UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO TECNOLÓGICO
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

LECTURE PLAN

1) Identification

Course: INE 410128 **-** Design and Verification of Security Protocols and Security Ceremonies
Credits: 3 créditos – 45 horas/aula
Professor: Jean Everson Martina

2) Prerequisites

There are no prerequisites for this course. Some prior familiarity with cryptography or formal methods may be helpful, but all necessary background will be covered in class.

3) Aim

Cryptographic Primitives. Security Properties. Classical Protocols. Threat Modelling. Protocol Verification Techniques. Advanced Security Protocols. Advanced Security Ceremonies. Formal Verification of Security Protocols and Security Ceremonies.

4) Objectives

General Objectives: Understand the concepts of security protocols and security ceremonies design and verification.

Specific Objectives:

- Understand security primitives as a way of yielding security
- Understand the relation between the different security properties and their compositions
- Review classical security protocols
- Understand the different threat models available for symbolic evaluation of security protocols and security ceremonies.
- Understand the security verification techniques available today
- Study advanced security protocols
- Study advanced security ceremonies
- Be able to apply formal verification techniques based on theorem provers on security protocols and security ceremonies.

5) Course Outline

- Cryptographic Primitives.
    - Symmetric cryptography [1.5 hours]
    - Asymmetric cryptography [1.5 hours]
- Security Properties.
    - Standard Properties [1 hours]
    - Advanced Properties [1 hours]
    - Properties' Composition [2 hours]
- Classical Protocols.

    - Needham-Schroeder Shared-Key Protocol [2 hours]
    - Yahalom [1 hours]
    - Woo-Lam [1 hours]
    - Needham-Schroeder Public-Key Protocol [1 hours]
- Threat Modelling.
    - Dolev-Yao [2 hours]
    - B.U.G Family [2 hours]
    - Advanced Threat Models for Symbolic Evaluation [2 hours]
- Protocol Verification Techniques.
    - Abstract State Machines [1 hour]
    - Belief Logics [1 hour]
    - Provable Security [1 hour]
    - State Enumeration [1 hour]
    - Strand Spaces [1 hour]
    - Theorem Provers [3 hours]
- Advanced Security Protocols.
    - Kerberos [2 hours]
    - SSL/TL [2 hours]
- Advanced Security Ceremonies.
    - Carlomagno et. al. approach [3 hours]
    - Security Ceremony Concertina [4 hours]
- Formal Verification of Security Protocols and Security Ceremonies.
    - Hands on theorem proving [8 hours]

6) Methodology

This is a project-oriented course intended to give students hands-on experience. We will see a variety of analysis techniques to evaluate security protocols and security ceremonies. A network protocol such as SSL (Secure Sockets Layer) may fail in four ways: the protocol design may be flawed, the cryptography may be inadequate, the implementation may be buggy or it can not cope with the humans in its ends.

This course is primarily concerned with techniques for identifying design flaws, but we will also talk about cryptography secure implementation and usability to the extent that they affect security protocol and security ceremony design.

The first part of the course will survey contemporary security protocols and their properties, including confidentiality, authentication, secure group communication, privacy, and anonymity. We will also cover cryptographic primitives, as well as standard formal models and tools used for mechanized verification of secure systems. We will then

The second part of the course will focus primarily on student projects, carried out individually or in small teams. A typical project may involve:

- Coming up with a security specification for a particular system and performing a detailed analysis of its properties; or
- Extending an existing tool or method to support analysis of a new class of security properties; or
- Conducting a theoretical study of the relationship between several models.

A selection of candidate projects will be provided, but students are encouraged to propose their own.

Lectures will be given in English to broaden the outreach of the course and to facilitate access to standard material of the area such as book, articles and manuals of the tools. Also the course may be joined by international partners under cooperation agreements with UFSC, where credits are interchangeable. A second but no least import reason for the Lecture to be conducted in English is that experts on the field will be invited to speak in some guest lectures. Guest Lectures will be limited to three throughout the semester and will cover some tools and techniques from the viewpoint of its creators.

The course will be conducted using the official departmental virtual conference room for all classes. In this sense the guest lecturers will use this platform, as well as some of the international students enrolled in the course. All the students will be required to join the virtual lecture room at the required time using the virtual conference software. The students MUST HAVE A WEBCAM for all the meetings so that participation can be attested. The lack of a webcam will imply in no record for attendance control purposes. For those who do not own a webcam, it will be lended by the lecturer. All the meetings will be recorded and made available for later viewing for the students. This course is a presential course over a virtual environment. In this sense it follows all University regulations regarding regular courses. No online self-study strategies will be applied.

7) Evaluation

The evaluation will be conducted over a final technical report written by the students, together or not with their research supervisors or the course professor. This technical report will be constructed over the semester with oversight of the course professor.

The technical report will be assessed using standard strategies used to evaluate conference papers. The technical reports will be evaluated over their readability, adherence to the proposed topic, contribution, coherence of the experimentation conducted and the results achieved.

Technical reports will be already graded using the standard grading system for the PPGCC program and will be the final grade achieved by the student. Technical reports with a pass mark should be fit for submission to the main conferences in the area of security protocols, formal methods or foundations of computer security.

8) Schedule

To be defined at the beginning of the semester with the students.

9) Bibliography

Formal Correctness of Security Protocols. Bella, G.. 2007. Springer
Threat Modeling: Designing for Security. Shostack, A.. 2014. Wiley
Isabelle/HOL: A Proof Assistant for Higher-Order Logic. Nipkow, T. and Paulson, L.C. and Wenzel, M.. 2003. Springer Berlin Heidelberg