IT security

Monday 15th April
Course day #10

Final course day
Ethics
Security breaches of 21st century

Niels Christian Juul (ncjuul@ruc.dk)
Niels Jørgensen (nielsj@ruc.dk)

We have covered all four themes :)

A. Computer security technology and principles (Part One in Stallings & Brown)	11th Feb 18th Feb 25th Feb
B. Software and system security (Part Two)	11th March
C. Management issues (Part Three)	4th March 18th March 25th March
D. Network security (Part Five)	1st April 8th April

Literature and exam questions for today

Stallings & Brown:
- 19.4: Ethical issues

Additional mandatory literature:
- Taylor Armerding. *The 18 biggest data breaches of the 21st century.* (18th Dec. 2018, www.csoonline.com).

Exam questions
- Q19: "Internet/E-mail security policy - from theory to examples"
- Q20: "Describe important, current data ethical dilemmas and how an ethical code of conduct can address them?"

Plan for today

- The five biggest security breaches of 21st century. (Niels J.)

Ethical codes. (Niels Chr.)

Course evaluation (continued from course day #9).

Q/A about the oral exam and the assignment.

Five biggest security breaches 21st century #1

First, I picked three US data breaches
(from the csonline article)

Yahoo, 2013-2014
- published in 20017

Data
- account data (passwords, names, emails)
- 3 billion user accounts
- users may have multiple accounts
- most passwords protected by weak form of hashing

Estimated cost
- 350 mill. usd
- (lower purchase offer from Verizon)

Five biggest security breaches 21st century #1 (cont.)

Hackers

- FBI suspected Russian hackers
  - perhaps intension to spy on Russian and US users of Yahoo
- used email with malign attachments
- + similar simple techniques
- gradually got more and more access
-

Lesson:

- password files must be salted and strongly hashed
- large websites must have extra measures to protect password file
  - such as residing on a separate host
  - and other measures

Five biggest security breaches 21st century #2

Heartland Payment Systems, 2008.
- a large finansial service institution
- 6th-8th largest payment processor in US

Data
- 134 mill. credit cards were compromised (card# + name)

Cost, impact
- Heartland lost approval for transaction processing for four months

Hacker:
- motive was to sell credit card data
- Albert Gonzales sentenced to 20 years
- (same A.G. convicted in TJ Maxx case)

Heartland PAYMENT SYSTEMS®

The Highest Standards | The Most Trusted Transactions

Five biggest security breaches 21st century #2 (cont.)

Malicious software on systems from 2007
- only discovered in late 2008 efter several months of analysis

To begin with, Heartland did not notice the malware
- alerted by Visa and Mastercard about suspicious transactions

Malicious software was propagated using SQL-injection attack
- webserver with relational database
- webclient is allowed to execute certain pre-defined SQL-queries
- SQL-injection attack is to force the webserver to execute SQL-commands defined by attacker
- effect similar to buffer overflow, though method is different

Heartland
PAYMENT SYSTEMS®
The Highest Standards | The Most Trusted Transactions

Five biggest security breaches 21st century #3

JP Morgen Chase, 2014
- largest bank in the US

Data
- on 76 mill. households
- two out of three US households
- names, addresses, phone numbers and email addresses
- no account information leaked
- no money transfers made
- info. could be used in phishing attacks

Hackers
- four israelis accused
- one sentenced 4,5 years
- another released, fined 403 mill. usd
  - (including fines for other hacks?)

Five biggest security breaches 21st century #3 (cont.)

Intruders had root/superuser privileges on 90% of servers

- gained access to a “forgotten server”
- that did not implement two factor authentication
- still required name/password of one employee

Five biggest security breaches 21st century #4

Not Petya
- important in terms of impact on company
- 200-300 usd ++
- (not a US company)
- (not a *data* breach)

Impacted company's ability to operate

Fake ransom message
- malware was purely destructive

Lessons include: update
- attack exploited Windows vulnerability for which patch existed

Five biggest security breaches 21st century #5

The failure to update SSL/TLS
- heartbleed vulnerability of OpenSSL library
- used in Mac, Linux, ..
- used by HTTPS and many other protocols
- discovered in 2014

Many websites took years to update OpenSSL
- in 2017 a study claimed 200.000 vulnerable websites
- so, do your updates
- even though it takes time and involves dependencies

Plan for today

The five biggest security breaches of 21st century. (Niels J.)

Ethical codes.

Course evaluation (continued from course day #9).

Q/A about the oral exam and the assignment.

Plan for today

The five biggest security breaches of 21st century. (Niels J.)

Ethical codes.

Course evaluation (continued from course day #9).

Q/A about the oral exam and the assignment.

Course evaluation

My reading of the students' evaluation
- in general, students express satisfaction with the course
  - with cases, student presentations,
    broad range of topics, friendly environment
- several students asking for more practical exercises
- some students
  - would like more external (business) presenters
  - feel teachers' presentations reiterate textbook

My take on the course's future
- retain textbook (even though centered on US/standards),
  cases, student presentations
- more practical exercises
  - nmap, wireshark, produce a certificate, ..
- perhaps an over-all case

DriveGreen security policy

Threat #1: ..
Threat #2: ..

Plan for today

The five biggest security breaches of 21st century. (Niels J.)

Ethical codes.

Course evaluation (continued from course day #9).

Q/A about the oral exam and the assignment.

Assignment

Hand-in May 1st at 12.00
- mandatory
- (though oral exam is by far the most important basis for grading)

Groups of up to three students may work together on an assignment
- each member hand in a copy
- all member names stated (front page of assignment)

4.800 - 48.000 characters
- 2-20 pages
- you are strongly encouraged to limit assignment to 2-5 pages
- for example, three pages provide space for 6-7 questions per page

Assignment example

Question 17: “What are the main security challenges of wireless networks?”

“I will explain the challenges using the fictive example of GreenDrive (provided in Niels J’s lecture). Company network includes laptops and mobiles which are connected by wi-fi to servers and internet. Challenges include rouge endpoints, rouge access points, and employees’ mobile phones that are weakened and possibly compromised. The challenges should be be identified in a written security policy”.

Assignment alternatives

An alternative style with keywords/headlines, for instance:

“Fictive example of GreenDrive (Niels J’s lecture). Company network: laptops + mobiles, connected by wi-fi to servers and internet. Challenges: rouge endpoints + rouge access points + weakened employees’ mobile phones. Written security policy”.

Especially if you use keywords/headlines, then remember:
- of course the keywords you provide must make sense
- use your own words - the plagiarism rules apply

Alternative topics: you may emphasize, for instance:
- The CIA++ goals
- The Wi-Fi standards
- ..

Oral presentation plus Q/A

Preliminary date: Thursday-Friday 6th-7th June.

Question 17: “What are the main security challenges of wireless networks?”

In your oral presentation, you may supplement your assignment,
by explaining, for instance

- why is a wireless network used in the first place?
- expand on the threats
- perhaps also mention some countermeasures (Q18)

In the Q/A section of the oral exam

- we will mainly ask questions about the selected exam question
- we may also ask questions about other exam questions
- and your assignment