



Design and Analysis of Security Protocols

INSE 7100, Fall 2004

Course Outline

Course Instructor

Dr. Mourad Debbabi, Professor,
Computer Security and Acceleration Research Group,
Concordia Institute for Information Systems Engineering,
Concordia University,
1425, René Lévesque CB-420-26
Montréal, Québec, H3G 1T7
Canada.
Phone: (514) 848-2424 Extension : 3166
Fax: (514) 848-3171
Email: debbabi@ciise.concordia.ca
Web: <http://www.ciise.concordia.ca/~debbabi>

Prerequisites

COEN 6311 or equivalent.

Lectures

- ✓ Time: Monday 17:45 to 20:15.
- ✓ Place: LS-323 SGW.

Office Hours

I will be available all Tuesdays from 2:00 PM to 4:00 PM.

Objectives

This course aims to give students a good grasp of the concepts, languages, methods and tools that are used in engineering modern security protocols. By the end of the course, the students will learn about:

- ✓ Cryptographic systems.
- ✓ Security protocols.
- ✓ Security properties.
- ✓ Security flaws.
- ✓ Specification of cryptographic protocols.

- ✓ Analysis of security protocols.

As a downstream result of the methods learnt in this course, the students will gain a significant expertise in:

- ✓ Algebraic calculi.
- ✓ Formal semantics.
- ✓ Logics.
- ✓ Type systems.
- ✓ Game semantics.

Description

In this course, methods used in the design and analysis of security protocols, as well as an introduction to existing cryptographic protocols will be presented. This course will cover the most important security properties such as authentication, secrecy, integrity, availability, atomicity, certified delivery and other properties. We will present a taxonomy of security attacks such as: freshness attacks, type attacks, parallel session attacks, implementation dependent attacks, binding attacks, encapsulation attacks and other forms of attack. We will address the approaches used in the specification of cryptographic protocols such as general-purpose formal languages, logical languages, operational languages and security calculi. We will address the analysis of cryptographic protocols with tools such as: Security logics, model-based and algebraic analysis, process algebra analysis and type-based analysis. The limitations of these formal methods and ad-hoc techniques will be covered.

Detailed Outline

- **Motivations and Background**
- **Cryptographic Prerequisites**
 - General principles.
 - Symmetric key cryptography.
 - Public key cryptography.
 - One-way hash algorithms.
- **Protocol Types**
 - Authentication protocols.
 - Key distribution protocols.
 - E-commerce protocols.
- **Security Properties**
 - Authentication.
 - Secrecy.
 - Integrity.
 - Availability.
 - Atomicity.
 - Certified delivery.
 - Other properties.
- **Flaw Taxonomy**
 - Freshness attacks.
 - Type attacks.
 - Parallel session attacks.

- Implementation dependent attacks.
- Binding attacks.
- Encapsulation attacks.
- Other forms of attack.
- **Cryptographic Protocol Specification**
 - General-purpose formal languages.
 - Logical languages.
 - Operational languages.
 - Security calculi.
 - The SPC calculus.
- **Security Property Specification**
 - Security logics.
 - ADM Logic.
 - Syntax.
 - Semantics.
 - Specification of security properties.
- **Cryptographic Protocol Analysis**
 - Logical analysis.
 - Model-based and algebraic analysis.
 - Process algebra analysis.
 - Type based analysis.
 - The DYMNA framework

Suggested Readings

Lecture notes will be available on the course web site. In addition, we suggest reading the following:

- M. Debbabi. Design and Analysis of Security Protocols. Lecture notes. CIISE, Concordia University, 2004.
- M. Abadi and A. D. Gordon. *A Calculus for Cryptographic Protocols: The SPI Calculus*. In the Proceedings of the Fourth ACM Conference on Computer and Communications Security. ACM Press, April 1997.
- M. Burrows, M. Abadi, R. Needham. *Logic of Authentication*. In the Proceedings of the Royal Society of London. Volume 426, 198, pp. 233--271.
- M. Debbabi, M. Mejri, N. Tawbi, and I. Yahmadi. *A New Algorithm for Automatic Verification of Authentication Cryptographic Protocols*. In the Proceedings of the DIMACS Workshop on Design and Formal Verification of Security Protocols, DIMACS Center, Core Building, Rutgers University, New Jersey, USA, September 1997.
- Douglas R. Stinson. *Cryptography: Theory and Practice*. Second Edition, Chapman & Hall/CRC, 2002.
- M. Debbabi, N. Durgin, M. Mejri and J. Mitchell. *Security by Typing*. In the International Journal of Software Systems for Technology Transfer, Springer Verlag, December 17th, 2002.

- K. Adi, M. Debbabi, and M. Mejri. *A New Logic for Electronic Commerce Protocols*. In the International Journal of Theoretical Computer Science, TCS, Volume/Issue 291/3 pp. 223-283, Elsevier.
- John Clark and Jeremy Jacob. *A Survey of Authentication Protocol Literature: Version 1.0*. Technical Report, November 1997. Available on the Web at the URL: <http://www-users.cs.york.ac.uk/jac/papers/drareview.ps.gz>
- Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. ISBN 0471128457, Published by John Wiley & Sons, 1996.

Evaluation Scheme

There will be:

- ✓ One quiz: 20%.
- ✓ One project: 30%.
- ✓ One final exam: 50%.

The project is to be done in groups of 3 students. The whole group will have to submit only one report and make a joint presentation. Your grade for the course will be based on your total mark. You must pass each component of the evaluation to pass the course.

Communication

The course web site can be accessed at the following URL:

<http://www.ciise.concordia.ca/~debbabi/inse7100.html>

Last minute changes, announcements and interesting links will be announced in this page.