UNIVERSITÀ DI PISA

CYBERSECURITY

GIANLUCA DINI

Academic year	2018/19
Course	COMPUTER ENGINEERING
Code	794II
Credits	9

Modules	Area	Type	Hours	Teacher(s)
CYBERSECURITY	ING-INF/05	LEZIONI	90	GIANLUCA DINI PERICLE PERAZZO

Obiettivi di apprendimento

Conoscenze
- Crittografia applicata
- Principi di analisi, progettazione e codifica di applicazioni e protocolli sicuri.

Modalità di verifica delle conoscenze
Prova scritta e prova orale.

Capacità
Sapere analizzare, progettare e realizzare protocolli ed applicazioni sicure.

Modalità di verifica delle capacità
Sviluppo e realizzazione di un progetto.

Prerequisiti (conoscenze iniziali)
Conoscenze di calcolo delle probabilità, teoria della complessità, linguaggi di programmazione, architettura del calcolatore, sistemi operativi, reti di calcolatori.

Programma (contenuti dell'insegnamento)
Applied cryptography
Symmetric Ciphers: one-time pad, stream-ciphers, and block-ciphers. The DES and AES ciphers. Encryption modes. Hash functions: message digest codes and message authentication code. Black box attacks: the birthday attack. Diffie-Hellman key establishment. Asymmetric ciphers: the RSA and ElGamal cryptosystems. Digital signatures, certificates, certification authorities, and public key infrastructures. The X.509v3 certificate format. Perfect forward security. Secure Pseudo-Random Generators. Performance and security of cryptosystems. Side-channel attacks: timing attack; fault-injection attacks; power analysis.
Programming secure applications
Buffer overflow. C/C++ secure coding. Secure coding hands-on. OpenSSL hands-on. Penetration testing and malware. Threat modeling: how to identify and prioritize vulnerabilities. Design and analysis of secure protocols. The BAN logic.
Case studies
IpSec: ESP and AH mode.
Secure Socket Layer: Handshake and Record protocol. Payment transactions over SSL.
Kerberos: basic scheme; the Ticket Granting Service; delegation: forwarding and proxiable tickets; realms.

Modalità d'esame
Svolgimento di un progetto, prova scritta e prova orale.

Pagina web del corso
http://www.iet.unipi.it/g.dini/Teaching/sncs/index.html