Introduction to Network Security

Daniel Bosk, Lennart Franked

Department of Information and Communication Systems (ICS),
Mid Sweden University, SE-851 70 Sundsvall.

natsak.tex 2068 2014-11-03 10:52:07Z danbos

Mittuniversitetet
MID SWEDEN UNIVERSITY

Overview

1. What's Network Security?
   - Introduction
   - Active and Passive Attacks
   - Layers and Cryptography
   - Key Management
2. This Course
   - Teachers
   - Course Platform
   - Study Guide
   - Examination

Overview

1. What's Network Security?
   - Introduction
   - Active and Passive Attacks
   - Layers and Cryptography
   - Key Management
2. This Course
   - Teachers
   - Course Platform
   - Study Guide
   - Examination

Introduction

- Network Security is an area of Information Security focusing on network communication.
- I.e. secure communication over an insecure medium.
- We want Alice to be able to send a message to Bob.
- None should be able to read what Alice sent, except Bob.
- Bob must be able to determine that it was in fact Alice who sent the message, not someone else pretending to be Alice.

Introduction

- There are several issues which must be solved.
- The most obvious is confidentiality.
- The next one is integrity.
- Then authenticity.
- Cryptography is used to solve (parts of) these problems.
- There are also problems such as availability.
- These properties ward off different types of attacks.

Active and Passive Attacks

- A passive attack is one in which the attacker just eavesdrops on communications.
- Hence, no modification is done.
- The converese is an active attack.
- Here the attacker may modify real messages, replay old messages, delete messages, and insert totally new ones.
- The attacks mentioned focus on the different properties mentioned above.
- Deleting messages is a problem with availability.
- The passive attacks focus mostly on confidentiality.

Active and Passive Attacks

- And then there are also attacks within each area.
- E.g. there are several types of attacks on crypto systems.

Layers and Cryptography

- Different security mechanisms, e.g. cryptography, can be applied in different layers.
- You can encrypt a document; then you can store it, or transmit it, over any medium, trusted or not.
- You can apply end-to-end encryption; then you can encrypt data chunk by chunk, or all together as a stream.
- If all together and you apply integrity checks, then if an error occurs, you'll have to resend everything.
- If in chunks, then maybe you can relate two cryptotexts to each other, and thus gain information.

Layers and Cryptography

- If hop-to-hop, then you hide who are communicating with whom, unlike in the end-to-end scheme.
- However, now you must trust all the nodes to properly reencrypt etc.

Key Management

- So far we've only talked about securing the communication.
- Using cryptography for this requires the use of keys.
- Alice and Bob can communicate using their keys.
- But, how do Alice and Bob agree on the keys to use?
- There are several solutions to this.
- One is by using asymetric (public key) cryptography.
- However, the problem of who is authenticated by which key still remains.
- We need some means to tie an identity and a key together.
- This is what key management is about.

Key Management

- There are of course several approaches to this.
- A key-distribution centre, such as Kerberos, is one example.
- Public-key infrastructure, such as X.509, is another.

Overview

1 What's Network Security?
- Introduction
- Active and Passive Attacks
- Layers and Cryptography
- Key Management

2 This Course
- Teachers
- Course Platform
- Study Guide
- Examination

Teachers

- Lennart Franked (examiner, course responsible, lecturer),
- Oscar Nylander (teaching assistant).

Course Platform

- The course platform used is Moodle.
- You'll find it at URL:

  `https://elearn20.miun.se/`.
- The course material is also available publicly at URL:

  `http://ver.miun.se/courses/security/natsak/`.
- However, you must sign in to Moodle to hand in assignments.

Study Guide

- Make sure to read the *whole* study guide.
- This document contains all information about the course.
- There is an overview of the schedule.
- You'll find the reading instructions for the course.
- You'll find information about late submissions and other topics related to not being on time.

Study Guide

- The main literature is *Network security essentials : applications and standards* [Sta13].
- You'll also have use of *Security Engineering* [And08].
- RFC 4949 [Shi07] (*Internet Security Glossary, Version 2*) is also of use for vocabulary.
- On top of this there are a few more RFCs and manuals.

Examination

- The main part of examination is the final exam.
- There's one lab on email security.
- There's one lab on intrusion detection.
- These cover the more practical parts of the course.
- Finally, there's a seminar on ethics.

Referenser I

[And08] Ross J. Anderson. *Security Engineering. A guide to building dependable distributed systems*. 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: http://www.cl.cam.ac.uk/~rja14/book.html.

[Shi07] R. Shirey. *Internet Security Glossary, Version 2*. RFC 4949 (Informational). Internet Engineering Task Force, Aug. 2007. URL: http://www.ietf.org/rfc/rfc4949.txt.

[Sta13] William Stallings. *Network security essentials : applications and standards*. 5th ed. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.