TDDD17

Information Security

Department of Computer and Information Science (IDA)
Division for Database and Information Techniques (ADIT)
Agenda

- Overview of the course
  - Information security
  - Topics
  - People

- Organization of the course
  - Prerequisites
  - Examination
  - Optional labs

Course leader
Nahid Shahmehri

Course assistant
Ulf Kargén
Information security
A super-complex problem

• Adding two numbers is a problem that is well defined and can be solved using the same logic every time.

• Cooking an omelet is a more complex problem to define, but in theory applying the same solution again and again should yield the same result.

• Raising children is a super-complex problem, where you can not expect the same results time after time by applying the same method. It is also hard to anticipate your next move.

• Information security is a super-complex problem, we may have a theory and experience to guide us, but we can not anticipate the results each time.
Information security
A super-complex problem

- Making information security even harder is the fact that it encompasses many disciplines from IT:
  - Network security
  - User authentication
  - System security
  - etc.

- Furthermore, it contains activities that require teams rather than single individuals:
  - Risk analysis
  - Business continuity planning
  - Disaster recovery planning
  - Physical security
**Microsoft in more hacking misery**
Microsoft has been hacked again by the Syrian Electronic Army just weeks after a blog and social media sites were attacked by the group.
Hackers hit Syrian Electronic Army
Microsoft hit in rash of site hacks

**Stick-on screens offer new horizons**
Researchers develop a transparent plastic display that they say can turn any window into a movie screen.
HP patents see-through screens
The science of materials

**Video**

- Is this your future living room?
- Inside Mumbai's new international airport
- Ivory Coast tackles cyber crime
- Hybrid tablet 'switches seamlessly'

**Other Top Stories**

- Collymore accuses Twitter over abuse
  Former footballer Stan Collymore accuses Twitter of not doing enough to combat abusive messages after he was targeted by internet trolls.

- Millions of German passwords stolen
  The passwords and other details of sixteen million email users in Germany have been stolen, according to the country's security agency.

- UK set for faster internet on the go
  Ofcom has approved the use of earth stations on moving vehicles, meaning faster internet services for those on the move.

- EU wants big fines for data breaches
- Spotify adds shop as Dre preps rival
- Fans help fund Jamaica bobsleigh bid
- Huge data theft hits South Korea
- Nintendo shares fall on loss warning
- Chrome extras targeted by ad firms
- Obama 'to end NSA data hoarding'
- EE rushes to fix broadband box risk
- Google unveils 'smart contact lens'
- Fridge sends spam emails
First page of *BBC News Tech* the 14:th of Januari 2015.

**US military's Twitter account hacked**

US Central Command's Twitter and YouTube accounts are suspended after being hacked by a group claiming to be supporters of Islamic State.

**Obama calls for stronger data privacy**

US President Barack Obama has unveiled new proposals on how consumers' personal data is handled.

**'Sony-inspired' hack ends game work**

A hack attack "inspired" by the recent attack on Sony has led a developer to cancel creation of a game featuring Kim Jong-un.

**Grand Theft Auto V delayed for PC**

**Microsoft hits out at Google team**

**Two dead in LG TV factory accident**

**Hackers 'disable extremist website'**

**Experts pledge to control AI work**

**Google doodle honours Kenyan pupil**

**Sony: 'No playbook' for hack attack**

**Netflix: VPN crackdown claim 'false'**

**Universal sues over prison mixtapes**

**Ageing-tech expert sought by DWP**

**Ukraine blames Russia for German hack**
Can the government ban encryption?

By Jane Wakefield
Technology reporter

Whenever the terrorist threat is increased, as it has been since the tragic events in Paris last week, so too are the calls from politicians to increase the powers of the people they employ to protect the public from such threats.

Those agencies can only do their job, the argument goes, if they have full access to the online chatter of those planning terrorist atrocities.

As the UK’s Prime Minister David Cameron put it in a speech this week - there should be no “means of communication” which “we cannot read”.

But in an era when communication takes many forms, and with the added problem that much of this communication is encrypted, how easy is it to turn this sound bite into reality?
CISO – Chief Information Security Officer

- Lawyers
- IT experts
- Human resources
- Media
- Security experts
- Team leaders for core-services
- Team leaders for internal support
- External contractors
- Governments
- Security personnel
- You!
Overview of topics

- Risk analysis
- Network security
- Identification & Authentication
- Trusted computing
- System security
- Business Continuity Planning
- Disaster Recovery Planning
- Physical Security
Risk analysis

- Risk analysis from an information security perspective.

- Three hands-on methods for risk analysis:
  - CORAS
  - ISRAM
  - Attack trees

Marcus Bendtsen
- PhD student at ADIT
- Research focused on probabilistic graphical models.
Network security

- Secure network design
  - Partitioning
  - Security devices
  - Trust relationships

- Network security protocols
  - Network layer (IPSec)
  - Transport layer (TLS)

- Marcus Bendtsen
  - PhD student at ADIT
  - Research focused on probabilistic graphical models.
System security

- Operating system security
- File system security
  - Security mechanisms
  - Hardware support
- Trusted computing
  - New challenges in security
  - Basic principles
  - Virtualization
  - Execution environments
  - Mobile devices
- Robert Malmgren
  - Independent consultant
  - Scada security expert
  - IDG top security expert
- Ben Smeets
  - Professor @ Lund
  - Engineer @ Ericsson
  - Expert in trusted computing and mobile devices
Identification and authentication

- Basic principles
- Biometric authentication
  - Fundamental principles
  - Various types of biometrics
  - Threats and attacks
- Tokens and statistics
  - Types of tokens
  - Threats and attacks
  - Passwords
- Amund Gudmundson Hunstad
  - Researcher at the Swedish Defence Research Agency
BCP, DRP and PS

• **Business continuity**
  • How to plan for continued operations during a disaster
  • Concepts, e.g. business impact, analysis, recovery strategies, testing for disaster

• **Disaster recovery planning**
  • How to plan for when a disaster has affected the operations

• **Physical security**
  • Locks and keys, fire, water, etc.

• **Marcus Bendtsen**
  • PhD student at ADIT
  • Research focused on probabilistic graphical models.
ORGANIZATION
Prerequisites

• Basic security course is required
  • We will assume that you know some basic things

• Different recommended prerequisites for different topics
  • You may decide which topics to focus on based on your interests and previous knowledge (more on this later).

• Network Security – Basic knowledge of TCP/IP networks is recommended

• System Security – Basic understanding of operating system design and computer hardware is recommended.
Prerequisites

• Capable of independent study and research
  • Essential in the project phase…
  • …but also for when studying for the exam.

• Capable of producing a good quality project report
Organization

- Several different but related topics
  - You will learn some more than others
  - You may choose which ones to focus on
  - Topics may change from year to year

- Optional labs (more ahead)
  - Network security
  - Identity management

- Written exam (4 credits) and project (2 credits)
Examination

• Written exam (4 credits)
  • One general and one in-depth question per topic
  • You need to answer some general and some in-depth questions
  • You choose which questions to answer
  • Best to make up your mind which areas before the exam

• Exam rules
  • You may answer at most **three** general questions and **three** in-depth questions
  • You may answer both the in-depth and general question for **one topic only**.
  • Otherwise we will randomly discard answers!
Examination

- Project (2 credits)
  - Work in groups of two (no exceptions)
  - Choose from a list of topics (first-come-first-serve)
  - Must meet intermediate milestones and deadlines
  - Must produce written report and presentation
Labs (optional)

- Each of the two optional labs gives 2 bonus in-depth points each.
- Offer only valid for first three exams given.
- Labs are optional for a reason – Additional recommended prerequisites apply.

- Authentication and authorization
  - Learn about third-party authentication and authorization with OpenID Connect.
  - Design and implement your own authentication method.

- Firewall configuration
  - Analyze network requirements and risks and configure a firewall.
Other information

- Detailed schedule on the course homepage
  - Note: There are several reserve time slots when there will be no teaching. Check the schedule on the course homepage!

- Hand-outs will be available on the course homepage before lectures (usually no later than 1 day before, but no guarantees)

- Course literature on the course homepage
  - Hand-outs
  - Collection of articles and book chapters
Linköpings universitet
expanding reality

www.liu.se