CS 668: Practical Cyber Security for Cyber Practitioners

Sandeep K. Shukla

IIT Kanpur

What do you need to know?

- If you are a
  - Chief Information Security Officer (CISO) or a member of CISO's team
- If you are part of a team
  - responsible for cyber security governance in an organization
  - figuring out what cyber threats an organization faces
  - doing cyber risk assessment of an organization
  - evaluating cyber resilience of an organization
  - carrying out cyber security audit of an organization
  - planning cyber security controls to be implemented to manage cyber risk
  - creating Incident Response Playbook
  - creating Cyber Crisis Management Playbook
  - planning cyber crisis drill at the organization

What is Cyber Security?

- Identify
- Protect
- Detect
- Respond
- Recover
- Govern

Who are the Attackers?

- Script Kiddies
- Hacktivists
- Cyber Criminals
- Organized Criminal Gangs
- Nation State Sponsored Advanced Persistent Threat Groups (APTs)

Why do they attack?

- Curious to display their skills
- Protesting an Organization and a Government’s actions and policies
- Making monetary gains
- Disabling a nationally critical organization or system
  - Banking System
  - Telecommunication Systems
  - Power Grid
  - Water Treatment and Sewage Processing Plants
  - Manufacturing
  - Transportation systems
  - Government services
  - Defence systems

Not all Targets are Equal

- Not all organizations and systems are equal targets
  - Impact is a part of the equation for targeting
- Not every system or asset within an organizations are equal
  - Systems/subsystems/assets involved in critical business processes can yield higher impact
- Not every individual are equal targets
  - Depends on the yield an attack can produce

Understanding the Geopolitics

- For large scale or high impact attacks on organizations or systems
  - Geopolitics plays a major role
- Attack on
  - Iranian Nuclear Uranium enrichment plant in 2009 - Stuxnet
  - Ukrainian Power Distribution Systems – 2015 and 2016
  - US Government Departments – Solarwind 2020
  - Indian Power Systems Operators and Ports in 2020-21
  - Indian government websites -- 2023

What not to expect from this class?

- How to hack or do VAPT? (CS 628 – Computer Systems Security)
- How to analyse malware? (CS 658 – Malware Analysis and Intrusion Detection)
- How to protect critical infrastructure from cyber-attacks?(CS631 – Cyber Security of Critical Infrastructure)
- How to analyse cryptographic protocols and algorithms? (CS 641 – Modern Cryptology)
- How to check for side channels in cryptography implementation? (CS666 – Hardware Security for IoT)
- Cryptography after Quantum Computing (CS 674 – Post Quantum Cryptography)
- Privacy and Cryptography (CS 670 – Crypto techniques for privacy preservation)