




Welcome to the CoGrammar

PKI and Man-in-the-middle Attacks

The session will start shortly...

Questions? Drop them in the chat. We'll have dedicated moderators answering questions.



Cyber Security Session Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
(Fundamental British Values: Mutual Respect and Tolerance)
- No question is daft or silly - **ask them!**
- There are **Q&A sessions** midway and at the end of the session, should you wish to ask any follow-up questions.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Academic Sessions. You can submit these questions here: [Questions](#)

Cyber Security Session Housekeeping cont.

- For all **non-academic questions**, please submit a query: www.hyperiondev.com/support
- We would love your **feedback** on lectures: [Feedback on Lectures](#)
- Find all the lecture **content** in you [Lecture Backpack](#) on GitHub.
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.

Safeguarding & Welfare

We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member, or you feel like something isn't right, speak to our safeguarding team:



Ian Wyles
Designated Safeguarding
Lead



Simone Botes



Nurhaan Snyman



Rafiq Manan



Ronald Munodawafa



Tevin Pitts

Scan to report a
safeguarding concern



or email the Designated
Safeguarding Lead:
Ian Wyles
safeguarding@hyperiondev.com

Stay Safe Series:

Mastering Online Safety One week at a Time

While the digital world can be a wonderful place to make education and learning accessible to all, it is unfortunately also a space where harmful threats like online radicalization, extremist propaganda, phishing scams, online blackmail and hackers can flourish.

As a component of this BootCamp the ***Stay Safe Series*** will guide you through essential measures in order to protect yourself & your community from online dangers, whether they target your privacy, personal information or even attempt to manipulate your beliefs.

Security Tip

"Enable login alerts for all your online accounts."

Why?

Login alerts notify you immediately if your account is accessed from an unrecognized device or location. This early warning system allows you to take quick action—such as changing your password or enabling multi-factor authentication (MFA)—to secure your account before further damage is done.

How to Enable:

- Check your account security settings for an option like "Login Alerts" or "Account Activity Notifications."
- Ensure the alerts are sent to a secure email or phone number that only you can access.

Stay proactive and keep hackers out by staying informed!

CoGrammar

PKI and Man-in-the-middle Attacks

December 2024

Learning Objectives & Outcomes

- Define and Explain the components and functions of PKI and the concept of Man-In-The-Middle (MITM) attacks.
- Explain how PKI secures communications and prevents attacks through authentication and encryption.
- Demonstrate how to identify secure communication (e.g., HTTPS) and use preventive measures like VPNs and digital certificates.
- Examine vulnerabilities in PKI systems and analyze how MITM attacks exploit unsecured communication channels.
- Design protocols or policies using PKI to secure sensitive information and defend against MITM attacks.

Polls

Please have a look at the poll notification and select an option.

What do you think is the primary function of encryption in cybersecurity?

- A. To protect data from being intercepted
- B. To verify identities
- C. To track communication logs
- D. I'm not sure

Polls

Please have a look at the poll notification and select an option.

Do you use Multi-Factor Authentication (MFA) for your personal or work accounts?

- A. Yes, always
- B. Sometimes
- C. Rarely
- D. No, never

Introduction to PKI

- **PKI (Public Key Infrastructure)**
 - a. Is a framework for managing digital certificates and public-private key pairs.
 - b. Ensures secure communication and data exchange over untrusted networks

Key Components of PKI

- **Certificate Authority (CA):** Issues and verifies digital certificates.
- **Registration Authority (RA):** Validates user requests before certificates are issued.
- **Digital Certificates:** Bind public keys to entities (e.g., users, servers).
- **Public and Private Keys:** Enable encryption and authentication.
- **Certificate Revocation List (CRL):** List of revoked certificates.

Uses of PKI

- Secure email communication (S/MIME).
- Website authentication (SSL/TLS).
- Digital signatures for document verification.
- Securing IoT devices and applications.

Understanding Man In the Middle Attack

- What is a MITM attack?
 - An attack where a malicious actor intercepts and potentially alters communication between two parties without their knowledge.

How MITM attack works

- Attacker intercepts communication (e.g., through public Wi-Fi).
- Acts as an intermediary, relaying messages while reading or altering data.
- Victims believe they are communicating directly.

Common Techniques

- **Eavesdropping:** Monitoring unencrypted data.
- **Session Hijacking:** Stealing session tokens.
- **SSL Stripping:** Downgrading HTTPS to HTTP.
- **DNS Spoofing:** Redirecting victims to fake websites.

PKI as a defense against MITM

How PKI Protects Against MITM:

- **Authentication:**
 - Digital certificates verify the identity of parties involved.
- **Encryption:**
 - Ensures data integrity and confidentiality using public and private keys.
- **Trust Hierarchy:**
 - CA ensures only trusted entities can obtain valid certificates.

PKI as a defense against MITM

- **Key Measures:**
 - Implement SSL/TLS for encrypted communication.
 - Use Extended Validation (EV) certificates for added trust.
 - Regularly update and patch systems.

Preventing against MITM Attacks

For Individuals:

- Avoid using public Wi-Fi for sensitive transactions.
- Verify HTTPS and the website's certificate.
- Use VPNs for secure browsing.

For Organizations:

- Enforce HTTPS for all communications.
- Use strong encryption algorithms.
- Regularly monitor and revoke compromised certificates.
- Educate employees about phishing and social engineering risks.

Preventing against MITM Attacks

Emerging Technologies:

- Certificate Transparency Logs for tracking certificate issuance.
- Advanced cryptographic protocols like TLS 1.3.

Polls

Please have a look at the poll notification and select an option.

What do you think is the most effective way to prevent MITM attacks?

- A. Using strong passwords
- B. Implementing encryption (SSL/TLS)
- C. Avoiding public Wi-Fi
- D. Not sure

Polls

Please have a look at the poll notification and select an option.

What key action will you take after learning about PKI and MITM attacks?

- A. Use MFA and strong authentication for my accounts
- B. Verify HTTPS and digital certificates for websites I visit
- C. Use a VPN on public Wi-Fi
- D. Review and update my security practices

Questions and Answers



Thank you for attending



Department
for Education

CoGrammar

