

Software Security Analysis

Chair of IT Security / I20
Prof. Dr. Claudia Eckert
Technical University of Munich

Fabian Kilger

kilger@sec.in.tum.de

Alexander Kuechler

alexander.kuechler@aisec.fraunhofer.de

Florian Wendland

florian.wendland@aisec.fraunhofer.de

Hannah Wester

hannah.wester@aisec.fraunhofer.de

February 02, 2023

What this seminar is about?

- ▶ Modern Software consists out many software components

What this seminar is about?

- ▶ Modern Software consists out many software components
- ▶ This software components can contain easily contain about 100.000 lines of code
 - ▶ e.g. OpenSSL has about 230000 LOC
 - ▶ the linux kernel even has about 21 million LOC

What this seminar is about?

- ▶ Modern Software consists out many software components
- ▶ This software components can contain easily contain about 100.000 lines of code
 - ▶ e.g. OpenSSL has about 230000 LOC
 - ▶ the linux kernel even has about 21 million LOC

- ▶ Is this secure?

Examples where it was not...

Apple Goto Fail

```
...
if ((err = ReadyHash(&SSLHashSHA1, &hashCtx)) != 0)
    goto ↓fail;
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto ↓fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto ↓fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto ↓fail;
    goto ↓fail;
    goto ↓fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto ↓fail;

err = sslRawVerify(ctx,
                  ctx->peerPubKey,
                  dataToSign,           /* plaintext */
                  dataToSignLen,       /* plaintext length */
                  signature,
                  signatureLen);
```

Do you remember other
accidents?

Software Analysis Techniques

An overview of **automated** software analysis techniques:

- ▶ Static code analysis
 - ▶ Dataflow analysis
 - ▶ Abstract interpretation
 - ▶ RegEx search for secret values
- ▶ Dynamic code analysis
 - ▶ Code Sanitizer (z.B. AddressSanitizer von Clang)
 - ▶ Fuzzing
 - ▶ Symbolic Execution
 - ▶ Binary Instrumentation

Course Organization

We will organize the seminar like a **scientific conference**. You will present your research in written and in a presentation to your peers.

The paper you will be writing will (most likely) be a *Systematization of Knowledge (SoK)* or *introductory* paper.

SoK papers do not propose a novel approach. They take a broader view on a topic, explain the core concepts and put the most relevant works in context.

Introductory papers explain the core concepts of a field, the problems they are applied to and ongoing research directions.

Course Organization

- ▶ Research & Paper Writing
 - Write a scientific paper of (exactly) 10 pages (excluding references and appendices)
 - We will use the standard Usenix Security L^AT_EX template
- ▶ Review Phase
 - Every participant creates 2-3 reviews of her/his peers
 - ~1 page/review
- ▶ “Camera Ready” Phase
 - Integrate the reviewers’ remarks, improve your paper as far as possible
 - Submit the “camera ready” version (final polished version)
- ▶ Presentation
 - 30 minutes presentation
 - 15 minutes discussion
- ▶ Language: English

Time Table (Draft!!!)

Today	●	Premeeting
27.02.2023	●	Start of topic assignments
18.04.2023	●	Session: How to write a research paper?
24.04.2023-28.04.2023	●	Individual Meeting: Literature Research and Outline
02.05.2023	●	Graceful drop out deadline
31.05.2023-02.06.2023	●	Individual Meeting: First Paper Version (outline fixed and 80% content)
19.06.2023	●	Submit your draft for review
03.07.2023	●	Submit Reviews
16.07.2023	●	Submit "camera-ready" version
20.07.+21.07.2023	●	Meeting: Presentations and discussion

Requirements

- “First version” Structure & main contents of the paper are fix. Introduction, conclusion, abstract might not be fully finished. Language does not have to be perfect, graphics might not be finished, some references might be missing. Focus on the “meat” of the paper!
- “Draft ” Paper should be mostly finished apart from small details.
- “Review” Provide *constructive* feedback on your fellows’ papers.
- “Camera Ready” The *perfect* and final version of your paper that you and your reviewers will be happy with. Correct formatting, correct citations, no typos.

Grading

The grading is composed of *mandatory* and *graded* parts:

Mandatory:

1. Timely submission of paper, reviews, final paper
2. Meetings with advisor
3. Reviews

Graded:

1. Paper (50%)
2. Experiments (10%)
3. Presentation + Discussion (30% + 10%)

Location

- ▶ In this room: 01.08.033

Registration

- ▶ 10 Slots
⇒ Send a letter of motivation to kilger@sec.in.tum.de until *14.02.2023*
- ▶ Register in the matching system
- ▶ *Register for this seminar until 15.02.2023.*

Letter of Motivation

Tell us about:

- ▶ Why are you interested in this seminar?
- ▶ What areas of Software Security Analysis interest you?
- ▶ *Optional:* Your previous experience with SSA-related topics

Q&A

Q&A