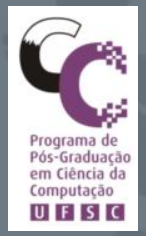
# Lecture Plan Overview

## Design and Verification of Security Protocols and Security Ceremonies

Programa de Pós-Graduacão em Ciências da Computacão
Dr. Jean Everson Martina

March-June 2019




UNIVERSIDADE FEDERAL
DE SANTA CATARINA

# Course Identification

- INE 410128 - Design and Verification of Security Protocols and Security Ceremonies

# Course Identification

- INE 410128 - Design and Verification of Security Protocols and Security Ceremonies
- 3 credits – 45 hours

# Course Identification

- INE 410128 - Design and Verification of Security Protocols and Security Ceremonies
- 3 credits – 45 hours
- Dr. Jean Everson Martina

# About the Lecturer

- B.Sc. In CompSci;

# About the Lecturer

- B.Sc. In CompSci;
- M.Sc. In CompSci;

# About the Lecturer

- B.Sc. In CompSci;
- M.Sc. In CompSci;
- Ph.D. In CompSci;

# About the Lecturer

- B.Sc. In CompSci;
- M.Sc. In CompSci;
- Ph.D. In CompSci;
- Several International Projects;

# About the Lecturer

- B.Sc. In CompSci;
- M.Sc. In CompSci;
- Ph.D. In CompSci;
- Several International Projects;
- Working on Cryptography, Digital Signatures, Security Protocols and Security Ceremonies.

# About the Students

I would like to know:

- Your Name and Affiliation;

# About the Students

I would like to know:

- Your Name and Affiliation;
- Academic Background;

# About the Students

I would like to know:

- Your Name and Affiliation;
- Academic Background;
- Interests in Security;

# About the Students

I would like to know:

- Your Name and Affiliation;
- Academic Background;
- Interests in Security;
- Prior knowledge on Security;

# About the Students

I would like to know:

- Your Name and Affiliation;
- Academic Background;
- Interests in Security;
- Prior knowledge on Security;
- Anything else you believe is important to share.

# Course Prerequisites

- There are no prerequisites for this course;

# Course Prerequisites

- There are no prerequisites for this course;
- Some prior familiarity with cryptography is good;

# Course Prerequisites

- There are no prerequisites for this course;
- Some prior familiarity with cryptography is good;
- Some prior familiarity with formal methods may be helpful;

# Course Prerequisites

- There are no prerequisites for this course;
- Some prior familiarity with cryptography is good;
- Some prior familiarity with formal methods may be helpful;
- All necessary background will be covered in class.

# Study Aims

- Cryptographic Primitives;

# Study Aims

- Cryptographic Primitives;
- Security Properties;

# Study Aims

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;

# Study Aims

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;
- Threat Modelling;

# Study Aims

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;
- Threat Modelling;
- Protocol Verification Techniques;

# Study Aims

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;
- Threat Modelling;
- Protocol Verification Techniques;
- Advanced Security Protocols;

# Study Aims

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;
- Threat Modelling;
- Protocol Verification Techniques;
- Advanced Security Protocols;
- Advanced Security Ceremonies;

# Study Aims

- 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.

# General Objective

Understand the concepts of security protocols and security ceremonies design and verification.

# Specific Objectives

- Understand security primitives as a way of yielding security;

# Specific Objectives

- Understand security primitives as a way of yielding security;
- Understand the relation between the different security properties and their compositions;

# 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;

# 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;

# Specific Objectives

- Understand the security verification techniques available today;

# Specific Objectives

- Understand the security verification techniques available today;
- Study advanced security protocols;

# Specific Objectives

- Understand the security verification techniques available today;
- Study advanced security protocols;
- Study advanced security ceremonies;

# Specific Objectives

- 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.

# Course Outline

- Cryptographic Primitives;

# Course Outline

- Cryptographic Primitives;
- Security Properties;

# Course Outline

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;

# Course Outline

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;
- Threat Modelling;

# Course Outline

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;
- Threat Modelling;
- Protocol Verification Techniques;

# Course Outline

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;
- Threat Modelling;
- Protocol Verification Techniques;
- Advanced Security Protocols;

# Course Outline

- Cryptographic Primitives;
- Security Properties;
- Classical Protocols;
- Threat Modelling;
- Protocol Verification Techniques;
- Advanced Security Protocols;
- Advanced Security Ceremonies;

# Course Outline

- 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.

# Methodology

- The first part of the course will survey contemporary security protocols and their properties, including confidentiality, authentication, secure group communication, privacy, and anonymity.

# Methodology

- 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.

# Methodology

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

# Methodology

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

# Methodology

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

# Methodology

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.

# Studying Strategies

- We will read a series of classical papers on the area;

# Studying Strategies

- We will read a series of classical papers on the area;
- Students are expected to have read the assignments for the week;

# Studying Strategies

- We will read a series of classical papers on the area;
- Students are expected to have read the assignments for the week;
- The off-class workload for this course is about 90 hours;

# Studying Strategies

- We will read a series of classical papers on the area;
- Students are expected to have read the assignments for the week;
- The off-class workload for this course is about 90 hours;
- Some lectures will be open discussions regarding the topics.

# Important to Notice!

- Lectures will be given in English;

# Important to Notice!

- Lectures will be given in English;
- The course may be joined by international partners;

# Important to Notice!

- Lectures will be given in English;
- The course may be joined by international partners;
- Experts on the field will be invited to speak in some guest lectures;

# Important to Notice!

- Lectures will be given in English;
- The course may be joined by international partners;
- Experts on the field will be invited to speak in some guest lectures;
- All the students will be required to join the virtual lecture room at the required time;

# Important to Notice!

- Lectures will be given in English;
- The course may be joined by international partners;
- Experts on the field will be invited to speak in some guest lectures;
- All the students will be required to join the virtual lecture room at the required time;
- The student MUST HAVE A WEBCAM for all the meetings so that participation can be attested;

# Important to Notice!

- Lectures will be given in English;
- The course may be joined by international partners;
- Experts on the field will be invited to speak in some guest lectures;
- All the students will be required to join the virtual lecture room at the required time;
- The student MUST HAVE A WEBCAM for all the meetings so that participation can be attested;
- All the meetings will be recorded;

# Important to Notice!

- Lectures will be given in English;
- The course may be joined by international partners;
- Experts on the field will be invited to speak in some guest lectures;
- All the students will be required to join the virtual lecture room at the required time;
- The student MUST HAVE A WEBCAM for all the meetings so that participation can be attested;
- All the meetings will be recorded;
- This Course follows all UFSC regulations regarding regular courses.

# Evaluation

- A final technical report written by the student;

# Evaluation

- A final technical report written by the student;
- The technical report will be assessed using standard strategies used to evaluate conference papers;

# Evaluation

- A final technical report written by the student;
- The technical report will be assessed using standard strategies used to evaluate conference papers;
- The technical report will be evaluated over their readability, adherence to the proposed topic, contribution, coherence of the experimentation conducted and the results achieved;

# Evaluation

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

# Schedule

- Tuesday 13:30-16:00 (BRT)

# Schedule

- Tuesday 13:30-16:00 (BRT)
- International participants should be aware that:
  - Time shifts during the semester
  - Your summer time will start (usually +1 hour);
  - Brazil is already out of summer time, so no time shift for us;

# Bibliography


- Formal Correctness of Security Protocols. Bella, G.. 2007. Springer
- Threat Modelling: 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

# Questions????

UNIVERSIDADE FEDERAL
DE SANTA CATARINA





UNIVERSIDADE FEDERAL
DE SANTA CATARINA