Know Your Threat Model

- **Threat model:** A model of who your attacker is and what resources they have
- One of the best ways to counter an attacker is to attack their reasons

Story…

- The bear race
- **Takeaway:** Even if a defense is not perfect, it is important to always stay on top of best security measures

I don’t have to outrun the bear. I just have to outrun you

Human Factors

- The users
  - Users like convenience (ease of use)
  - If a security system is unusable, it will be unused
  - Users will find way to subvert security systems if it makes their lives easier
- The programmers
  - Programmers make mistakes
  - Programmers use tools that allow them to make mistakes (e.g. C and C++)
- Everyone else
  - Social engineering attacks exploit other people's trust and access for personal gain

Design in security from the start

- When building a new system, include security as part of the design considerations rather than patching it after the fact
  - A lot of systems today were not designed with security from the start, resulting in patches that don’t fully fix the problem!
- Keep these security principles in mind whenever you write code!

Security Services and Mechanisms

TABLE 1/X.800

Illustration of relationship of security services and mechanisms

Service \ Mechanism	Encipherment	Digital signature	Acces control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y	·	·	Y	·	·	·
Data origin authentication	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	·	·	·	·	·
Connection confidentiality	Y	·	·	·	·	·	Y	·
Connectionless confidentiality	Y	·	·	·	·	·	Y	·
Selective field confidentiality	Y	·	·	·	·	·	·	·
Traffic flow confidentiality	Y	·	·	·	·	Y	Y	·
Connection Integrity with recovery	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	Y	·	·	Y	·	·	·	·
Selective field connection integrity	Y	·	·	Y	·	·	·	·
Connectionless integrity	Y	Y	·	Y	·	·	·	·
Selective field connectionless integrity	Y	Y	·	Y	·	·	·	·
Non-repudiation. Origin	·	Y	·	Y	·	·	·	Y
Non-repudiation. Delivery	·	Y	·	Y	·	·	·	Y

· The mechanism is considered not to be appropriate.

Y Yes: the mechanism is considered to be appropiate, either on its own or in combination with other mechanisms.

Note – In some instances, the mechanism provides more than is necessary for the relevant service but could nevertheless be used.

Supplementary materials

- Internet Security Glossary, v2 – produced by Internet Society (ISOC) https://datatracker.ietf.org/doc/html/rfc4949
- X.800 – OSI network security

  https://www.itu.int/rec/dologin_pub.asp?lang=f&id=T-REC-X.800-199103-I!!PDF-E&type=items

Summary for Chapter 1

- Have learned:
  - Security requirements
  - Attack models
  - X.800 secure architecture, security services, mechanisms

Review Questions

- William Stallings (WS), “Network Security Essentials”, 6th Global Edition
- RQ 1.1 - 1.3
- Prob 1.5