Welcome to

13. Summary and Exam Preparation

KEA Kompetence Computer Systems Security

Henrik Kramselund he/him han/ham hlk@zencurity.com @kramse

Slides are available as PDF, kramse@Codeberg

13-summary-software-security.tex in the repo security-courses

Goals and Plan for today

Go through exam reading list, Literature list walkthrough, Subject list walkthrough

Trial exam, show how it works

Photo by Chris Benson on Unsplash

Literature list walkthrough

Our reading list is at:

https://github.com/kramse/kea-it-sikkerhed/blob/master/softwaresikkerhed/lektionsplan.md

Not all are required reading for the exam!

We will now go through the list and comment, ask questions

Selection criteria and goals:

- You should be able to read books, presentations, papers, vulnerability disclosures, hacker zines.
  Example Smashing The Stack For Fun And Profit, Aleph One
- You should be able to find and use tools and frameworks
  Example MITRE ATT&CK, OWASP guides,

Some are classic texts or from organisations and people you should KNOW after this course

A lot of resources are also linked throughout the course presentations

Overview Diploma in IT-security

Afgangsprojektet (15 ECTS)	
Der udvikles løbende nye valgfag til Diplom i it-sikkerhed. Disse vil løbende blive beskrevet i en allonge (bilag 2) til studieordningen.	
Sikkerhed i it-governance (it-sikkerhedsledelse) (5 ECTS)	Softwaresikkerhed (10 ECTS)
Videregående sikkerhed i it-governance (Videregående sikkerhedsledelse) (5 ECTS)	
Systemsikkerhed (10 ECTS)	
Netværks- og kommunikationssikkerhed (10 ECTS)	

Go through exam Curriculum

Primary literature:

- *The Art of Software Security Testing Identifying Software Security Flaws* Chris Wysopal
  ISBN: 9780321304865, AoST or the Green Book
- Web Application Security, Andrew Hoffman, 2020, ISBN: 9781492053118 called WAS below

Required reading are:

- Curriculum: Basically the chapters from the books AoST chapters 1-12 and WAS chapter 1-21
- Extra curriculum: lower priority, not all details are expected to be remembered Grayhat chapters 1-2, general programming and Grayhat chapters 11-13, buffer overflow
- We will now go through the curriculum and comment, ask questions

Our reading list is at:
https://github.com/kramse/kea-it-sikkerhed/blob/master/softwaresikkerhed/lektionsplan.md

Course Description

From: STUDIEORDNING Diplomuddannelse i it-sikkerhed August 2018
Indhold Modulet fokuserer på sikkerhedsperspektivet i software, blandt andet programkvalitet og fejlhåndterings samt datahåndterings betydning for en software arkitekturs sårbarheder. Elementet introducerer også til forskellige design-principper, herunder "security by design".

Viden Den studerende har viden om:
Hvilken betydning programkvalitet har for it-sikkerhed ift.:

- Trusler mod software
- Kriterier for programkvalitet
- Fejlhåndtering i programmer
- Forståelse for security design principles, herunder:
- Security by design
- Privacy by design

Færdigheder Den studerende kan:
Tage højde for sikkerhedsaspekter ved at:

- Programmere håndtering af forventede og uventede fejl
- Definere lovlige og ikke-lovlige input data, bl.a. til test
- Bruge et API og/eller standard biblioteker
- Opdage og forhindre sårbarheder i programkoder
- Sikkerhedsvurdere et givet software arkitektur

Kompetencer Den studerende kan:

- Håndtere risikovurdering af programkode for sårbarheder.
- Håndtere udvalgte krypteringstiltag

Final word is the Studieordning which can be downloaded from

https://kompetence.kea.dk/uddannelser/it-digitalt/diplom-i-it-sikkerhed

Studieordning_for_Diplomuddannelsen_i_IT-sikkerhed_Aug_2018.pdf

Subject list walkthrough

- 1. Trusler mod software, oversigt over hvordan sårbarheder i software opstår
- 2. Sikkerhed i udviklingsprocesser, Secure Software Development Lifecycle
- 3. Sikkerhed i web applikationer
- 4. Softwareproblemer med håndtering af hukommelse
- 5. Forbedret sikkerhed med opbygning af software i komponenter
- 6. Håndtering af tekststrenge i software, herunder tegnsæt
- 7. Netværksangreb mod software
- 8. Audit af software, samt almindelige fejl der skal håndteres
- 9. Security design og principper for sikkert design

Deliverables and Exam

- Exam
- Individual: Oral based on curriculum
- Graded (7 scale)
- Draw a question with no preparation. Question covers a topic
- Try to discuss the topic, and use practical examples
- Exam is 30 minutes in total, including pulling the question and grading
- Count on being able to present talk for about 10 minutes
- Prepare material (keywords, examples, exercises) for different topics so that you can use it to help you at the exam

Mundtlig eksamen og formalia

Eksamen varer samlet set i 30 minutter og forløber i 4 faser:

1. Du trækker indledningsvist ét af de 10 ovenstående emner
2. Du forklarer indledende emnet støttet af egne slides i op til 10 minutter
3. Herefter uddyber og diskuteres emnet i en dialog på 10 – 15 minutter
4. Afslutningsvist er der 5 minutters votering og karaktergivning

Karakteren vil være en helhedsbedømmelseaf din viden om emnet samt din evne til at uddybe og diskutere relevante IT-sikkerhedsmæssige elementer. Der gives karakter efter 7 trins skalaen.