Session 09

Enterprise Security

CS 7349

Spring 2024

World Changers
Shaped Here

SMU

© Shaibal Chakrabarty

Contents

- Security News of the Week
- House Keeping
- Class Presentation
- Concepts: Enterprise Security Overview, Business Impact

Sources: Netscout/Radware; Cryptography and Network Security, William Stallings;

House Keeping

- Status of Teams for Term Paper? Presentations?
- Research Paper Feb deliverables;
- Checkpoint on 02/19; Guest Speaker Week of 02/26
- Exam1 published; Quiz to be published
- Research paper – 3 pages due. Expectations (Abstract/Intro/Current Research/Solution/References)
- A word on prioritization and project management

Outside Classroom studies

Sources: Shaibal Chakrabarty, University of Utah campus

Security News of the Week – Spring 2024

Ukrainian Raccoon Infostealer Operator Extradited to US

Alleged Raccoon Infostealer operator Mark Sokolovsky is awaiting trial in the US, after being extradited from the Netherlands.

Russian Cyberspies Exploit Roundcube Flaws Against European Governments

Russian cyberespionage group targets European government, military, and critical infrastructure entities via Roundcube vulnerabilities.

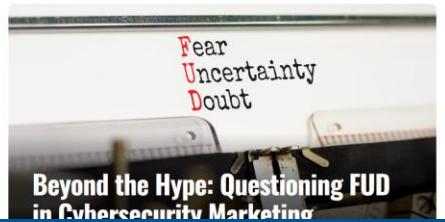
Ransomware Group Takes Credit for LoanDepot, Prudential Financial Attacks

The BlackCat/Alphv ransomware group has taken credit for the LoanDepot and Prudential Financial attacks, threatening to sell or leak data.

New Google Initiative to Foster AI in Cybersecurity

Google's new AI Cyber Defense Initiative focuses on boosting cybersecurity through artificial intelligence.

iOS Trojan Collects Face and Other Data for Bank Account Hacking



TRENDING

1. New Wi-Fi Authentication Bypass Flaws Expose Home, Enterprise Networks
2. Ex-Employee's Admin Credentials Used in US Gov Agency Hack
3. FBI Dismantles Ubiquiti Router Botnet Controlled by Russian Cyberspies
4. Microsoft Confirms Windows Exploits Bypassing Security Features
5. CISA Urges Patching of Cisco ASA Flaw Exploited in Ransomware Attacks
6. Neiman Marcus Says Hackers Breached

Source: securityweek.com

CS 7349 – Tying it all together

INTRODUCTION TO DS7349 AND THE THREAT LANDSCAPE	HASH FUNCTIONS	ENTERPRISE SECURITY
INTRODUCTION TO NETWORKS	MESSAGE AUTHENTICATION CODES	SECURITY – CLOUD, WIRELESS/5G, DDoS, SASE, IoT, SDN, Smart Cities
SYMMETRIC KEY CRYPTO	KEY MANAGEMENT	FRAMEWORKS, STANDARDS, OPERATIONS, Governance/Risk/Compliance
USING SYMMETRIC KEY CIPHERS	IDENTITY AND ACCESS MANAGEMENT	REVIEW/ADDITIONAL TOPICS
RANDOMNESS AND PSEUDORANDOM NUMBERS		
PUBLIC KEY CRYPTO/Team Paper		

Confidentiality **Integrity** **Availability** **Networks/Application**

Spring schedule

Date	Week/Unit	Learning Material	Assignment
01/17/2024	1/1	Intro to Data and Network Security	Stallings Ch 1; Quiz#1;Start project team, select project and inform instructor
Jan 22, 24	2/2	Intro to Computer Networks	Submit Quiz #2; Project team confirms problem with instructor/Homework 1 issued/Term paper checkpoint
Jan 29, 31	3/3	Symmetric Key Cryptography	Stallings Ch 2-3; Submit Quiz #3; First Project Draft (Title, authors, abstract and Intro)/
Feb 5, 7	4/4	Using Symmetric Key Ciphers	Stallings Ch 3-6; Submit Quiz#4 (ch03 and ch06); Homework #2 issued
Feb 12, 14	5/5	Randomness and Pseudorandom Numbers	Stallings Ch 7; Submit Quiz #5/Term Paper Checkpoint
Feb 19, 21	6/6	Public Key Cryptography	Stallings Ch 9-10; Submit Quiz #6/Case Study Due/
Feb 26, 28	7/7	Hash Functions/	Stallings Ch 11; Submit Quiz #7; Paper Interim Draft; Exam 1 issued
Mar 4, 6	8/8	Message Authentication Codes	Stallings Ch 12; Submit Quiz#8;
Mar 11, 13	9/9	SPRING BREAK!!!	
Mar 18, 20	03/10	Key Management and Key Distribution	Stallings Ch 14; Submit Quiz #10/Term paper checkpoint/Start on project presentation/Case Study
Mar 25, 27	04/11	User Authentication	Stallings Ch 15; Submit Quiz #11/
Apr 1, 3	12/12	Network Security	Stallings Ch 17; Submit Quiz #12; Presentation check/Exam #2
Apr 8, 10	13/13,14	Privacy, Security Ethics	
Apr 15, 17	14	Applications: AI and Quantum Computing	Submit Final Project Paper
Apr 22, 24	15	Open	Presentations of Term Project by class/
Apr 29		Wrap up and Review	
This schedule is subject to changes. All assignments are due by 11:59pm of the due date. Earlier submissions are encouraged and welcome. Do not wait till the last moment.			
You will have 2 weeks to complete most assignments.			

Book: Cryptography and Network Security by William Stallings, 8th edition

Class Presentation - Special Topic

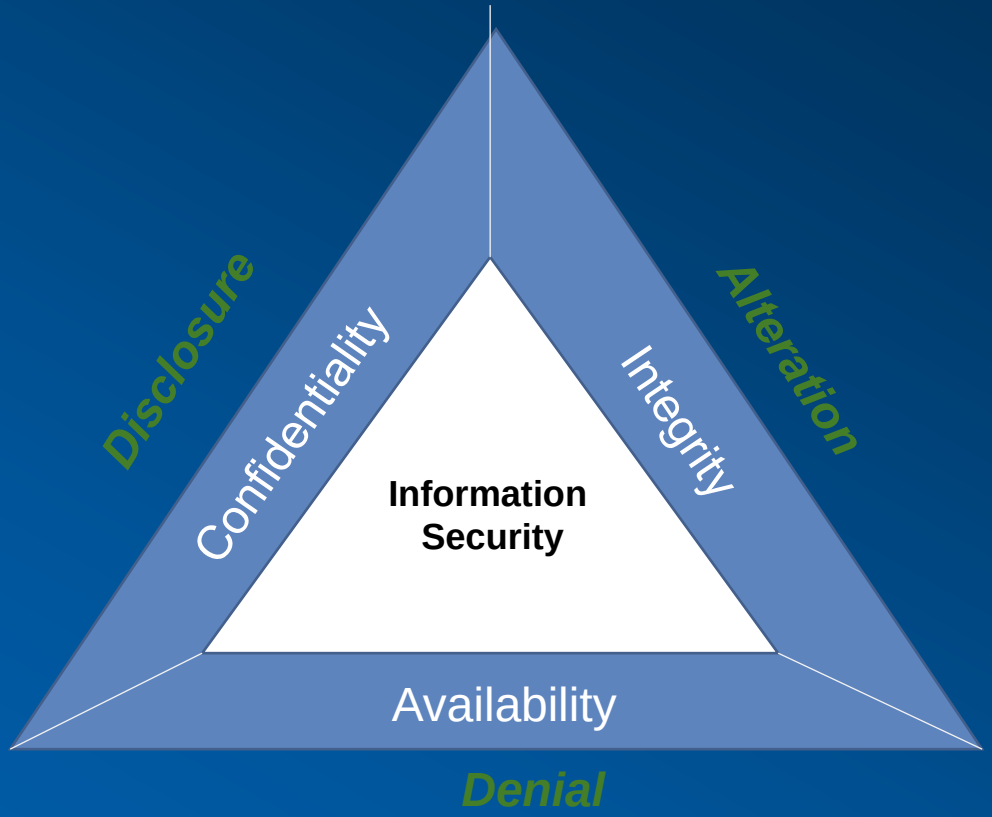
- Any topic of your interest: Work, ~~school~~, play
  - Can be a question/answer, wonderment, information
  - **Security related; NOT term paper related; NO course topic**
  - Strict time limits 5 mins + 3 mins Q&A
- Schedule – as per roster
  - ~~Adu, Aliliele~~, ~~Braden~~, ~~Cho~~, ~~Dominguez~~, ~~Garcia~~, Garza, ~~Gibbs~~, Guo, ~~Hennes~~, Jackson, Kharwadhkar, Kucera, Lei, Liang, Lim, Lin, Liu, Magee, Mandalaneni, Mathew, Miller, Nagamanickam, DPatel, PPatel, Pittman, Sanaboyina, Singh, Skochdopole, Swigart, Taghavi, Wang, Werth, Zhai

Project Timeline (For 9 page paper)

- Jan: First project draft 1 page, basically your Introduction section, plus title, authors and abstract, some references
- Feb: Interim draft 3 pages, basically your intro and related work, plus basic description of your solution
- Mar: Draft 6 pages. Detailed solution, analysis, references
- Apr: Final paper 9 pages. Submit, with presentation

A LaTex template and example paper will be provided

InfoSec, CIA, Threats



Source: “Information Security Illuminated”, Solomon and Chapple, 2005, Sudbury, MA:Jones and Bartlett.

Network Security Basics

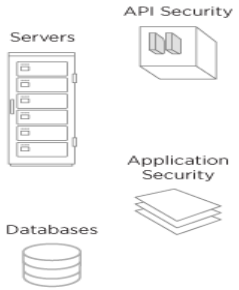
The IT Security Chain

upwork™

The more links in your network's chain—databases, cloud-based servers, APIs, and mobile applications—the more potential vulnerabilities you face. Here's an overview of areas of IT security to consider.

IT Security

NETWORK SECURITY



- Security Engineering
- Vulnerability Testing
- Penetration Testing
- Network Intrusion Detection Systems (NIDS)
- Firewalls

INTERNET SECURITY

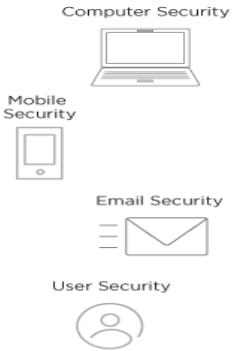
- HTTPS
- SSL Certificates
- OAuth 2.0

CLOUD SECURITY

- OAuth 2.0
- Web Sockets

WIRELESS SECURITY

END POINT SECURITY



- VPNs
- Encryption
- Anti-Malware

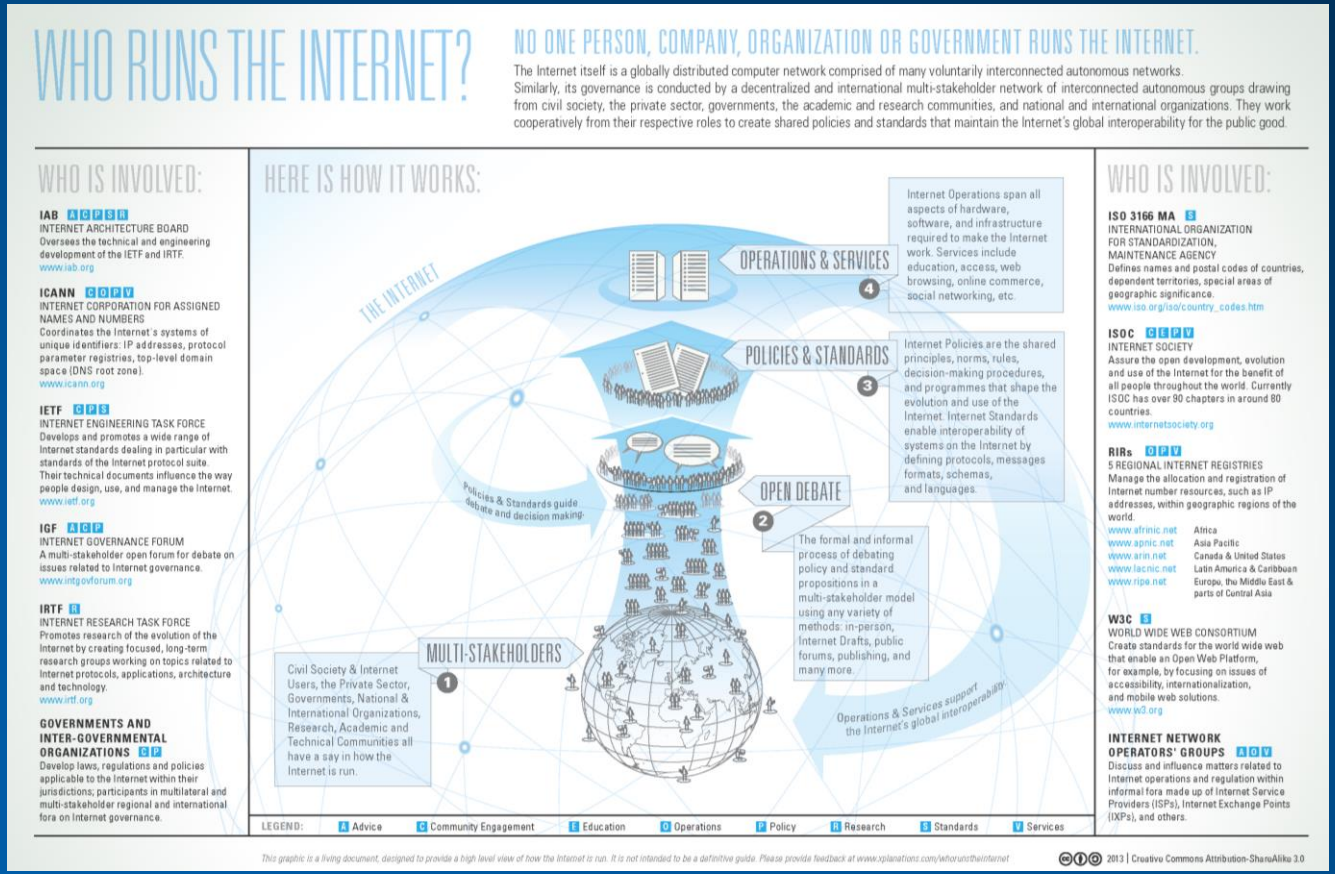
Source: Upwork Global, Inc

Layered Standards Architectures

Super Layer	TCP/IP	OSI	Hybrid TCP/IP–OSI
Application	Application	Application	Application
		Presentation	
		Session	
Internet	Transport	Transport	Transport
	Internet	Network	Internet
Single network	Subnet access	Data link	Data link
		Physical	Physical

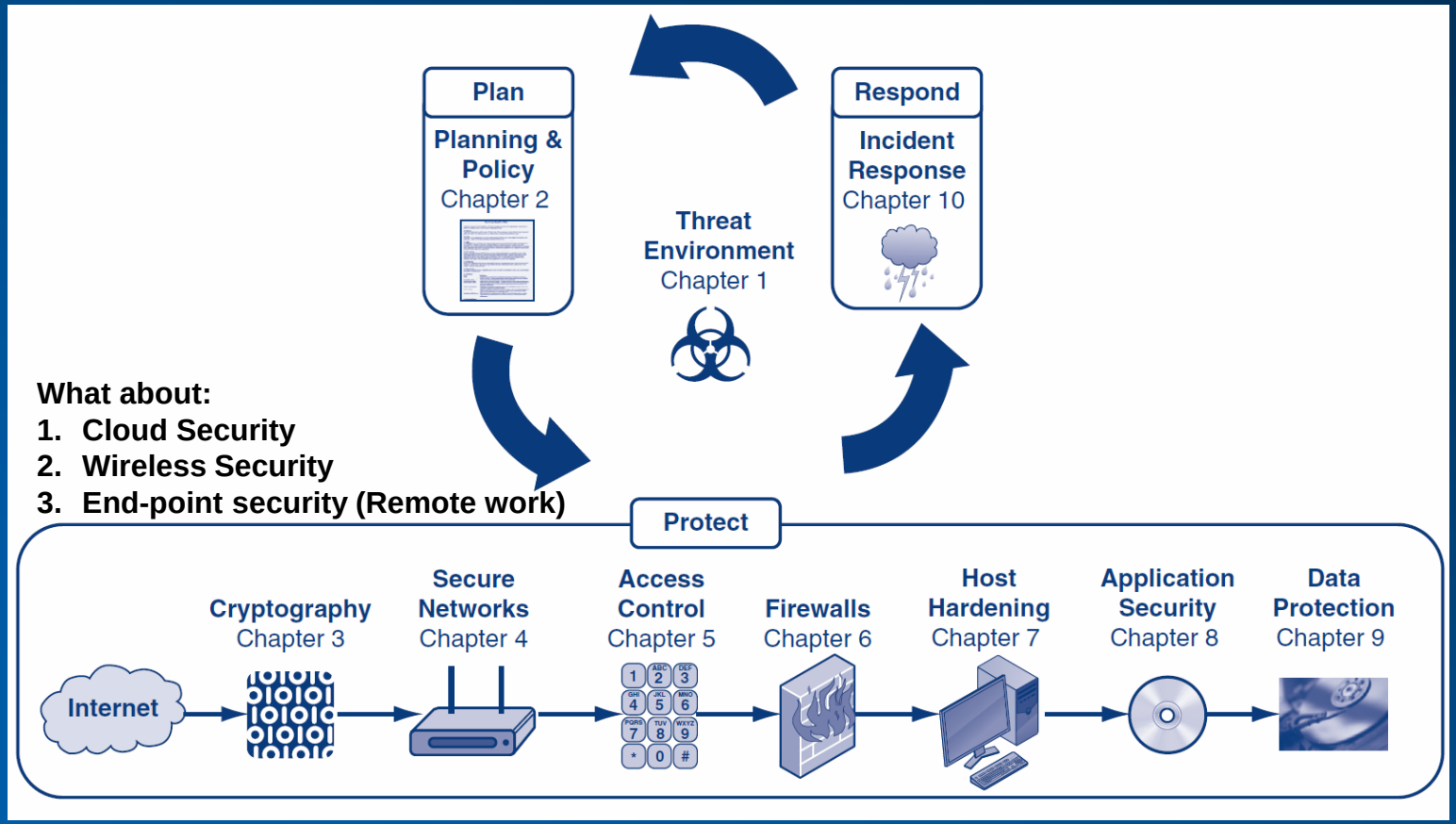
Source: Panko and Boyle, Pearson 5e

The Mother of all Networks



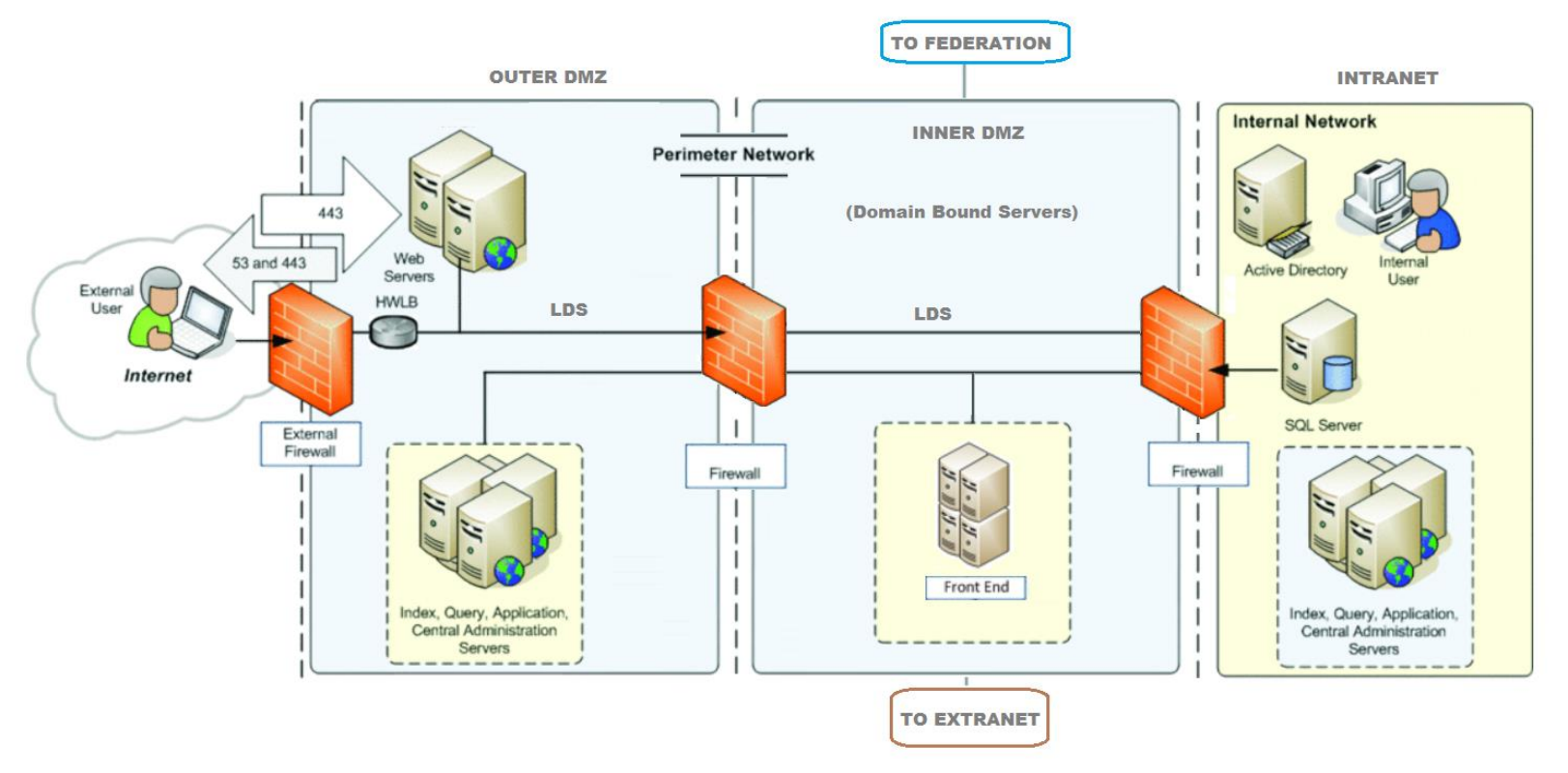
Source: https://upload.wikimedia.org/wikipedia/commons/e/ed/Who-Runs-the-Internet-graphic.png

Corporate Computer Security

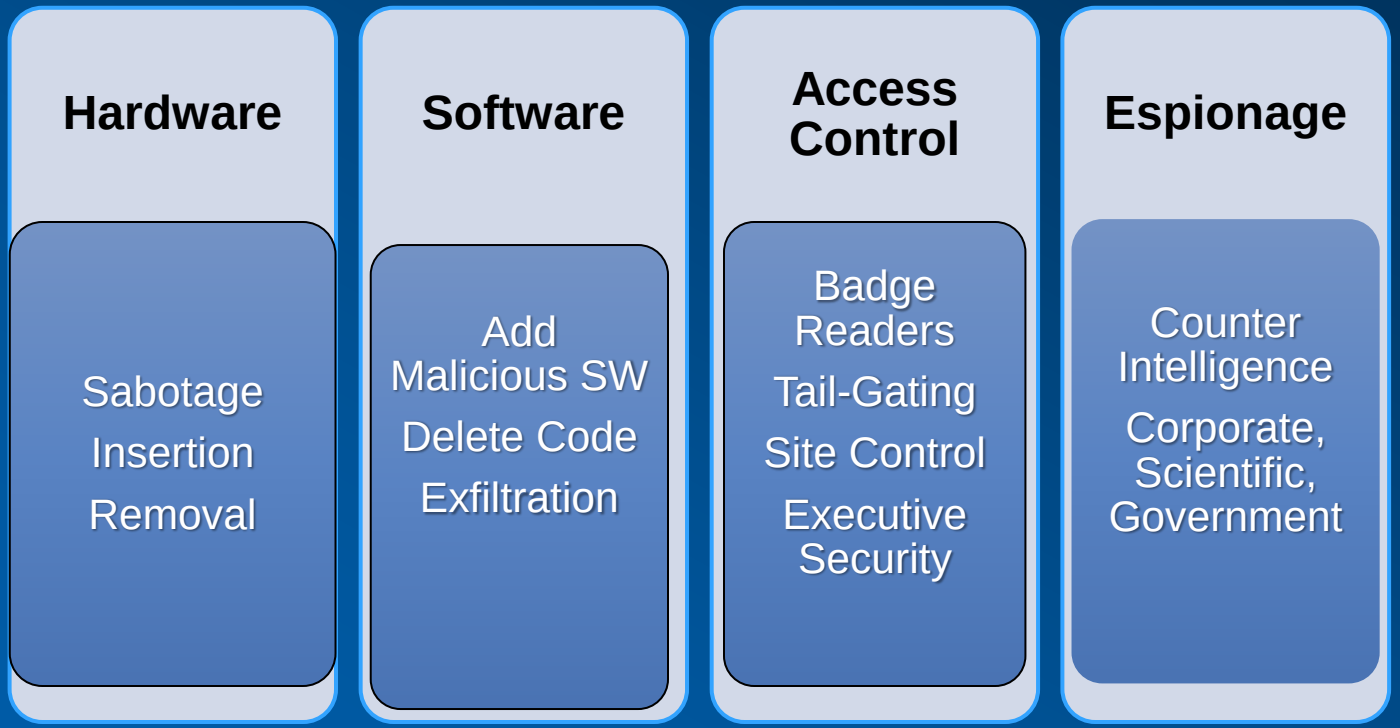


Source: Corporate Computer Security by Panko and Boyle

Basic Enterprise Security Architecture



“Physical Layer” Enterprise Security



Thank You!

World Changers
Shaped Here

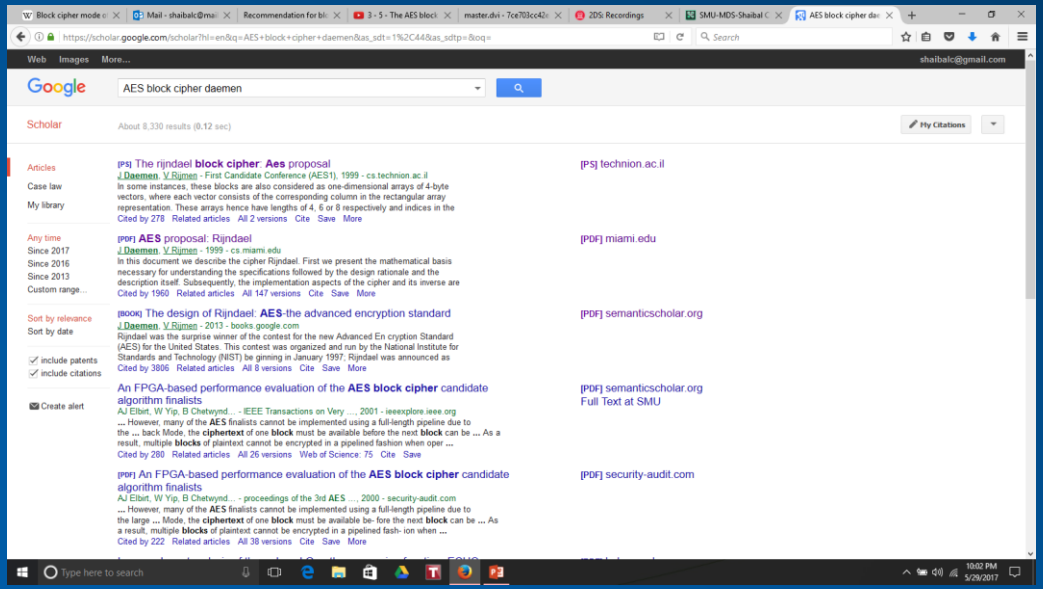
SMU®

Project – 2nd deliverable

- Refine Abstract and Intro
- Write down 1 page of current research on the topic with a storyline to show how your novel approach differs
- Prepare the section of your solution, your architecture, your data/introduction to your simulation
- Ensure you have a MINIMUM of 3 pages including abstract, intro, current research and references.

Peer reviewed publications

- https://scholar.google.com/
- Get your references from here, and download IEEE, ACM and other papers from CUL. (http://www.smu.edu/cul)



Project Reports

- **Use the LaTex template** provided for your project paper submissions.
- **Read** the Sample paper and **follow** its directions as appropriate in writing your paper.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents.
- https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)

Project Abstract and Intro

- **Abstract** structure (125-150 word limit for 9 pages)
  - start with statement of what is presented (2 sentences)
  - motivate the problem (2-3 sentences)
  - discuss details of what is done at a high level (1-2 sentences)
  - state the main conclusions (1-2 sentences)
- **Introduction** basic structure (the rest of page 1):
  - motivate the problem further
  - state the problem in detail
  - state the basic work done/approach taken
  - State the contributions of your paper (2nd last paragraph)
  - state the outline for the rest of the paper (final paragraph)
    - Conclusions are not stated in the introduction.

Project Paper

- **Use the LaTex template** provided for all of your project paper submissions.
- Your paper is expected to be publishable
  - High quality research, well written, reproducible results based on paper contents. 9 pages exactly. No more, no less
  - https://scholar.google.com/ for references (NOT cnn.com, foxnews.com, cnbc.com; YES ietf.org, ieee.org,…itu-t)
  - https://www.overleaf.com/read/brpdfvsxsjww#8886a4 ←Paper template