



Subject Overview & Introduction to Cybersecurity

**COMP90073
Security Analytics**

Dr. Sarah Erfani & Dr. Yi Han, CIS

Semester 2, 2021

Lecturers:

- Dr Sarah Erfani, MC Level 3, Room 3.3321, sarah.erfani@unimelb.edu.au
- Dr Yi Han, yi.han@unimelb.edu.au

Tutor:

- Yujing Mark Jiang, yujing.jiang@unimelb.edu.au

Lectures:

- Tuesdays and Thursdays, 14:15–15:15pm, Zoom

Tutorials: (per your registration) Start in Week 2

Consultation session:

- Fridays 2-3pm, Zoom

Lecture Materials:

- Lecture slides available on LMS, lectures recorded on Lecture Capture

Feedback:

- During/after lecture
- Tutorials
- Discussion board
- Consultation sessions
- Assignment feedback
- Sarah/Yi (by announcement or by appointment)

Subjects:

- COMP90049 Introduction to Machine Learning (Knowledge Technologies), or COMP30027 Machine Learning
- COMP90007 Internet Technology, or COMP30023 Computer Systems

Skills:

- Data structures & algorithms coding in Python
- Familiarity with formal mathematical notation
- Basic understanding of statistics and information theory

This subject does not include programming language tuition.

Assessment:

- 60% exam, 40% project

Requirements:

- 20/40 project hurdle, 30/60 exam hurdle, 50/100 overall

Projects:

- Project 1 will be released in week 2 and due in week 5.
- Project 2 will be released in week 5 and due in week 11.
(Dates to be confirmed in project specification on subject LMS site)
- You are expected to complete these individually.
- We will discuss the project in more detail over the coming weeks.

Note that the non-teaching week is between weeks 8 and 9.

- **Aim:**

“Security Analytics will examine how we can automate the analysis of our data to better detect and predict security incidents and vulnerabilities within our networks and organisations.”

- **Indicative Content:**

“The subject will first introduce the types of data sources that are relevant to detecting different types of security threats in practice.

The second part of the subject will introduce methods from machine learning that are widely used for cyber security analysis.

The third part of the subject will introduce some of the theoretical challenges and emerging issues for security analytics research, based on recent trends in the evolution of security threats.”

What the Subject Covers

- Exposure to a range of computing technologies for:
 - Understanding network traffic.
 - Accomplishing tasks that may not be well-specified or well-understood.
 - Exploring vulnerabilities of machine learning.
- A broader understanding of the kinds of things that can – and can't – be accomplished computationally.
- Insight into some research activities in computing, why they are undertaken, and how.

Week 1-4 (Yi):

- Cybersecurity landscape
- Network security & attacks
- Botnet and DDoS

Week 5-8 (Sarah):

- Unsupervised machine learning
- Anomaly detection
- Alert management

Week 9-12 (Yi):

- Adversarial machine learning – vulnerabilities
- Adversarial machine learning – explanation, detection and defence
- Adversarial reinforcement learning

There is no prescribed text. You may find these useful:

- Sumeet Dua and Xian Du, Data Mining and Machine Learning in Cybersecurity, 2011.
- Chio and Freeman, Machine Learning and Security, 2018.
- Goodfellow et al., Deep Learning, 2016.
<https://www.deeplearningbook.org/>
- Bhattacharyya et al., Network Traffic Anomaly Detection and Prevention: Concepts, Techniques, and Tools, 2017.
- Han et al., Data Mining Concepts and Techniques, 2000
- Harold F. Tipton, Official (ISC)2 guide to the CISSP CBK, 2010

- Rising Cybersecurity Attacks
- Current Cyber Security Talent Gap
- Core Cyber Security Principles
- Key Access Control Concepts
- Access Control Principles




Rising Cybersecurity Attacks

- Overall trend
 - Cybercrime costs globally: \$3 trillion in 2015 → \$10.5 trillion in 2025
 - 3rd largest economy



Cybercrime costs.

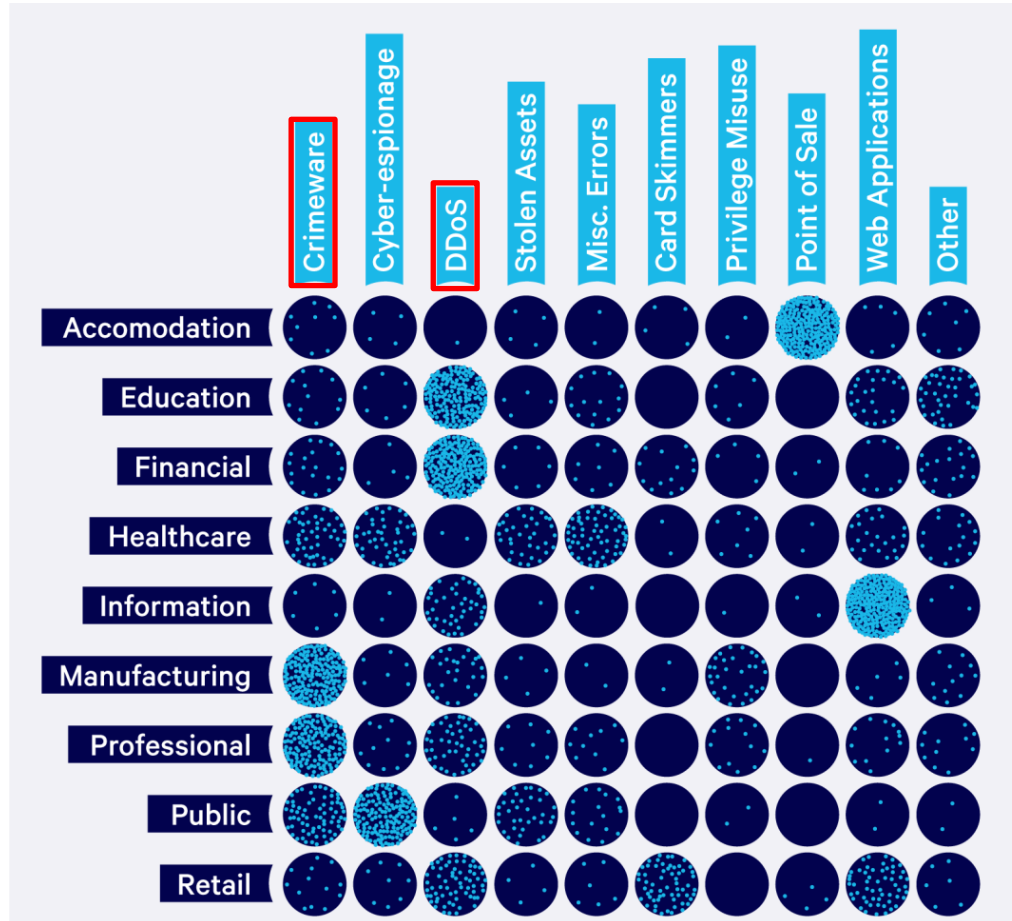
Source: <https://www.embroker.com/blog/cyber-attack-statistics/>

Country/Territory	GDP (US\$ M)
 United States [†]	21,433,226
 China ^{†[n 10]}	14,342,903
 Japan [†]	5,081,770

[https://en.wikipedia.org/wiki/List_of_countries_by_GDP_\(nominal\)](https://en.wikipedia.org/wiki/List_of_countries_by_GDP_(nominal))

Rising Cybersecurity Attacks

- Cyber incidents by industry

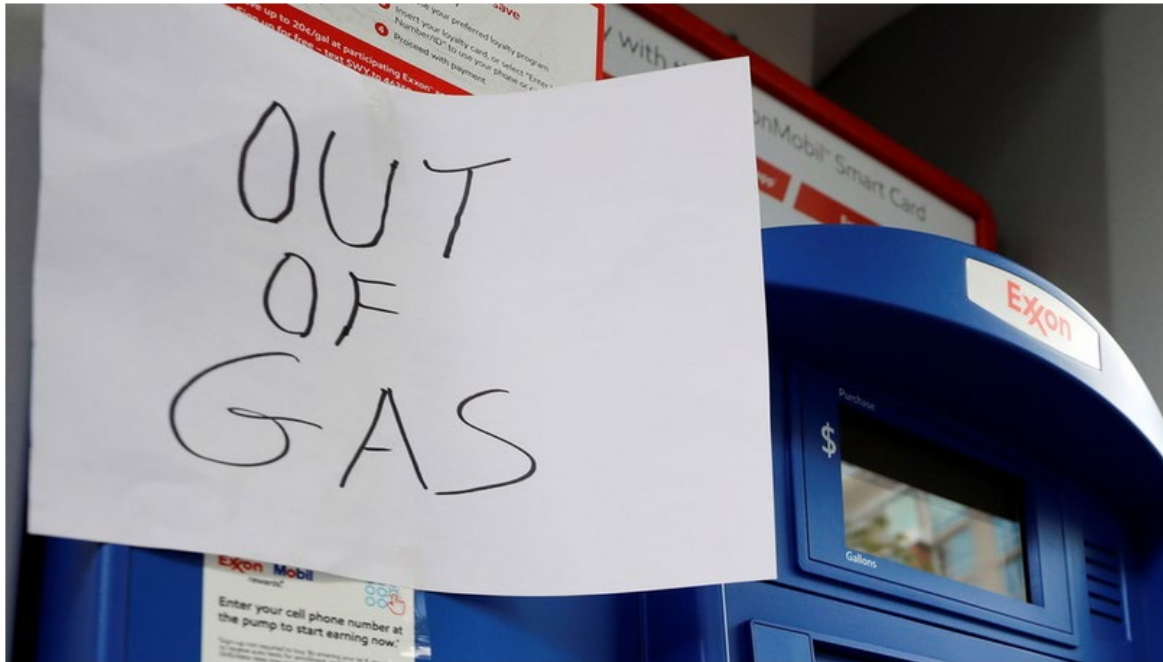


- Incidents

- Oil pipeline hit by DarkSide ransomware group

Colonial Pipeline CEO confirms paying \$4.4 million ransom to hackers, says he did it for America

19 May, 2021 19:01



A sign at a gas station after a cyberattack crippled Colonial Pipeline. © Reuters / Yuri Gripas

Source: <https://www.rt.com/usa/524269-colonial-pipeline-ransom-hackers/>

Rising Cybersecurity Attacks



<https://www.youtube.com/watch?v=HBP4meBn4OE>

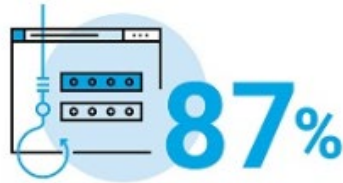
Rising Cybersecurity Attacks



Information Security and Privacy in the Times of COVID-19



say threat actors will
increase cyberattacks
on individuals



say rapid shift to work
from home **increased**
risk of data privacy
and protection issues



say threat actors will
take advantage of the
pandemic to disrupt
organizations



→ **ONLY 51% ARE HIGHLY CONFIDENT** in their
security team's ability to **detect and respond** to
these cyberthreats during the pandemic.

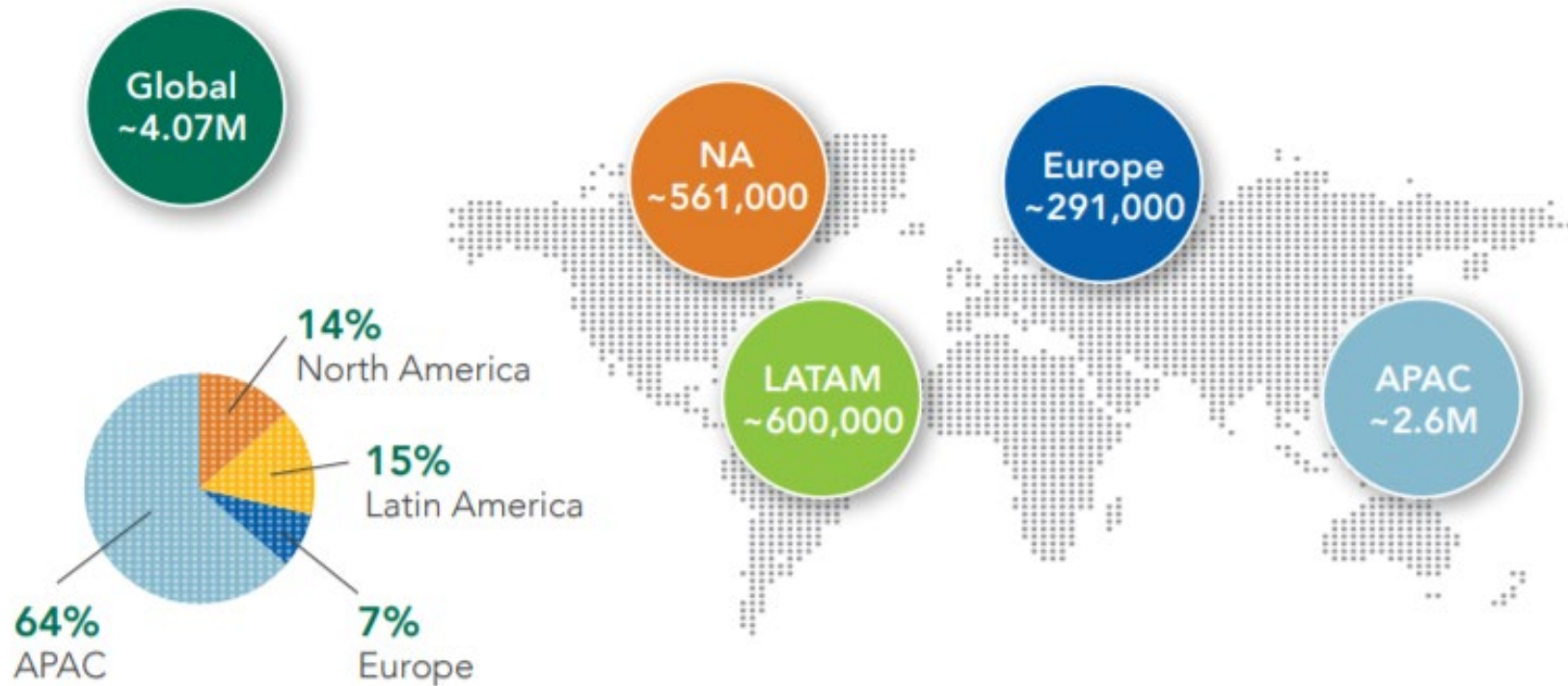
SOURCE: ISACA's COVID-19 Study, April 2020, www.isaca.org/covid19study

- Rising Cybersecurity Attacks
- **Current Cyber Security Talent Gap**
- Core Cyber Security Principles
- Key Access Control Concepts
- Access Control Principles

- Increasing cyber attacks drives the demand for Cybersecurity talent
 - According to Forbes, “As hackers ramp up attacks with increasingly sophisticated methods and tools that are readily available for purchase on the dark web, the "white hats" need all the help they can get. According to recent estimates, there will be as many as **3.5 million unfilled positions in the industry by 2021.**”
 - According to CSOonline, “The percentage of organizations reporting a problematic shortage of cybersecurity skills continues to increase. Here are the results from the last four surveys:
 - 2018-2019: 53%
 - 2017-2018: 51%
 - 2016-2017: 45%
 - 2015-2016: 42%”

Current Cybersecurity Talent Gap

The Cybersecurity Workforce Gap by Region



Source: (ISC)2 Cybersecurity Workforce Study, 2019

NEWS

Australians pessimistic that cybersecurity skills gap will be closed within a decade

But training providers, looking outside the industry for “a new breed of cybersecurity talent”, are doing their part to help



By David Braue

CSO | 13 DECEMBER 2019 11:18 AEDT

\$400 million: The cost of Australia's cyber security skills shortage

Australia's cyber security skills shortage worse than expected: AustCyber



Rohan Pearce (Computerworld)

28 November, 2018 10:34





AUSTRALIA'S CYBER SECURITY SECTOR COMPETITIVENESS PLAN

Key findings

Tackling the cyber security skills shortage

New research, undertaken exclusively for this updated Sector Competitiveness Plan, draws on a range of job market data showing that the skills shortage in Australia's cyber security sector is more severe than initially estimated and is already producing real economic costs.

Australia may need almost 18,000 additional cyber security workers by 2026 for sector to harnesses its full growth potential. The workforce shortfall has significant economic consequences. In 2017, the domestic cyber security sector is estimated to have forfeited up to \$405 million in revenue, which companies could have generated if they had been able to find enough cyber security workers to fill existing vacancies.

What You Will Learn

- Evaluate the suitability of different types of monitoring data for detecting security incidents
- Describe and implement a range of pattern recognition and machine learning algorithms for use in security analytics
- Select algorithms appropriate to a given security analysis task
- Apply pattern recognition and machine learning techniques to non-trivial security analysis tasks
- Evaluate computational techniques for security analytics to solve real-world problems, based on their accuracy and efficiency
- Discuss theoretical challenges and emerging trends for security analytics research

- Rising Cybersecurity Attacks
- Current Cyber Security Talent Gap
- **Core Cyber Security Principles**
- Key Access Control Concepts
- Access Control Principles

- **Confidentiality, Integrity, Availability (CIA triad)**
 - Ensuring the core concepts of availability, integrity, and confidentiality are supported by adequate security controls designed to mitigate or reduce the risks of loss, disruption, or corruption of information

- **Confidentiality** supports the principle of “least privilege” by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis
 - Data classification: an important **measure** to ensure confidentiality of information
 - E.g., public information, internal use only, confidential
 - Identification, authentication, and authorization through access controls are **practices** that support maintaining the confidentiality of information

- Sample **control** - information encryption
 - Symmetric cryptography
 - Require both the sender and the receiver to have the same key and algorithms
 - Example:
 - » Data Encryption Standard (DES), insecure due to small key size – 64-bit key(56 bits actual key)
 - » Triple DES, increased key length – 168 bits
 - » Advanced Encryption Standard (AES), supports 128, 192 and 256 bits key
 - Asymmetric cryptography
 - Two different keys are used, the sender uses the **public** key for encryption while the receiver uses the **private** key for decryption
 - Example, RSA, Diffie-Hellman

- **Integrity** is the principle that *information* should be protected from intentional, unauthorized, or accidental changes
 - *Information* stored in files, databases, systems, and networks must be relied upon to accurately process transactions and provide accurate information for business decision making
 - Sample controls – segregation of duties, approval checkpoints

- **Availability** is the principle that ensures that information is available and accessible by users when needed
 - Two primary areas affecting the availability of systems
 - 1) Denial of service attacks
 - 2) Loss of service due to a disaster
 - Sample controls – up-to-date system, tested incident management, disaster recovery planning

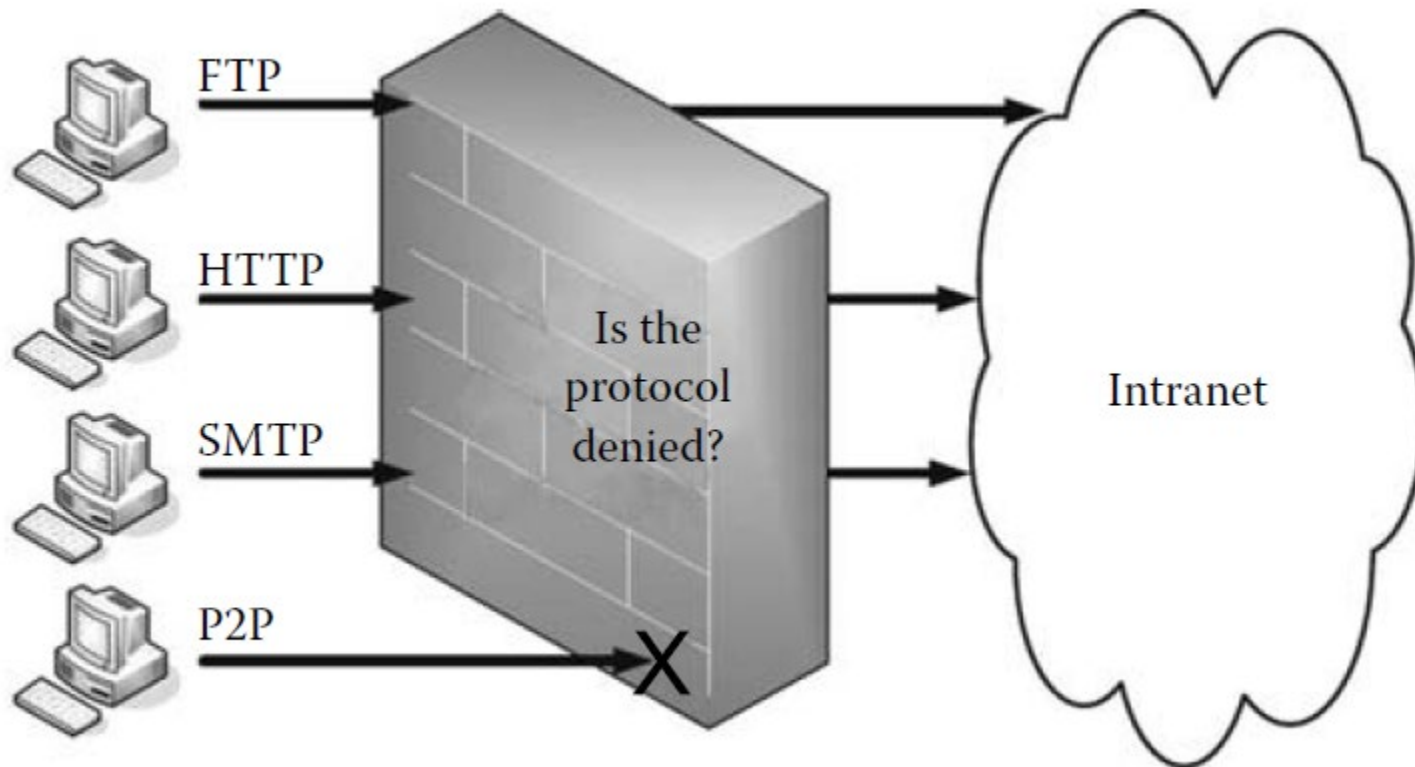
- Rising Cybersecurity Attacks
- Current Cyber Security Talent Gap
- Core Cyber Security Principles
- **Key Access Control Concepts**
- Access Control Principles

Key Access Control Concepts

- **Access control** is the process of allowing only authorized users, programs, or other computer systems (i.e. networks) to observe, modify, or otherwise take possession of the resources of a computer system. It is also a mechanism for limiting the use of some resources to authorized users.
- Four key attributes
 - 1) Specify which users can access a system
 - 2) Specify what resources those users can access
 - 3) Specify what operations those users can perform
 - 4) Enforce accountability for those users' actions

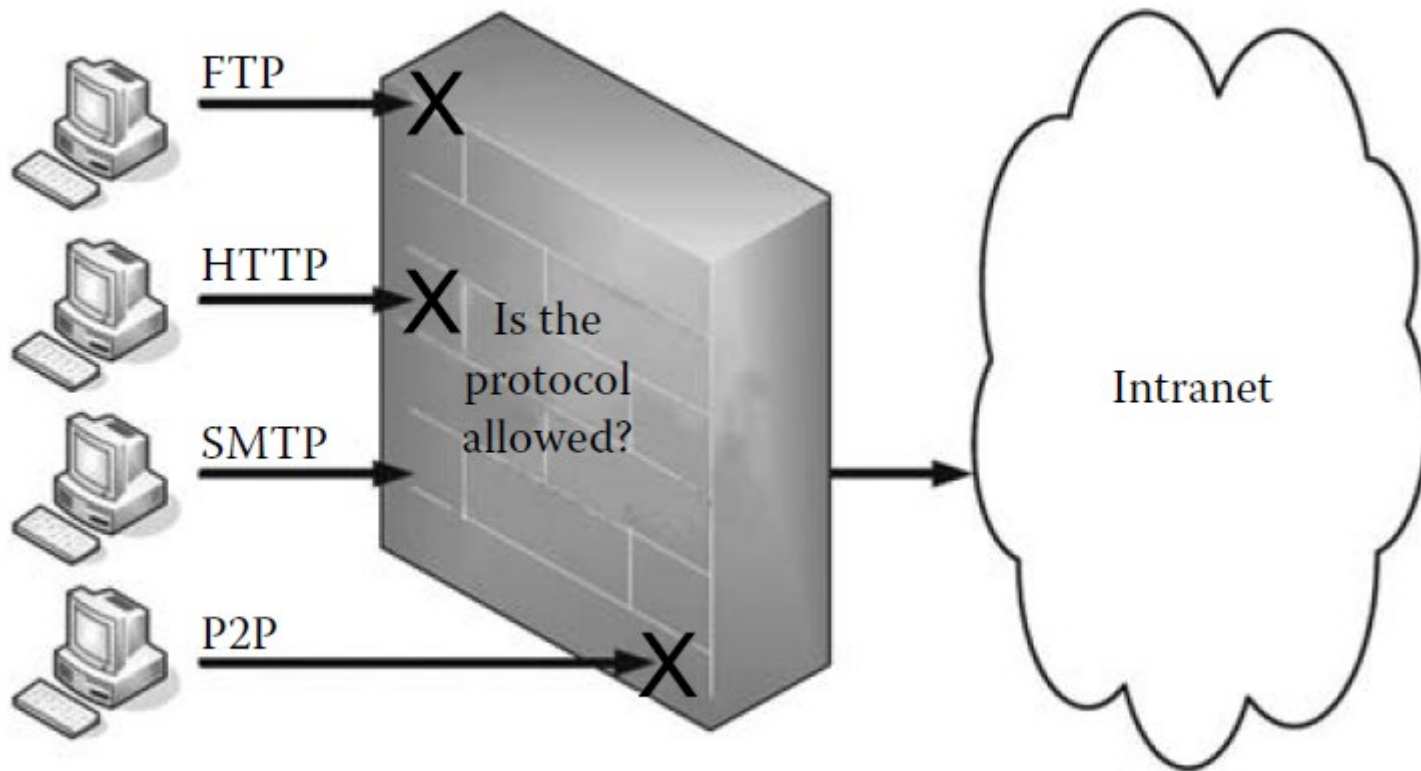
Key Access Control Concepts

- Determining a default stance
 - **Allow-by-default:** allowing access to any information unless there is a specific need to restrict that access



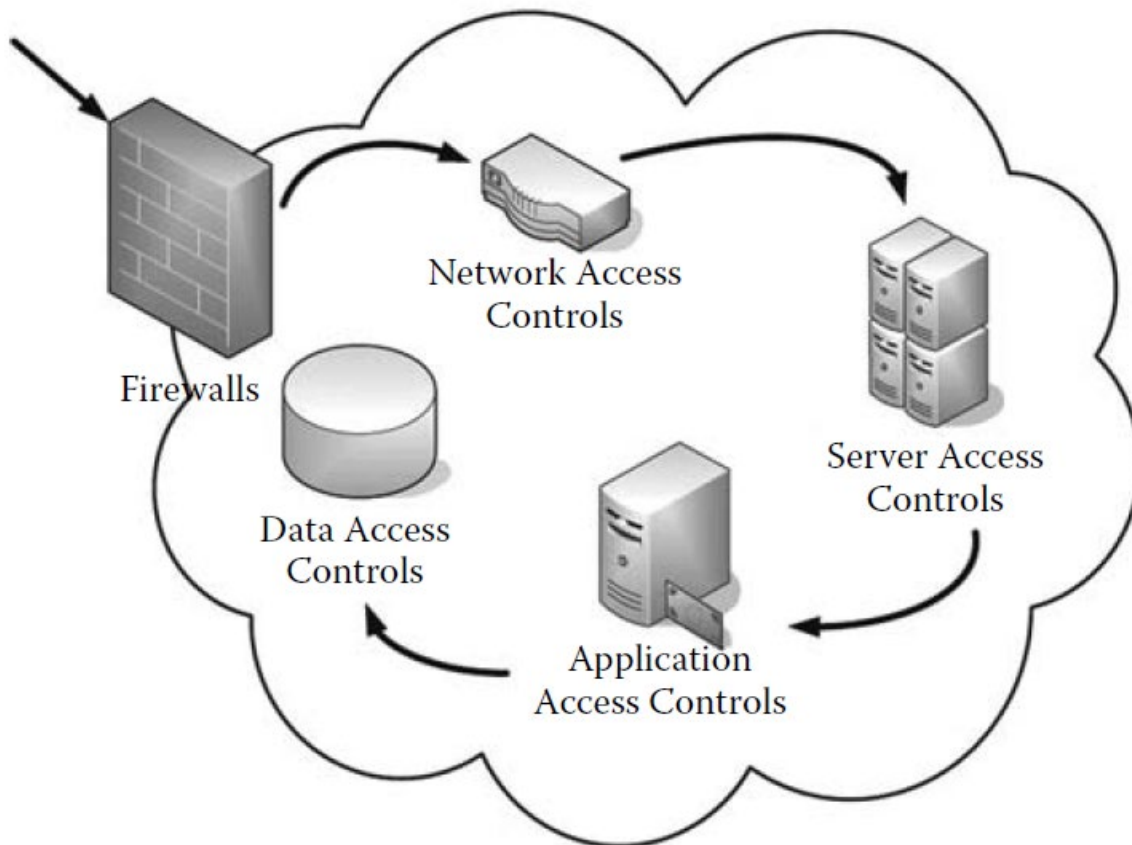
Key Access Control Concepts

- **Deny-by-default:** blocking all attempts to access information and resources unless that access is specifically permitted



Key Access Control Concepts

- **Defence in Depth** – practice of applying multiple layers of security protection between an information resource and a potential attacker



Network security:

- Firewalls
- Virtual private network (VPN)

System/application security:

- Antivirus software
- Authentication and password
- Encryption
- Logging and auditing
- Multi-factor authentication
- Vulnerability scanners
- Intrusion detection systems (IDS)

- A General Process
 - 1) *Defining resources*: specifically defining the resources that exist in the environment for users to access
 - 2) *Determining users*: defining who can access a given resource
 - 3) *Specifying the users' use of the resources*: specifying the level of use for a given resource and the permitted user actions on that resource

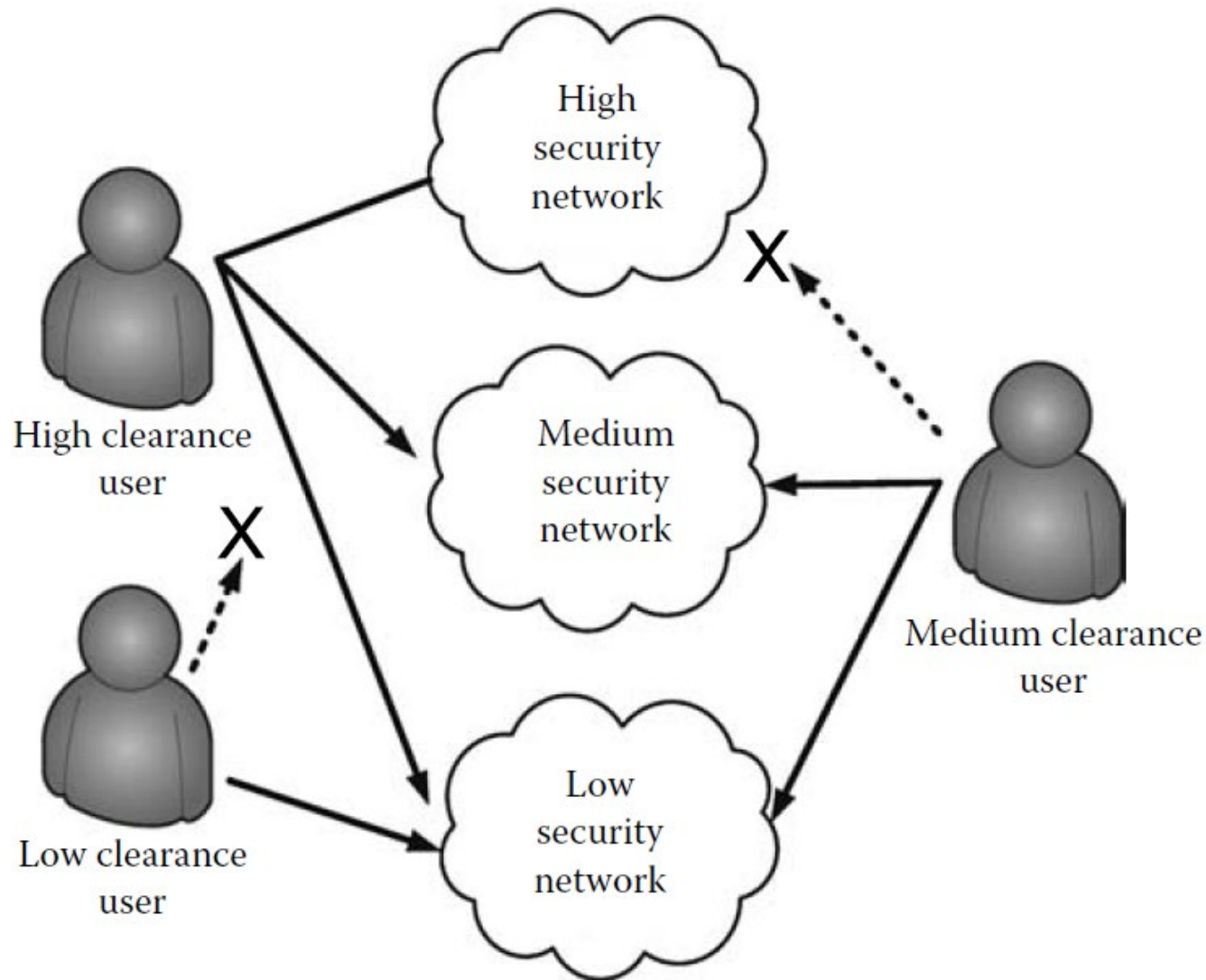
- Rising Cybersecurity Attacks
- Current Cyber Security Talent Gap
- Core Cyber Security Principles
- Key Access Control Concepts
- **Access Control Principles**

- **Access Control Policy:** specifying the guidelines for how users are identified and authenticated and the level of access granted to resources
- **Separation of Duties:** altering the way people perform their work functions
- **Least Privilege:** requires that a user or process be given no more access privilege than necessary to perform a job, task, or function
- **Need to Know:** defines a bare minimum access need based on job or business requirements

Access Control Principles

- **Compartmentalization:** the process of separating groups of people and information such that each group is isolated from the others and information does not flow between groups
 - E.g., an organization might compartmentalize (both logically and physically) a team working on mergers and acquisitions so that the information that team is working on will not leak to the general employee population and lead to a potential insider trading problem
- **Security Domain:** an area where common processes and security controls work to separate all entities involved in these processes from other entities or security domains
 - E.g., all systems and users managing financial information might be separated into their own security domain, and all systems involved in e-commerce activity might get their own security domain

Access Control Principles



- Core cyber security principle
 - Explain CIA triad
 - Apply the appropriate controls to protect CIA
- Key access control concepts
 - Describe access control and four key attributes
 - Compare allow-by-default and deny-by-default
 - Explain “Defense in Depth”
 - Describe a general process for access control
 - Describe access control principles

- [1] Harold F. Tipton, 2010, *Official (ISC)2 guide to the CISSP CBK, Second Edition*, SciTech Book News