Introduction to INFOF514

Christophe Petit & Liran Lerman

INFO-F514:
Protocols, cryptanalysis and mathematical cryptology, 2021-2022

What this course is about

- Modern cryptology and cryptanalysis tools; design, analysis and implementation of cryptographic primitives and protocols
- Critical analyzis of some current issues in the field
  $\rightarrow$ privacy-preserving contact tracing apps this year
- Research topics and methods in cryptology

Content

Lecturers

Christophe Petit

- E-mail: christophe.petit@ulb.be
- Background on mathematical cryptography
- Presenting first part of the course

Liran Lerman

- E-mail: llerman@ulb.be
- Background on applied cryptography
- Presenting second part of the course

Invited lectures by industry experts

Learning approaches

- Regular lectures (either on-campus or online)
- Your own preparation to lectures
- Your own (guided) reading of research papers
- Project

Lectures: content

Week	Topic
1	Introduction to the course and privacy-preserving contact tracing apps
2	"Provable security"
3	Homomorphic encryption
4	Zero-knowledge proofs
5	Cryptanalysis
6	Post-quantum cryptography
7	Security/Crypto in industry (Part 1)
8	Security/Crypto in industry (Part 2)
9	Threat model
10	Deep Learning-based Side-channel Analysis
11	Biometric authentication
12	Secure software implementation

Lectures: organization

Before each lecture

- Read associated research paper and answer related questions
- You are welcome (but not requested) to submit your answers; they do not count towards the final mark
- Purpose: prepare for course and evaluation

Lectures: organization

Before each lecture

- Read associated research paper and answer related questions
- You are welcome (but not requested) to submit your answers; they do not count towards the final mark
- Purpose: prepare for course and evaluation

During the lectures

- We will go over the slides quickly, assuming you have already discovered their content and tried to understand it
- We will answer any questions you will ask

Evaluation: group project

- Evaluation based on group project on a topic of your choice
- Two reports
  - group report (75% of the mark)
  - individual report (25% of the mark)

Purpose:

Select/expand your knowledge/understanding of crypto beyond what is covered in the lectures

Group work at the time of COVID

Tasks:

- Form a small group
- Choose a research problem and paper
- Submit a project proposal on UV
- Study the paper
- Write the reports on your findings
- Submit the reports on UV

Use as much as possible the following tools:

- Overleaf
- Zoom/Teams/Jitsi
- Git

Deadlines

February 25, 2022: Build your group and choose a project

- Form your own group
- Five students per group
- Identify your project topic
- Identify at least one research paper related to crypto
- Submit a one-page description of your project by the deadline on UV

Penalty of up to 5% of the project mark can be applied if document not submitted by the deadline

Deadlines

April 8, 2022: Progress report: brief statement on

- Progress made so far on the project
- Workload distribution
- Difficulties encountered so far

Penalty of up to 5% of the project mark can be applied if document not submitted by the deadline

Deadlines

May 23, 2022: Submit group report including:

- At most 15 pages (including references and appendices);
- Introduction motivating/defining the problem;
- Description of the paper's main contributions;
- Explanation of their assumption/methodology/ideas/results;
- When appropriate:
  Description of your own attempts at reproducing their findings;
- Explain why the results are important;
- Explain what are their current limitations;
- Possibly compare the paper to other approaches.

Group report counts towards 75% of the project mark

Late submission penalized by 10% per day

Deadlines

May 30, 2022: Submit individual report including:

- At most 5 pages;
- Summarize the project (4 pages);
- Explain how the work was distributed among students (1 page).

Individual report counts towards 25% of the project mark

Late submission penalized by 10% per day

More information available on UV

Our expectations

- Prepare the lectures beforehand
- Be curious
- Be critical of references you read, including our own lectures
- Participate fairly to the project
- Don't be shy in asking questions !

Content

COVID-19

- On December 2019: WHO China Country Office informed of pneumonia, detected in Wuhan (Hubei province, China)
- Coronavirus disease
- Caused by SARS-CoV-2 virus;
- On February 4, 2022 (5:30pm CET)[1]:
  - 386,548,962 cases
  - 5,705,754 deaths

[1] https://covid19.who.int

Fighting the COVID-19 pandemic

- Testing
- Isolate villages/cities/provinces
- Wearing masks / Social distancing / cleaning hands
- **Track close contacts of COVID-19 victims**

Purpose of contact tracing:
alert users that were close to infected users over prolonged period of time

Issue of contact tracing:
keep privacy[2] with new design under time pressure

[2] E.g., avoid to publish social relationships between users

Functional requirements

Functional requirements for Coronalert[3]:

- Acceptable precision level: tradeoff between false positives[4] and false negatives;
- Avoid of false/incorrect reporting of infections: i.e., without test;
- Fast solution: notify people before they develop initial symptoms;
- International interoperability: work in as many countries as possible;
- Must work on majority of current smart phones;
- User-friendlines.

Other functional requirements:

- Low battery/CPU usage;
- Run in background.

[3] From "*Coronalert: A Distributed Privacy-Friendly Contact Tracing App for Belgium*", Corona App Task Force, Version 1.3, 17 August 2020.

[4] Increase detection of infected people from 2m to 20m increases false positives rate.

Privacy/Security requirements

Privacy/Security requirements for Coronalert:

- No location information;
- No information about who is infected by whom, where and when;
- As little information as possible is centrally stored (in Belgium);
- Data disappear 14 days after last reported infection;
- All stored information can be removed at the end of the pandemic;
- Not possible to use system or data for other purposes;
- After receiving positive test, not required to notify other citizens.

Some limits related to privacy requirements, e.g.:

- User A is completely isolated;
- Then A only meets user B;
- If A is identified as being "at risk" from app, A deduces B infected A.

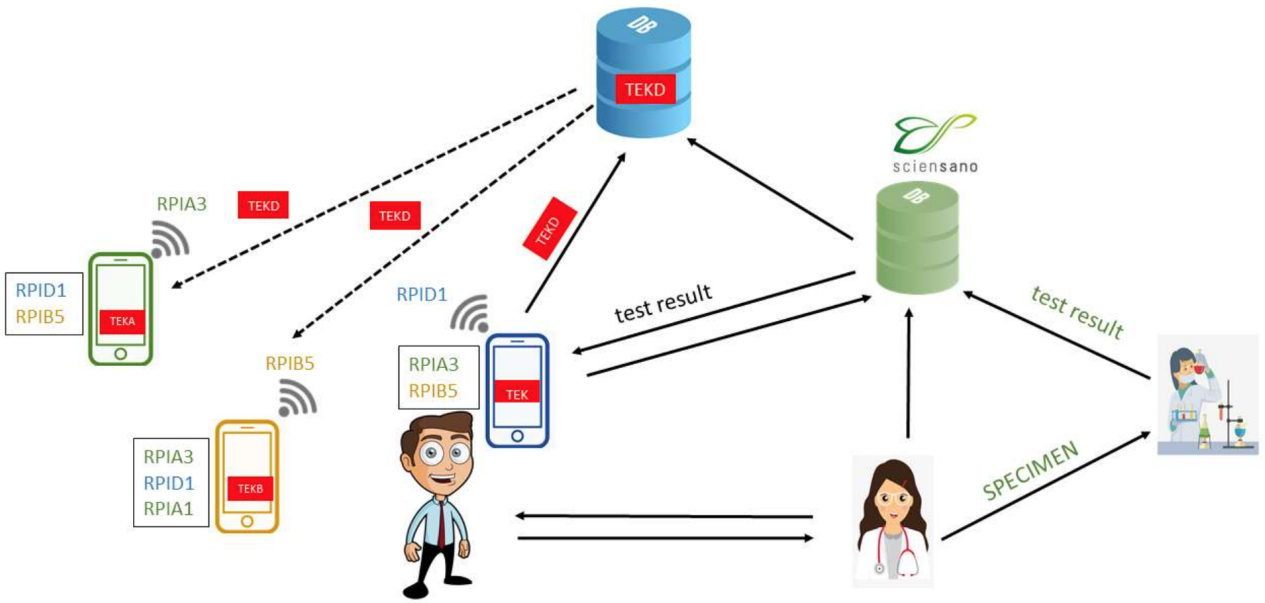
Privacy/security requirements

Privacy/security requirements for Coronalert:

- Maximum transparency should be pursued, e.g.:
  - open source code;
  - publishing the assessments.
- Solution based on state-of-the-art
  - encryption;
  - communications security;
  - secure development practices;
  - user authentication.

Description of DP-3T[6] architecture

DP-3T Protocol created in 2020 by international consortium of Technologists/Legal experts/Engineers/Epidemiologists



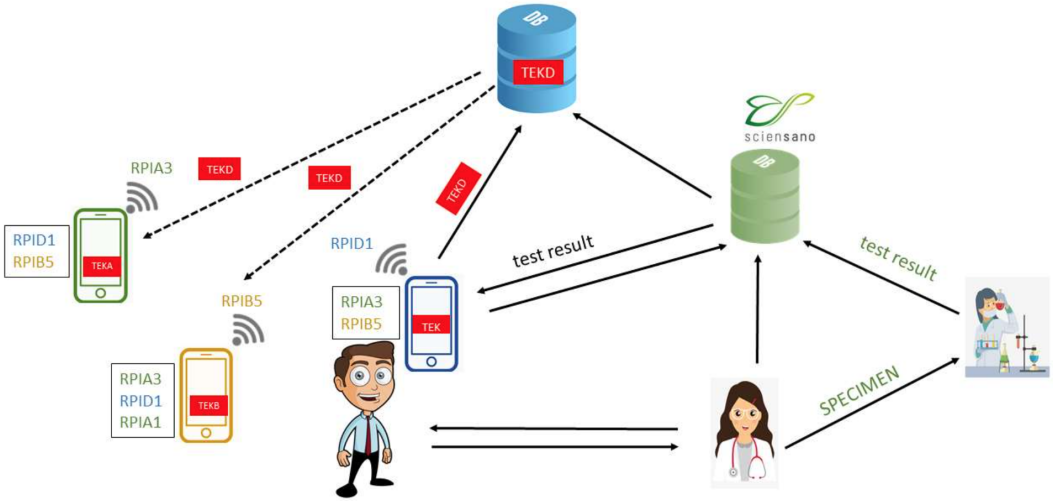
[5]

See also www.youtube.com/watch?v=D__UaR5MQao

[5] From "*Coronalert: A Distributed Privacy-Friendly Contact Tracing App for Belgium*", Corona App Task Force, Version 1.3, 17 August 2020.

[6] Distributed Privacy-Preserving Proximity Tracking

Description of DP-3T architecture



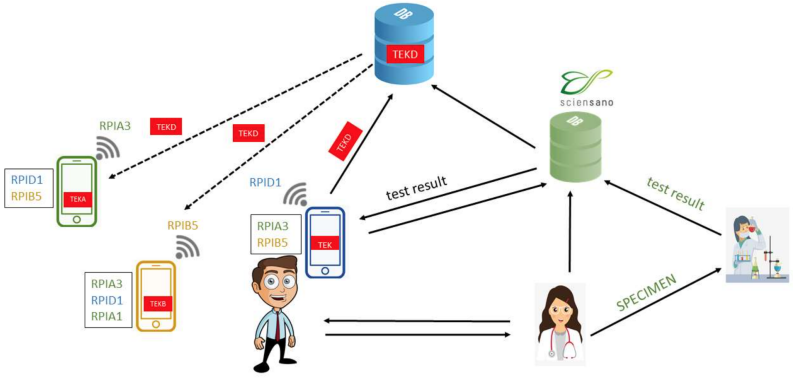
High level description:

- App runs on Android and iOS supporting BLE[7];
- App sends random anonymous Bluetooth beacons to users;
- App gets information on infected users from central server;
- Server collecting test results hosted by Sciensano[8].

[7] Bluetooth Low Energy

[8] National public health institute of Belgium

Description of DP-3T architecture



The app has several phases:

- Installation;
- Operation;
- Infection / Testing / Notification;
- Contact tracing;
- Stopping the system.

Installation phase

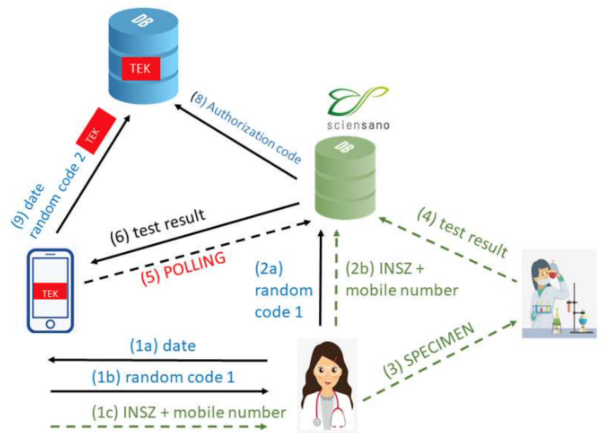
- App generates new key TEK every day;
- App generates Bluetooth token (ephID) based on TEK
- App broadcasts Bluetooth tokens.

Operation phase

- Broadcast of Bluetooth token several times per day;
- Change of Bluetooth token several times per day[9];
- In parallel: collect broadcasted Bluetooth tokens nearby with day/signal strength;
- In parallel: remove old broadcasted Bluetooth tokens (>14 days).

[9] To prevent user tracking

Infection / Testing / Notification



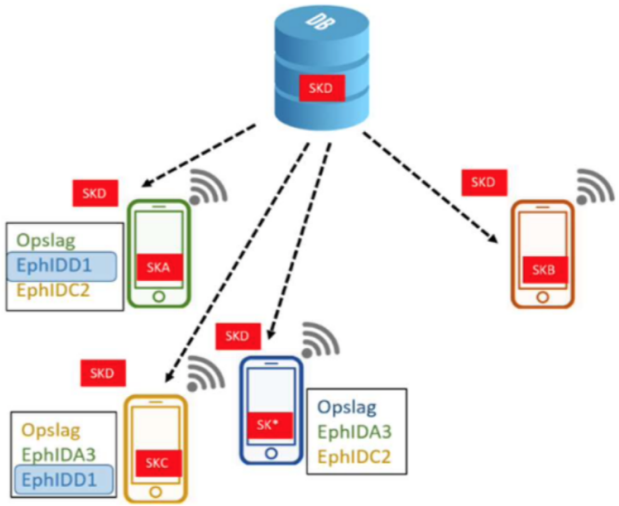
If user has symptoms/infection risk:

- User communicates INSZ/NISS[10] and mobile number to doctor;
- Doctor inserts date user became contagious into user's app;
- App stores date when sample is taken;
- App informs user about the test result;
- If test result positive, app asks user to upload TEK[11] of infectious days in central database.

[10] Identification number

[11] Secret keys are removed from database after 14 days

Contact tracing



- App (of other users) downloads[12] keys and associated infectious days;
- If app detects a risk (i.e., it's done locally[13]), app informs user[14].

[12] From central database

[13] Central server has no proximity information

[14] Not in real time to protect privacy of infected user

Stopping the system

If the system is stopped:

- No new keys are loaded into central database;
- Database empty after 14 days (since no new keys);
- User can uninstall app.

Security evaluation of Coronalert

How security assessment was carried out in practice

- Public report[15] from NVISO on Coronalert Application;
- Identification of security issues impacting confidentiality, authenticity and availability of application's data;
- Security review of app. based on OWASP[16];
- Security configuration review of cloud services used by app. based on (among others[17]) CIS Benchmarks[18];
- Validation of compliance with privacy rules[19]
- Score of vulnerabilities based on CVSS;

---

[15] https://coronalert.be/wp-content/uploads/2020/10/Report-Coronalert-Application-Security-Assessment-Public-Report_vFINAL.pdf

[16] Provide security requirements for mobile apps and web application

[17] E.g., NVISO expertise

[18] https://www.cisecurity.org/benchmark/amazon_web_services/

[19] From Interfederal Committee Testing & Tracing and the Belgian Data Protection Authority

Security evaluation

Security evaluation constraints:

- Evaluation of specific version of app.
- Evaluation of app. on specific version of OS (IOS & Android)
- Several parts not evaluated (i.e., outside the ToE), e.g.:
  - Generation of Bluetooth tokens/TEK by Google/Apple;
  - Security of medical professional's connection to Sciensano;
  - Licensing verification of third party software libraries.
- Limited amount of:
  - Time;
  - Budget (to buy SW/HW);
  - Human resources;
  - Knowledge by evaluators on security;
  - Knowledge on future attacks.

Security evaluation

Web Application-level assessment[20] of:

- Authentication
- Input validation
- Communication
- Access control
- Error handling
- ...

Infrastructure-level assessment of:

- Services using TCP ports
- Services using UDP ports

[20] Based on OWASP Application Security Verification Standard

Security evaluation

Mobile Application-level assessment[21] of:

- Data Storage
- Cryptography
- Authentication Management
- Build settings
- Network Communication

White-box approach:
full access to mobile app. source code & documents

Requires knowledge in several crypto/security topics
(which is the purpose of this course)

[21] Based on OWASP Mobile Application Security Verification Standard

Risks from threat model assessment

Example of risks:

As a malicious user, I should not be able to find a vulnerable version of a third party library used in the mobile application or backend services when reviewing the open source codebase.

As a malicious user, I should not be able to go through the open sourced codebase and uncover secrets in the form of e.g. hardcoded connection credentials that are still actively used in the normal operation of the production environment.

Requirements

Example of functional requirements:

- As a malicious user, I cannot successfully submit my TEKs if I do not have a positive test result;
- As a malicious user, I cannot submit my TEKs several times for a single positive test result.

Example of privacy requirements:

- As an attacker with access to another user's device, I cannot deduce if the user has been tested;
- As an attacker with access to another user's device, I cannot deduce if the user has been tested positive.

Security evaluation

Application-level reviews:

- Medium risk (CVSS=5.9):
  - Issue: no application password
  - Impact: if (unlocked) phone lost, privacy issue on state[22] of owner
  - Mitigation: application password
  - Mitigation: remove test result after first read
- Low risk (CVSS=3.7):
  - Issue: misconfigured TLS services between app. and cloud back-end
  - Impact: intercept traffic
  - Mitigation: update configuration of TLS services[23]

[22] I.e., Infected or not by the COVID-19 virus

[23] E.g., remove support old ciphers and old TLS versions

Security evaluation

Cloud-level Review:

- Medium risk (CVSS=5.5):
  - Issue: lack of access restriction to cloud services environment
  - Impact: if passwords leak, read/modify/delete data/services
  - Mitigation: add location restriction
- Low risk (CVSS=3.3):
  - Issue: third party (AWS) protects data of users
  - Impact: read/modify/delete data/services
  - Mitigation: no cloud-based solution
- Low risk: see report for other risk

Other (major) vulnerabilities were found & corrected during development

Connections to this course

Week	Topic
1	Introduction to the course and privacy-preserving contact tracing apps
2	"Provable security"
3	Homomorphic encryption
4	Zero-knowledge proofs
5	Cryptanalysis
6	Post-quantum cryptography
7	Security/Crypto in industry (Part 1)
8	Security/Crypto in industry (Part 2)
9	Threat model
10	Deep Learning-based Side-channel Analysis
11	Biometric authentication
12	Secure software implementation

Connections to this course (2)

Other relevant topics not covered in the lectures

- Secure communication protocols (TLS, etc)
- Blockchain technologies
- ...

feel free to pick one for your project !

Questions?

- One who is afraid of asking questions is ashamed of learning (Danish proverb)
- No one is without knowledge except he who asks no questions (African proverb)
- The important thing is not to stop questioning. (Albert Einstein)