet till böter eller fängelse i högst två år. *Lag (2012:280).*

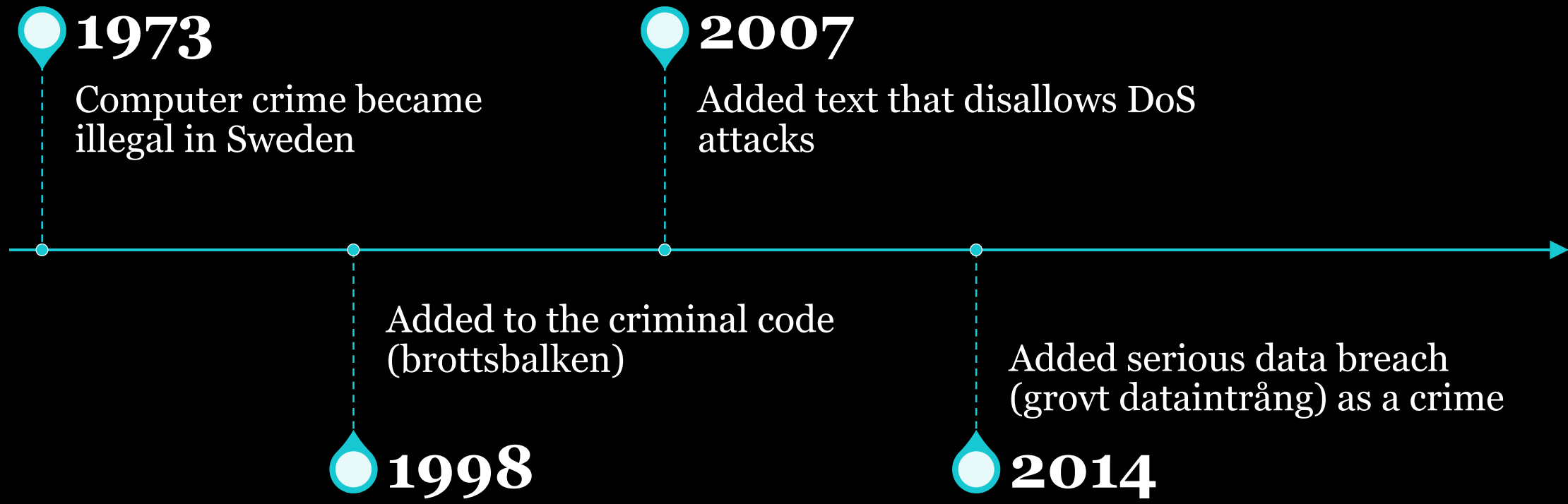
Anyone who without permission obtains access to a message, which a postal or telecommunications carrier conveys as a postal item or in an electronic communication network, is sentenced for breaching postal or telecommunications secrecy to a fine or imprisonment for a maximum of two years. Law (2012:280).

Brottsbalken 4 kapitlet 9 c §

Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.

Anyone who without permission obtains access to data that is intended for automated processing or without permission changes, erases, blocks or enters such data into a register is sentenced for data breach to a fine or imprisonment for a maximum of two years. The same applies to anyone who without permission, through any other similar measure, seriously interferes with or prevents the use of such information.

Some history



Case NJA 2014

- A Swedish policeman L.-E.N. searched for himself in the Police's registry of suspects in 2010
- L.-E.N. had authorization to access the systems in his job role
- The search on himself was not performed as part of his job-related duties as a police officer
- Convicted of data breach by the Swedish supreme court

Case RH 2015-5

- In 2009 an employee of a company installed the software Google Talk on his job computer without permission (and in violation of company policies)
- Convicted in the lower court but acquitted in the Court of appeal (Hovrätten)
- The reason: installing software is not “entry of information into registers” (införande av uppgift i register) and therefore not criminalized
- Exactly what kinds of unwanted software installations that are illegal seems not so well-defined.

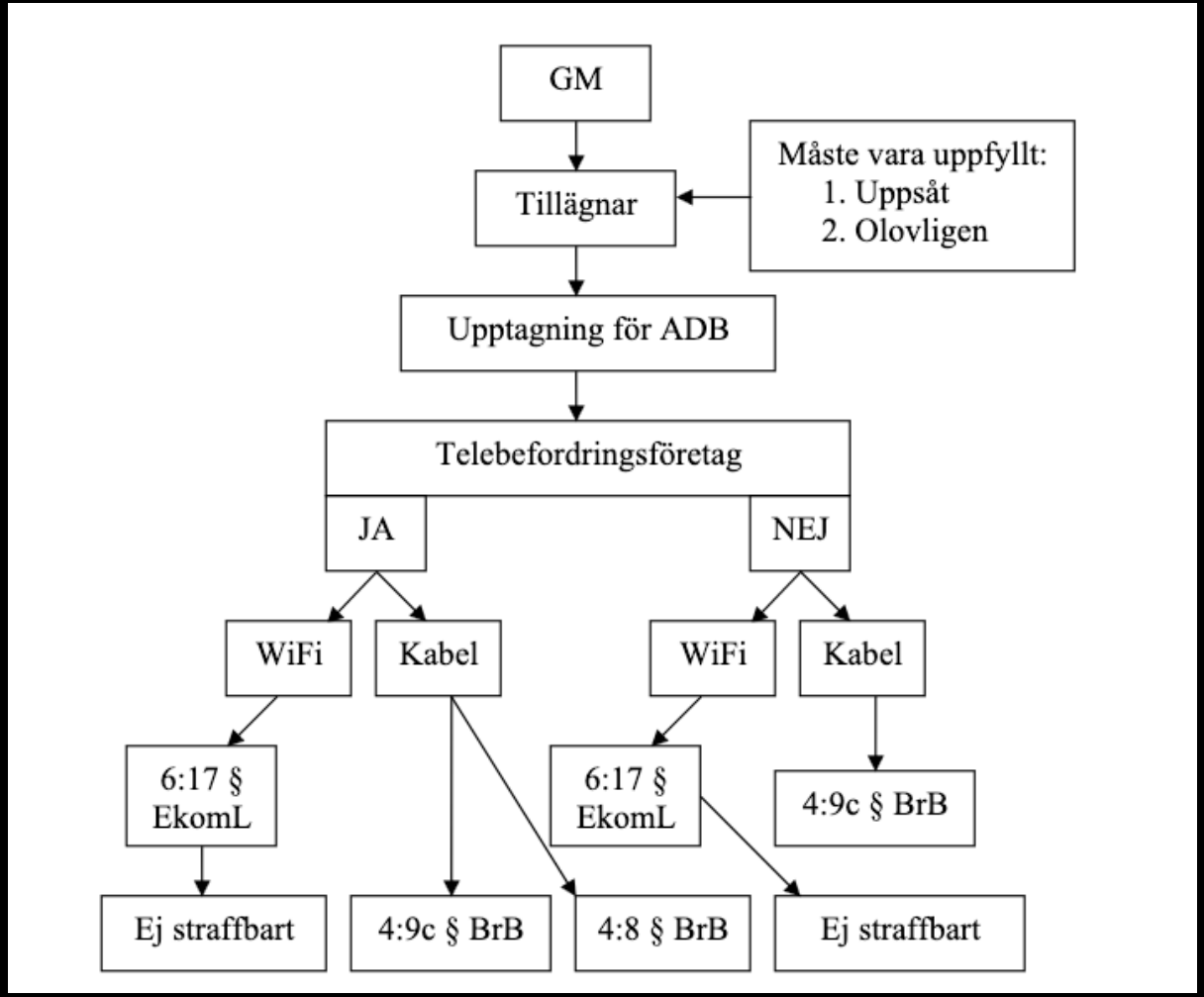
E. Woodcock, Svensk Juristtidning 2015, https://svjt.se/svjt/2015/862

Case RH 2006:80

- Member of cracker group DrinkOrDie downloaded copyrighted software and developed cracks
- The cracks were distributed to other cracker groups
- Acquitted in the lower court (right to reverse engineer), but sentenced in the Appeals Court for copyright infringement
- The right to reverse engineer only applies to private use

Non-trivial to decide

- Hypothethic Sniffing case
- ADB: Automated processing
- EkomL: Law on electronic communication
- I. Rydlund “Otillåtet eller inte? En analys av dator- och datarelaterade gärningar ur ett brottsbalksperspektiv”, Lund 2004



Very few convicted cases

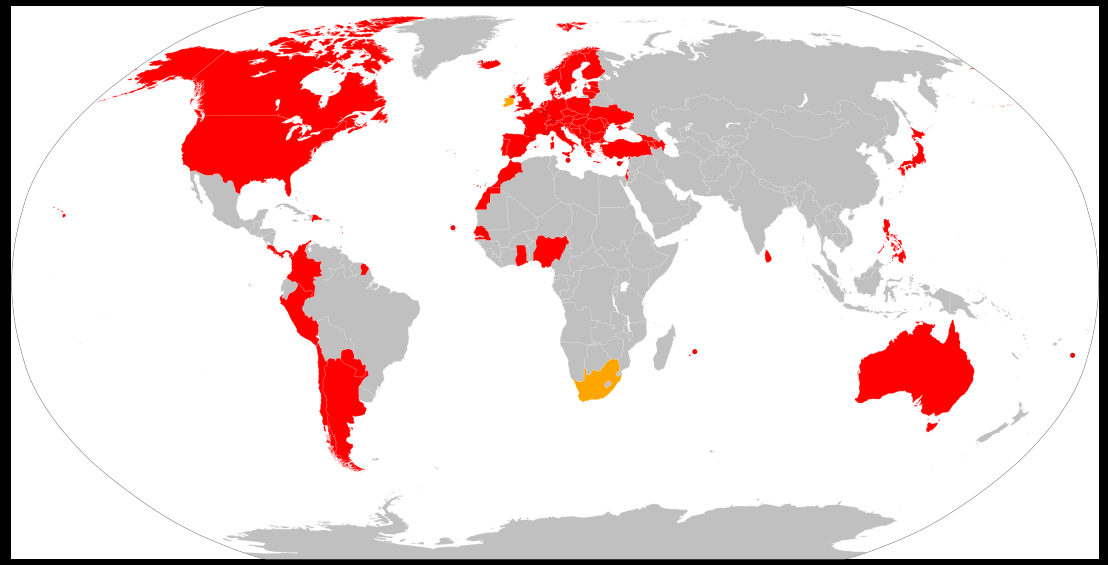
	Överbelastning		Skadlig kod		Registerslag.		Sociala med.		Övrigt		Totalt
	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel	Antal	Andel	Antal
Personuppklarade ärenden	1	4 %	0	0 %	24	24 %	0	0 %	2	1 %	27
… varav åtal väcks	1	4 %	0	0 %	19	19 %	0	0 %	2	1 %	22
… varav strafföreläggande	0	0 %	0	0 %	5	5 %	0	0 %	0	0 %	5
Avskrivning/nedläggning	23	85 %	125	81 %	62	63 %	119	99 %	232	96 %	561
… varav direktavskrivning	10	37 %	49	32 %	20	20 %	76	63 %	167	70 %	322
… varav FU läggs ned	13	48 %	76	49 %	42	42 %	43	36 %	65	27 %	239
Saknas avslutande beslut	3	11 %	30	19 %	13	13 %	1	1 %	6	3 %	53
Totalt	27	100 %	155	100 %	99	100 %	120	100 %	240	100 %	641

https://bra.se/download/18.57223f611841889cd023b5/1666871966529/2022_Polisanmalda_dataintrang.pdf

International law

Budapest Convention on Cybercrime

- Council of Europe + observer states
- Signed 2001, entered into force 2004
- Harmonizing legal frameworks and enabling mutual legal assistance



UN Cybercrime Treaty

- Resolution passed in 2019
- Negotiated since 2022
- Aiming to finalize 2024
- Main points of discussion/contention: scope, human rights safeguards, etc

EU law

EU regulates heavily on cybersecurity

- NIS and NIS2 directives
- General Data Protection Regulation (GDPR)
- EU Cybersecurity Act (regulates ENISA)
- Cyber Resilience Act (CRA)

EU regulates businesses, not crimes

US law

Computer Fraud and Abuse Act (CFAA)

- Enacted in 1986, amended several times since
- Criminalizes
  - Accessing a computer without authorization or exceeding authorization
  - Causing damage to computers
  - Extortion involving computers
  - …
- Severe penalties (up to 10 years), and allowing civil cases
- International reach

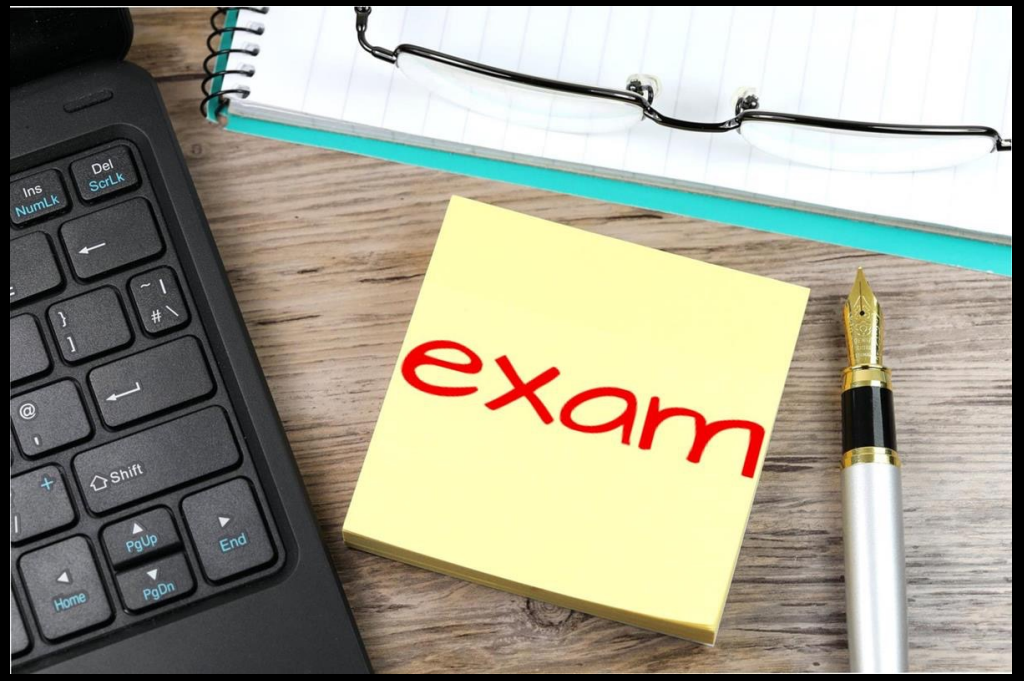
Digital Millennium Copyright Act (DMCA)

- More wide-ranging than Swedish copyright law
- Strict anti-circumvention provisions
- Exemptions exist, including a temporary one for “good-faith security research”
- More reading:
  - Weigle, Katherine (2018) "How the Digital Millennium Copyright Act Affects Cybersecurity”, Intellectual Property Brief: Vol. 9 : Iss. 1 , Article 1. Available at: https://digitalcommons.wcl.american.edu/ipbrief/vol9/iss1/1
  - https://www.eff.org/issues/coders/reverse-engineering-faq

On the exam

Exam

- 15 multiple choice questions
- 10 needed to pass
- Each question 0 or 1 point. All correct options needed to get 1p.



Det här fotot av Okänd författare licensieras enligt CC BY-SA

Exam practicalities

- Performed in the computer lab rooms on the computers
- No internet access, no aids allowed
- Simple text file, all instructions and questions are found in the text file.

Example question

- Which of the following authorized actions on data are explicitly prohibited by the Swedish criminal code?
  - A: changing
  - B: erasing
  - C: waiting for
  - D: obtaining access to

Example question #2

- Launching a Denial-of-Service (DoS) attack against a major Internet Service Provider (ISP) is
  - A: Illegal
  - B: Legal since a major ISP can handle it
  - C: The legal status of DoS attacks in Sweden is not clear

Example question #3

- Which of the following are legal directives or acts from the European Union related to cybersecurity?
  - A: ENIST
  - B: GDPR
  - C: NIS2
  - D: DMCA