# Software Security Analysis

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

#### Fabian Kilger kilger@sec.in.tum.de

### Fabian Franzen

franzen@sec.in.tum.de

### Alexander Küchler

alexander.kuechler@aisec.fraunhofer.de

#### Konrad Weiss

konrad.weiss@aisec.fraunhofer.de

#### Florian Wendland

florian.wendland@aisec.fraunhofer.de

#### Hannah Wester

hannah.wester@aisec.fraunhofer.de

#### Tobias Specht

tobias.specht@aisec.fraunhofer.de

### Oliver Braunsdorf

oliver.braunsdorf@aisec.fraunhofer.de

# What this seminar is about?

► Modern Sofware consists out many software components

## What this seminar is about?

- ▶ Modern Sofware consists out many software components
- ▶ This software components can contain easylly 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 Sofware consists out many software components
- ▶ This software components can contain easylly 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 = ReadvHash(&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;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto ↓fail:
err = sslRawVerifv(ctx.
                   ctx->peerPubKev.
                   dataToSign.
                                             /* plaintext */
                                             / * plaintext length */
                   dataToSignLen
                    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.

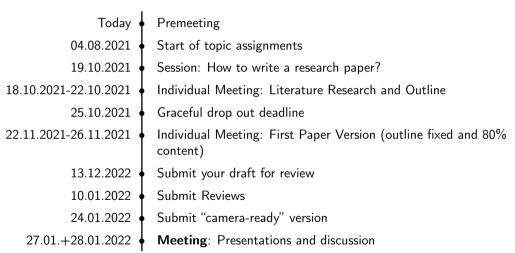
SoK papers do not propose a novel approach. They take a broader view on a topic, explain the core concepts and put the <u>most relevant works</u> in context.

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 LATEX 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!!!)





## 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 <u>you and your reviewers</u> 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

- ► To be honest: We do not know yet, because of Covid-19
  - If onsite teaching is possible, in a room at TUM or Fraunhofer AISEC
  - ► Otherwise: Online via BBB

# Registration

- ▶ Registration using the matching system
- ▶ Register for this seminar until 20.07.2021.

Q&A

Q&A

