

## Security Engineering Fall 2015

*Lecture 01 – Introduction to the course*  
*Prof. Fabio Massacci,*  
*Ms Kate Launets*

## Lecturers

- **Main lecturers**

- Prof. Dr. Fabio Massacci
  - Office hours by appointment in class
  - Can try your luck by email
- Ms. Katerina Labunets
  - Office hour by appointment via email



- **Others**

- Industry guest speakers

## The “Usual” Course

- **The usual lectures/labs**
  - Prof. does theory + Assistant does exercises
  - Prof. does technique + Assistant does programs
  - Prof+Assist = Oracles resolving all doubts
- **The usual exam**
  - Prof gives well defined problem,
  - Students mirroring exercises/code solutions
- **The usual project**
  - Developing a project (i.e. code)
  - Prof. knows exactly requirements
- **This course is not a “Usual” course**

## Why I don't want to teach a “usual” course

- **Reality is very different from the usual course**
  - Problem is not well defined
    - Already a big step if customers realize they have a problem
  - Customers don't know the solution
    - Otherwise they won't be paying you in the first place
  - Decision must be justified and understood by them
    - They won't pay just because you found a solution in a book
    - They don't read code. They paid you for that.
- **The course's idea**
  - Teach you security engineering with a process as close as possible to real life including presenting and justifying your choices
- **Consequence → the course is challenging (= tough)**
  - 40% hate it (too much work), 30% love it (learned a lot)
  - Still one of the popular courses

## Why you don't want me to teach a "usual" course

- **If you can only write programs → you're done for**
  - You must also be able to make decisions and communicate them to upper management
- **Italian Industry Assoc. ICT Salary (24-30 yrs old)**
  - Web Developer/ IT/Network Administrator – 21-26K€
  - Programmer/Analyst – 29-41K€
  - Sys Engineer/Architect – 31-44K€
  - Sw Project Leader/IS Manager – 47-78K€
  - CIO – 98K€/year
- **So better write a management report...(at least once)**

9/21/2015

Massacci - Paci - Tran - Security Engineering

► 5

## Course principles

- **Objective:**
  - Learn how to secure engineer a real life problem from high level management and early security requirements down to security architecture
- **Methodology**
  - Lecturers present methodology in class
  - Students apply it on case study
- **What do you have to prepare**
  - Presentations justify the solution to the customers
    - And they are never happy (but you get early feedback)
  - Deliverable is an executive report to justify your choices
    - You submit it into installments as in real life (here to get feedback)
    - Only at the end you get the money
- **This year customer (not decided yet)**
  - ePayment - Poste Italiane (IT), Remotely Operated Tower by Eurocontrol/SESAR, Digital Cinema by Technicolor

9/21/2015

Massacci - Paci - Tran - Security Engineering

► 6

## Cognitive Levels: why the course is tough

- **Knowledge**
  - Recall things by memory (eg repeat a proof from a book)
- **Comprehension ← Most theory course stops here**
  - Justify methods and procedures
- **Application ← Most design courses stops here**
  - Apply concepts and principles to new situations
- **Analysis**
  - Understanding relationships between parts (content & structure)
- **Synthesis ← This course**
  - Ability to put parts together to form a new whole
- **Evaluation ← The best should arrive here**
  - Conscious ability to judge the value of material

9/21/2015

Massacci - Paci - Tran - Security Engineering

► 7

## Security Management Principles

- **Governance, Risk Management and Compliance**
  - Identify Threats and Risk to your assets
  - Mitigate those with Sec
  - Deploy the Controls
  - Monitor their effectiveness
  - Check security indicators
  - Revise periodically



21/09/2015

Massacci-Paci-Security Engineering

► 8

### What you are protecting?

- **A Case study from an industrial company**
  - ePayment - Poste Italiane (IT) or Remotely Operated Tower by Eurocontrol/SESAR, Digital Cinema
- **But irrespective of actual case study most modern architecture are of the form below**

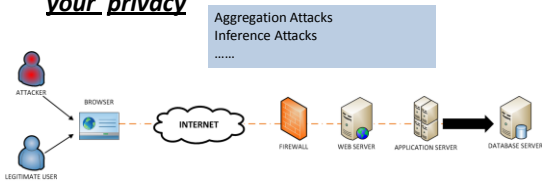


### Specific Technologies will cover...

- **The following security viewpoints**
  - Users (Database) Security
  - Web Application Security
  - Network Security
  - Cloud or Mobile Security
    - Depends on case study
- **A price to pay**
  - There are only so many hours in 6 ECTS...
  - So we won't cover all aspects in details

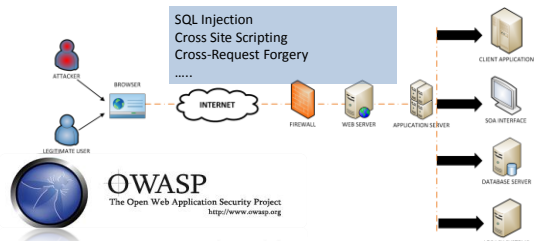
### Users (Database) Security

- **We will review how data confidentiality, integrity can be broken and how to protect your privacy**



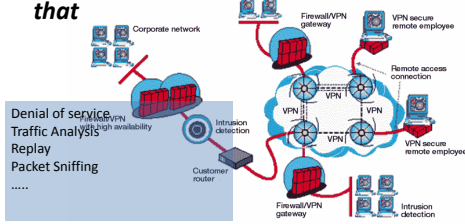
### Application Security

- **We will review how an HTTP session can be hijacked and how you can prevent that**



## Infrastructure Security

- We will review how your network can be attacked and how you can protect against that



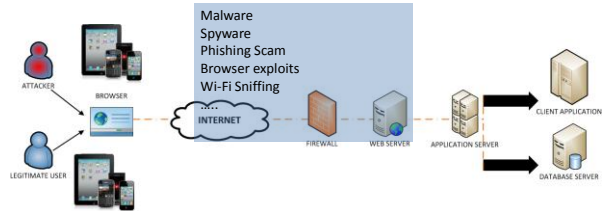
21/09/2015

Massacci-Paci-Security Engineering

▶ 13

## Mobile Security (bonus if we have time)

- We will review the attacks that can target your mobile devices and how to prevent them



21/09/2015

Massacci-Paci-Security Engineering

▶ 14

## Activity

- Apply two methods for risk assessment **CORAS** and **SecRAM** to the case study scenario
- Cover three levels
  - user/Database Security, Web Application Security, Network Security
- For every type of technology
  - Identify the security threats and security controls that mitigate the threats
  - Document the application of the methods and the results
- Report them
  - in written form by a short report
  - By making a presentation in class

21/09/2015

Massacci-Paci-Security Engineering

▶ 15

## How to report your work: Report

### 1. Structure of the report

- Target of Evaluation
- Users Threats & Controls
- Application's T&C
- Infrastructure's T&C

### 2. Delivery

- In installment
- Download template from Web

SECURITY ENGINEERING REPORT  
Student Name and Last Name, StudentID

1. TARGET OF EVALUATION (3-7 pages)

2. SECURITY THREATS AND CONTROLS (3-7 pages)

3. APPLICATION'S T&C (2-3 pages)

4. INFRASTRUCTURE'S T&C (2-3 pages)

5. SUMMARY OF RESULTS (1-2 pages)

THREAT	CONTROL	EFFECTIVENESS

6. SUMMARY OF RESULTS (1-2 pages)

THREAT	CONTROL	EFFECTIVENESS

REFERENCES

1. P. ...

2. ...

3. ...

4. ...

5. ...

6. ...

21/09/2015

Massacci-Paci-Security Engineering

▶ 16

## Course Logistics

- **Basic course**
  - 12 weeks of 4 hours of lectures
  - 2 weeks of 4 hours of students' presentations
- **Practice work**
  - Students' presentations
  - Students' intermediate reports
- **Final Exam in January**
  - Final report
  - Final Presentation (with a industry customer)

21/09/2015

Massacci-Paci-Security Engineering

▶ 17

## Grading

- **Final report is the sum of the intermediate reports**
  - Final report determine the bulk of your vote
  - Final presentation of the work is around 20%
    - This is given by an industry person who will review your threats and security controls for relevance and appropriateness
    - His/her judgement is what counts
- **Intermediate Deliveries**
  - You can ignore them and submit everything at the end.
    - This is always your right as a student taking any course
    - Statistics says you are not going to make the grade
  - Intermediate reports are mandatory

21/09/2015

Massacci-Paci-Security Engineering

▶ 18

## Evaluating your own methods...

- **You will help us to evaluate CORAS and SecRAM with respect to**
  - Actual efficiency
  - Actual effectiveness
  - Easy of use, usefulness, intention to use
- **You will provide us feedback on the methods through**
  - Post-Task Questionnaire
  - Individual Interviews
- **Honest feedback are important to us!!!**

21/09/2015

Massacci-Paci-Security Engineering

▶ 19

## Rule of the game

- **Real life is not built out of 2 hours classes spread across 14 weeks semester**
  - Attending lectures is optional but well-advised
  - Delivering class' presentations is optional but well-advised
  - Delivering reports as scheduled is mandatory
  - Attending final exam is mandatory
- **On "I took this text from a colleague of mine"**
  - Remember I have been a student myself, thinking "he is not going to find it" is not going to be easy
  - If you are able to have people working for you and can sell their work as yours only as if they didn't existed, great, you'll be the next Steve Jobs
  - In all other cases (statistics is against you on) that's called plagiarism and is forbidden.
  - You will fail the class and that's it.

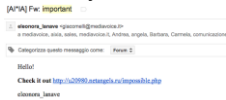
21/09/2015

Massacci-Paci-Security Engineering

▶ 20

## Rules of Engagement

- **Asking questions in class is always the best policy**
  - Your colleagues may be interested in the answer
  - Things are easier to explain
  - The prof gets hundreds email per day...
    - Today 9am – 14 am (66 emails and counting)
- **Do your homework first**
  - “I can’t bother to find the answer, I will ask the prof.”
    - Q: “I don’t remember to whom the deliverable should be submitted”
    - A: “read my slides”
- **Write with “[SecEng-2015]” in the subject**
  - “important” is a no go
    - Got 57 in the last months
  - “urgent” is not better



## Wednesday

- **Exercise will take place in Room PC201**
- **Comprehensibility Exercise**
  - CORAS Model
  - SECRAM Model
- **You will have to “look at a model” (for example as if you were participating to a presentation as a customer) and answer some questions**
  - Questions are in varying level of complexity
- **Yes, we know that you know nothing of the models → this is the whole point of the exercise**

## Reading Materials

