



# 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



# 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

Chinese hackers use Apple's iOS to steal data

## Mysterious 'MMS Fingerprint' Hack Used by Spyware Firm NSO Group Revealed

The existence of a previously unknown infection technique used by spyware firm NSO Group is suggested by a single line in a contract between NSO and the telecom regulator of Ghana.

## New Wi-Fi Authentication Bypass Flaws Expose Home, Enterprise Networks

## Beyond the Hype: Questioning FUD in Cybersecurity Marketing



### 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



# CS 7349 – Tying it all together

INTRODUCTION TO CS7349 AND THE  
THREAT LANDSCAPE

INTRODUCTION TO NETWORKS

SYMMETRIC KEY CRYPTO

USING SYMMETRIC KEY CIPHERS

RANDOMNESS AND PSEUDORANDOM  
NUMBERS

PUBLIC KEY CRYPTO/Team Paper

HASH FUNCTIONS

MESSAGE AUTHENTICATION CODES

KEY MANAGEMENT

IDENTITY AND ACCESS MANAGEMENT

ENTERPRISE SECURITY

SECURITY – CLOUD, WIRELESS/5G, DDoS,  
SASE, IoT, SDN, Smart Cities

FRAMEWORKS, STANDARDS, OPERATIONS,  
Governance/Risk/Compliance

REVIEW/ADDITIONAL TOPICS

**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	
<b>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.</b>			
<b>You will have 2 weeks to complete most assignments.</b>			

**Book: Cryptography and Network Security by William Stallings, 8<sup>th</sup> 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





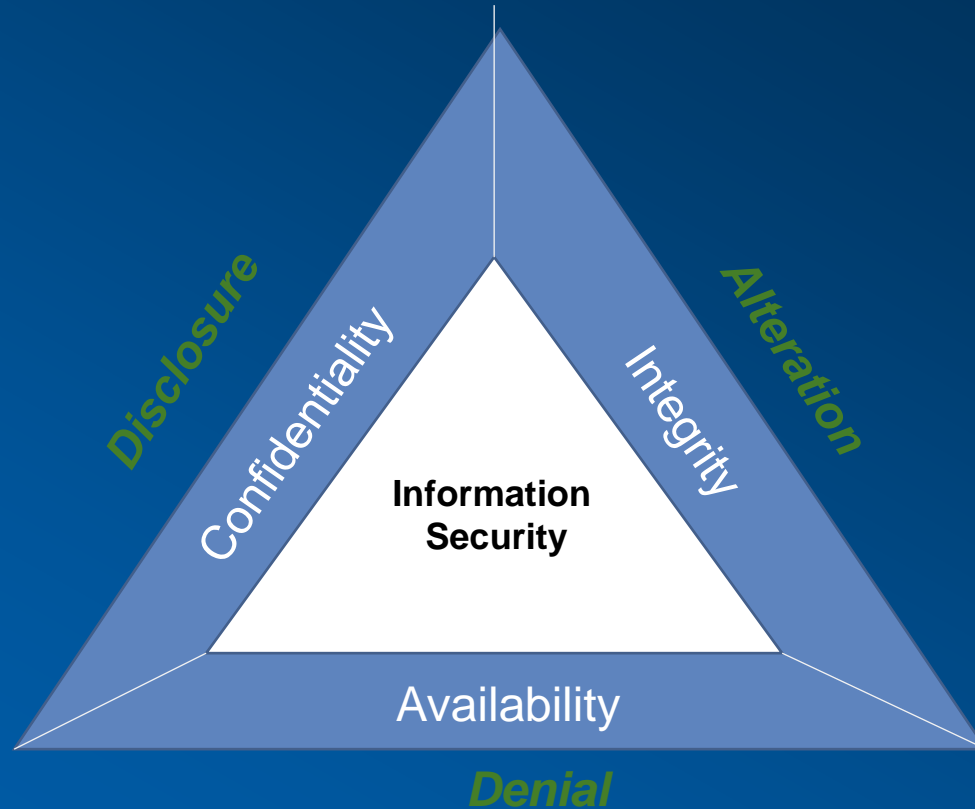
# Project Timeline (For 9 page paper)

- 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

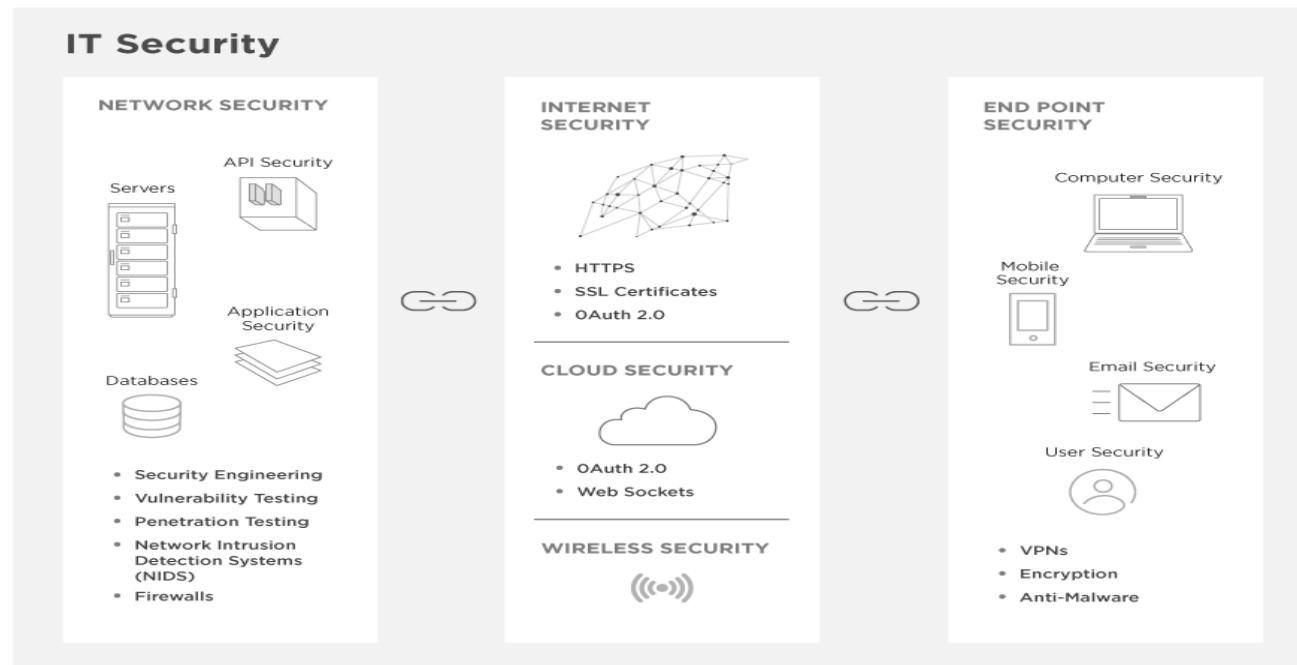


# Network Security Basics

## 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.



# 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



# The Mother of all Networks

## WHO RUNS THE INTERNET?

### NO ONE PERSON, COMPANY, ORGANIZATION OR GOVERNMENT RUNS THE INTERNET.

The Internet itself is a globally distributed computer network comprised of many voluntarily interconnected autonomous networks. Similarly, its governance is conducted by a decentralized and international multi-stakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities, and national and international organizations. They work cooperatively from their respective roles to create shared policies and standards that maintain the Internet's global interoperability for the public good.

### WHO IS INVOLVED:

#### IAB

**INTERNET ARCHITECTURE BOARD**  
Oversees the technical and engineering development of the IETF and IRTF.  
[www.iab.org](http://www.iab.org)

#### ICANN

**INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS**  
Coordinates the Internet's systems of unique identifiers: IP addresses, protocol parameter registries, top-level domain space (DNS root zone).  
[www.icann.org](http://www.icann.org)

#### IETF

**INTERNET ENGINEERING TASK FORCE**  
Develops and promotes a wide range of Internet standards dealing in particular with standards of the Internet protocol suite. Their technical documents influence the way people design, use, and manage the Internet.  
[www.ietf.org](http://www.ietf.org)

#### IGF

**INTERNET GOVERNANCE FORUM**  
A multi-stakeholder open forum for debate on issues related to Internet governance.  
[www.intgovforum.org](http://www.intgovforum.org)

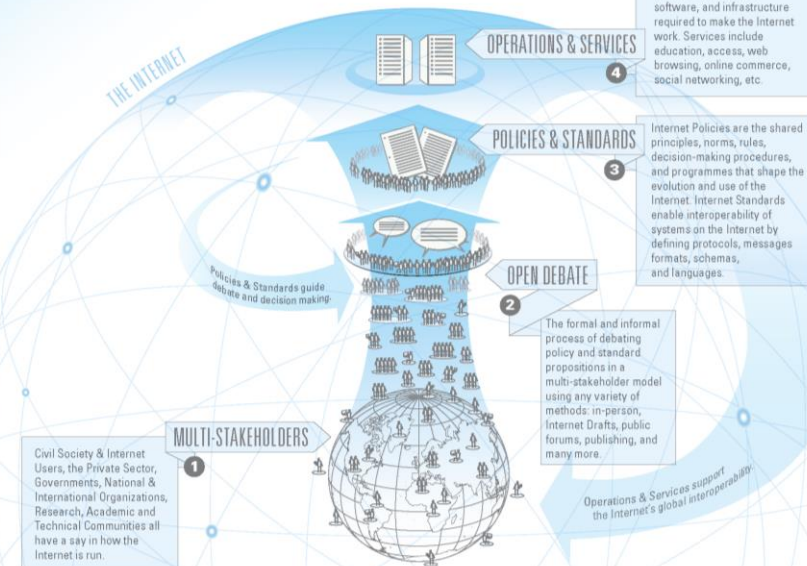
#### IRTF

**INTERNET RESEARCH TASK FORCE**  
Promotes research of the evolution of the Internet by creating focused, long-term research groups working on topics related to Internet protocols, applications, architecture and technology.  
[www.ietf.org](http://www.ietf.org)

#### GOVERNMENTS AND INTER-GOVERNMENTAL ORGANIZATIONS

Develop laws, regulations and policies applicable to the Internet within their jurisdictions; participants in multilateral and multi-stakeholder regional and international fora on Internet governance.

### HERE IS HOW IT WORKS:



LEGEND: 1 Advice 2 Community Engagement 3 Education 4 Operations 5 Policy 6 Research 7 Standards 8 Services

### WHO IS INVOLVED:

#### ISO 3166 MA

**INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, MAINTENANCE AGENCY**  
Defines names and postal codes of countries, dependent territories, special areas of geographic significance.  
[www.iso.org/iso/country\\_codes.htm](http://www.iso.org/iso/country_codes.htm)

#### ISOC

**INTERNET SOCIETY**  
Assure the open development, evolution and use of the Internet for the benefit of all people throughout the world. Currently ISOC has over 90 chapters in around 80 countries.  
[www.internetsociety.org](http://www.internetsociety.org)

#### RIRs

**5 REGIONAL INTERNET REGISTRIES**  
Manage the allocation and registration of Internet number resources, such as IP addresses, within geographic regions of the world.  
[www.afnic.net](http://www.afnic.net) Africa  
[www.apnic.net](http://www.apnic.net) Asia Pacific  
[www.arin.net](http://www.arin.net) Canada & United States  
[www.lacnic.net](http://www.lacnic.net) Latin America & Caribbean  
[www.ripe.net](http://www.ripe.net) Europe, the Middle East & parts of Central Asia

#### W3C

**WORLD WIDE WEB CONSORTIUM**  
Create standards for the world wide web that enable an Open Web Platform, for example, by focusing on issues of accessibility, internationalization, and mobile web solutions.  
[www.w3.org](http://www.w3.org)

#### INTERNET NETWORK OPERATORS' GROUPS

Discuss and influence matters related to Internet operations and regulation within informal fora made up of Internet Service Providers (ISPs), Internet Exchange Points (IXPs), and others.

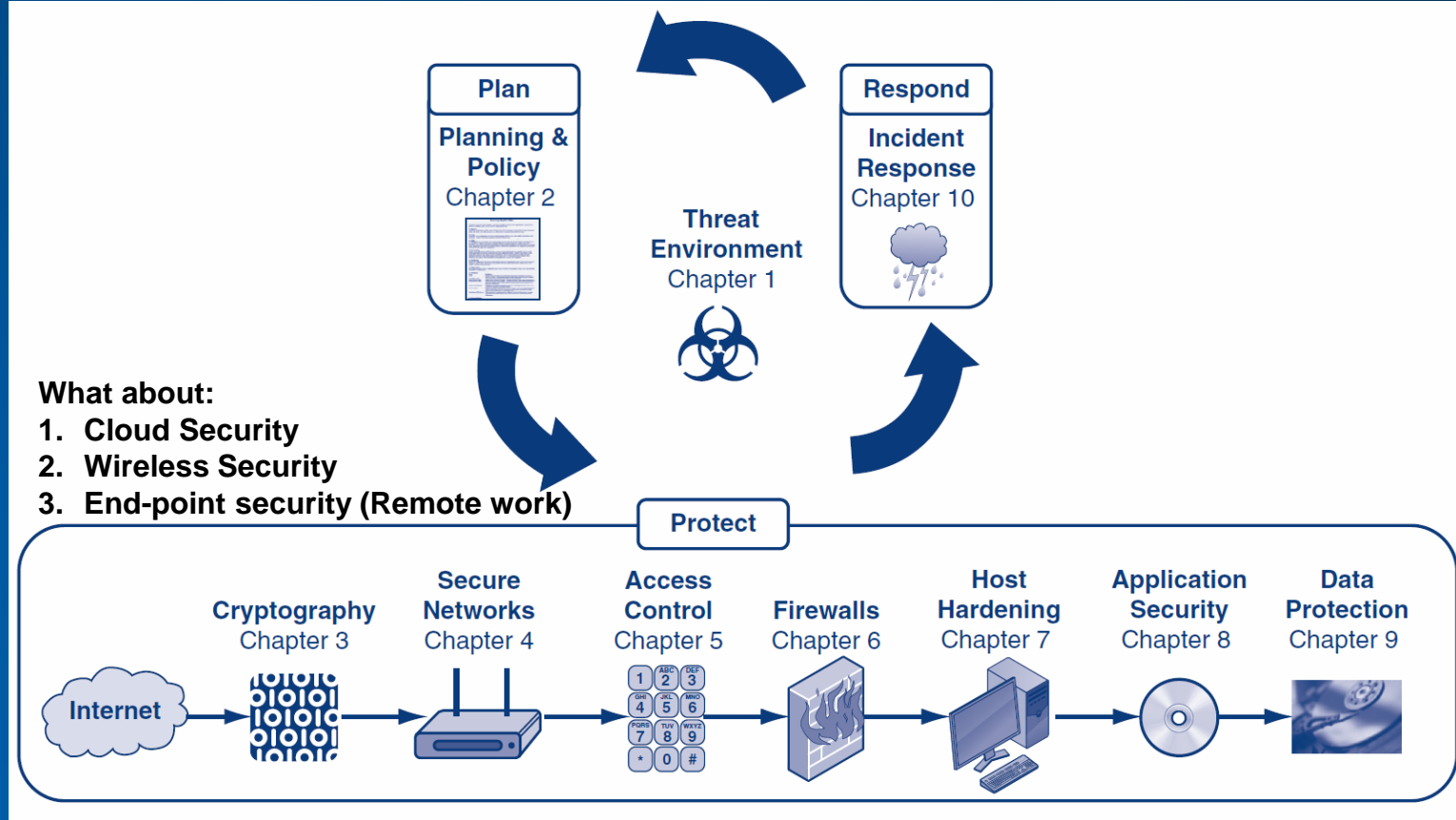
This graphic is a living document, designed to provide a high level view of how the Internet is run. It is not intended to be a definitive guide. Please provide feedback at [www.xplanations.com/whorunstheinternet](http://www.xplanations.com/whorunstheinternet)

© 2013 Creative Commons Attribution-ShamAlkai 3.0

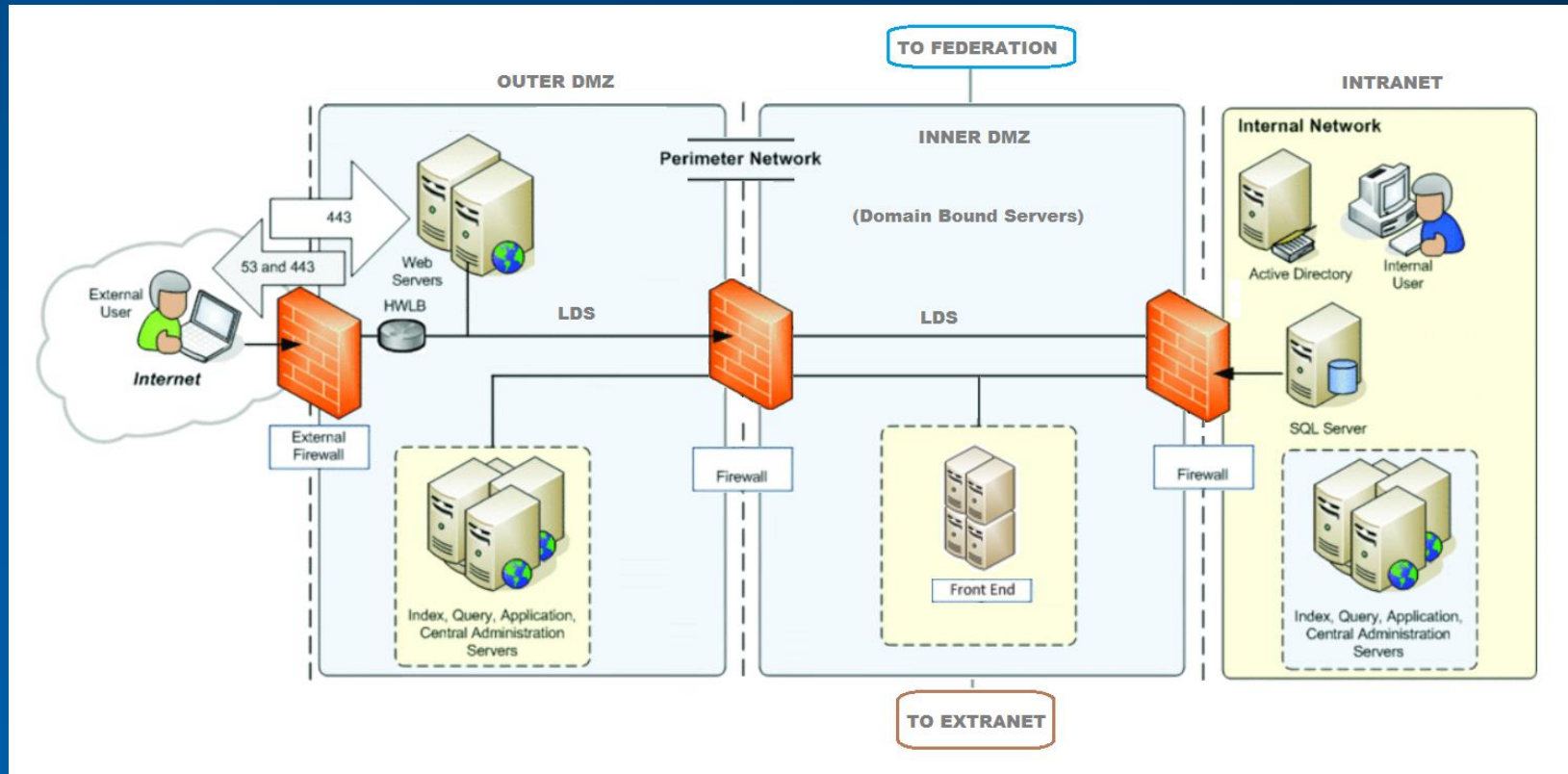




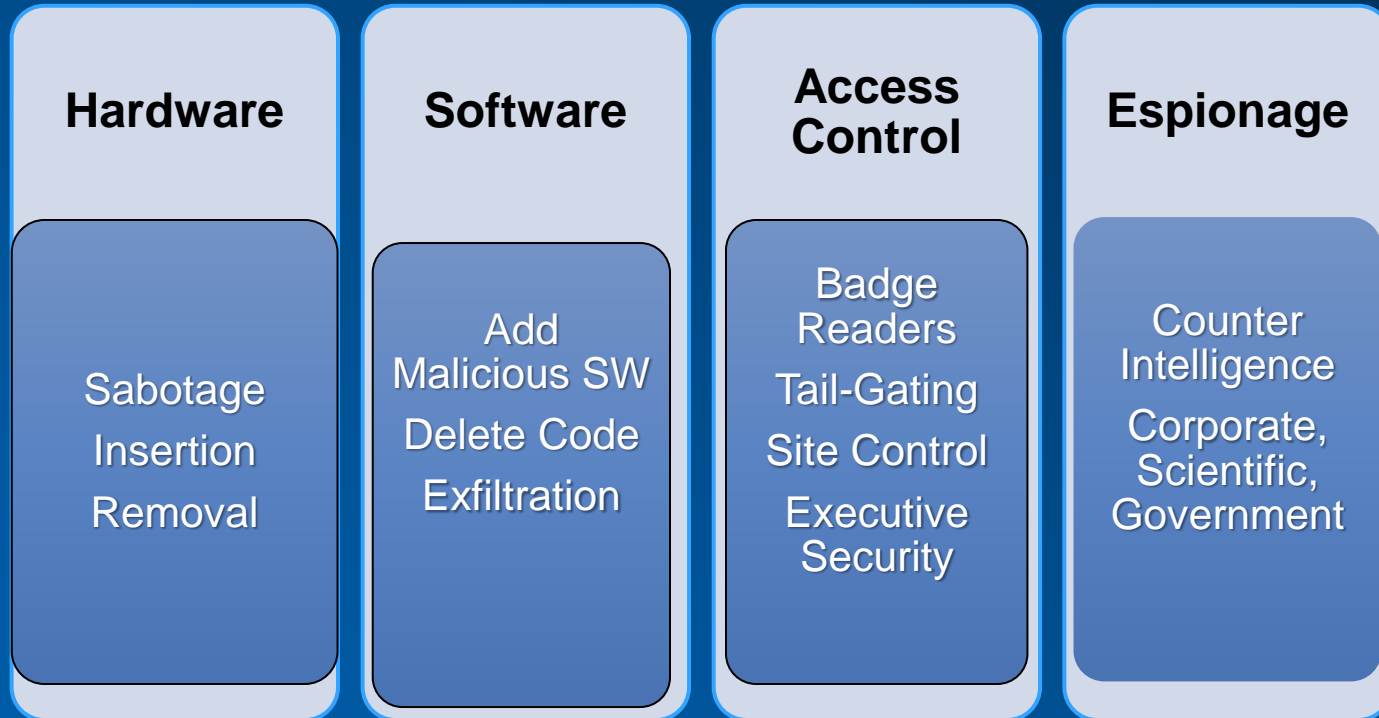
# Corporate Computer Security



# Basic Enterprise Security Architecture



# “Physical Layer” Enterprise Security



# Thank You!

World Changers  
Shaped Here



SMU®

# Project – 2<sup>nd</sup> deliverable

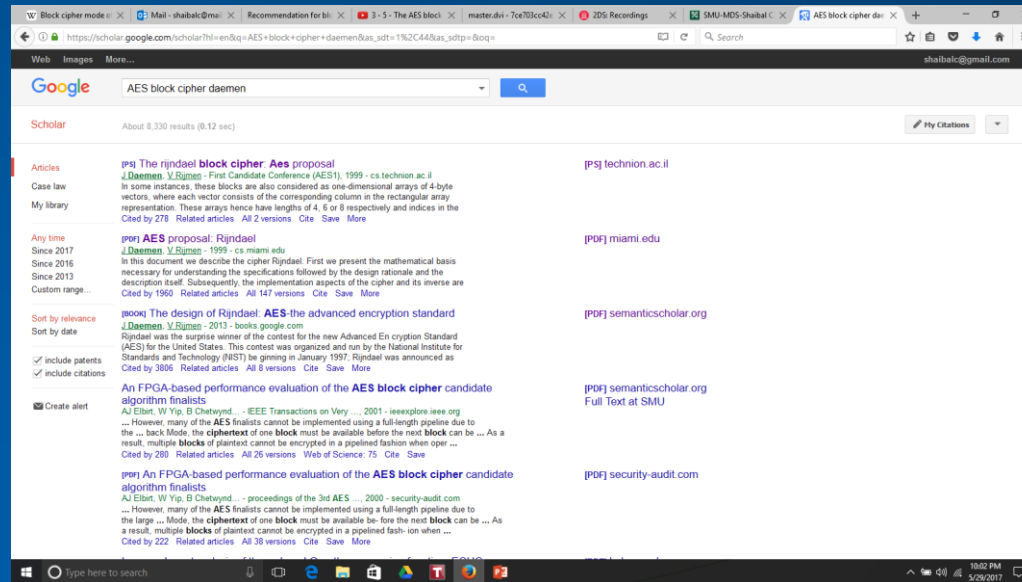
- Refine Abstract and Intro
- Write down 1 page of current research on the topic with a storyline to show how your novel approach differs
- Prepare the section of your solution, your architecture, your data/introduction to your simulation
- Ensure you have a MINIMUM of 3 pages including abstract, intro, 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 (2<sup>nd</sup> 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

