CMPT 318

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.

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

**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.**

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.

the efforts invested in addressing risks

within the focus zone are commonly referred to as

information security

.

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

this new group of very-high impact risks that now requires our attention is commonly referred to as cyberrisk

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

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

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.

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

Signature-based intrusion detection systems

, or IDS, are the oldest form of

detecting malicious activity via network traffic. This form of detection requires

knowledge about

what malicious activity “looks like”

so one can create a

signature to detect a known attack whenever it happens again

A virus signature is a continuous sequence of bytes that is common for a certain malware sample. That means it’s contained within the malware or the infected file and not in unaffected files

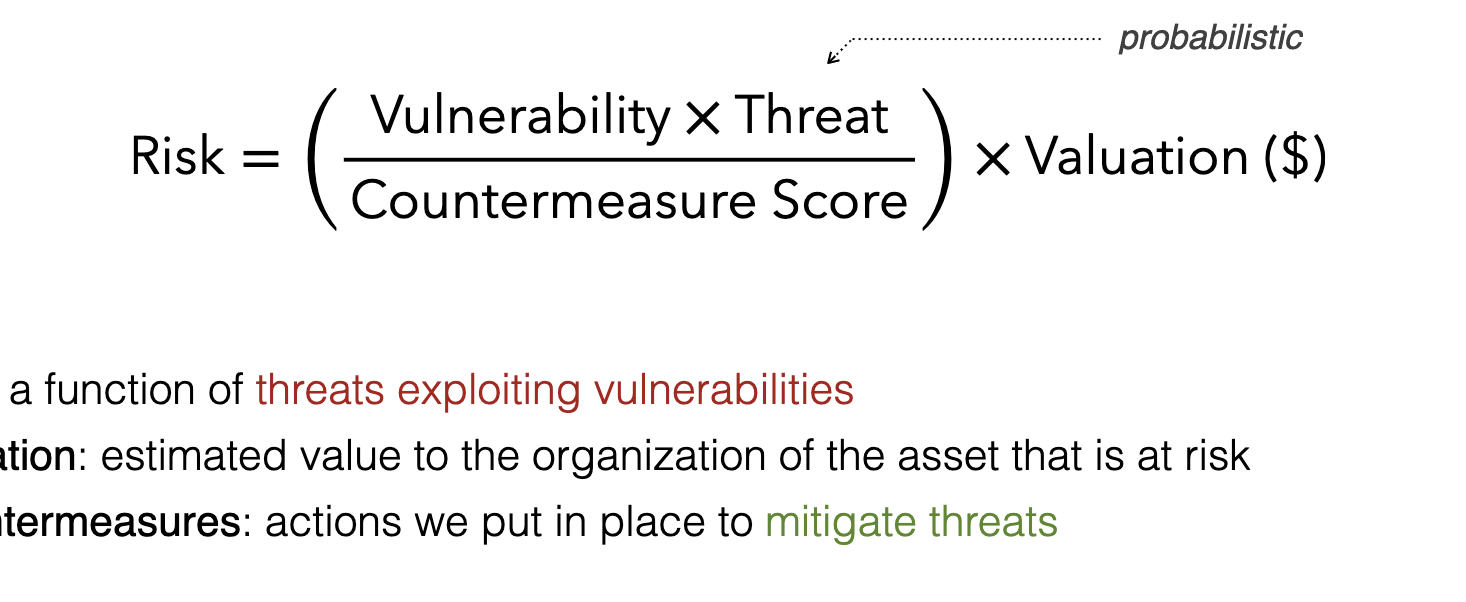
Anomaly detection- These approaches define NORMAL PATTERNS in network traffic or individual computer operations and then scan continuously for patterns that depart from the norm sufficiently to cause information system operators to suspect malicious activity

An intrusion detection system, or IDS, is typically either a software application or a hardware device that monitors incoming and outgoing network traffic for signs of

malicious activity or violations of security policies. Intrusion detection systems and IDS products are often likened to intruder alarms, notifying you of any activity that might compromise your data or network

cybersecurity risk is the probability of cyberattacks occurring multiplied by the potential damages that would result if they actually occurred

.A botnet is a group of Internet-connected devices, each of which runs one or more bots. Botnets can be used to perform Distributed Denial-of-Service attacks, steal data, send spam, and allow the attacker to access the device and its connection. The owner can control the botnet using command and control software



**Assets**

People, property, and information

•

employees, clients and customers along with other invited persons such as

contractors or guests

•

tangible and intangible assets that can be assigned a value: networks,

servers, IP, reputation and proprietary information such as trade secrets

•

databases, software code, encryption keys, critical company records, many

other intangible items

**Threat**

Anything that can exploit a vulnerability

•

intentionally or accidentally, and

•

obtain, damage, or destroy an asset.

A threat is what we’re trying to protect against.

A threat, in the context of computer security, refers to anything that

has the

potential to cause serious damage

to a computer system. A threat is something

that may or may not happen.

**Vulnerability**

Anything that can be exploited by a threat to gain unauthorized access to an

asset

A vulnerability is a weakness or gap in our protection efforts.

**Risk**

**Potential for loss, damage or destruction of an asset by a threat exploiting a**

**vulnerability**

**Risk is the intersection of assets, threats, and vulnerabilities.**