Security engineering
Autumn 2018

Instructors	Maciej Korczyński and Thomas van Oudenhove
Address	IMAG building, 700 avenue Centrale, Room 420 (Maciej Korczyński)
Telephone No.	+33 457 421 692 (Maciej Korczyński)
Email	maciej.korczynski@univ-grenoble-alpes.fr (PGP key ID: 1BDA32F6) Thomas.van-oudenhove-de-saint-gery@grenoble-inp.fr

Course Description

The introduction to security course involves introductory lectures on security architectures, network, system, and web security, attack strategies, introduction to cryptography, and secure protocols. It also involves practical labs (TP), case studies on selected aspects of security to be presented by each student individually and semester-long group project. Course materials can be found on chamilo http://chamilo.grenoble-inp.fr/courses/INGENIERIEDELASECURITE/. The course materials are password protected (pass: "security2018")

Grading Breakup and Summary

- Short presentations by each student on a selected subject: 10%
- Final Exam: 30%
- Practical assignments: 25%
- Project: 35%
  - Mid Project Report: 10%
  - Final Report/Presentation: 25%

Short presentations

Each student will choose one of the subjects that will be presented in the class (20 minutes per presentation) on the 10/01, 11/01, and 18/01. Students may propose their own subject, which needs to be approved by the instructor. Please send me an e-mail starting with "RIE2 short topic" and give the titles of the four preferred topics before October 5 2018.

Each student is asked to prepare 5 samples of single-choice questions related to their talks and send it to the course instructor at the day of their presentation. Please write in the email subject "RIE2 short questions". Similar questions might appear during the exam.

1. DDoS-as-a-Service (booters, types of protocols used, victims)
2. Online Services for DDoS attack mitigation (strategies, Cloudflare, Akamai)
3. Mirai Botnet (IoT security, mitigation)
4. Stuxnet (SCADA systems; operation, discovery and mitigation of Stuxnet)
5. DNSSEC protocol (goals, implementation, deployment)
6. Tor (Onion Service Protocol, anonymity network)
7. Crypto currencies (technical background, popular currencies, Coincheck hack)
8. Darkweb (architecture, description of selected markets, available services)
9. Kali OS (pentesting tools, examples of attacks)
10. BGP hijacking (technical details, incidents, mitigation)
11. Heartbleed (OpenSSL library, discovery, exploitation)
12. GDPR law and its implications (conflict between consumer privacy and security)
13. Ransomware (operation, mitigation, Petya malware)
14. Exploitation of Digital Certificates (motivation, methods, usage of free certs)
15. Shodan (Search engine for Internet-connected devices, security implications)
16. Avalanche (operation, used techniques, malware families, criminal operation)
17. LDAP (Lightweight Directory Access Protocol, specification)
18. Analysis of free HTTP(S) proxies (amount of free proxies, operational details)

Final exam

It will cover all aspects discussed during the lectures and short presentations. The exam

will take place on January 31, 2019 and will last 1h30. During the exam you will not be allowed to have additional materials.

Practical assignments

Six laboratory sessions (TP) will cover a variety of practical aspects of security: system and network administrations/security, tools and the usage of secure protocols. During the laboratory sessions each student will be required to work individually, write and deliver reports to the instructor before the next lab session (in case of the last lab, please deliver the report before the next CTD). Note: students will be working on virtual machines. Please make sure that you save your virtual machine image on an external drive, a USB key or in the cloud after each TP session, as you will be working on the same images afterwards.

Project

One of the most important parts of the course is the project. It will be carried in groups of 4 students. You can select one of the following project proposals:

1. **Spam trap.** Students will select one of the available implementations of a mail spam trap, deploy it, and analyze the incoming traffic. In particular, email addresses of senders, domains, and IP addresses of spam emails. They will analyze the content of incoming email messages (including domains appearing in their content), if they represent phishing emails and will identify phishing campaigns (if it is against banks, PayPal, etc.). Students will recognize if the IP addresses of spam senders belong to hosting providers (compromised server or rented machine), or to an IP address from Internet Service Provider indicating a compromised end host. You will crosscheck with the existing databases if the IP addresses are already recognized as malicious (e.g.: https://www.abuseipdb.com) and if the domains are already blacklisted (e.g.: https://www.virustotal.com). You could compare the data from your spam trap with data collected using our spam traps from different locations. The questions could be: do you see the same attackers? Why?

2. **IoT/SSH honeypot.** Students will select one of the available implementations of honeypots and will deploy it. In particular, they will capture the traffic towards ports 22 and 23. They will analyze the intrusions, in particular IP addresses of devices trying to connect to the machine, logins and passwords used by the attackers to break in. Students will determine if the IP addresses of the attackers belong to specific devices (such as compromised IoT devices). They may use https://www.shodan.io or other available tools. They will check if the IP addresses are already blacklisted by other security organizations (for example: https://www.abuseipdb.com). If the preliminary part is completed successfully then students may test high-interaction honeypot and analyze commands executed by the attackers just after they successfully log in to the devise (your honeypot).

3. **Generating phishing domains.** Students will generate domain names that are similar to names of several online banking and payment services (paypal.com, credit-agricole.fr, etc.) that can be used in phishing attacks. For example, if the original domain is bankofamerica.com, the phishing domain can be bankofamericaa.com. Students will use the existing tools (API) such as https://dnstwister.report. They will analyze if they are registered. If they are registered then they will verify if domains contain phishing websites or they represent defensive registrations (i.e.: they are registered by, for example, banks). Or they are parked and by who. If they are not registered, students will check if they can be registered, for example, by attackers. You could think about what could the banks do about those domains.

4. **Content analysis of phishing domains.** Students will first obtain (real-time) phishing feeds. That is, domains blacklisted by OpenPhish, Anti-phishing working group, Phishtank, etc. They will find and test (or develop) a tool to perform a similarity check of the content of an original website (e.g. PayPal) to other websites

to determine if the website is a part of phishing campaign against PayPal, banks, or other services. They will download the content of the website from the server and try to learn some information about the attackers (identity, fingerprinting, i.e.: mail addresses, similar features of the code, etc.)

5. **Rigging Alexa 1M.** Students will analyze strategies to manipulate the domain popularity list published daily by Amazon (http://s3.amazonaws.com/alexa-static/top-1m.csv.zip). Students will answer what can be security implications of manipulating this list and other available domain popularity lists (e.g.: https://majestic.com/reports/majestic-million), and will develop method(s) to put a selected domain as high as possible in the Alexa 1M popularity list.

The progress of the project will be evaluated at each CTD session. The purpose is to ensure that (a) projects are on track and (b) to strategize in case there are any bottlenecks in the project. Students should maintain milestones/tasks achieved (as bullet points) as well as a list tasks to be carried out before the next CTD session.

Mid-Project Report
Students will be expected to submit a 1-page mid-project report (in French or English) by 22/12/2018 (hard deadline) on the milestones achieved, challenges faced and how you overcame them, and a list of future tasks to be carried out and a plan for the execution of the tasks. Please write in the email subject "RIE2 mid report".

Final Report
The final report should be written in a form of report and should contain an introduction, background information, description of the methodology, tools and datasets used in the study, your findings (in detail), and brief conclusions. It should also contain documentation and should describe all the steps necessary to reproduce the project setup. It can be written in French or English. The length of the paper should be between 4 and 6 pages. The grammar mistakes will not be the subject of evaluation. The report should be submitted by midnight of 22/01/2019 (hard deadline). Please write in the email subject "RIE2 final report".

We suggest (it is not required) that you write your final report using LaTeX. It is the tool in which most computer science papers are written. While it has a small start-up cost, it is much easier to collaboratively write research papers using LaTeX than using Word. Here is a sample LaTex paper (http://www.cs.cmu.edu/~dga/15-744/S07/sample.tar.gz) and a MS Word template (sample file: http://www.acm.org/sigs/publications/pubform.doc).

Final Presentation
Each group is required to present their findings in a form of a 45 minutes presentation on 24/01/2018. Each member of the group should present during 10 minutes. The remaining 5 minutes are reserved for questions.

Short presentations

Topic	Date	Presenter
DDoS-as-a-Service	10/01	Kilian Erraes
Online Services for DDoS attack mitigation	10/01	Anthony Surgot-Meulien
Mirai Botnet	11/01	Yassine Houboub
DNSSEC protocol	11/01	Lionel FERRAFIAT
Tor	18/01	Romain Benit
Crypto currencies	18/01	Acyl Ghanay
Darkweb	18/01	Nicolas Baratto
Kali OS	11/01	Florian Segura
BGP hijacking	11/01	Otman El Azzouzi
Stuxnet	18/01	Samir Oukdim
GDPR law and its implications	11/01	Maxime MALLET
Ransomware	18/01	Alexandre Blanca

Exploitation of Digital Certificates	10/01	Adrien Sipasseuth
Avalanche	18/01	Adrien Facchin
LDAP	11/01	Mohamed Saouli
Analysis of free HTTP(S) proxies	10/01	Aurel-Delord Chendjou

Projects
Group 1 Topic: Spam trap Members: Nicolas Baratto, Otman El Azzouzi, Alexandre Blanca, Anthony Surgot-Meulien IP address of the server: 107.191.126.184
Group 2 Topic: IoT/SSH honeypot Members: Yassine Houboub, Samir Oukdim, Acyl Ghanay, Aurel-Delord Chendjou IP address of the server: 167.88.113.110
Group 3 Topic: Generating phishing domains Members: Romain BENIT, Maxim MALLET, Mohamed SAOULI, Lionel FERRAFIAT IP address of the server: 168.235.102.73
Group 4 Topic: Content analysis of phishing domains Members: SEGURA Florian, ERRAES Kilian, FACCHIN Adrien, SIPASSEUTH Adrien IP address of the server: 168.235.95.231

Planning			
Class date	Class Timings	Class type	Room
27/09	11-12h, 13h30-17h	CTD	H203
04/10	8h30-12h	CTD	D109
04/10	13h30-17h	TP	E300
18/10	13h30-17h	TP	D200
25/10	13h30-17h	TP	D200
08/11	13h30-17h	TP	D200
15/11	8h30-12h	TP	D201
15/11	13h30-17h	CTD	D109
22/11	13h30-17h	TP	D200
29/11	13h30-17h	CTD	D109
06/12	13h30-17h	CTD	D109
07/12	13h30-17h	CTD	(TBA)
20/12	13h30-17h	CTD	H102
10/01	13h30-17h	CTD	H102
11/01	9h45-12h, 13h30-17h	CTD	H102
18/01	9h45-12h, 13h30-17h	CTD	H102
24/01	13h30-17h	CTD	H102
31/01	13h30-17h	Exam CTD	D109