

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

Maximilian Kaul

maximilian.kaul@aisec.fraunhofer.de

February 01, 2021

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 1.4 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 1.4 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;
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
- ▶ Rebuttal & “Camera Ready” Phase
 - Integrate the reviewers’ remarks, improve your paper as far as possible
 - Submit the “camera ready” version (final polished version)
 - Write a *rebuttal*, i.e. a response summarizing how you addressed the reviewers’ remarks
- ▶ Presentation
 - 20 minutes presentation
 - 10 minutes discussion
- ▶ Language: English

Time Table (Draft!!!)

Today	●	Premeeting
01.03.2021	●	Start of topic assignments
13.04.2021	●	Session: How to write a research paper?
03.05.2021	●	Graceful drop out deadline
04.05.2021	●	Intermediate Presentations
26.05.2021	●	Submit your first version (outline finished, 80% of content) for review
08.06.2021	●	Submit Reviews
05.07.2021	●	Submit your rebuttal + “camera-ready” version
08.07+09.07.2021	●	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!
- “Review” Provide *constructive* feedback on your fellows’ papers. //
- “Rebuttal” Your answer to the reviewer. Explain which suggestions you incorporated in the final version. If you do not agree with any suggestions, provide a short justification.
- “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. Participation in discussions

Graded:

1. Paper (50%)
2. Review (10%)
3. Experiments (15%)
4. Presentation (25%)

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 16.02.2021.*

Q&A

Q&A