T-110.5290
Seminar on Network Security

Today's agenda

1. Organization and overview
2. Course theme: security policies
3. Project topics
4. Timetable
5. Signing up for the course
6. First draft, full draft, final paper
7. What is a good seminar paper?

Organization

- Responsible teacher: Tuomas Aura
- Course assistant: Petri Savolainen
- All course material will be in Noppa
- Email alias: t-110.5290@tkk.fi
- Optima for paper and comments submission
- English course: Roger Munn
  - attendance mandatory for KIE-98.1700 (1cr)

Overview

- T-110.5290 Seminar on Network Security P (4 cr)
- Final-year MSc-level course
- Students write a technical paper (~7 pages)
  - format of a technical or scientific conference publication
- Requirements:
  - writing the paper (60%)
  - presentation in a two-day seminar (25%)
  - acting as opponent for another student (15%)
- Individual work, no groups
- Max ~30 participants by application

Course theme 2009

- Security policies – their specification and implementation
- Any security mechanism implements a policy, although not always explicitly specified
- Security failures are violations of the policy
- To design secure systems, we need to ask what is the (implicit) security policy
- Engineers need to understand the distinction between policy and implementation

Topic introductions

- Topics will be made available in Noppa
  (when Noppa is back online)
- Possible propose your own topic, but that has not always led to good results
  - Need a tutor anyway

- Tutors: please introduce yourself first, then use 1-2 minutes on each topic

Topics by Erka Koivunen

How to secure information about handling of sensitive information

In this assignment you should familiarise yourself with general telecommunications equipment (routers, DSLAMs, DHCPd, MSCs, GGSNs etc.) and understand what kinds of traffic logs they produces and how this information should be secured in order for the operators to comply with the law and regulations.

Limited User Account on Windows - just a dream?

In this assignment you should familiarise yourself with the policy enforcement tools available for the Microsoft Windows platform and devise a plan to lock down a user's desktops without compromising their ability to do their work. Alternatively, you can use other operating systems platforms such as Linux or OS X in an enterprise environment.

Acceptable Use Policies and their enforcement by the Internet Service Providers

In this assignment you should familiarise yourself with the requirements imposed on the Finnish ISPs and network access service providers by the regulation. You should compare how these requirements are translated into the service agreements, Netiquettes and other forms of AUPs. You should also discuss whether the rules are enforceable.

Topics by Sanna Suoranta

Privacy policies for student data at a university

This project will investigate the privacy and confidentiality policies for implemented at TKK for handling personal data of students.

Using student data for research

The goal of this seminar project is to investigate the regulations and norms that are in place for handling personally identifiable data about students when it is used for scientific research

Security policies for Single Sign On in Service Ecosystems

The goal of this seminar project is to investigate the security policies of currently used mashup services and think what kind of policies are needed for single sign on in distributed mashup services.

Topics by Boris Nechaev

Frameworks, toolkits and software suites for automated analysis of security policies

Debugging security policies is also non-trivial and as well prone to mistakes. To make the debugging and verification process more reliable a number frameworks for automated analysis of security policies have been implemented. The goal of this study is to make a survey of existing policy analysis toolkits and make comparison between them if applicable. (Note: The tutoring will be mostly by e-mail.)

Policies in Bro IDS

Bro is a popular Unix-based open-source Intrusion Detection System (IDS) used for both real-time intrusion prevention and off-line network traces analysis. The goal of this work is to give an overview of Bro IDS and its extensions, study Bro policy mechanism and scripting language, describe implications of event analyzer and policy layer separation. For those interested in hands-on experience with Bro a possible extension of the study is to implement own simple Bro policy script.

The role of XACML in defining access control policies

XACML is an XML-based language designed to standardize and thus simplify the process of defining access policies. The goal of this study is to describe the role of XACML in specifying access control policies as well as to illuminate its various use cases, extensions and evaluation engines.

Topics by Jukka Ylitalo

Accountability in publish-subscribe architectures

Weitzner et al. present an alternative viewpoint to privacy policies in the Internet in [1]. Instead on relying on access control and encryption to protect sensitive information they propose that laws and systems are needed to hold people accountable for the misuse of personal data. The research target is to analyze how some of the Weitzner's ideas can be applied to information-centric networks. More precisely, the work concentrates on the accountability-system aspects (not on legislation) in so-called next-generation publish-subscribe networks [2].

Topics by Bill Brumley

Randomart in OpenSSH

Randomart is basically a text-based hash visualization. It just seems to have popped up and is already deployed in e.g. Ubuntu. See: http://alibash.livejournal.com/200301.html . But what are the security properties? Nobody seems to know (or ask?), and it's already out there! There could be a ton of interesting things to look at: 1. What is the range of the function? ("How many possible randomarts?") 2. Can we get useful (pre-)pre-images? 3. Can we get useful "close" pre-images? (It's like Where's Waldo...) 4. Could even do an experiment on how "close" they have to be for people to notice. Key-words: Privacy, accountability, information-centric networks

Topics by Elena Reshetova

Symbian OS Platform Security Model

The first part of this assignment is to study the main principles of Symbian OS Security model: Symbian capabilities, data caging, Symbian trusted computing base. The next step is to get familiar with the Platform Security Environment for developers (such as developer's certificates, package signing tools and so on) and understand the Symbian signed model. The last step of the assignment is to develop a small program on Symbian, sign it by using the Symbian Signed process and experiment with it on a real device.

Mandatory Access Control in SELinux

The goal of the assignment is to study the basic mandatory access policies, which are supported by SELinux (such as domain type enforcement mechanism (DTE), multi-level security mechanism (MLS), and role-based access Control (RBAC) model), and understand how they can be used to make a reasonable SELinux policy.

Sandboxing and jailing in Unix OSs

The goal of this assignment is to study the different sandboxing techniques, such as the chroot jail (Unix), the FreeBSD jail, and the BitFrost security system, compare them and study the possible ways of breaking out of some of them (for example how to break the chroot jail).

Topics by Jukka Valkonen

Vulnerability disclosure policies

In order for vendors to fix bugs and vulnerabilities in their products, they must be reported by the discoverer. To make this possible, the vendors should have policies specifying how users can report such errors in an easy and reliable way. The goal of the topic is to write survey on different vulnerability disclosure policies.

Topics by Sachin Gaur

Privacy policy for location sharing

Location sharing is coming up as a promising feature on social media. However, experts have raised concern about privacy concerns related to it. The student is expected to write a literature survey and make a comparative analysis of different proposed techniques available for privacy protection and access control in location sharing.

AI, Persuasion, Game theory and other approaches to make/improve privacy policies

The goal of this project is to write a literature survey on the persuasion techniques the can be used to guide users to make safe choices for privacy.

Topics by Andrei Gurtov

Access control with flat namespaces

Flat Internet namespaces have several benefits e.g. for supporting host mobility and multihoming, and access control in firewalls based on stable identifiers. However, some organizations prefer to aggregate hosts for access control, e.g. enable all hosts from TKK to access the ACM digital library. The goal of this task is to survey mechanisms to include hierarchy information into a flat name space.

Topics by Mika Rautila

Same origin policy in web browsers

In this assignment consider implications of same-origin policy in modern browsers. Is the mechanism adequate or is it too restrictive? Compare how the policy is implemented is some popular web browsers.

Browser programming and access control policies

It is quite common that web users are accessing several web pages simultaneously or during a browser session. It is also common that the data on a web page is collected from several sources, and that web pages contain client side programs (e.g., JavaScript). In these circumstances it is crucial that access to data stored in browser's memory is controlled carefully. In this assignment study the access control mechanisms used in browsers to protect data.

Certificate validation policies

In this assignment study how certificates are validated in browsers. What factors affect the validation process? How a user could be misled into believing that he/she is accessing the correct site? How it could be made easier for the user to detect a phishing attempt?

Topics by Mikko Särelä

Security policies for capability based distributed denial of service resistance

Distributed denial of service attacks are a major problem in the current Internet. One potential solution to the problem lies with capabilities, i.e. requiring senders to have permission to send before network delivers packets to the specified destination. The purpose of this work is to review major capability based proposals and analyze the access control policies needed with such schemes.

Security policies for filtering based distributed denial of service resistance

Distributed denial of service attacks are a major problem in the current Internet. One potential solution to the problem lies with filtering, i.e. letting the receiver inform the network about unwanted flows, so they can be blocked. The purpose of this work is to review major filtering based proposals and analyze potential filtering policies with such schemes.

Topics by Petri Savolainen

Filtering and throttling Peer-to-Peer traffic

Using peer-to-peer file sharing software is deemed unacceptable in a number of networks including the Helsinki university HUPNet. In this topic, the student should write a survey on the various means used by network operators in enforcing this "no p2p" policy.

DDoS attacks and publish-subscribe

The goal of the seminar project is to explain the concept denial-of-service attacks, introduce the publish-subscribe paradigm, and explain and the way in which this paradigm could act as a cure against denial-of-service attacks. Are publish-subscribe networks really immune to DDoS attacks?

Firewalls in enforcing acceptable use policies

What kind of acceptable use policies can be enforced using firewalls? Are firewalls effective in enforcing these policies? What kind of implications do different firewall policies have on legitimate uses of the networks?

Topics by Jani Heikkinen

Privacy policies in location-based services

As the number of location-based services (LBS) is increasing rapidly, the privacy policies given by the services flourish with different kinds of terminology and assertions. In this seminar work, you will systematically analyze existing LBS privacy policies to get an overall understanding of the differences among the policies.

Privacy policies for location histories

In this seminar work, you will search for and analyze policies that consider location data retention and location histories. Central to the topic are questions such as who is able or entitled to access the histories, and in what ways the access can be controlled by the target.

Topics by Tony Joki-Kyyny

Using SIM credentials for enforcing access control policies in P2PSIP

The paper should investigate how SIM cards and the credential son them can be used for enforcing operator policies and for protecting the users. In particular, how can the SIM card b used for enforcing access control policies in a P2PSIP network? Could parts of RELOAD (I-D) protocol be implemented on a SIM card or in another safe execution environment to improve the security of policy enforcement?

Enforcing security policies in open protocols

The new open protocols like P2PSIP/RELOAD are open and standardized and intended for use on open networks. What problems does this pose to the network operator and the security of the service?

Topics by Antti Ylä-Jääski

Secure data filtering and aggregation in wireless sensor networks

There are many proposals for routing protocols that forward the data from remote sensors via other sensors or other wireless routers towards the sink. The seminar paper should explore proposed secure routing and data aggregation protocols for sensor networks that allow filtering of false data before it reaches the sink.

Timetable (in Noppa)

Tue 8.9. 16-19 in T2	Introductory meeting, English essay, signup open
Fri 11.9. 12:00 (midday)	**Deadline** for signup
Tue 15.9.	Accepted students and topics, meeting with tutor
Fri 18.9. 10-12 T5	**Scientific English** 1st meeting
Tue 29.9. 12:00 (midday)	**Deadline: 1st draft paper submission** 1 page, references
Tue 6.10.	Feedback from your tutor
Fri 9.10. 10-12 T5	**Scientific English** 2nd meeting
Tue 20.10. 12:00 (midday)	**Deadline: full draft paper submission** 5-7 pages
Tue 3.11. 12:00 (midday)	**Deadline: opponent comment submission**
Tue 3.11.	Feedback from your tutor
Fri 6.11. 10-12 T5	**Scientific English** 3rd meeting
Fri 20.11 10-12 T5	**Scientific English** extra support meeting
Tue 24.11. 12:00 (midday)	**Deadline: final paper submission**
Tue 1.12. 16-18 T2	Meeting with all students: practical arrangements
Fri 4.12 9-11 T5	**Scientific English** presentation meeting
Tue 8.12. 12:00 (midday)	**Deadline: slide submission**
Thu-Fri 10-11.12. 8-17 (full day) TUAS building, TU1171-72	**Two-day seminar**, participation required
Tue 15.12. 12:00 (midday)	**Deadline: opponent comment submission**
Tue 15.12.	Grade suggestions and feedback from tutors

Signing up for the course

- Students sign up by sending an application to t-110.5290@tkk.fi
  - Your name and student number in the subject line
  - Given name, family name
  - Student number
  - E-mail address
  - Your cc.hut.fi account username (for Optima account)
  - Participation in the integrated English course (Yes/No)
  - Your major and minor subjects (or MSc program)
  - Your transcript of completed courses (OODI) as PDF
  - Your 5 favorite topics numbered from 1 to 5
    - Tutor name and topic title
    - Optional: brief justification for the choice or own ideas
  - Justification for taking the course: why now?

First draft (29.9.)

- Outline: logical and makes a point (a message, central theme, focus, something to say)
- At least one page of text (readable English)
- Key references
- Use Latex and Bibtex
- Tutors should help especially with the outline and finding good references

Full draft (20.10.)

- 5-7 pages using the Latex template
- Most of the text and main ideas written, structure close to final
- References: original or authoritative, relevant, correct, up-to-date
- One week later, deadline for tutor and opponent comments

Final Paper (24.11.)

- 5-7 pages
- Structure of a technical conference publication, using the course Latex template
- Correct and readable English
- Correct citations and sufficient references

Contents of a good seminar paper

- Makes a small contribution to technical or scientific knowledge
  - Original work with the student's own idea, analysis, evaluation, comparison, summary, example, experiences etc.
- The reader learns something
- Uses diagrams and examples
- Covers a wide area extensively or a smaller area in depth
- Helpful references to high-quality scientific literature and authoritative technical sources

Format of a good seminar paper

- Readable and correct English
- Neutral and objective style suitable for scientific and technical writing
- Structure of a conference paper: abstract, introduction, background, body sections, conclusions, references, (appendices)
- Correct and sufficient in-text citations to acknowledge sources; correct and consistently formatted references

Cut and paste? – just don't!

- Do not cut and paste text or images from the web or somewhere else
- Do not cut and paste even if you plan to change it later
- Do not rewrite somebody else's text sentence by sentence
- Anyone found copying even a small amount of someone else's work will fail the course and may face further disciplinary action
- Every submission must include the following statement: "This submission is my own work and does not include any material produced by others, except when clearly marked as such."

Questions?