Trends in Cyber Security

By: Farid Khan

Topics

- Cybersecurity
- Claude Shannon
- Security Framework
- Security Model
- The Future Landscape:
- Quantum computing

Definition

Cybersecurity: The ability to protect or defend the use of cyberspace from cyber attacks

Cyberspace: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Photo: © Stanley Rowin

Claude Shannon

- “Communication theory of secrecy systems” 1949:
- Created the idea of confusion and diffusion, one-time pad, unconditionally secure
- Shannon ideas on information theory and rise of computational complexity made strong cryptographic systems possible

Security Framework

1. System model: clear definition or description of the system that is being tested. For example: source code for a software system, formal specifications of the state transitions etc.
2. Threat model: Clearly define the attackers computational strength and attackers access to the system. For instance: Adversary can get hold of encrypted data, build malicious web sites.
3. Security properties: Security goals may be formulated as properties that we can hope to prevent the attacker form violating. It must be unambiguously associated to the system.

Security Model

Authenticated Encryption: form of encryption that ensures confidentiality and integrity

MAC (message authentication code): provide integrity but no confidential

CPA -secure: provides confidentiality but no integrity

**So how we should combine them?

TLS: security protocol that protects web traffic. encrypt - then MAC

IPsec: protocol used to create private tunnels over the public internet. MAC then encrypt

SSH: logging in to remote machines. Encrypt, MAC and checksum!!

**which is better? Perform threat modeling