BLOOMING

Inclusion and Diversity in STEAM

Piano di lezione

Mettere in sicurezza il futuro: comprendere la sicurezza delle reti e la crittografia

---

Obiettivo:

- Gli studenti apprenderanno le basi della sicurezza delle reti, incluse le minacce più comuni, l'importanza della crittografia e i metodi per proteggere i dati durante la trasmissione. La lezione introdurrà concetti chiave come la crittografia, la sicurezza resistente ai computer quantistici e il rilevamento degli attacchi in tempo reale.

Materiali:

- Proiettore per le slide sui concetti di sicurezza delle reti
- Dispense sugli attacchi più comuni (man-in-the-middle, denial of service, phishing, ecc.)
- Laptop o computer per esercitazioni simulate di sicurezza di rete
- Strumenti/software di sicurezza di rete (ad es. Wireshark, strumenti base di crittografia)
- Accesso a Internet per ricercare vulnerabilità e difese delle reti

---

Informazioni di base:

La sicurezza delle reti si riferisce alle pratiche e tecnologie progettate per proteggere l'integrità, la riservatezza e la disponibilità dei dati trasmessi attraverso le reti. Con l'aumento della complessità degli attacchi informatici, è fondamentale implementare misure di sicurezza robuste come crittografia, firewall e sistemi di rilevamento in tempo reale. Le minacce emergenti, come il calcolo quantistico,

Co-funded by the European Union

Erasmus+
Enriching lives, opening minds.

pongono nuove sfide ai metodi crittografici tradizionali, rendendo la **crittografia resistente ai quanti** un campo di studio cruciale.

1. Introduzione alla sicurezza delle reti (15 minuti):

- Presentare una panoramica sull'importanza della sicurezza delle reti nell'era digitale.
- Spiegare come le reti siano vulnerabili a vari attacchi (MITM – man-in-the-middle, DoS – denial of service, phishing).
- Introdurre termini di base come crittografia, firewall e protocolli di rete, evidenziando l'importanza di proteggere i dati in trasmissione.
- Accennare alla sfida emergente del calcolo quantistico, che mette a rischio i sistemi crittografici tradizionali.

2. Attacchi comuni alle reti e difese (20 minuti):

- Suddividere la classe in piccoli gruppi, assegnando a ciascun gruppo un attacco comune (MITM, DoS, phishing o SQL injection).
- Ogni gruppo deve ricercare e presentare:
    - Come funziona l'attacco
    - Quali danni può causare
    - Metodi per prevenirlo o mitigarne gli effetti (es. crittografia, firewall, autenticazione a più fattori)
- Dopo ogni presentazione, discutere l'importanza dei protocolli di sicurezza capaci di rilevare e prevenire tali attacchi.

3. Attività pratica: simulazione del traffico di rete e rilevamento degli attacchi (30 minuti):

- Creare una rete simulata con un tool come Wireshark.

- Far osservare agli studenti traffico normale e traffico malevolo per comprendere come rilevare attacchi come MITM e DoS.
- Identificare potenziali vulnerabilità della rete simulata e proporre difese (es. crittografia più robusta, segmentazione di rete).
- Guidare gli studenti nella cifratura dei dati con software di crittografia di base e mostrare come i dati cifrati siano protetti durante la trasmissione.

4. Esplorare la crittografia resistente ai quanti (15 minuti):

- Introdurre il concetto di calcolo quantistico e spiegare perché minaccia i metodi crittografici tradizionali (come RSA ed ECC).
- Presentare la **crittografia resistente ai quanti**, che utilizza algoritmi progettati per resistere ad attacchi condotti con computer quantistici.
- Spiegare come ricercatori come la dott.ssa **Anca Jurcut** stiano sviluppando questi algoritmi per garantire comunicazioni sicure anche in futuro.

Visualizzazione e discussione:

- Dopo la simulazione, utilizzare un flipchart o una lavagna per creare una mappa visiva dei diversi livelli di sicurezza di rete (firewall, crittografia, sistemi di rilevamento delle intrusioni, ecc.).
- Discutere come questi livelli collaborino per creare una rete sicura.
- Invitare gli studenti a riflettere su come i protocolli di sicurezza potrebbero evolversi con la diffusione del calcolo quantistico e sul ruolo centrale del rilevamento degli attacchi in tempo reale nella sicurezza futura.

Punti di discussione aggiuntivi:

- **Applicazioni della sicurezza di rete:** spiegare la sua importanza in settori come banche, sanità, governo e uso personale (es. transazioni online, email, social media).
- **Il futuro della crittografia:** discutere con gli studenti su come gli algoritmi resistenti ai quanti proteggeranno i dati nell'era del calcolo quantistico.
- **Hacking etico:** introdurre il concetto di hacking etico, in cui esperti di sicurezza testano volontariamente le reti per scoprirne le vulnerabilità e rafforzarne le difese.

Valutazione:

Chiedere agli studenti di scrivere una riflessione su:

- Quale attacco di rete hanno trovato più pericoloso e perché.
- Come la crittografia protegge i dati durante la trasmissione.
- Perché il calcolo quantistico rappresenta una sfida per i metodi crittografici attuali e come la crittografia resistente ai quanti aiuti a superare questa sfida.

Valutare:

- le presentazioni di gruppo,
- la partecipazione all'attività pratica,
- la capacità di rilevare attacchi e proporre difese.