# SECTION 1
# Cybersecurity

Dr. Uwe Glässer, Professor, Computing Science - Software Technology Lab
Amir Yaghoubi Shahir, PhD candidate, Software Technology Lab, sayaghou@sfu.ca

© 2017-2022 Uwe Glässer. All Rights Reserved.

# Contents

1.1 Perspectives 3
1.2 Practicalities 5
1.3 Overview and Grading 9
1.4 Career Perspectives 12
1.5 Cybersecurity - Introduction 14
1.5.1 Evolving Threat Landscape
1.5.2 Decisive Action Needed
1.5.3 Cybercrime
1.5.4 Attacking Critical Infrastructure
1.5.5 Where’re We Heading?
1.5.6 Definition of Cybersecurity
1.5.7 Advanced Persistent Threats
1.6 Cybersecurity Strategy 41
1.6.1 Measures and Countermeasures
1.6.2 Signatures
1.6.3 Shift from Signature-Only to Anomaly-Based Detection
1.6.4 Cyber Security Operations Centre
1.7 What Exactly Is Cyber Risk? 53
1.7.1 Threat, Vulnerability, and Risk
1.7.2 Risk Assessment
1.8 Engineering Trustworthy Systems 60

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.1 Perspectives

- This course introduces **cybersecurity** (cyber security) and explores cyber situational awareness concepts and threat intelligence models.
- **Cyber security analytics** and **probabilistic modeling** for threat detection and response (mitigative action) will play a central role.
- Coursework involves using the **R language** and software environment for statistical computing and graphics.
- Fundamental principles and practices of cybersecurity **risk assessment**, **intrusion detection and prevention** methods and their application to critical infrastructure protection will be discussed in detail.

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.1 Perspectives (cont.)

Topics include:

- Cyber threat analysis and intrusion detection
- Advanced persistent threats and zero day exploits
- Time series analysis and forecasting
- Probability theory and probabilistic modeling
- Stochastic processes and Markov models
- Anomaly detection and scoring methods
- Risk assessment and management
- Blockchain technology

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.2 Practicalities

- Office Hours

  Offered as Zoom sessions

  Teachings Assistants - Tuesdays, TBA

  Instructor - Fridays, 14:00-15:00 via Zoom

  Office hours may end after 20 minutes in case of no attendance.

- Special Sessions

  Last week of classes: **One extra hour** needed for term project presentations on Nov 30 and Dec 1 & 2 - see also on course page

- Tutorials

  R language and software environment for statistical computing

  During regular class hours as will be announced

© 2017-2022 Uwe Glässer. All Rights Reserved.

- Course Home Page

  https://coursys.sfu.ca/2022fa-cmpt-318-d1/pages/

- Course Materials

  **Lecture slides** will be posted regularly **after** class.

  **Tutorial slides** will be posted regularly **after** class.

  Reading materials will be posted as needed.

  No single textbook covers the entire curriculum.

© 2017-2022 Uwe Glässer. All Rights Reserved.

- Recommended Books

**An Introduction to Statistical Learning: with Applications in R**,
Gareth James, Daniela Witten, Trevor Hastie, and Robert Tibshirani,
Springer, 2017, ISBN 978-1461471370

**Fundamentals of Machine Learning for Predictive Data Analytics**,
John D. Kelleher, Brian Mac Namee, and Aoife D'Arcy,
The MIT Press, 2020, ISBN 978-0262044691.

**How to Measure Anything in Cybersecurity Risk**,
Douglas W. Hubbard and Richard Seiersen,
John Wiley & Sons, 2016, ISBN 978-1119085294

© 2017-2022 Uwe Glässer. All Rights Reserved.

- The Cybersecurity Discipline

"A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an **interdisciplinary** course of study, including aspects of law, policy, human factors, ethics, and risk management."[1]

*Source:* Join Task Force on Cybersecurity Education (ACM, IEEE, AIS and IFIP)
Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity
Version 1.0 Report - 31 Dec. 2017

[1] While cybersecurity is an interdisciplinary course of study, it is fundamentally a computing-based discipline.

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.3 Overview and Grading

<table>
<tr><th colspan="3">CMPT 318 - Overview</th></tr>
<tr><th>Lectures</th><th>Tutorials</th><th>Tasks</th></tr>
<tr><td>SECTION 1<br>Outline and Introduction</td><td rowspan="2">TUTORIAL 1-5<br>R language and software environment<br>-<br>TUTORIAL 6<br>Q&A style</td><td rowspan="4">Reading Assignments<br>-<br>Marked Group Assignments<br>-<br>Test 1<br>Test 2<br>Test 3<br>-<br>Term Project:<br>Intrusion detection for cyber-physical systems</td></tr>
<tr><td>SECTION 2<br>Cyber Security Analytics</td></tr>
<tr><td>SECTION 3<br>Anomaly Detection</td><td rowspan="2">OFFICE HOURS<br>Teaching Assistants<br>-<br>Instructor</td></tr>
<tr><td>SECTION 4<br>Blockchain or Cyber Risk</td></tr>
<tr><td colspan="3">Term Project Evaluation - Presentations and Reports</td></tr>
</table>

© 2017-2022 Uwe Glässer. All Rights Reserved.

# Grading

- Assignments (**20%**)

  Reading assignments

  Marked assignments

- 3 Tests (**30%**)

  Tests to be announced at least one week prior to the test date

  Cover subjects from reading materials

  Short questions with concise answers

- Term project (**50%**)

  Presentation 15%, Report 35%

- **Active** class participation (up to 5%) - Bonus points!

© 2017-2022 Uwe Glässer. All Rights Reserved.

- Term Project (continued)

*"One must learn by doing the thing;*
*for though you think you know it,*
*you have no certainty, until you try." —Sophocles*

**Working in teams of 3 team members**

Project is organized in two parts:
Project report + oral presentation
Who contributed what to the project needs to be documented.

**Meet early** and **meet often** to overcome logistic challenges.

Project teams shall be finalized by Tuesday, **September 20!!!**
Decide on your availability for the final presentation session

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.4 Career Perspectives

- Security sales
- IT auditor / Security Analyst
- Security administrator

- Vulnerability assessor
- Security engineer
- Network administrator

- Forensics
- Software developer
- Ethical hacker / penetration tester
- Cryptographer

**Least technical**

**Most technical**

Source: ISACA, Vancouver

© 2017-2022 Uwe Glässer. All Rights Reserved.

# Job Market Analysis

The demand for post-secondary education in cybersecurity is steadily growing, with commercial and government sectors facing **a widening gap** between their needs to hire in this field and the number of skilled workforce available.

Data and facts from leading analysts like Gartner and other recognized sources confirm the projected talent shortage:

Cyber Seek, 2022[2]:

- 714,548 online job listings for cybersecurity-related positions from May 2021 through April 2022.
- 1,091,575 estimated number of workers employed in cybersecurity-related jobs from May 2021 through April 2022.

**Go for it … NICE!**

[2] CyberSeek (2022). National Initiative for Cybersecurity Education (NICE). U.S. Department of Commerce. Retrieved from https://www.cyberseek.org/heatmap.html

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.5 Cybersecurity - Introduction

Source: CartoonStock

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.5.1 Evolving Threat Landscape

Cyberattacks are increasing in frequency, severity, and sophistication[3]:

*Figure 1: Average Ransom Payment (converted to CAD from USD), 2018 to 2020 (Source: [2])*

[3] *Source [2]:* Canadian Centre for Cyber Security. National Cyber Threat Assessment 2020. Communications Security Establishment, Government of Canada, 2020.

© 2017-2022 Uwe Glässer. All Rights Reserved.

Responding to the **globally evolving threat landscape**, cybersecurity technology is advancing, but not fast enough to **keep pace with the threat**.

Information security breaches routinely compromise protection of **sensitive data and information**, exposing

- personal identities
- intellectual property
- financial assets.

The result is mounting damages in the **hundreds of billions of dollars**, erosion of trust in conducting business and collaboration in cyberspace, and risk of catastrophic events that could cause crippling damage to companies and even entire countries.[4]

[4] O. Sami Saydjari. Engineering Trustworthy Systems: A Principled Approach to Cybersecurity. Communications of the ACM, Vol. 62, No.6, June 2019, 63-69.

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.5.2 Decisive Action Needed

Canada is one of the most connected countries in the world. We live our lives online and need to be able to **trust our cyber systems.**

Digital technologies and the internet are increasingly important to innovation and economic growth. A safe and secure cyberspace is critical for Canada's competitiveness, economic stability, and long-term prosperity.[5]

[5] Canadian Centre for Cyber Security. National Cyber Threat Assessment 2018. Communications Security Establishment (CSE), Government of Canada, 2018.

© 2017-2022 Uwe Glässer. All Rights Reserved.

**National Cyber Threat Assessment 2020**, Canadian Centre for Cyber Security stated: “State-sponsored threat actors conduct cyber espionage against critical infrastructure in Canada and other allied nations.”

This includes reconnaissance and intelligence-gathering in the energy, aerospace and defence sectors.

© 2017-2022 Uwe Glässer. All Rights Reserved.

# Why do we care?

## Discussion

1. What do cyber threats mean realistically?
2. Are YOU concerned PERSONALLY?
3. Future impact on individuals, society and economy?

© 2017-2022 Uwe Glässer. All Rights Reserved.

"So many of our transactions are now conducted in cyberspace that we have developed dependencies we could not even have imagined a generation ago. To be dependent is to be vulnerable. We have grown cheerfully dependent on the benefits of our online transactions, even as we observe the growth of cyber crime. We remain largely oblivious to the potential catastrophe of a well-targeted cyberattack."

— Ted Koppel, 2015

© 2017-2022 Uwe Glässer. All Rights Reserved.

LifeLabs®

https://customernotice.lifelabs.com

© 2017-2022 Uwe Glässer. All Rights Reserved.

"*In 2016, the world saw cyberattacks transcend technology targets to that of wetware*—human beliefs and propensity to action. *The notion of* ***hacking democracy itself*** *came into light, posing an existential threat to entire governments and ways of life through what is sometimes known by the military as* influence operations."

— (O. SAMI SAYDJARI, 2019)

Official Trailer (video)

# 1.5.3 Cybercrime

## Ransomware

The National Security Agency headquarters in Maryland. A leaked N.S.A. cyber weapon, EternalBlue, has caused billions of dollars in damage worldwide.
A recent attack took place in Baltimore, the agency's own backyard.

In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc
— The New York Times

(Nicole Perlroth and Scott Shane May 25, 2019)

A tale of two cities: Why ransomware will just get worse
Texas hit by ransomware — 22 small cities took full punch

(arstechnica.com, August 21, 2019)

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.5.4 Attacking Critical Infrastructure

**Critical infrastructure** refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. … Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects and significant harm to public confidence.

Source: Public Safety Canada

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.5.4 Attacking Critical Infrastructure

**Critical infrastructure** refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government. … Disruptions of critical infrastructure could result in **catastrophic loss of life**, adverse economic effects and significant harm to public confidence.

Source: Public Safety Canada

## Critical Infrastructure Sectors

There are **16 critical infrastructure sectors** whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Source: US Cybersecurity & Infrastructure Security Agency
https://www.cisa.gov/critical-infrastructure-sectors

© 2017-2022 Uwe Glässer. All Rights Reserved.

CRITICAL MANUFACTURING SECTOR

© 2017-2022 Uwe Glässer. All Rights Reserved.

Electric power grids, communication networks, oil and gas pipelines, intelligent transportation systems, hospitals and other critical infrastructure provide vitally important services; any major disruption would have severe consequences for public safety and national security.

**Advanced threats** targeting such infrastructure, often in the form of ***zero-day exploits***[6], may not only cause temporary service disruptions but can cripple major components physically, causing lasting damage that threatens human safety beyond comprehension.

[6] Zero-day exploits target security hardware-software system flaws not known prior to an attack, making them virtually invisible to and unstoppable by conventional cybersecurity protection.

© 2017-2022 Uwe Glässer. All Rights Reserved.

# Supervisory Control

Supervisory control is a form of Industrial Control System, or ICS, widely used for industrial automation of cyber-physical systems, or CPS. Such systems typically comprise many individual controllers or control loops operating in a decentralized manner to monitor and control a physical process producing goods or providing services (Industry 4.0).

- …
- …

© 2017-2022 Uwe Glässer. All Rights Reserved.

# Supervisory Control

Supervisory control is a form of Industrial Control System, or ICS, widely used for industrial automation of cyber-physical systems, or CPS. Such systems typically comprise many individual controllers or control loops operating in a decentralized manner to monitor and control a physical process producing goods or providing services (Industry 4.0).

- Automation is vital for the **continuous operation** of critical infrastructure and the services it provides. Electric power grids, public water utilities and smart transportation networks routinely rely on supervisory control systems, with increasing integration of computation, networking and physical processes.

- …

© 2017-2022 Uwe Glässer. All Rights Reserved.

# Supervisory Control

Supervisory control is a form of Industrial Control System, or ICS, widely used for industrial automation of cyber-physical systems, or CPS. Such systems typically comprise many individual controllers or control loops operating in a decentralized manner to monitor and control a physical process producing goods or providing services (Industry 4.0).

- Automation is vital for the **continuous operation** of critical infrastructure and the services it provides. Electric power grids, public water utilities and smart transportation networks routinely rely on supervisory control systems, with increasing integration of computation, networking and physical processes.

- Automation enhances cost efficiency, quality of service delivery and safe operation of critical assets. Despite the benefits, increasing reliance on automation in light of the evolving cyber threat landscape also increases the **attack surface** for advanced persistent threats and amplifies the risk of cascading effects.

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.5.5 Where’re We Heading?

Source: Wikipedia

© 2017-2022 Uwe Glässer. All Rights Reserved.

Here goes your privacy ...

© 2017-2022 Uwe Glässer. All Rights Reserved.

# Botnets

## Mirai[7], BASHLITE and Carna

The Mirai botnet, composed primarily of embedded and IoT devices, emerged as a high-profile **distributed denial-of-service** (DDoS) threat in late 2016 when it overwhelmed several high-profile targets with massive DDoS attacks.

- Starting in September 2016, a spree of massive distributed denial-of-service (DDoS) attacks temporarily crippled Krebs on Security, OVH, and Dyn. The initial attack on Krebs **exceeded 600 Gbps in volume** — among the largest on record.
- This overwhelming traffic was sourced from hundreds of thousands of some of the Internet's least powerful hosts — Internet of Things (IoT) devices — under the control of the botnet named Mirai (Japanese for "the future").
- The botnet infected nearly 65,000 IoT devices in its first 20 hours before reaching a steady state population of 200,000– 300,000 infections.
- Mirai has spawned many variants that follow the same infection strategy, leading to speculation that "IoT botnets are the new normal of DDoS attacks."

[7] Source: Manos Antonakakis et al., Understanding the Mirai Botnet, 26th USENIX Security Symposium, 2017.

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.5.6 Definition of Cybersecurity

"To understand the term cybersecurity, we must first define the term cyberrisk.

Figure 1

**Cyberrisk** is not one specific risk. It is a group of risks, which differ in technology, attack vectors, means, etc. We address these risks as a group largely due to two similar characteristics: A) they all have a potential great impact B) they were all once considered improbable.

To understand this we start with a visual representation of the traditional risk curve:

Figure 1 is a simple graph that shows the **correlation between the probability of a risk occurrence and its potential impact**. As we move to the right, risk's potential impact increases. At the far right of the risk curve we see a "long tail"—a group of very high impact risks with a very low probability of occurrence. (Naturally, organizations have resource constraints and focus their efforts on addressing the risks with high probability of occurrence and potentially significant impact.)"

Source: Barzilay, 2017

© 2017-2022 Uwe Glässer. All Rights Reserved.

Figure 2

"Next, let us define focus zone (depicted in Figure 2 below) as the area containing the risks to which the organization directs its mitigation efforts. The size of the focus zone is determined by factors such as risk appetite, cost effectiveness, the CISO's attitude, organizational culture, availability of resources and relative threat landscape.

As illustrated below, the efforts invested in addressing risks within the focus zone are commonly referred to as information security. Those risks include traditional malwares (viruses, trojans, spyware, adware, etc.), standard phishing attacks, standard distributed denial of service (DDoS) attacks, standard hacking activities, etc."

© 2017-2022 Uwe Glässer. All Rights Reserved.

Figure 3

"Of course, something has changed recently. The threat landscape evolved to the point that risks that were once considered unlikely began occurring with regularity. The increased probability of **very-high-impact risk occurrences** is illustrated in Figure 3 below as Item 1.

This trend can be attributed to higher maturity of attack tools and methods, increased exposure, increased motivation of attackers, and better detection tools enabling more visibility. With that said, we must accept that some of this shift is a result of our increased awareness to this new, highly focused group of risks.

The change to the threat landscape forces us to **expand an organization's focus zone** to include these previously excluded risks—illustrated below as Item 2."

© 2017-2022 Uwe Glässer. All Rights Reserved.

Figure 4

"This new group of very-high-impact risks that now requires our attention is commonly referred to as cyberrisk. As illustrated in Figure 4, efforts invested in addressing cyberrisks are known, naturally, as cybersecurity.

This group of risks includes all sorts of strange scenarios: organization specific, specially designed malwares; manipulated hardware and firmware; the usage of stolen certifications; spies and informants; exploiting vulnerabilities in archaic hardware; attacking third party service providers; etc. This list also includes what are known as **advanced persistent threats**."

© 2017-2022 Uwe Glässer. All Rights Reserved.

"Some might consider information security and cybersecurity as two different disciplines, but I would argue that cybersecurity is a subdiscipline of information security (see Figure 5).

Figure 5

Cybersecurity is the sum of efforts invested in addressing cyberrisk, much of which was, until recently, considered so improbable that it hardly required our attention.

We must remember that the shift of the risk curve represents an ongoing trend. Very-high-impact risks will become increasingly frequent, forcing us to become better at protecting assets and devising creative solutions to mitigate risks."

Source: ISACA News, 2017

© 2017-2022 Uwe Glässer. All Rights Reserved.

# 1.5.7 Advanced Persistent Threats

An advanced persistent threat, or APT, is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or group targeting a specific entity (either a private organization, a state or both for business or political motives).

APT processes require **a high degree of covertness over a long period of time**:

- advanced signifies sophisticated techniques using malware to exploit vulnerabilities in systems;
- persistent suggests that an external command and control system is continuously monitoring and extracting data from a specific target;
- threat indicates human involvement in orchestrating the attack.

APT usually refers to a group, such as a government or organized crime, with both the capability and the intent to target, persistently and effectively, a specific entity.

This commonly refers to cyber threats, in particular espionage using a variety of intelligence gathering techniques to access sensitive information. The purpose of these attacks is to **place custom malicious code** (through social engineering and spear phishing) on computers for specific tasks and to **remain undetected for the longest possible period**.

© 2017-2022 Uwe Glässer. All Rights Reserved.

# Kill chain

Actors behind advanced persistent threats create a growing risk to organizations' financial assets, intellectual property, and reputation by following a continuous process, the kill chain.

Source: Dell SecureWorks

Commodity threat means casting the net wide, not knowing what specific targets may be compromised.

Hactivism is the subversive use of computers and computer networks to promote a political agenda or a social change.

© 2017-2022 Uwe Glässer. All Rights Reserved.