Advanced Web Security

Introduction

People

- Lectures and course responsibility
  - Martin Hell (martin.hell@eit.lth.se)
- Home Assignments & Laboratory
  - Jonathan Sönnerup (jonathan.sonnerup@eit.lth.se)

Course goals

- Get deeper understanding of certain web based techniques/protocols/procedures related to security
- Understand how some advanced cryptographic techniques can be used to construct security solutions
- Get hands-on experience of some web application based attacks and defences.

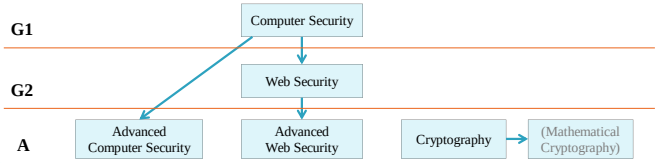
Layout

- 7 lectures
  - Lecture notes and slides will be available before or after lecture
  - Not everything will be covered by lectures
- 5 sets of home assignments
  - Basis for your grade (U/3/4)
- 1 Laboratory
  - Need to pass (0/1)
- Oral exam
  - If you want to change grade (4 → 5)
- For this you get 7.5 hp

Advanced level (A-Course)

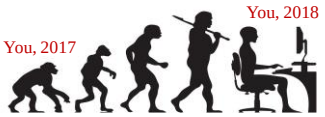
Högskolelagen:

- Jämfört med grundnivå, så ska A-nivåkurser
  1. Innebära fördjupning avseende kunskaper, färdigheter och förmågor
  2. Ytterligare utveckla studenternas förmåga att självständigt integrera och använda kunskaper
  3. Utveckla studenternas förmåga att hantera komplexa företeelser, frågeställningar och situationer
  4. Utveckla studenternas förutsättningar för yrkesverksamhet som ställer stora krav på självständighet eller för forsknings- och utvecklingsarbete

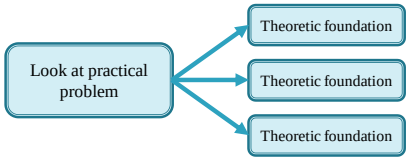


More Course Goals

- Train engineering skills



- Give theoretic understanding from practical problem – not the other way around



Home Exercises

- 5 sets of home exercises. Each set consists of 3 subsets
- **A-type**
  - Quite simple, check basic understanding of material
  - 8 randomly chosen problems (out of x > 8), you solve them individually
  - 0-1 points on each (one decimal)
- **B-type**
  - Look at related material
  - 2-4 problems, you solve them in groups of 1-2 people
- **C-type**
  - One additional problem if you want grade 4, solve in groups of 1-2 people

Grading

- **A-type** (40 points in total)
  - Grade 3: 25
  - Grade 4: 32.5
- **B-type**
  - Finishing all problems will give you grade 3
- **C-type**
  - Finishing all problems will give you grade 4
- You need grade 3 on A and B to get grade 3
- You need grade 4 on A, grade 3 on B and grade 4 on C in order to get grade 4

- If you qualify for grade 4, you can get grade 5 after taking an oral exam
  - Talk to Martin if you are interested in this

Handing in and marking A-type assignments

Handing in A-assignments

- A-type are handed in online
- **Your solution is anonymous. No name should be on your solutions sheet**
- Hand in one pdf file. Remember to include the question as well as the answer

- More details will be given on webpage

Handing in and marking A-type assignments

Marking A-assignments

- You will typically not mark assignments that you solved yourself (but some will overlap)
- You will be responsible for marking 2 other assignments
  - These will be given to you after the deadline for solutions
  - Upload your marking sheet before the deadline for markings.
- Marking sheet
  - For each assignment, give score 0.0-1.0 and **motivate** the score. A typical motivation could be to provide a reference to where the answer can be found (slide, page number in lecture notes or external source).
  - Failure to motivate the score will result in reduction of your own score
  - A mistake in marking gives no penalty if your marking attempt is serious
- Two students will mark your assignment
  - Your result will be visible after deadline for handing in markings
  - Your score is the average of the two scores
  - If you do not agree on the score, contact Jonathan.

Handing in and marking B- and C-type assignments

- All assignments will be answered in or uploaded to Moodle.
- Code and reports will also be sent to urkund

- Some problems will be marked manually, but most will be marked automatically by Moodle
  - You have one chance to provide the correct answer
  - There will be test quizzes that you can use to test your answers

- You may program in any language of your choice
  - BUT…Python is strongly recommended over Java, C and C++

Rules for home exercises

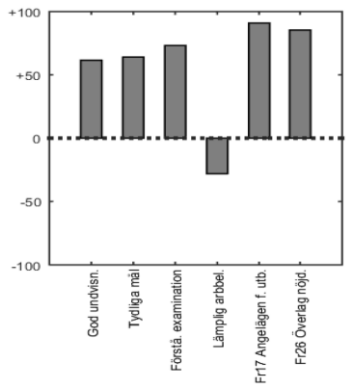
- You are allowed and encouraged to discuss all aspects of the exercises with your classmates
- All solutions should be constructed individually
  - or in groups of 2 for B-type and C-type
- Answers, or parts of answers, copied from other sources are not allowed.
- You are allowed, and sometimes must, use information from sources outside the lecture notes
  - It is your responsibility to find this information and it is a part of the course to actually find it and correctly relate it to the topics discussed on lectures
- **Keep the deadline!**
  - It will not be possible to upload any files after the deadline.
  - Instead, you can replace your file for A-type assignments as many times as you want before the deadline.

- **Feedback:** Jonathan will announce office hours where you are welcome to get feedback on your assignments. See webpage.

Laboratory

- Week 7.
  - Three slots, study week 7. Sign up on web page.
- Will cover some topics you learnt in the Web Security course, with focus on deeper understanding
  - SQL injections
  - XSS attacks
  - ModSecurity (which you did not learn in Web Security)

Last year



Some comments

Good, but time consuming

En av de bästa kurserna jag läst. Den kändes relevant. Arbetsbördan var visserligen ganska tung men man lärde sig verkligen mycket och såhär i efterhand känns det som att väldigt mycket fastnade dessutom.

Different views on peer assessment

Hemuppgifterna var ett grymt bra sätt att arbeta med materialet, man lärde sig väldigt mycket av att först jobba med det själv, och sedan repetera och se någon annans tolkning med kamratgranskningen.

Att man fick en bred förståelse pga rättningen av andra elevers arbete.

Det känns som att rättningen av A-uppgifterna hade kunnat fungera lite bättre, men vet inte riktigt hur.

Other Comments

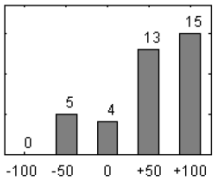
På något sätt måste man lösa problemet med folk som åker snålskjuts på de ambitiösa. Den personen jag jobbade med kommer i dagsläget få en 4a i denns kurs, men denna har i själva verket inte förstått någonting eftersom jag gjort alla inlämningar.

Changes: Fewer assignments this year. You can also do even fewer if you only want grade 3.

Course specific evaluation questions (from 2014)

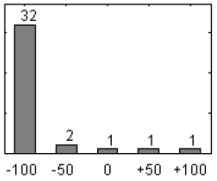
Resultatet av de kamraträttade uppgifterna kändes överlag rättvist.

+51



Jag hade hellre haft en traditionell skriftlig tenta.

-85



Course content

- Electronic payments
  - How do credit and debit card payments work, online and offline?
  - Untraceable e-cash, how can we produce electronic money that can not be traced to a particular user and cannot be double spent?
  - How can micropayments be realized?
  - Application of cryptography: Bitcoin (crypto currencies)
- Anonymity
  - What is anonymity and how can it be enforced?
  - What limitations exist?
  - How does Tor achieve anonymity and to which extent?

Course content

- eVoting
  - What is required by a secure voting system?
  - Is it possible to securely vote over the Internet?
  - How can a voting protocol be implemented?
- Secure messaging with OTR
  - How can we allow people to talk online, guaranteeing confidentiality and integrity but introduce deniability?
  - How can we use low entropy secrets in order to negotiate secure symmetric keys in the presence of a MitM?

Course content

- Single Sign-on + OAuth
  - How can single sign-on be realized using e.g., OpenID and SAML?
  - How can services get access to each other using OAuth?
- Data representation and PKI
  - How can we represent the data when sending it over a network or storing it on files?
  - How do we represent a public key, or a private key?
  - How are certificate represented?
  - How can we use asymmetric cryptography without a PKI?

Assumed knowledge

- It is assumed that you have taken
  - Computer Security
  - Web Security
- …and that you are familiar with
  - Symmetric vs. Asymmetric encryption
  - Hash functions
  - Digital signatures
  - Message authentication codes
  - Diffie-Hellman key exchange
  - Certificates
  - General understanding of web technologies