UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Cyber Security Risk Assessment
Fall 2016

Lecture 01 – Introduction to the course

Prof. Fabio Massacci,

Dr Kate Launets

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Lecturers

- ***Main lecturers***
  - Prof. Dr. Fabio Massacci
    - Office hours by appointment in class
    - Can try your luck by email
  - Dr. Katerina Labunets
    - Office hour by appointment via email
- ***Others***
  - Dr. Luca Allodi
    - Office hour by appointment via email
  - Industry guest speakers

UNIVERSITY OF TRENTO - Italy

Digital MASTER SCHOOL

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***

UNIVERSITY OF TRENTO - Italy

Digital MASTER SCHOOL

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 pay you for that.
- ***The course's idea***
  - Teach you cyber security risk assessment with a process as close as possible to real life including presenting and justifying your choices

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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 Admin. – 21-26K€
  - Programmer/Analyst – 29-41K€
  - Sys Engineer/Architect – 31-44K€
  - Sw Project Leader/IS Manager – 47-78K€
  - CIO – 98K€/year
- ***So, write a management report…at least once***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Course principles

- ***Objective:***
  - Learn how to assess the risks in a real life problem from high-level controls down to security architecture
- ***Methodology***
  - Lecturers present methodology in class
  - Students apply it on various industrial 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 "final" customer (not decided yet)***
  - ePayment - Poste Italiane (IT), Digital Cinema by Technicolor, Smart Grid etc.

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

What Students Think

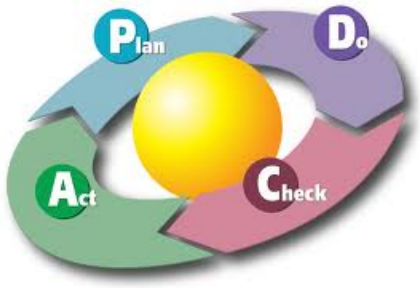
- ***Is the effort proportionate to the credits?***
  - No: 0
  - More No than Yes: 4
  - More Yes than No: 17
  - Yes: 20
  - Score: 85% (Department Average 84%)
- ***Are you satified with the course?***
  - No: 0
  - More No than Yes: 3
  - More Yes than No: 21
  - Yes: 17
  - Score: 93% (Department Average 81%)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Security Management Principles

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

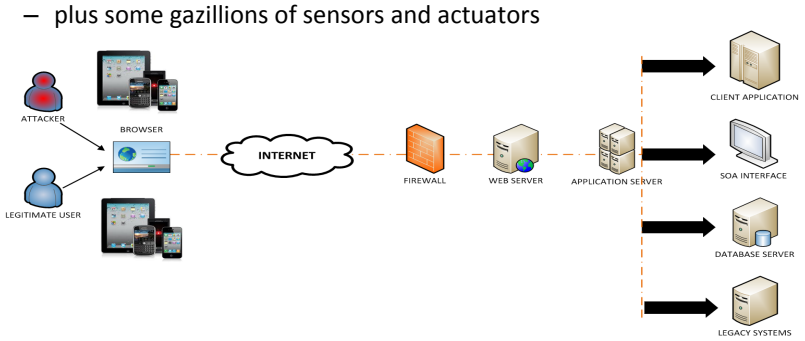


UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

What you are protecting?

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



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Make up your grade

- ***Comprehensibility (Up 2/30)***
  - Can you tell risks by looking at a risk assessment artefact (eg a table or a uml-style model)?
- ***Step-by-Step Risk Assessment Exercise (up to 12/30)***
  - Industrial Case: Remote Virtual Control Tower
  - Industrial Catalogue: EuroControl
    - You will have to sign a Non-Disclosure Agreement
  - Identify Assets, Identify Threats, Identify Pre and Post Controls (each 3/30)
- ***Assess Vulnerabilities Exercise (Up to 8/30)***
  - CVSS (Common Vulnerabilities Scoring System), world standard
  - Identify risk from description "as they arrive" in a CERT Bulletin (4/30)
  - Identify risk as they "apply to you" on your infrastructure (4/30)
- ***Final Project (Up to 14/30)***
  - Draft a complete risk assessment of an industrial case study
  - Evaluation by Industry experts

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

The "On-Going" Case study

- ***The Business Case***
  - At Airports there is control tower to guide airplanes n landing and take-off
  - Personnel is very expensive as needs to have turns, good training, etc. etc.
  - But some airport have very few flghts
- ***The Solution***
  - Remote and Virtual Control Tower
  - Move everything into a centralized location and replace the "Over the Window" view with fully virtualized centers with sensors etc.
  - Obvisouly security is kind of a problem…

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

The "On-Going" Methodology

- ***SESAR SECRAM***
  - Methodology developed by SESAR Project (Open Sky) specifically to address the case study
- ***EuroControl Catalogue***
  - Specifically targetted to provide a first set of threat and corresponding security
  - It is confidential, so you will have to sign a Non-Disclosure Agreement
  - Every student will have his/her own catalogue **on paper and watermaked**
  - **If you don't return it, you don't pass the exam**
    - (and I will make sure you don't graduate either)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

How to report your work: Report

1. ***Structure of the report***
   1. Target of Evaluation
   2. Threats and Risk Assessment
   3. Pre-Controls
   4. Post-Control
2. ***Delivery***
   1. In installment during Exercises
   2. In single shot for final 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 summarise 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 summarise 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. GAX95-09598., 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.

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Course Logistics

- ***Basic course***
  - 12 weeks of 4 hours of lectures
- ***Practice work (Partially graded)***
  - Exercises in Computer Room (graded)
  - Quizzes to answer at home (not graded)
- ***Final Exam in January (graded)***
  - Final report
  - Final Presentation (with a industry customer)

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Rule of the game

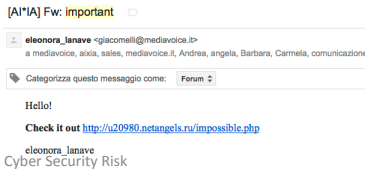
- ***On "I took this text from a collegue of mine"***
  - Remember I have been a student myself, thinking "he is not going to find it" is going to disappoint you
- ***IF***
  - you are able to have people working for you and you can sell their work as yours as if they didn't existe → Great, you're the next Steve Jobs → 30 cum Laude is deserved
- ***ELSE***
  - That's called plagiarism and is forbidden.
  - You will fail the class and that's it.
- ***Statistics is against you on the IF clause***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

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 before 10:30 (… 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 "[CybRisk]" in the subject***
  - "important" is a no go
  - "urgent" is not better



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Wednesday

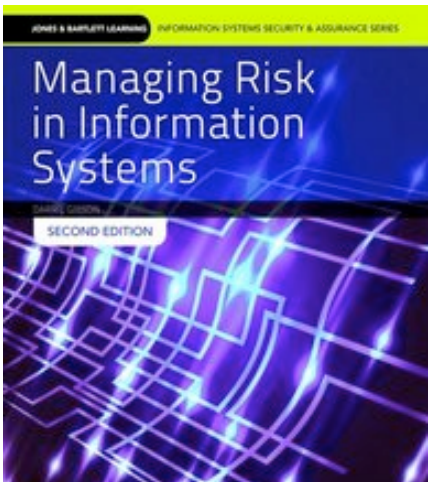
- ***Exercise will take place in Room PC201***
- ***Comprehensibility Exercise***
  - "Tabular" Description of a Risk Assessment
  - Or a "Graphical" Description
- ***You will have to "look at the artefact" (for example as if you were participating to a presentation as a customer) and answer some questions***
  - 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***

UNIVERSITY OF TRENTO - Italy

Digital MASTER SCHOOL

Textbook

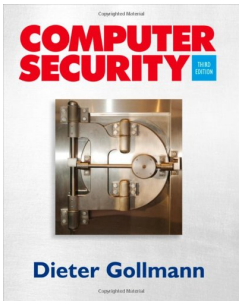
- Darril Gibson. Managing Risk in Information Systems, 2nd edition.
- *http://www.jblearning.com/catalog/9781284055955/*

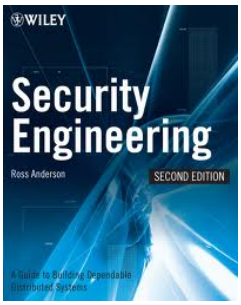


UNIVERSITY OF TRENTO - Italy

Digital MASTER SCHOOL

Reading Materials





ACM DL DIGITAL LIBRARY

Google scholar