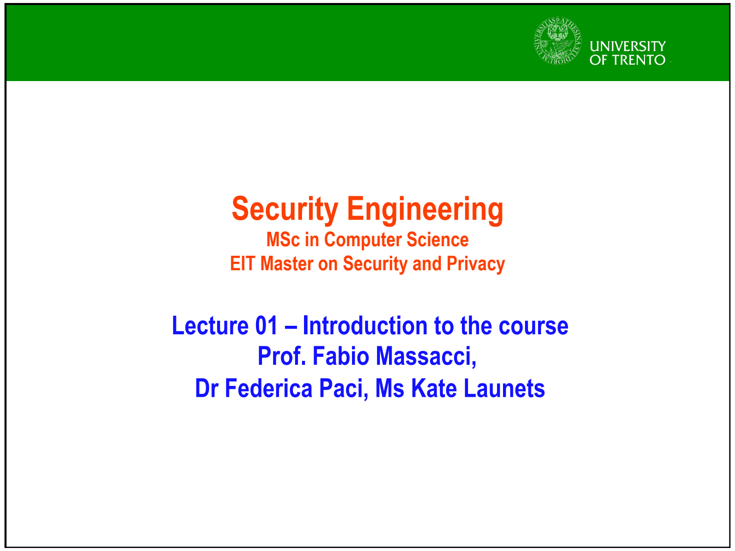


UNIVERSITY OF TRENTO

Security Engineering

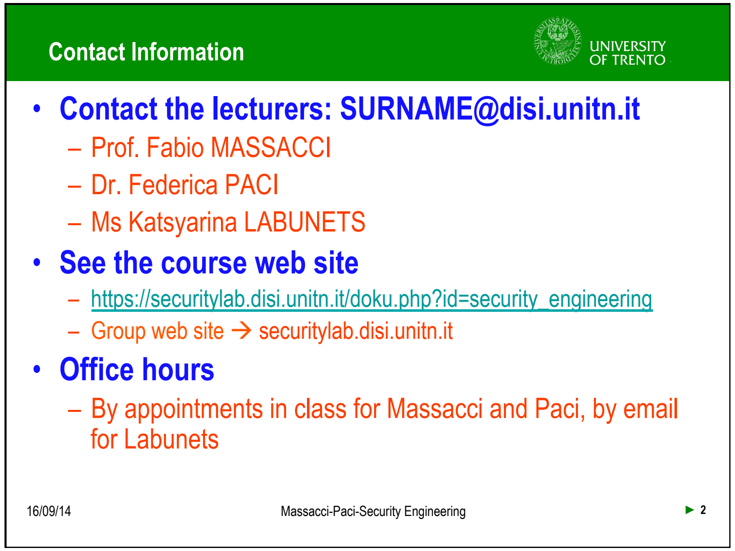
MSc in Computer Science

EIT Master on Security and Privacy

Lecture 01 – Introduction to the course

Prof. Fabio Massacci,

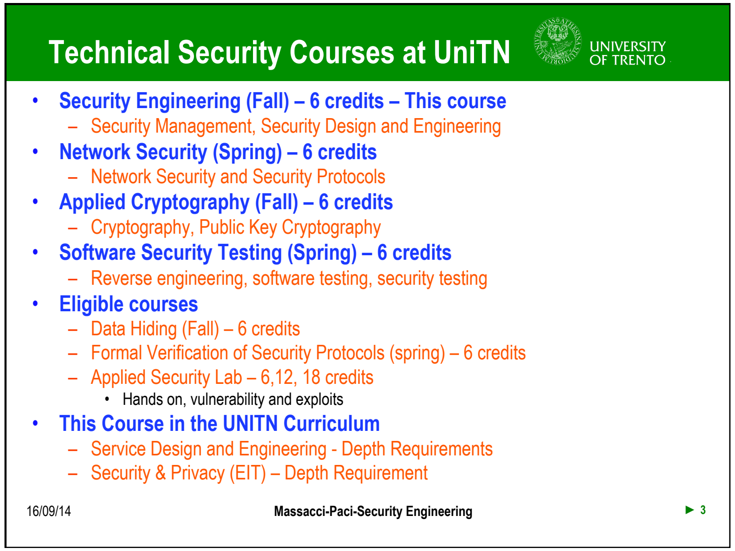
Dr Federica Paci, Ms Kate Launets



Contact Information

UNIVERSITY OF TRENTO

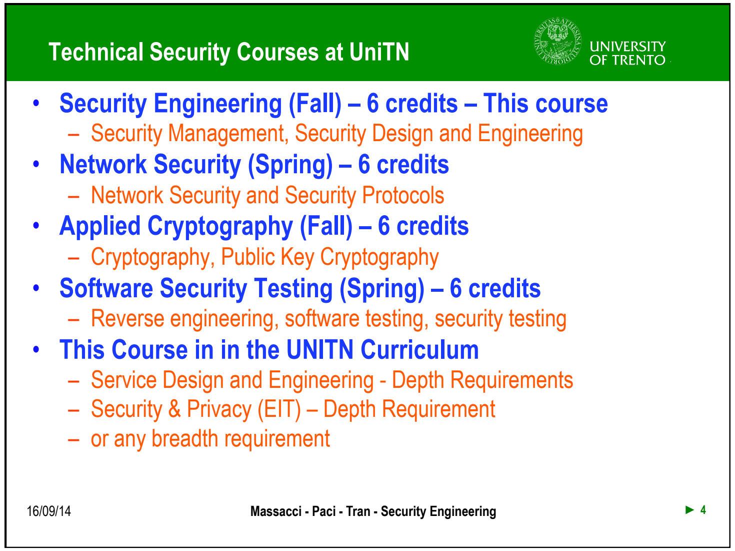
- Contact the lecturers: SURNAME@disi.unitn.it
  - Prof. Fabio MASSACCI
  - Dr. Federica PACI
  - Ms Katsyarina LABUNETS
- See the course web site
  - https://securitylab.disi.unitn.it/doku.php?id=security_engineering
  - Group web site → securitylab.disi.unitn.it
- Office hours
  - By appointments in class for Massacci and Paci, by email for Labunets



Technical Security Courses at UniTN

UNIVERSITY OF TRENTO

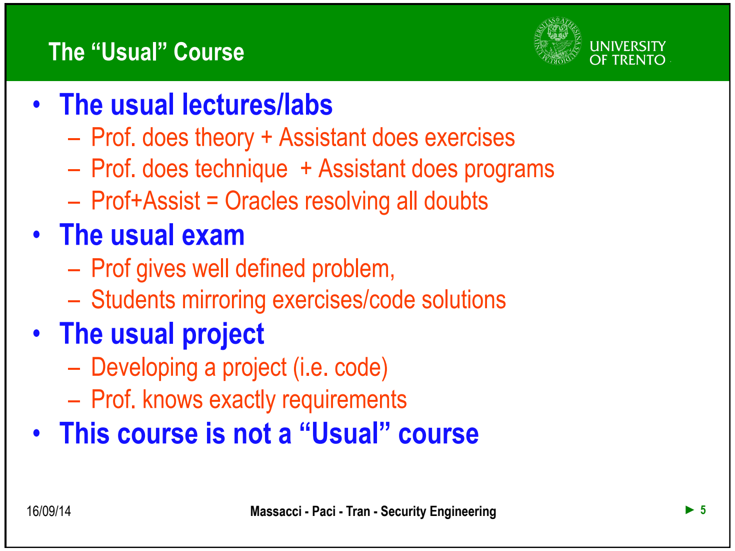
- Security Engineering (Fall) – 6 credits – This course
  - Security Management, Security Design and Engineering
- Network Security (Spring) – 6 credits
  - Network Security and Security Protocols
- Applied Cryptography (Fall) – 6 credits
  - Cryptography, Public Key Cryptography
- Software Security Testing (Spring) – 6 credits
  - Reverse engineering, software testing, security testing
- Eligible courses
  - Data Hiding (Fall) – 6 credits
  - Formal Verification of Security Protocols (spring) – 6 credits
  - Applied Security Lab – 6,12, 18 credits
    - Hands on, vulnerability and exploits
- This Course in the UNITN Curriculum
  - Service Design and Engineering - Depth Requirements
  - Security & Privacy (EIT) – Depth Requirement



Technical Security Courses at UniTN

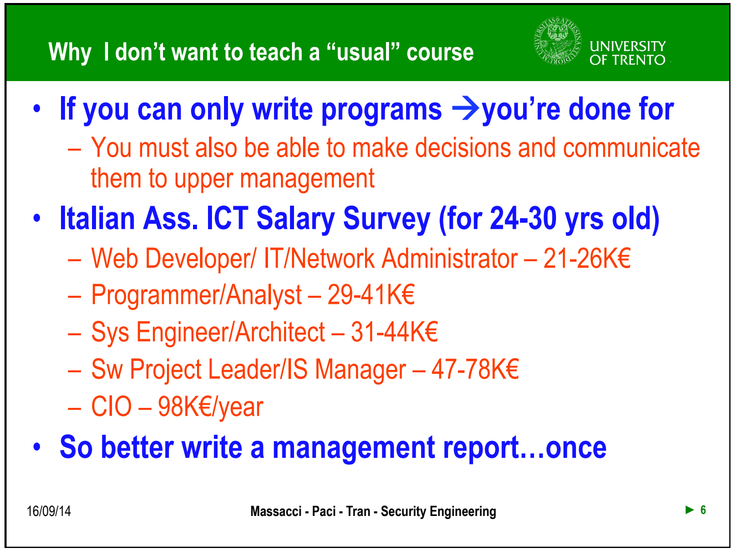
UNIVERSITY OF TRENTO

- Security Engineering (Fall) – 6 credits – This course
  - Security Management, Security Design and Engineering
- Network Security (Spring) – 6 credits
  - Network Security and Security Protocols
- Applied Cryptography (Fall) – 6 credits
  - Cryptography, Public Key Cryptography
- Software Security Testing (Spring) – 6 credits
  - Reverse engineering, software testing, security testing
- This Course in in the UNITN Curriculum
  - Service Design and Engineering - Depth Requirements
  - Security & Privacy (EIT) – Depth Requirement
  - or any breadth requirement



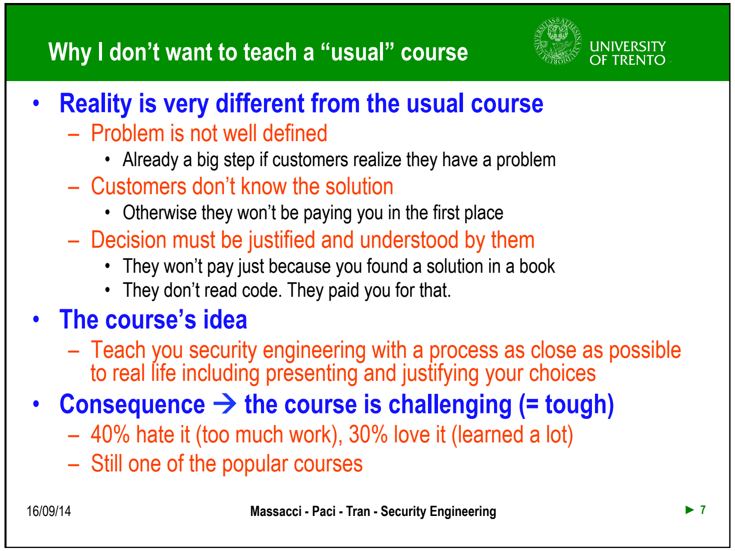
The "Usual" Course

- 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



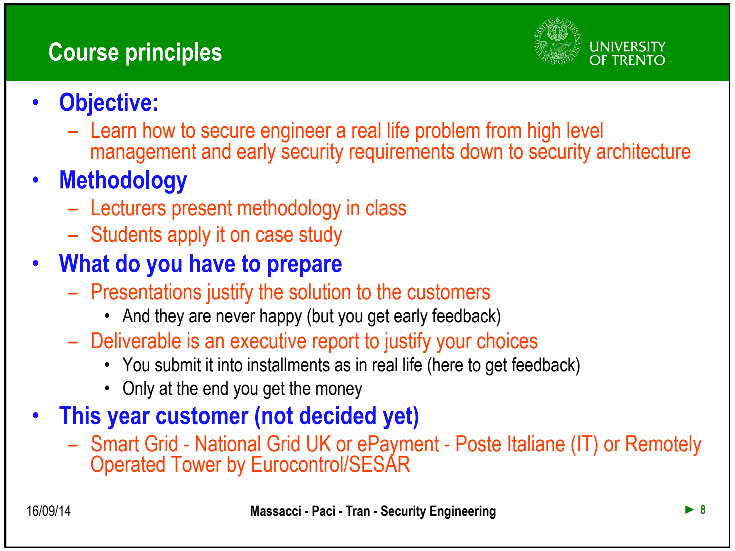
Why I don't want to teach a "usual" course

- 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 Ass. ICT Salary Survey (for 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…once



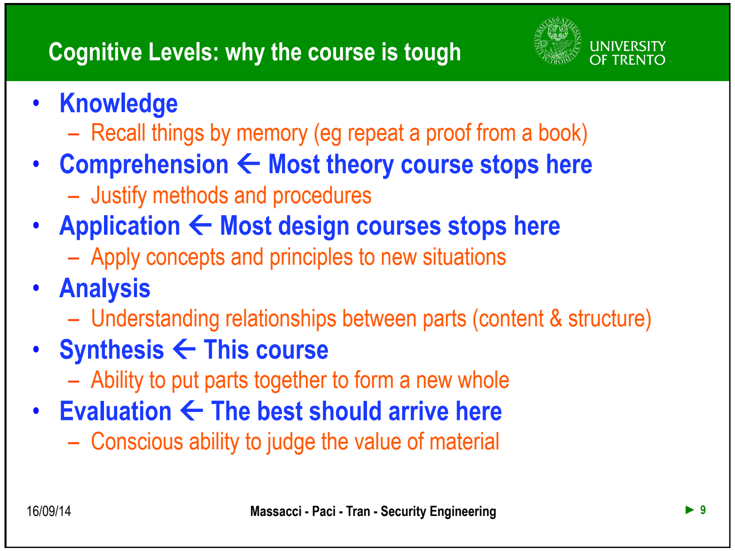
Why I don't want to teach a "usual" course

- 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



Course principles

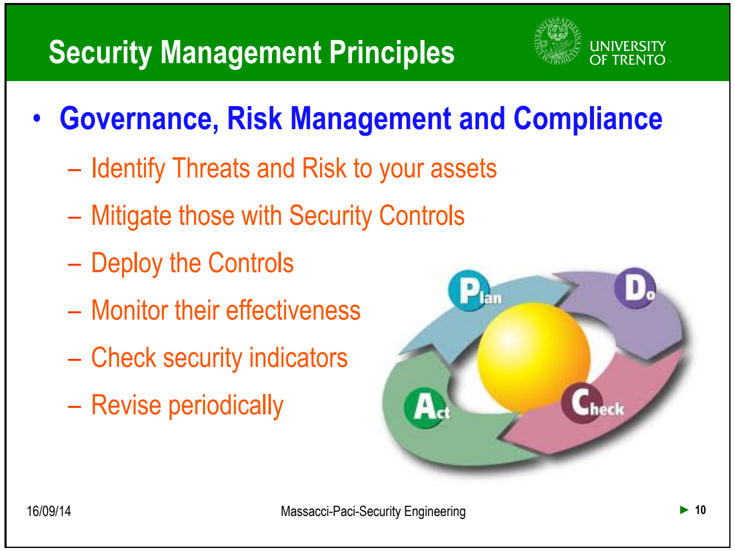
- Objective:
  - Learn how to secure engineer a real life problem from high level management and early security requirements down to security architecture
- Methodology
  - Lecturers present methodology in class
  - Students apply it on case study
- What do you have to prepare
  - Presentations justify 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)
  - Smart Grid - National Grid UK or ePayment - Poste Italiane (IT) or Remotely Operated Tower by Eurocontrol/SESAR



Cognitive Levels: why the course is tough

UNIVERSITY OF TRENTO

- 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

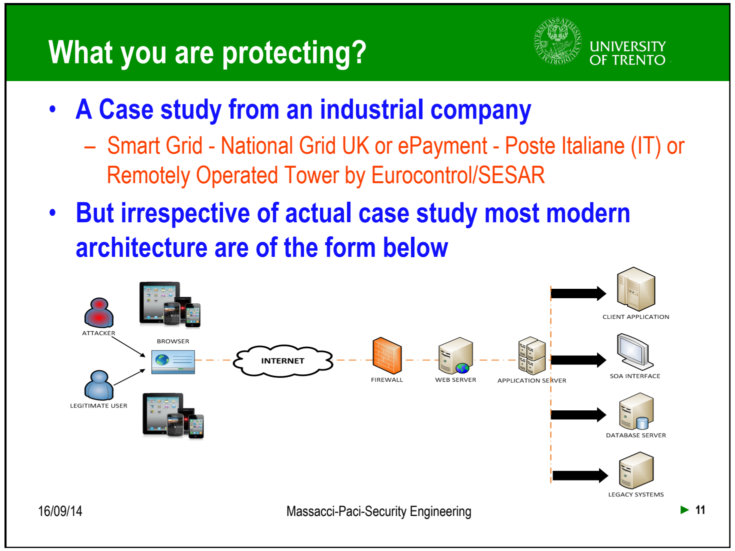


Security Management Principles

UNIVERSITY OF TRENTO

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

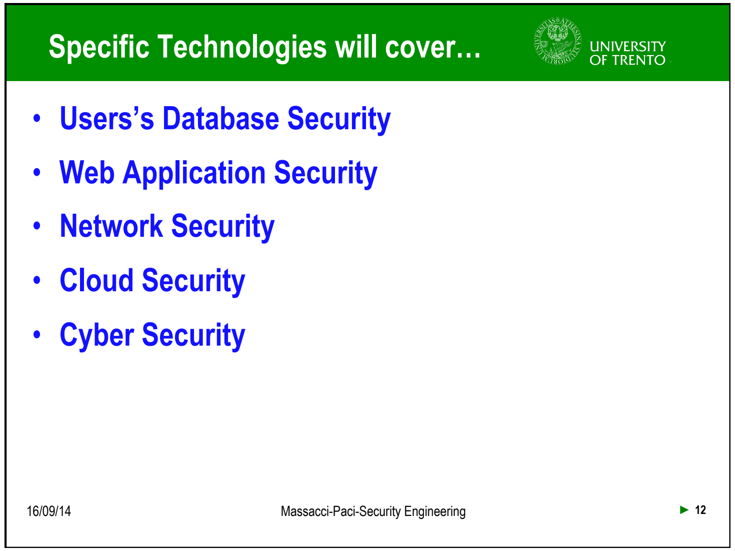
Plan
Do
Check
Act



What you are protecting?

UNIVERSITY OF TRENTO

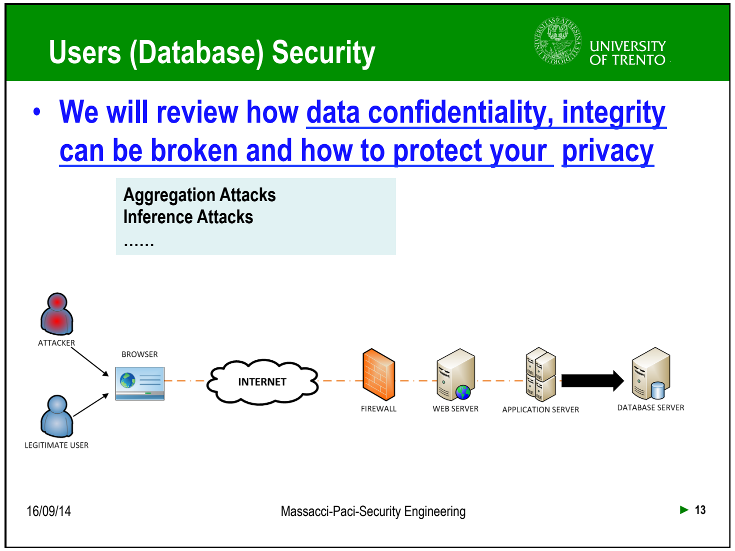
- A Case study from an industrial company
  - Smart Grid - National Grid UK or ePayment - Poste Italiane (IT) or Remotely Operated Tower by Eurocontrol/SESAR
- But irrespective of actual case study most modern architecture are of the form below



Specific Technologies will cover…

UNIVERSITY OF TRENTO

- Users's Database Security
- Web Application Security
- Network Security
- Cloud Security
- Cyber Security



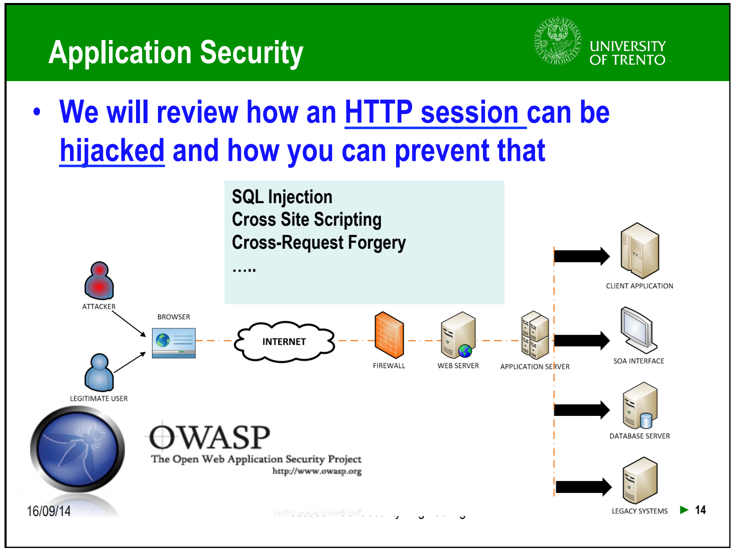
Users (Database) Security

UNIVERSITY OF TRENTO

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

Aggregation Attacks
Inference Attacks
……

16/09/14 Massacci-Paci-Security Engineering ▶ 13



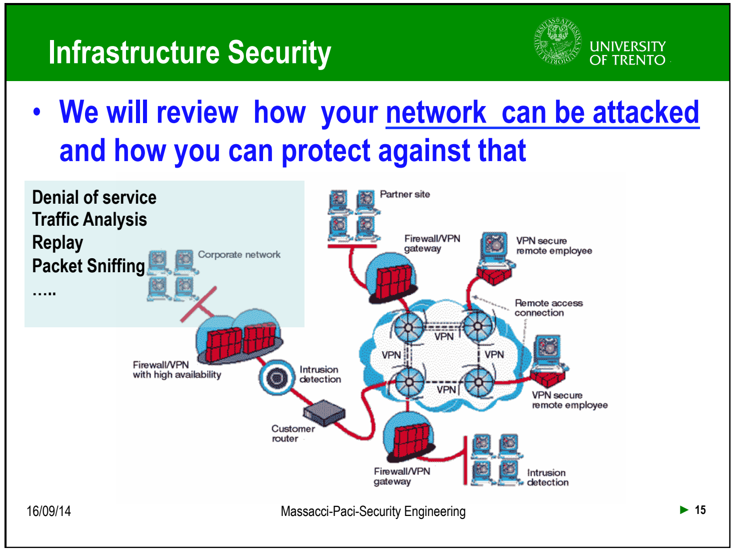
Application Security

UNIVERSITY OF TRENTO

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

SQL Injection
Cross Site Scripting
Cross-Request Forgery
…..

16/09/14 ▶ 14



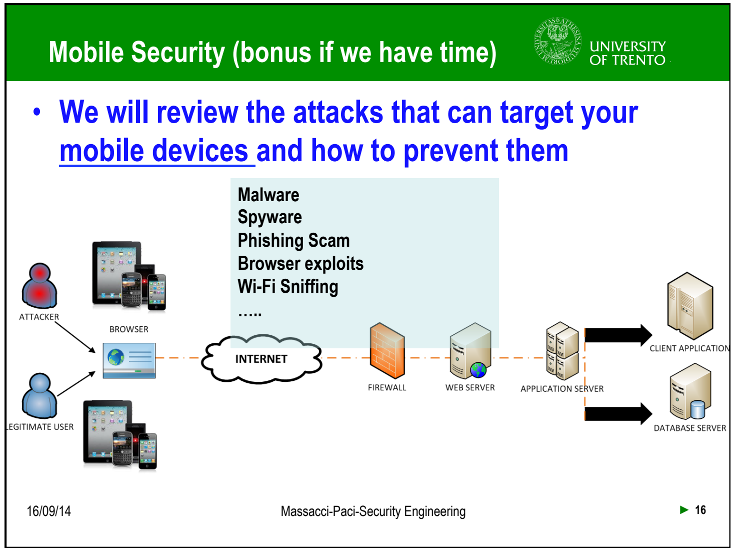
Infrastructure Security

UNIVERSITY OF TRENTO

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

Denial of service
Traffic Analysis
Replay
Packet Sniffing
…..

16/09/14 Massacci-Paci-Security Engineering ▶ 15



Mobile Security (bonus if we have time)

UNIVERSITY OF TRENTO

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

Malware
Spyware
Phishing Scam
Browser exploits
Wi-Fi Sniffing
…..

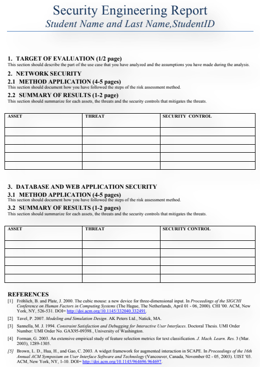
16/09/14 Massacci-Paci-Security Engineering ▶ 16

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

How to report your work: Report

1. Structure of the report
   1. Target of Evaluation
   2. Users Threats & Controls
   3. Application's T&C
   4. Infrastructure's T&C
2. Delivery
   1. In installment
   2. Download template from Web



Security Engineering Report

Student Name and Last Name,StudentID

1. TARGET OF EVALUATION (1/2 page)

This section should describe the part of the use case that you have analyzed and the assumptions you have made during the analysis.

2. NETWORK SECURITY

2.1 METHOD APPLICATION (4-5 pages)

This section should document how you have followed the steps of the risk assessment method.

2.2 SUMMARY OF RESULTS (1-2 page)

This section should summarize for each assets, the threats and the security controls that mitigates the threats.

ASSET	THREAT	SECURITY CONTROL

3. DATABASE AND WEB APPLICATION SECURITY

3.1 METHOD APPLICATION (4-5 pages)

This section should document how you have followed the steps of the risk assessment method.

3.2 SUMMARY OF RESULTS (1-2 pages)

This section should summarize for each assets, the threats and the security controls that mitigates the threats.

ASSET	THREAT	SECURITY CONTROL

REFERENCES

[1] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (The Hague, The Netherlands, April 01 - 06, 2000). CHI '00. ACM, New York, NY, 526-531. DOI= http://doi.acm.org/10.1145/332040.332491.

[2] Tavel, P. 2007. *Modeling and Simulation Design*. AK Peters Ltd., Natick, MA.

[3] Sannella, M. J. 1994. *Constraint Satisfaction and Debugging for Interactive User Interfaces*. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[4] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. *J. Mach. Learn. Res.* 3 (Mar. 2003), 1289-1305.

[5] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE. In *Proceedings of the 16th Annual ACM Symposium on User Interface Software and Technology* (Vancouver, Canada, November 02 - 05, 2003). UIST '03. ACM, New York, NY, 1-10. DOI= http://doi.acm.org/10.1145/964696.964697.

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)

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
  - Intermediate presentations are optional

What you need to be aware of …

UNIVERSITY OF TRENTO

- **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 feeback on the methods through**
  - Post-Task Questionnaire
  - Individual Interviews
- **Honest feedback are important to us!!!**

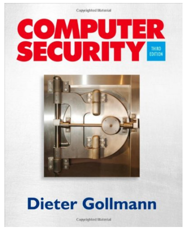
Rule of the game

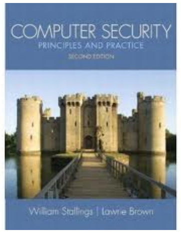
UNIVERSITY OF TRENTO

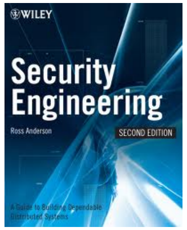
- **Real life is not built out of 2 hours classes spread across 14 weeks semester**
  - Attending lectures is optional but well-advised
  - Delivering class' presentations is optional but well-advised
  - Delivering reports as scheduled is mandatory
  - Attending final exam is mandatory
- **On "I took this text from a collegue of mine"**
  1. Remember I have been a student myself, thinking "he is not going to find it" is not going to be easy
  2. 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
  3. In all other cases (statistics is against you on (1+2)) that's called plagiarism and is forbidden.
  4. You will fail the class and that's it.

Reading Materials

UNIVERSITY OF TRENTO







Google scholar

ACM DL DIGITAL LIBRARY

CiteSeerx beta