# CMSC 33250: Graduate Computer Security

## Lecture 4: SSL & TLS (Applied Crypto)

Grant Ho, Fall 2023

# Logistics

Project Proposals due this Friday (Oct 13) by 5:00pm

- 1-2 pages, submitted on Gradescope
- List of group members in the class & external collaborators/advisors
- State research problem/key questions
- Key technical challenges that work needs to solve
- High-level sketch for your approach (methods)
- Evaluation plan & rough milestone timeline for making progress during the quarter

# Overview: SSL & TLS

# What is SSL / TLS?

**Last Week:** DoS Attacks = disrupting Availability

**Goals of TLS:** Provide Confidentiality, Integrity, and Authenticity

- Most familiar example: Secure web browsing (HTTPS)
- Threat Model: Man-in-the-Middle (MITM) Attacker

# What is SSL / TLS?

**Last Week:** DoS Attacks = disrupting Availability

**Goals of TLS:** Enable 2 parties to securely communicate over network

- Most familiar example: Secure web browsing (HTTPS)
- Threat Model: Man-in-the-Middle (MITM) Attacker
- Provides 3 key security properties:
  - Confidentiality: attacker can't learn any meaningful content
  - Integrity: attacker can't modify contents without parties knowing
  - Authenticity: both parties connect with exactly who they intend to

# SSL / TLS Protocol: Three key stages

1) Getting + Verifying server's certificate (authenticity)
   - Ensures client knows they're talking to the actual server they want

2) Performing key exchange protocol to establish shared secret keys
   - Allows parties to create shared secret that attacker doesn't know

"Hand shake"

3) Symmetric crypto w/ shared key to encrypt + MAC all packets sent between two parties (confidentiality + integrity)
   - Prevents attacker from tampering with / learning anything from packets

# Today's Papers

Today's papers focus on the first two stages (TLS "handshake"):

1) Attacks on certificate validation:
"The most dangerous code in the world…"

2) Attacks on key exchange protocols:
"Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice"

# Context for Today's Papers

Attacks on SSL / TLS came up occasionally, but community felt pretty good about their security

- Decades of research studying the security of underlying crypto protocols (symmetric key crypto, key exchange, etc.)
- Prominent open-source code: lots of eyes + lots of times = few bugs?

Around 2011: Series of high-profile attacks/issues -> renewed attention

- Major CA breaches (Comodo + DigiNotar) [2011]
- Snowden leaks [2013]
- Major vulnerabilities: "goto fail" [2014], HeartBleed [2014], etc.