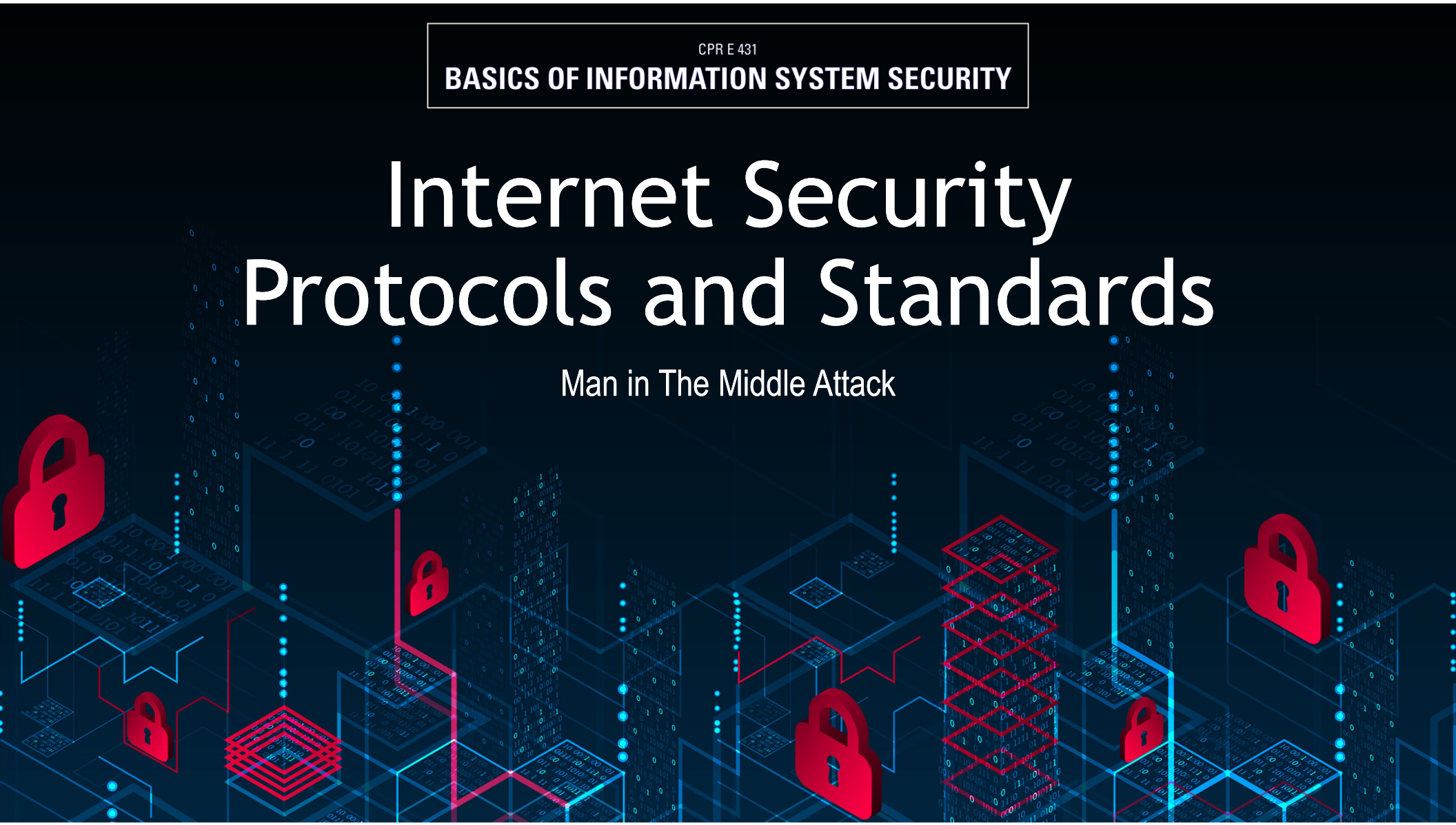
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Internet Security Protocols and Standards

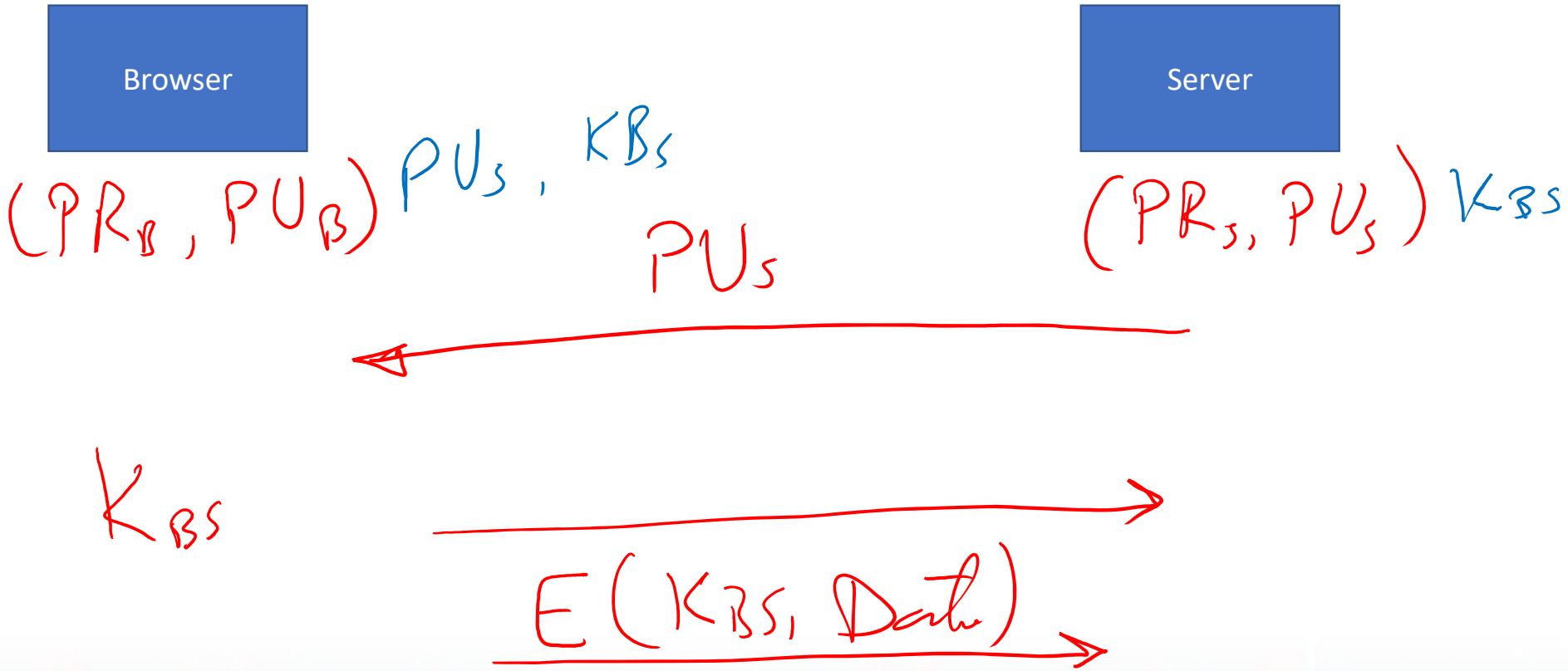
Man in The Middle Attack



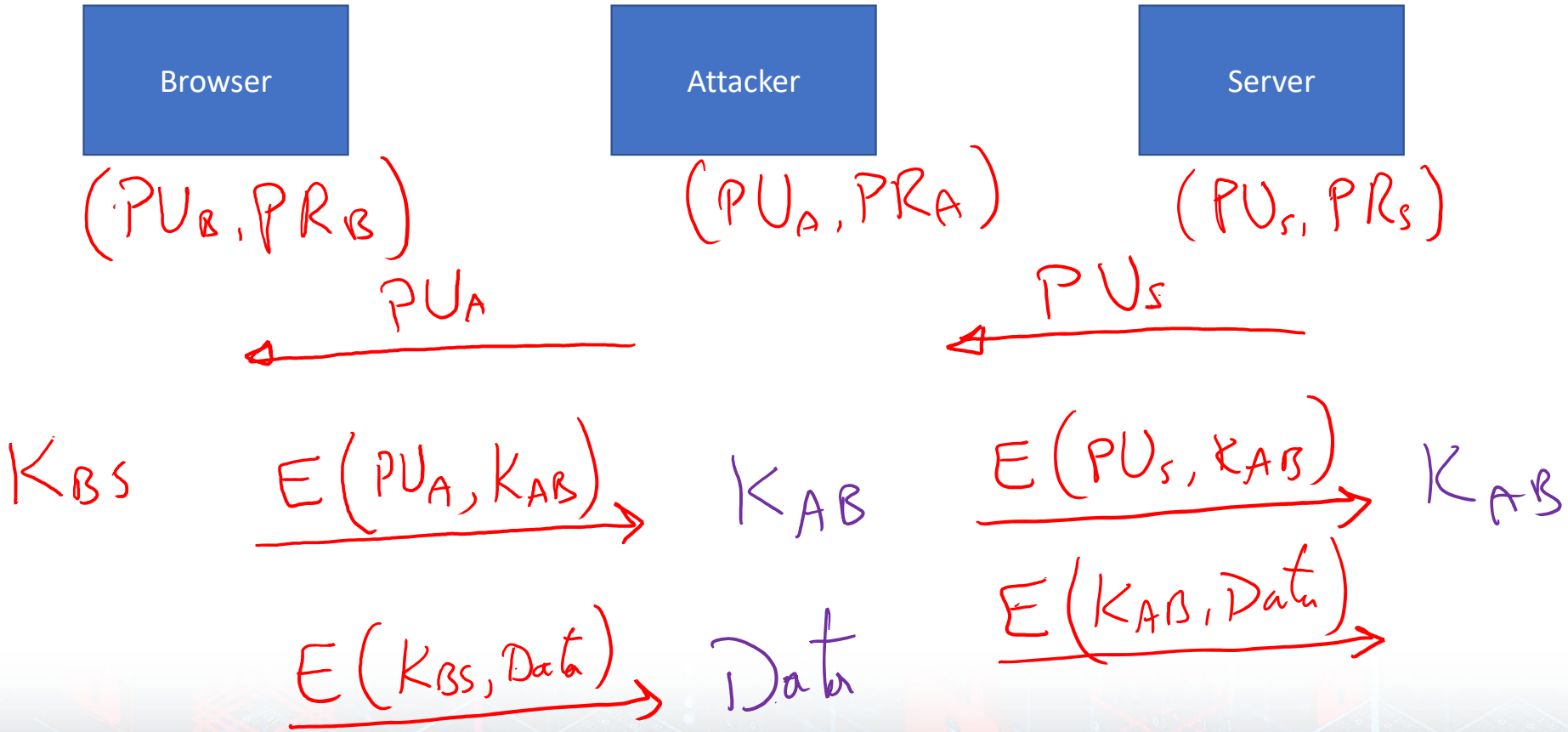
Video summary

- SSL/TLS Vulnerability
- MiTM Attack
- Countermeasure (Certificates)

Public Key for Key Exchange, Symmetric for Data

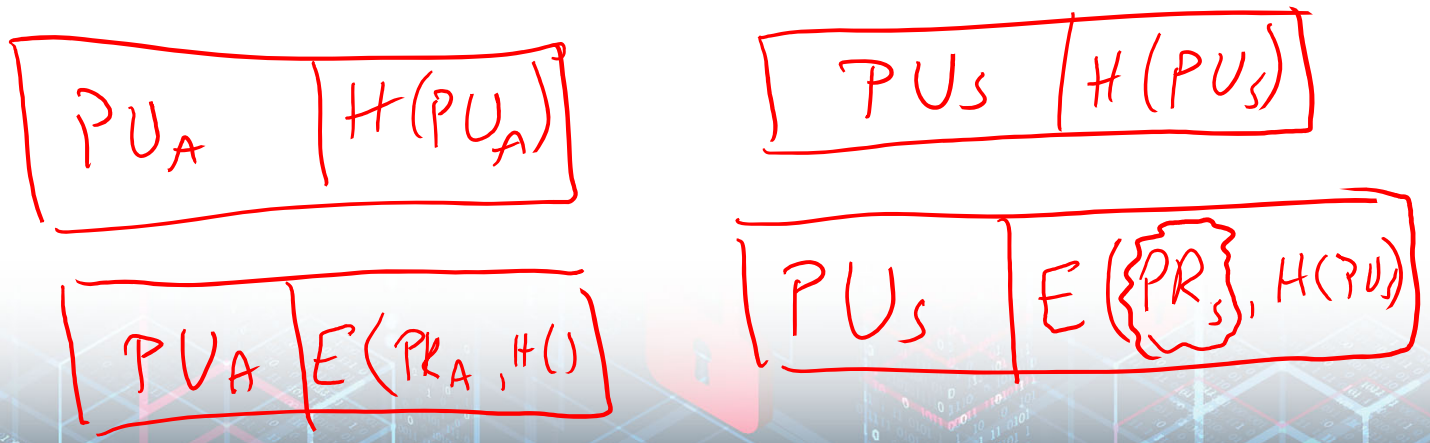


Man in The Middle Attack (MiTM)



Countermeasure (Certificates)

- The issue here is that the public key of the server is sent without any verification of the identity of the server
- Browser has to check and make sure that PUs is related to the server not the attacker
- Solution ➔ Use Certificates (public key of the server + hash of the key)



Video summary

- SSL/TLS Vulnerability
- MiTM Attack
- Countermeasure (Certificates)