Security Engineering

Juan E. Tapiador
Department of Computer Science, UC3M
jestevez@inf.uc3m.es

Universidad Carlos III de Madrid

Fall 2011 – 4th year BSc in Computer Science, 6 ECTS
Tue 14:30 – 16:00 (reduced groups, practicals)
Wed 12:30 – 16:00 (all, theory)

What is this course about?

This is a course about cybersecurity understood as an engineering discipline. As such, we' ll focus not only on technical aspects, but also on things that make real-world security hard: human factors, operational restrictions, legal constraints, etc.

We' ll cover various topics, including access control systems, network security, authentication protocols, malware, EM emanations & physical security.

Throughout the course we' ll try to pay special attention to `*security thinking*' , i.e. the ability to think up ways to attack a system and to conceive worst-case scenarios, particularly those that imply thinking outside the box.

Detailed info here (the page needs some polishing up…): http://www3.uc3m.es/reina/Fichas/Idioma_2/218.13893.html

Contents

1 Security Engineering: Overview

assets; vulnerabilities; attacks; human factors; security principles; prudent practices

2 Access Control Models and Systems

operating system security; MAC and DAC models; BLP model; Biba model; Lattice models; Chinese wall; MLS systems; difficulties and practical failures

3 Network Security

cryptographic protocols; authentication; attacks; implementation flaws; formal verification; network attacks, firewalls; IDS; malware

4 Physical Security

accidents; break-ins; comms interception; EM leakages; data loss; surveillance;

Recommended literature for the course

1 Ross Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems. 2nd ed., Wiley, 2008

2 Dorothy Denning. Information Warfare and Security. Addison-Wesley, 1998

3 Pfleeger & Pfleeger: Security in Computing. 4th ed., Prentice Hall, 2007

4 Rolf Oppliger: Technologies for the World Wide Web. 2nd ed., Computer Security Series. Artech House Publishers, 2003

5 J.R. Vacca (Ed.): Computer and Information Security Handbook. Elsevier, The Morgan Kaufmann Series in Computer Security, 2009.

What you really want to know: Assessment

Option 1: Regular

Final mark computed as:

a) Practicals: 40%

b) Open assessment (report/essay): 20%

c) Written assessment: 40% (it' s *compulsory* to pass it!)

If you choose to do just c), then the final mark is 0.6 times the mark obtained in the assessment.

Option 2: Extraordinary

Option 2.1 – For those who failed a) and/or b) but passed c) Hand in revised material. The final mark is computed as above.

Option 2.2 – Seat a written assessment. Final mark is the mark obtained. (Not recommended at all!)