Introduction to Web Application Security

Daniel Bosk

Department of Information and Communication Systems (ICS),
Mid Sweden University, Sundsvall.

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

Overview

Overview

Introduction

- It's an interdisciplinary area.
- Makes use of e.g. cryptography, psychology, economics.
- The goal is for things to work as intended, even while facing a powerful adversary.

Introduction

- Information Security is the very general sense of the subject.
- It includes Computer Security and Network Security.
- But it also includes physical security and even management.

Introduction

- Web Application Security is a subset of Computer and Network Security.
- Hence, in this course, we'll have a bit of both.

Overview

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

Introduction

- Computer Security is concered with the happenings of the insides of the computer.
- I.e. things related to the operating systems, applications and users.
- A more specific example could be ensuring that an application cannot access the memory of another application.
- Otherwise one user could access the content of another user via these applications.

Introduction

- As indicated above, one of the central problems is access control.
- This makes authentication also an issue.
- Hence, we need proper ways for users to authenticate themselves.
- These programs mustn't malfunction, since then a malicious user might be able to authenticate themselves as someone else.
- That makes software security an important area as well.

Introduction

- Software security wants to ensure the correct functioning of software in general, hence applications.
- This ranges from buffer overruns to code injections and beyond.

Overview

Web Application Security

- As can be seen above, Web Application Security, needs both Computer and Network Security.
- The reason why this is so:
  - The Web servers are essentially running applications in the normal sense.
  - The user interface, however, is on the other end of a network connection.
- Anyone can connect to this application.

Teachers

- Daniel Bosk (examiner, course responsible, lecturer),
- Nayeb Maleki (lecturer).

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/owasp/`.
- However, you must sign in to Moodle to hand in assignments.

Teaching and Tutoring

- The teaching will be accomplished by
  - individual reading,
  - lectures,
  - workshops,
  - tutoring sessions.
- Daniel will give most lectures.
- Nayeb will give all workshops.
- Tutoring sessions (handledning) are one hour sessions where you can ask questions and discuss problems.

Teaching and Tutoring

- Use the course forums and tutoring sessions!
- These are the place to ask questions and discuss things relevant to the course.
- Daniel is on 80 % leave for doctoral studies. So, replies to email will be even slower than usual.
- Nayeb also has a busy inbox. Replies to emails will be slow.
- So the most efficient means of communication are the forums, tutoring sessions, and, if there's time, also the lectures.

Teaching and Tutoring

- You are recommended to read the material before the lecture.
- This way you can ask better questions and get better answers during the lectures.

Teaching and Tutoring

- You are expected to have read the material before the workshops.
- This is because the workshops are more practical, like teacher lead labs.

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 all lectures and workshops.
- You'll find information about late submissions, other topics related to not being on time, how to deregister from the course, etc.

Study Guide

- The detailed times for all meetings (lectures, workshops, presentations) are in the University's central schedule.
- The URL is: `https://portal.miun.se/web/student/schedule`.
- There's also a link to it in the course platform.

Study Guide

- The main literature is *Computer Security* [Gol11].
- You'll also have use of *Security Engineering* [And08].
- RFC 4949 [**rfc4949**] (**rfc4949**) is also of use, it's a dictionary.
- On top of this comes the OWASP material:
  - *OWASP Top 10 - 2013* [OWASP13],
  - *OWASP Testing Guide* [MKC08],
  - *OWASP Application Security Verification Standard 2014* [ASVS14].

Examination

- The main part of examination is the project.
- This is examined through a written report (and hand-in of the project).
- The second part is an audit of a project which is not your own.
- This is examined through a written report and an oral presentation.
- Everything else is for your learning only.
- (The project is of course for learning too, but is also examined.)

Referenser I

[ASVS14] Sahba Kazerooni, Daniel Cuthbert, Andrew van der Stock, and Krishna Raja, eds. *OWASP Application Security Verification Standard 2014*. 2014. URL: https://www.owasp.org/images/5/58/OWASP_ASVS_Version_2.pdf.

[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.

[Gol11] Dieter Gollmann. *Computer Security*. 3rd ed. Chichester, West Sussex, U.K.: Wiley, 2011. ISBN: 9780470741153 (pbk.)

Referenser II

[MKC08] Matteo Meucci, Eoin Keary, and Daniel Cuthbert, eds. *OWASP Testing Guide*. 2008. URL: http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf.

[OWASP13] The Open Web Application Security Project. *OWASP Top 10 - 2013. The Ten Most Critical Web Application Security Risks*. June 2013. URL: http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf.