Sicurezza dei Computer e delle Reti

Sintesi della lezione introduttiva

Università di Roma Tor Vergata – Docente: Giuseppe Bianchi

Obiettivi del Corso

Il corso ha lo scopo di fornire una comprensione approfondita dei principali **primitivi crittografici** utilizzati in informatica. Si cercherà di capire non soltanto come vengono applicati questi meccanismi, ma soprattutto come possono essere utilizzati impropriamente, generando così vulnerabilità. Un altro obiettivo cardine è la conoscenza dei protocolli di sicurezza di Internet, analizzando strumenti e metodologie moderne per l'esplorazione e lo sfruttamento delle tecnologie.

Contestualizzazione del Corso

La sicurezza informatica è un campo vasto e articolato. Una parte rilevante riguarda la gestione delle *vulnerabilità* e le tecniche di **ethical hacking** che puntano a individuare e correggere falle nei sistemi ICT. Vengono affrontati anche aspetti di sicurezza delle infrastrutture di rete e i meccanismi base per la difesa di sistemi e reti. La classe si concentra su *come utilizzare correttamente la crittografia* e sui protocolli Internet, con cenni specifici alla difesa dei sistemi dall'hardware alle tecnologie di localizzazione (canali laterali).

Messaggi Chiave

Un messaggio fondamentale della materia è che **una buona crittografia può essere utilizzata male**. La maggior parte dei gravi incidenti di sicurezza derivano da protocolli mal progettati o vulnerabili. Il corso offre esempi pratici e rivede concetti di base, con particolare attenzione a come si costruiscono protocolli di sicurezza affidabili, focalizzandosi sui casi di TLS e IPsec: come sono stati progettati e perché sono state fatte certe scelte.

Storie dal Mondo Reale

Un esempio classico di errore pratico è quello legato alla percezione errata della sicurezza: spesso si tende a fidarsi di algoritmi di crittografia avanzata (come AES usato nei sistemi militari), senza considerare configuarzioni improprie che possono annullare la protezione, come l'uso di vettori di inizializzazione (`IV`) nulli o difetti storici nei protocolli come WEP per WiFi e nel 2G. Il recente attacco *ZeroLogon* del 2020 dimostra come errori nella progettazione possano avere conseguenze critiche.

Sillabo del Corso

Il corso è diviso in più moduli:

- **Crittografia di base** (circa 1.5 CFU): tecniche di attacco e contromisure, costruzioni fondamentali (cifrari a flusso, cifrari a blocchi, funzioni hash), Merkle-Damgard, NMAC e HMAC, funzioni pseudo casuali, gestione delle chiavi, algoritmi a chiave pubblica, firme digitali, ecc. Questo modulo si intreccia parzialmente con la sicurezza infrastrutturale.
- **Autenticazione e supporto ai protocolli di rete** (circa 1.5 CFU): meccanismi di base, PPP, PAP, CHAP, password monouso, EAP, autenticazione nelle reti mobili (3G, 4G, 5G), RADIUS, vulnerabilità correlate, DIAMETER, infrastrutture a chiave pubblica (PKI).
- **Analisi approfondita di TLS e IPsec** (circa 3 CFU): analisi degli handshake, gestione delle chiavi RSA e Diffie-Hellman (anonimo, fisso, effimero), forward secrecy, composizione MAC e crittografia, principali attacchi (BEAST, Oracle, CRIME, ROBOT, ecc.), differenze tra TLS 1.2 e 1.3, VPN con IPsec, protocollo IKE, confronto TLS vs IPsec.
- **Crittografia avanzata** (circa 3 CFU): secret sharing (segredo banale, schema di Shamir), commitment, secret sharing verificabile (Feldman, Pedersen), computazione multi-partito sicura, generazione distribuita delle chiavi, matrici di controllo d'accesso, crittografia threshold, firme threshold, crittografia ellittica (ECDH, ECDSA), mappe bilineari, pairing, cifratura basata su identità, accenni alla Attribute-Based Encryption.
- **Temi extra** (tempo permettendo): TESLA, Merkle Trees, Blockchain, sicurezza dello storage, sicurezza nelle reti wireless, temi specifici presentati da esperti ospiti.

Modalità del Corso

Esistono due percorsi, uno da 6 CFU che si ferma ai concetti su TLS/IPsec e copre circa i 2/3 delle lezioni, e uno da 9 CFU che include l'intero programma.

Esami

Negli anni passati erano previsti tre prove scritte intermedie e una prova orale (o mista). Quest'anno probabilmente si ridurrà a due prove scritte.

Materiale didattico e riferimenti

Alcuni testi consigliati:

- Jean Philippe Aumasson, *Serious Cryptography*, No Starch Press, 2018 – ottima trattazione pratica.
- Nadjid Nakhjini, Mahsa Nakhjini, *AAA and Network Security for Mobile Access*, Wiley, 2005 – materiale sui protocolli principali.
- Stephen Thomas, *SSL and TLS Essentials*, Wiley, 2000 – monografia su TLS/SSL (datata ma valida).
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, *Handbook of applied cryptography*, 2001 – disponibile online, non introduttivo.
- Materiali integrativi e dispense verranno forniti durante il corso.

Comunicazioni e Mailing List

Per le comunicazioni viene utilizzata la mailing list iss@lists.uniroma2.it. Registrazione su `https://lists.uniroma2.it/index.html/info/iss` anche se il docente userà principalmente Teams; occorre assicurarsi di essere nel team dedicato.