Software Vulnerabilities: Exploitation and Mitigation

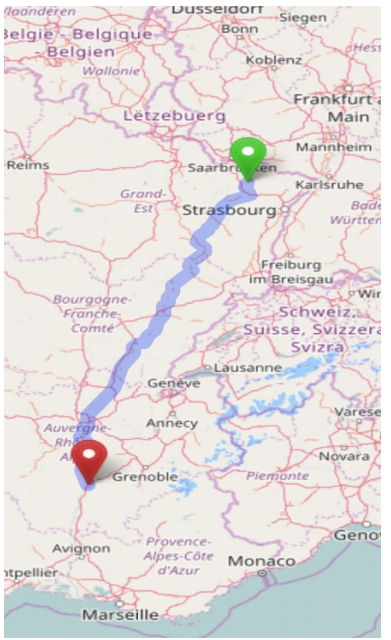
Introduction

(18 Feb. 2019)

Alexandre Bartel
alexandre.bartel@uni.lu

About me

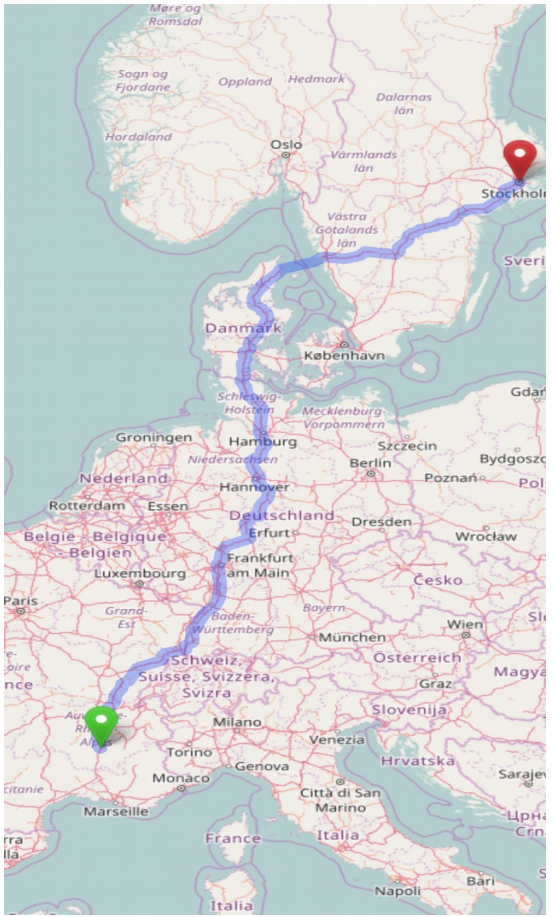
Engineering School in Valence (FR)



Source: wikimedia, openstreetmap

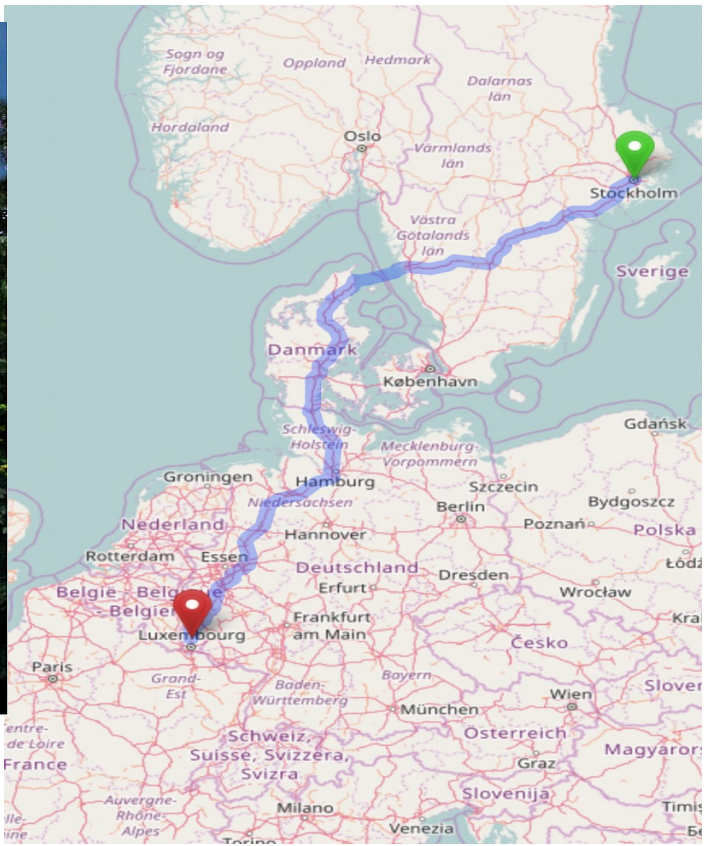
KTH in Stockholm

Source: wikimedia, openstreetmap

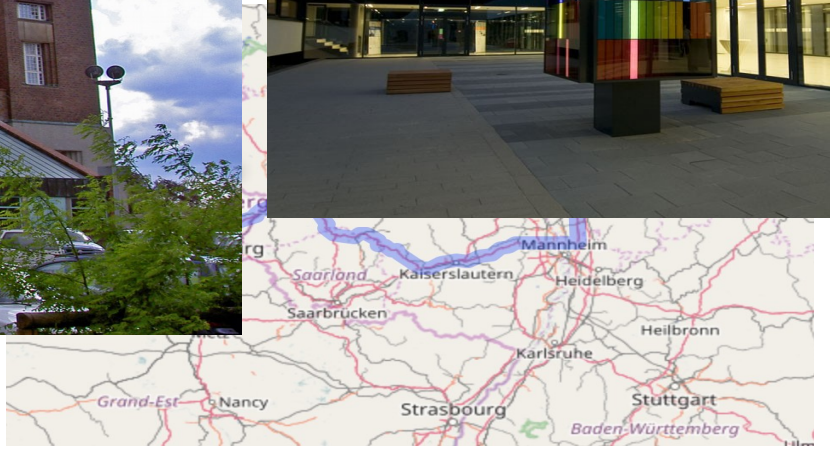


PhD in Luxembourg

Source: wikimedia, openstreetmap



Post-Doc in Darmstadt (DE)



Source: wikimedia, openstreetmap

TECHNISCHE UNIVERSITÄT DARMSTADT

SOFTWARE ENGINEERING GROUP

Research Scientist at SnT / Serval

Source: wikimedia

- Software vulnerability detection, exploitation & mitigation techniques
- Static analysis for Android

UNIVERSITÉ DU LUXEMBOURG

SnT securityandtrust.lu

Research Scientist at SnT / Serval

- Analysis of Java exploits (**CCS**'2016)
- Analysis of Android data leaks (**ICSE**'2015, **PLDI**'2014)
- Analysis of Android Component Communication (**USENIX Security**'2013)
- Non-academic publications:

Research Scientist at SnT / Serval

- Current work:
  - Fuzzing
  - Vulnerability exploitation
  - Understanding (Android) malware

Research Scientist at SnT / Serval

Source: wikimedia

My office (do not come without an appointment!)

Block E building, office E110

Campus Kirchberg

6, rue Richard Coudenhove-Kalergi

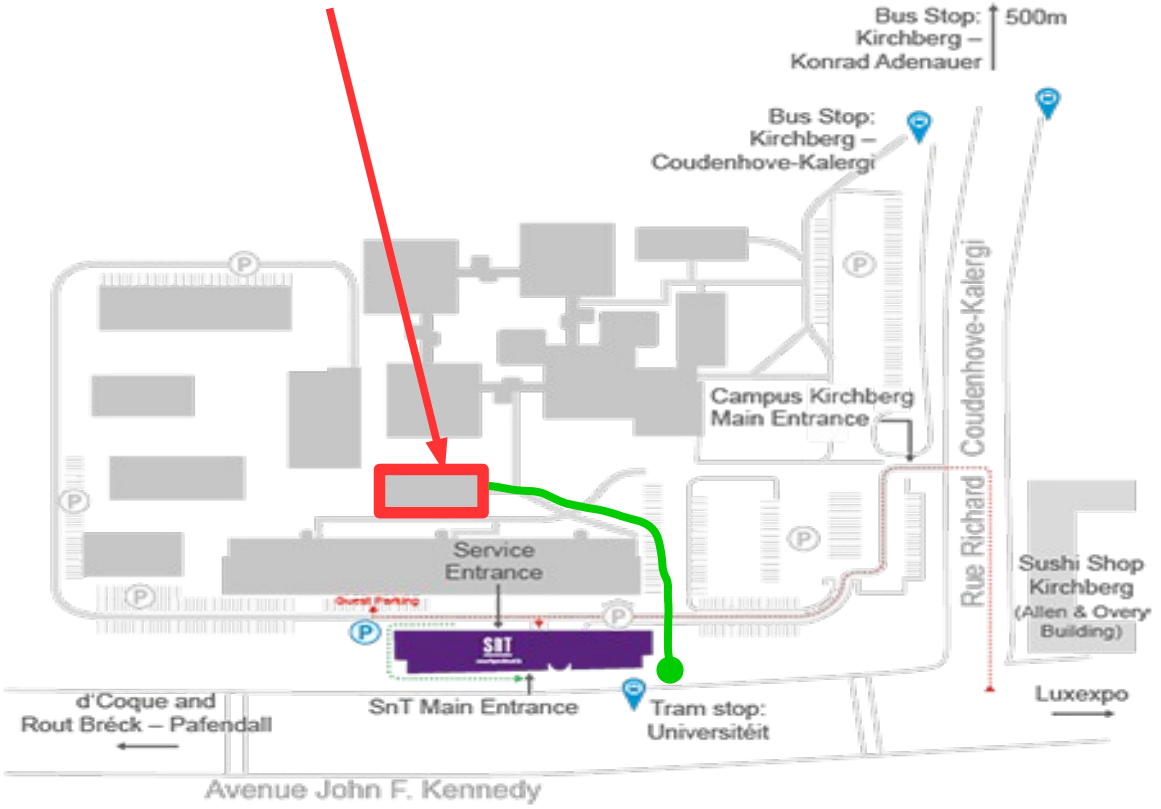
L-1359 Luxembourg-Kirchberg

How to contact me?

alexandre.bartel@uni.lu

Research Scientist at SnT / Serval

Source: wikimedia



Outline of this course

Structure of this course

- Location: Campus Belval, **Room MSA 3.370 / MSA 3.010**
- Lecture structure: on **Mondays** between **14:00** and **16:30**
  - 14h00 to 15h00: **Lecture**
  - 15h00 to 15h15: break
  - 15h15 to 16h30: **Lab**
- First lecture: February 18
- Last lecture: May 27
- Project: May 13 – May 27
- Project presentations: May 27
- Exam: No date yet

Course Calendar

Nom	BARTEL
Prénom	Alexandre

The planning has been generated acordingly to the selected filters

Début	Fin	Cours	Enseignant	Salle
18/02/2019 14:00	18/02/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
25/02/2019 14:00	25/02/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
04/03/2019 14:00	04/03/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.010
11/03/2019 14:00	11/03/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.010
18/03/2019 14:00	18/03/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
25/03/2019 14:00	25/03/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
01/04/2019 14:00	01/04/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
08/04/2019 14:00	08/04/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
29/04/2019 14:00	29/04/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
06/05/2019 14:00	06/05/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
13/05/2019 14:00	13/05/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
20/05/2019 14:00	20/05/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370
27/05/2019 14:00	27/05/2019 16:30	Software Vulnerabilities: Exploitation and Mitigation	BARTEL Alexandre, KLEIN Jacques, LE TRAON Yves	MSA 3.370

Course Calendar

Janvier			Février			Mars			Avril			Mai			Juin		
1	M	Jour de l'an	1	V	Ella	1	V	Aubin	1	L	Hugues	1	M	Jérémie	1	S	Justin
2	M	Basile	2	S	Présentation	2	S	Charles	2	M	Sandrine	2	J	Boris	2	D	Blandine
3	J	Geneviève	3	D	Blaise	3	D	Guénolé	3	M	Richard	3	V	Philippe	3	L	Kévin
4	V	Odilon	4	L	Véronique	4	L	Casimir	4	J	Isidore	4	S	Sylvain	4	M	Clotilde
5	S	Edouard	5	M	Agathe	5	M	Olive	5	V	Irène	5	D	Judith	5	M	Igor
6	D	Mélaine	6	M	Gaston	6	M	Colette	6	S	Marcellin	6	L	Prudence	6	J	Norbert
7	L	Raymond	7	J	Eugènie	7	J	Félicité	7	D	Jean-Baptiste	7	M	Gisèle	7	V	Gilbert
8	M	Lucien	8	V	Jacqueline	8	V	Jean	8	L	Julie	8	M	Désiré	8	S	Médard
9	M	Alix	9	S	Apolline	9	S	Françoise	9	M	Gautier	9	J	Pacôme	9	D	Diane
10	J	Guillaume	10	D	Arnaud	10	D	Vivien	10	M	Fulbert	10	V	Solange	10	L	Landry
11	V	Pauline	11	L	Ntr. D. de Lourdes	11	L	Rosine	11	J	Stanislas	11	S	Estelle	11	M	Barnabé
12	S	Tatiana	12	M	Félix	12	M	Justine	12	V	Jules	12	D	Achille	12	M	Guy
13	D	Yvette	13	M	Béatrice	13	M	Rodrigue	13	S	Ida	13	L	Rolande	13	J	Antoine
14	L	Nina	14	J	Valentin	14	J	Mathilde	14	D	Maxime	14	M	Matthias	14	V	Elisée
15	M	Rémi	15	V	Claude	15	V	Louise	15	L	Paterne	15	M	Denise	15	S	Germaine
16	M	Marcel	16	S	Julienne	16	S	Bénédicte	16	M	Benoît-Joseph	16	J	Honoré	16	D	Jean François Régis
17	J	Roseline	17	D	Alexis	17	D	Patrice	17	M	Anicet	17	V	Pascal	17	L	Hervé
18	V	Prisca	18	L	Bernadette	18	L	Cyrille	18	J	Parfait	18	S	Eric	18	M	Léonce
19	S	Marius	19	M	Gabin	19	M	Joseph	19	V	Emma	19	D	Yves	19	M	Romuald
20	D	Sébastien	20	M	Aimée	20	M	Printemps	20	S	Odette	20	L	Bernardin	20	J	Silvère
21	L	Agnès	21	J	Damien	21	J	Clémence	21	D	Anselme	21	M	Constantin	21	V	Eté
22	M	Vincent	22	V	Isabelle	22	V	Léa	22	L	Alexandre	22	M	Emile	22	S	Alban
23	M	Banard	23	S	Lazare	23	S	Victorien	23	M	Georges	23	J	Didier	23	D	Audrey
24	J	François de Sales	24	D	Modeste	24	D	Catherine	24	M	Fidèle	24	V	Donatien	24	L	Jean-Baptiste
25	V	Conversion de Paul	25	L	Roméo	25	L	Annonciation	25	J	Marc	25	S	Sophie	25	M	Prosper
26	S	Paule	26	M	Nestor	26	M	Larissa	26	V	Alida	26	D	Bérenger	26	M	Anthelme
27	D	Angèle	27	M	Honorine	27	M	Habib	27	S	Zita	27	L	Augustin	27	J	Fernand
28	L	Thomas d'Aquin	28	J	Romain	28	J	Gontran	28	D	Valérie	28	M	Germain	28	V	Irénée
29	M	Gildas				29	V	Gwladys	29	L	Catherine	29	M	Aymar	29	S	Paul
30	M	Martine				30	S	Amédée	30	M	Robert	30	J	Ferdinand	30	D	Martial
31	J	Marcelle				31	D	Benjamin				31	V	Visitation			

Course Overview

- This course features four parts:
  - Part 1: Principles of Computer Security & Software Development
  - Part 2: Memory Attacks and Defenses
  - Part 3: High Level Attacks and Defenses
  - Part 4: Finding Software Vulnerabilities

Course Overview

Part 1 : Principles of Computer Security & Software Development

a. Software Life Cycle

b. Confidentiality, Integrity, Availability

c. Authentication, Access Control

d. Software Vulnerabilities

Course Overview

Part 2: Memory Attacks and Defenses

a. Buffer overflow

b. Heap overflow

c. Integer overflow

d. String format vulnerabilities

e. Type confusion

f. Use After Free

Part 3: High Level Attacks and Defenses

a. SQL injection

b. OS command injection

c. Cross-Site Scripting

d. Confused deputy

Course Overview

Part 4: Finding Software Vulnerabilities

a. Static Program Analysis

b. Dynamic Program Analysis (Fuzzing)

If interested: “Introduction to Static Program Analysis” course on Thursdays

Who should take this course?

- Interest in computer security
- Interest in programming

Background

- Knowledge of one programming language (ex: C, Java)
- Knowledge of operating system (ex: process, stack, heap)

Reading Material

- For most lectures will be given a list of reading material
  - Mostly research papers related to the topic
  - Reading them will help you understand the topic better

Labs

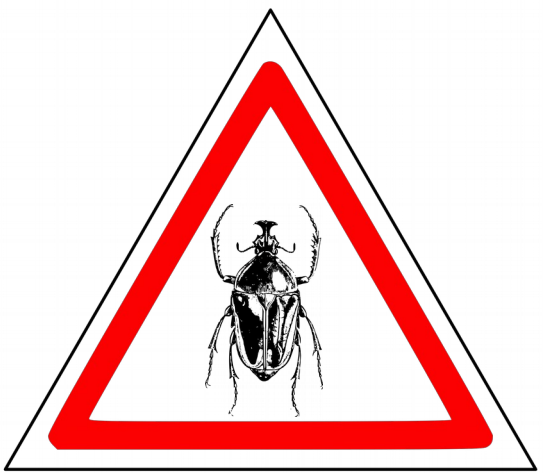
- After every lecture there will be a lab (about 2 hours)
- A report has to be written for each lab and send to the following e-mail: alexandre.bartel@uni.lu with the following subject:
  - MICS-SOFTVULN2019 Lab[X] [student name]
- Deadline: the day before the next lab at 23:50

Grading

- 50% lab assignments (30%) and project (20%)
- 20% readings and exercises (might be merged with labs)
- 30% exam(s)

Warning

- In this course you will learn how to detect vulnerabilities…
- … but also how to exploit them.
- **DO NOT EXPLOIT ANY VULNERABILITY IN THE REAL WORLD**
- If you find a vulnerability (good for you!) use a “responsible vulnerability disclosure” process.



Questions?

Access to git repository

Lecture slides and labs are published in a git repository. You can only access the repository if your ssh key is associated with it. If you do not have a public/private ssh key pair, generate one using the following commands:

$ ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
$ ssh-add ~/.ssh/id_rsa

Send your **PUBLIC** key (ending in .pub) to:

alexandre.bartel@uni.lu

You can now clone the git repository:

$ git clone ssh://gitolite@abartel.net/mics2019svem.git

For Windows Users

- Download https://www.git-scm.com
- Git bash
- $ ssh-keygen -t rsa
- $ eval `ssh-agent -s`
- $ ssh-add .ssh/id_rsa
- $ git clone