ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

DTC-TEL-612 Security in Communications Systems

SEMESTER: Fall

CREDITS: 4.5 ECTS (3 hrs. per week: 2 Theory + 1 Lab, on average)

LANGUAGE: English

DEGREES: MIT

Course overview

This course highlights the dangers of security threats and describes the most common techniques to break the security of a system. Many different attacks are described and tested in the lab, including XSS, CSRF and attacks against SSL. The course also covers Security policy, Management, and Standards.

Prerequisites

Previous knowledge is required on network communications, web applications, and introduction to cryptography. Some programming skills are required for lab practices and exercises in class.

Course contents

Theory:

Chapter 1 – Introduction and class overview

Cyber security in 2015, High profile data breaches, Inside the day of a security professional.

Chapter 2 – Browser and HTTP fundamentals

Anatomy of the web, HTTP requests and responses, Sessions and cookies, Browser security features, Same Origin Policies, Entity and JavaScript encoding, Modern HTML5 features, Cross-domain requests, Post messages and local storage, Browser fingerprinting.

Chapter 3 – Security Architecture and Security Analysis Methodologies

Security Architecture, Threats and defense strategies - STRIDE, Code review and traffic analysis, Secure Development Lifecycle, Security Analysis Methodologies.

Chapter 4 – Attacks against the application layer, and defenses.

Insecure direct object references, Security misconfigurations, Broken authentication, Broken session management, Broken authorization, RTL attacks, Attacks on CAPTCHA, Leveraging open metadata, Weak password hashing, DNS rebinding.

Chapter 5 – Common web vulnerabilities

OWASP top 10, Cross-Site Scripting XSS, Cross-Site Request Forgery CSRF, XML External Entity attacks, Clickjacking, Open redirects, SQL Injection, Blind SQL Injection, Denial of Service, Mutation XSS attacks, Same Origin Method Execution.

Chapter 6 – Attacks against SSL/HTTPS and defenses

Fundamentals of SSL, Man-in-the-Middle attack, certificates and certificate pinning, Mixed content HTTPS/HTTP, Bypassing HSTS transport security, SSL Stripping, BREACH, LUCKY 13, RC4 biases, POODLE, Heartbleed.

Chapter 7 – More advanced side channel attacks

Padding oracles (BEAST), Timing and caching attacks, Attacks leveraging Unicode, Content sniffing and polyglots, Rosetta flash, SMB relay, Geoinference.

Chapter 8 – Mobile devices security

The sandbox models, Android security overview, iOS Security overview, Mobile Device Management, Testing mobile applications.

Chapter 9 – Security management systems

Management standards, Security policies, Security controls, Network access, Identity management, Risk assessment.

Chapter 10 – Security Monitoring and Computer Forensics

Intrusion Detection systems (IDS), Network firewalls, Cyber forensics, Anomaly detection, Incident Response, APTs.

Chapter 11 – Policies and security governance

Business integrity, Privacy management, Fraud prevention, Vulnerability and threat management, Business Continuity Plans (BCP), Enterprise information security policy.

Chapter 12 – Information Trust and Regulatory Compliance

Introduction to international certifications and standards. Security in different industrial sectors: PCI DSS, FISMA, GLBA, SOX, ISO 27001 and HIPAA, Spanish Data Protection Law (LOPD), Common European Union security compliance initiatives, Data residency and privacy issues.

Laboratory:

There are exercises related with many different techniques. The exercises change every year depending on current vulnerabilities, software version and patches, etc. Exercises always included are: XSS, CSRF, SQL injection, SSL attacks, network traffic sniffing, SSL Stripping.

Textbook

- John R. Vacca, Managing Information Security, Second Edition - http://www.amazon.com/Managing-Information-Security-Second-Edition/dp/0124166881
- Michal Zalewski ,The Tangled Web: A Guide to Securing Modern Web Applications http://www.amazon.com/The-Tangled-Web-Securing-Applications/dp/1593273886

Grading

The overall grade is obtained as follows:

- Final exam: 50%.
- Other exams during the term: 20%
- Homework and Lab reports 30%.