Discipline(s) : Infomatique et télécommunications

SECURITY PROTOCOLS

Nature	UE

RESPONSABLES

Barbara Kordy

OBJECTIFS

The objective of this course is to provide students with an in-depth knowledge regarding methods and tools for the specification, design, and symbolic verification of security protocols in various domains.

KEYWORDS

Communication protocols, security property, (strong, weak) secrecy, authentication, aliveness, agreement, synchronisation, Dolev-Yao adversary, man-in-the-middle attack, symbolic protocol verification

PREREQUISITES

First order logic

CONTENTS

The following topics will be covered in this course:

Introduction to cryptography (if necessary): symmetric and asymmetric cryptography, hash functions;
Formal ways of specifying a protocol: Alice & Bob notation, message sequence charts, Horn clauses, constraint systems, applied pi calculus;
Attacker models: passive and active attackers, Dolev-Yao adversary, knowledge inference;
Formal specification of security properties: weak and strong secrecy, indistinguishability property, authentication (aliveness, agreement, synchronization), anonymity;
Man-in-the-middle attacks;
Protocol verification with a bounded number of sessions: constraint systems;
Protocol verification with an unbounded number of sessions: Horn Clauses;
Symbolic versus computational models for protcol verification;
Tools for automatic verification of security protocols: ProVerif, Scyther, OFMC, APTE, etc.

LEARNING OUTCOMES

After a successful completion of this course, the students should be able to:

Specify a protocol in a suitable formal framework;
Formally define the security property against which the protocol should be checked;
Select an appropriate verification tool to analyze the protocol;
Detect logical flaws in improperly designed or implemented protocols.

APPARTIENT À

Master 2 informatique parcours Science Informatique

Mise à jour le 17 juillet 2017

CONTACT(S)

Département Informatique et télécommunications
École normale supérieure de RennesCampus de Ker LannAvenue Robert Schuman
35170 BRUZ
Tél. : 02 99 05 52 43
E-mail
Site Internet