IT Security Practicals
Course overview

Sebastian Ramacher, Philipp Harb, Martin Mandl, Samuel Sprung, Stefan Steinegger

October 3, 2016

Password for all downloads

itssNwSjZP

Goals

- Learn how cryptographic primitives work.
- Learn usage of primitives in protocols.
- Learn about practically relevant implementation attacks.

Team

Philipp Harb

Martin Mandl

Samuel Sprung

Stefan Steinegger

Contact

- Newsgroup: tu-graz.lv.it-sicherheit
- Via Email: itsec-team@iaik.tugraz.at
- (If neeeded) Question time about one week before the submission deadlines.

Tasks

- Task 0: Registration
- Task 1: TLS (part 1)
- Task 2: TLS (part 2)
- Task 3: Blockchain

Course Schedule - Important Dates

Date & Time	Remark
2016.10.03 16:00	Registration. Task 0.
2016.10.10 23:59	Registration. Task 0 deadline.
2016.10.10 16:00	Presentation of Task 1.
2016.10.31 23:59	Task 1 submission deadline.
2016.11.07 16:00	Presentation of Task 2.
2016.12.05 23:59	Task 2 submission deadline.
2016.12.12 16:00	Presentation of Task 3.
2017.01.16 23:59	Task 3 submission deadline.
2017.01.23–2017.01.27	Group interviews

Table: Course schedule.

Rules

- Groups of two members. If you cannot find a partner, we will assign you one.
- Use Git repository to coordinate teamwork and submission
- Mandatory group interviews:
  - Explain the theoretical fundamentals and attacks
  - Explain your work
  - Explain why git statistics look abnormal
  - Inspect and discuss your results (Einsichtnahme)
- All deadlines are hard.

Grading

- Sum of points per task divided by all possible points scaled by performance at the group interviews.
- 1: $\geq 87.5\%$, 2: $\geq 75\%$, 3: $\geq 62.5\%$, 4: $\geq 50\%$.
- You will get a grade if you submit something for any of the tasks.
- In case you get less than 50% you can fix / extend the submission for the task where you submitted something but got the least points until four weeks after the end the course.

Git

- One repository per group
- Usage is mandatory
- Configure real user names and email address
  - `git config --global user.name "John Doe"`
  - `git config --global user.email "jd@student.tugraz.at"`
- Tag your submissions.
- Reference: `http://progit.org/book/`

Task 0: Group registration

- Group registration via STicS.
- First members registers group and invites other member.
- Make sure to share password.
- Make sure to select KU as topic.

What we provide . . .

- Framework with testcases.
- `FRAMEWORK-README.txt`
- Virtual machine image (64-bit Debian jessie)
- x86-64 architecture only

Using the Framework

- Requirements:
  - CMake 2.8
  - GCC 4.9 or newer
  - Boost.Test
- Everything pre-installed on virtual machine image
- Each tasks will have their own make targets.

Next Steps

- Task 0 deadline: 2016.10.10 23:59
- Git repositories containing framework after Task 0 deadline.
- Specification for Task 0 will be available later today.
- Virtual machine reference image will be available later today.
- Watch the newsgroup for announcements.

Questions