
Week 1
NYU
Spring 2025
CS6813: Information Security and Privacy
Instructor: Mo Satt
moshe.satt@nyu.edu
[*] Slides based upon materials maintained by Justin Cappos at NYU and Dr. Edward G. Amoroso (eamoroso@tag-cyber.com)
NYU

Week 1

Instructor: Mo Satt

https://www.linkedin.com/in/mosatt/

M.S. Cyber Security,
NYU Tandon School of Engineering, 2020
Chief Information Security Officer (CISO)
2019 NYU Cyber Scholar
Graduate of NYU CS Bridge Program

Fun Facts: Former DJ of music show on WNYU.ORG/WNYU 89.1 FM titled: “Artificial Inspiration” (featuring AI-generated music) and Amateur (Ham) Radio Operator, N2YU

NYU

Week 1

Other Cyber Security Classes at Tandon:

(Check Albert for Availability)

CS 6823: Network Security
CS 9163: Application security
CS 6903: Applied Cryptography
CS 6573: Penetration Testing and Vulnerability Analysis
CS 6803: Information Systems Security Engineering and Management
CS 6963: Digital Forensics
CS 9223: Selected Topics in CS:
Art Of Binary Exploitation: Mobile and Embedded Systems
Introduction to Offensive Security
Privacy in the Electronic Society
Mobile Security
Security Analytics

NYU

Week1

Course Schedule:

Lecture	Topic(s)	Date
Lecture 1	**Introduction to the Course**	Jan 21, 2025
Lecture 2	**Security Design Principles**	Jan 28, 2025
Lecture 3	**Threat Modeling**	Feb 4, 2025
Lecture 4	**Security Policies**	Feb 11, 2025
Exam 1	Covers Lectures 1-4	Feb 25, 2025
Lecture 5	**Access Control (1): Operating Systems, phones**	Mar 4, 2025
Lecture 6	**Authentication and IAM**	Mar 11, 2025
Lecture 7	**Access Control (2): IFC, O-Cap**	Mar 18, 2025
Lecture 8	**Lesson 8: Containerization: VMs, SFI, DoS**	Apr 1, 2025
Exam 2	Covers Lectures 5-8	Apr 8, 2025
Lecture 9	**Privacy and Key Management**	Apr 15, 2025
Lecture 10	**Software validity and rights**	Apr 22, 2025
Lecture 11	**Injection attacks and defenses**	Apr 29, 2025
Lecture 12	**Cryptography**	May 6, 2025
Final Exam	Covers Lectures 1-12	May 13, 2025

Week 1

Expectations:

About your background:

- Reasonable programming skills (Python)
- “Wikipedia level" understanding of:

networks, operating systems, C programming, virtual machines, etc.

You'll need basic competency for the class to make sense!

- Consistent workload
- Practical / exploration focused
- Background reading (see webpage)

Be sure to keep up!
If you need help, ask!

Week 1

Expectations:

All students are expected to be familiar with and to conscientiously observe all of the health and safety rules and policies the University has put in place in response to the COVID-19 pandemic.

Most prominently, this includes:

- Compliance with NYU's vaccine and uploading requirement and policy
- Compliance with NYU's masking rules
- Compliance with the University's events and gatherings guidelines
- Compliance with the University's visitors, vendors, and affiliates rules
- Compliance with the University rules regarding building access
- Compliance with required testing and physical distancing for those who are not fully vaccinated
- Compliance with the University's directives involving isolation, quarantine, reporting, and other public health measures

https://www.nyu.edu/life/safety-health-wellness/coronavirus-information.html

NYU

Week 1

Emergencies

- Call 911 to reach New York City Emergency Services,
then call NYU Public Safety at (212) 998-2222 to report the emergency

- Urgent Medical Needs: Call the Student Health Center at (212) 443-1000

- Urgent Mental Health Needs: Call the Wellness Exchange **24/7** hotline at (212) 443-9999 or call NYU Public Safety 24/7 at (212) 998-2222

- For more info:
https://www.nyu.edu/students/health-and-wellness/wellness-exchange/emergencies.html

NYU

Week 1

Course Conduct

Tests are open notes/open book but are to be taken individually.

If collaboration on assignments is permitted, this will be clearly stated in the assignment.

You can discuss concepts
...but **not code**

If you feel the need to cheat, cheat off me! Or better yet the TAs (office hours)

Academic dishonesty will be harshly punished!

Week 1

About this class

Philosophy: learn by doing hands-on (practical exercises).

Lectures will provide basic information.

Assignments will reinforce important concepts.

Strongly dislike cheaters!
Only thing about teaching worse than grading ☺

I will treat you like an adult.

NYU

Week 1

Important Resources

Read the entire syllabus published on NYU Classes!

Instructor: Mo Satt <moshe.satt@nyu.edu>

Office hours: Tuesdays after class 9:00 - 9:30 PM

NYU

Week 1

What will I learn?

1) A deeply ethical security mindset!

2) Some or all of the following:

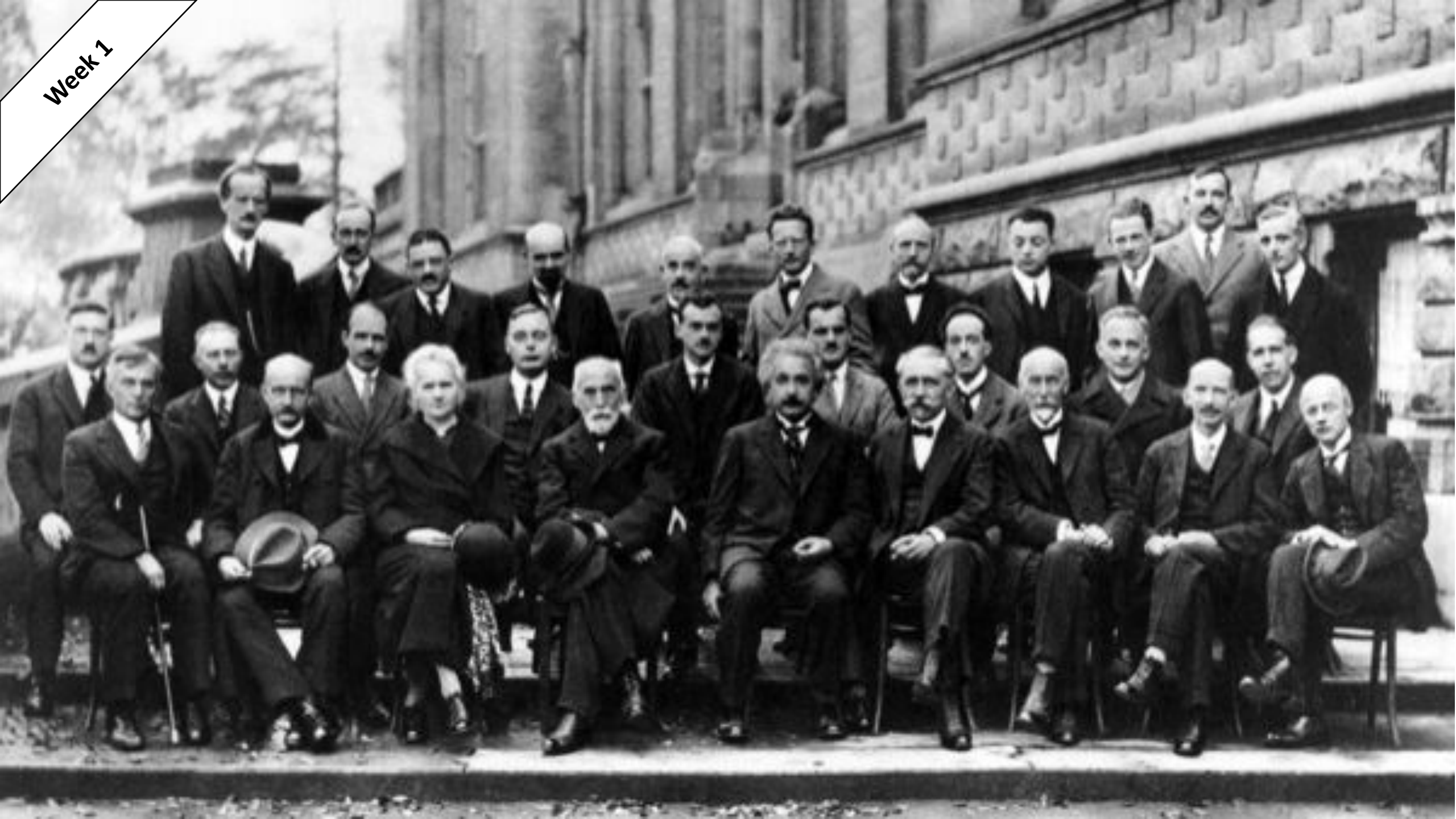
- Security primitives, design principles, Privacy on the web, Security policies, threat modeling, Information Flow Control, Object capability systems
- OS / mobile security models, SFI, OS / programming language virtualization security, PIR, Tor, PKI, Kerberos, trust revocation
- Protocol-based attacks, confused deputy problem, code / data confusion attacks, TOCTTOU flaws, side-channel attacks, buffer overruns, ASLR, return-oriented programming, memory protection

Week 1

Grading

Exam 1 : 20%
Exam 2 : 20%
Final Exam: 25%
Discussions: 5%
Online Labs: 15%
Programming Labs: 15%

Week 1



Week 1

Albert Einstein
Old Grove Rd.
Nassau Point
Peconic, Long Island

August 2nd, 1939

F.D. Roosevelt,
President of the United States,
White House
Washington, D.C.

Sir:

Some recent work by E.Fermi and L. Szilard, which has been communicated to me in manuscript, leads me to expect that the element uranium may be turned into a new and important source of energy in the immediate future. Certain aspects of the situation which has arisen seem to call for watchfulness and, if necessary, quick action on the part of the Administration. I believe therefore that it is my duty to bring to your attention the following facts and recommendations:

In the course of the last four months it has been made probable - through the work of Joliot in France as well as Fermi and Szilard in America - that it may become possible to set up a nuclear chain reaction in a large mass of uranium,by which vast amounts of power and large quantities of new radium-like elements would be generated. Now it appears almost certain that this could be achieved in the immediate future.

This new phenomenon would also lead to the construction of bombs, and it is conceivable - though much less certain - that extremely powerful bombs of a new type may thus be constructed. A single bomb of this type, carried by boat and exploded in a port, might very well destroy the whole port together with some of the surrounding territory. However, such bombs might very well prove to be too heavy for transportation by air.

The United States has only very poor ores of uranium in moderate quantities. There is some good ore in Canada and the former Czechoslovakia, while the most important source of uranium is Belgian Congo.

In view of this situation you may think it desirable to have some permanent contact maintained between the Administration and the group of physicists working on chain reactions in America. One possible way of achieving this might be for you to entrust with this task a person who has your confidence and who could perhaps serve in an inofficial capacity. His task might comprise the following:

a) to approach Government Departments, keep them informed of the further development, and put forward recommendations for Government action, giving particular attention to the problem of securing a supply of uranium ore for the United States;

b) to speed up the experimental work,which is at present being carried on within the limits of the budgets of University laboratories, by providing funds, if such funds be required, through his contacts with private persons who are willing to make contributions for this cause, and perhaps also by obtaining the co-operation of industrial laboratories which have the necessary equipment.

I understand that Germany has actually stopped the sale of uranium from the Czechoslovakian mines which she has taken over. That she should have taken such early action might perhaps be understood on the ground that the son of the German Under-Secretary of State, von Weizsäcker, is attached to the Kaiser-Wilhelm-Institut in Berlin where some of the American work on uranium is now being repeated.

Yours very truly,

A. Einstein

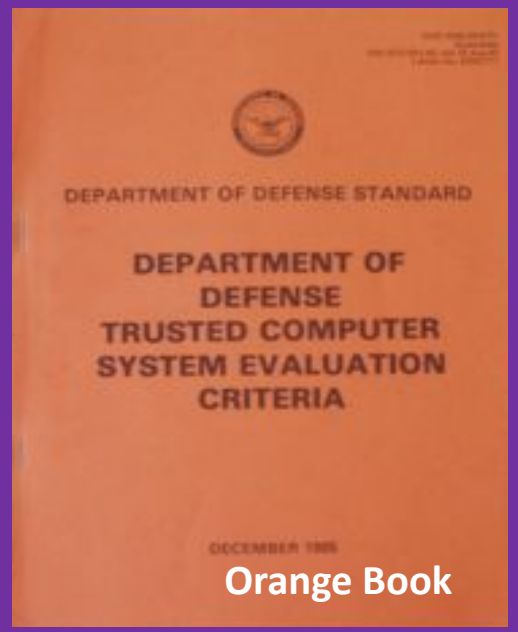
(Albert Einstein)


Week 1

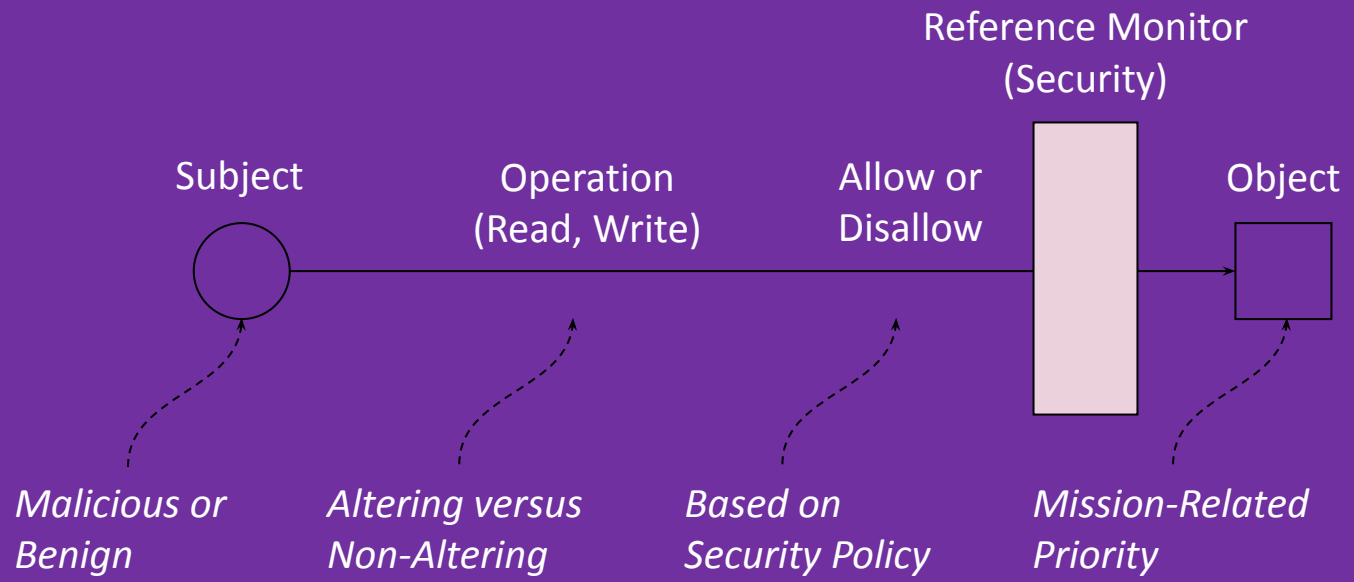
Week 1

Cyber Security: Subject-Object Reference Model

James Anderson



Orange Book



Week 1

Cyber Security: Basic Operational Framework

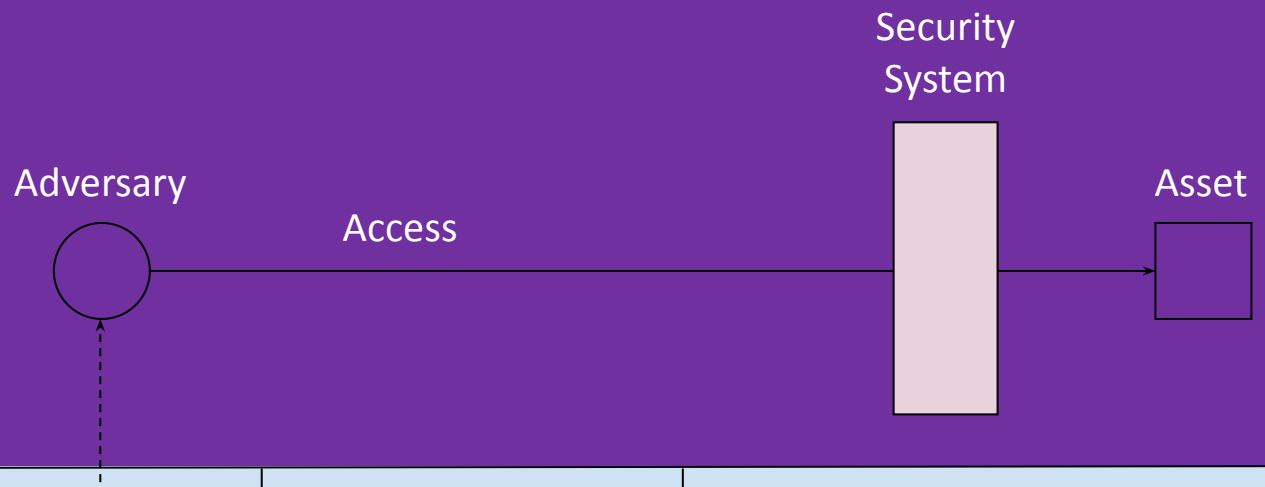
Adversary trying to access an asset, and have a security system in between

Attacker goes around firewalls, making them obsolete for defense. Insider threats (malicious/non-malicious).

Look at security holistically

Week 1

Cyber Security: Adversary Types



Adversary Type	*Motivation*	*Defining Attributes*
Hacker	Mischief	Individually Capable, Predictable
Hacktivist	Anger	Group Capable, Unpredictable
Criminal	Greed	Well Funded, Financial Motivation
Nation-State	Dominance	World Class Capability and Support

Week 1

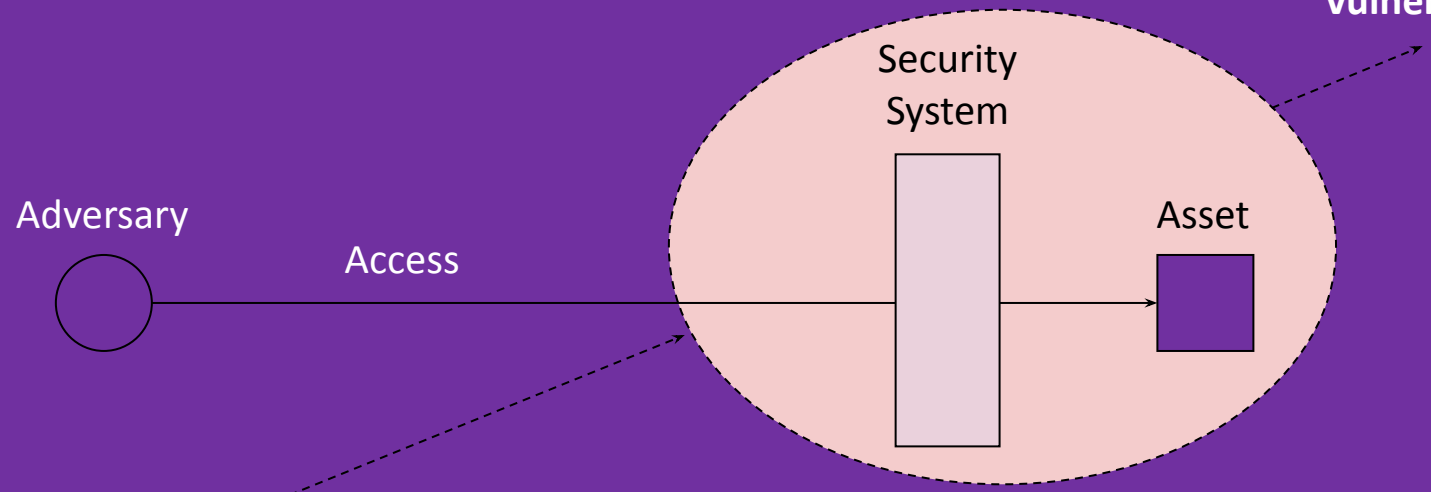
Cyber Security: Vulnerability Types

Vulnerability Type	*Root Cause*	*Defining Attributes*
System Flaw	Complexity	Insufficient design, test, build, operate
Lack of Security	Budget	Attention not paid to proper protection
Human Actions	Ignorance	Lack of security awareness and training
Organizational	Irresponsibility	Inadequate staff, procedures, and process

Week 1

Cyber Security: Threat Types

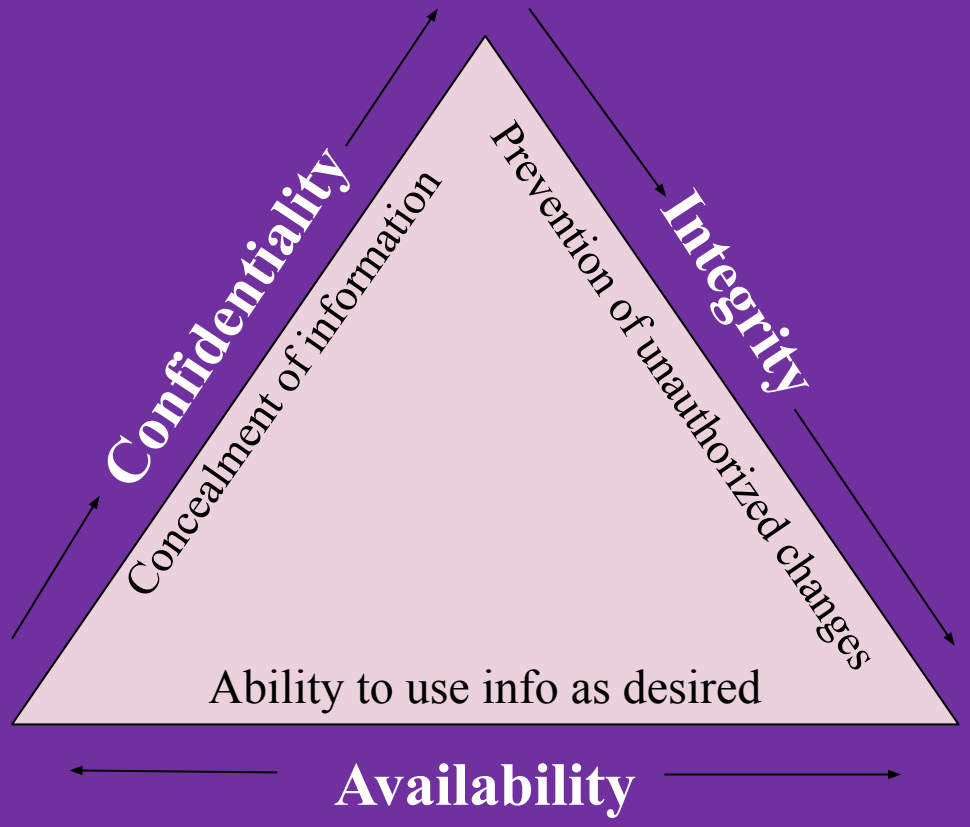
Need both **threat** and **vulnerabilities** to be a risk



Threat Type	*Motivation*	*Defining Attributes*
Disclosure	Secrets	Personal and Business Information
Integrity	Degradation	Remote Operational Control/Change
Denial of Service	Disruption	Distributed Botnet Attacks Common
Theft/Fraud	Money/Goods	Ingenious and Clever Means for Theft

Week 1

Primary Issues



Confidentiality: prevention of unauthorized disclosure of information

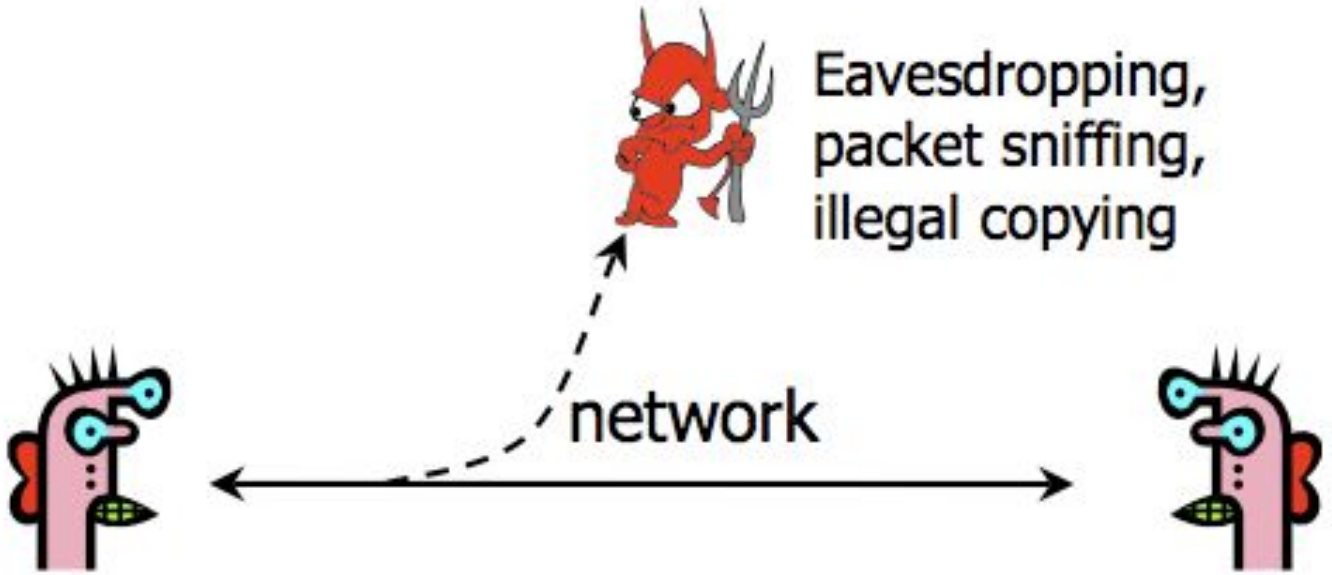
Integrity: prevention of unauthorized modification of information

Availability: ability to withstand unauthorized withholding of information or resources

NYU

Confidentiality (Privacy)

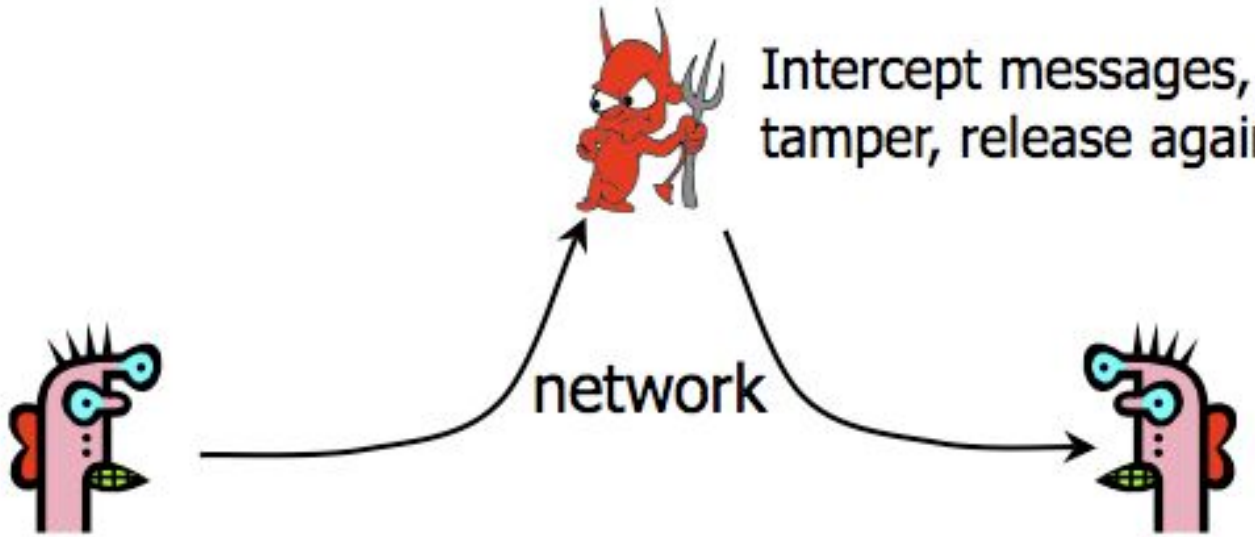
- Confidentiality is concealment of information



Week 1

Integrity

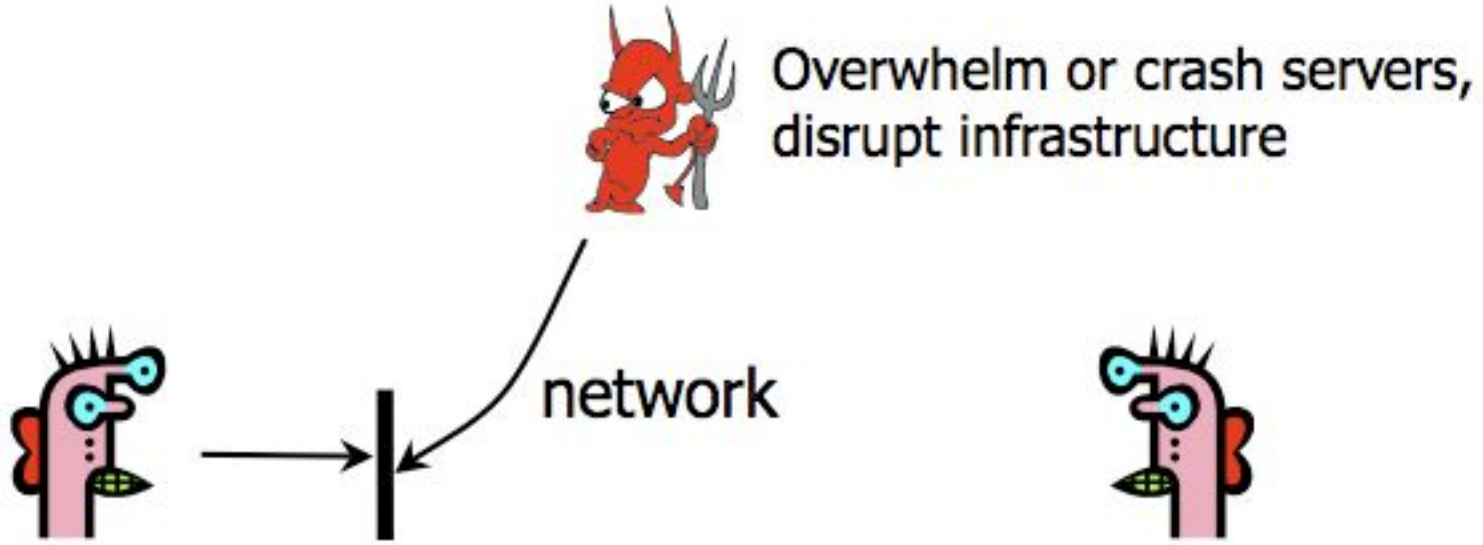
- Integrity is prevention of unauthorized changes



NYU

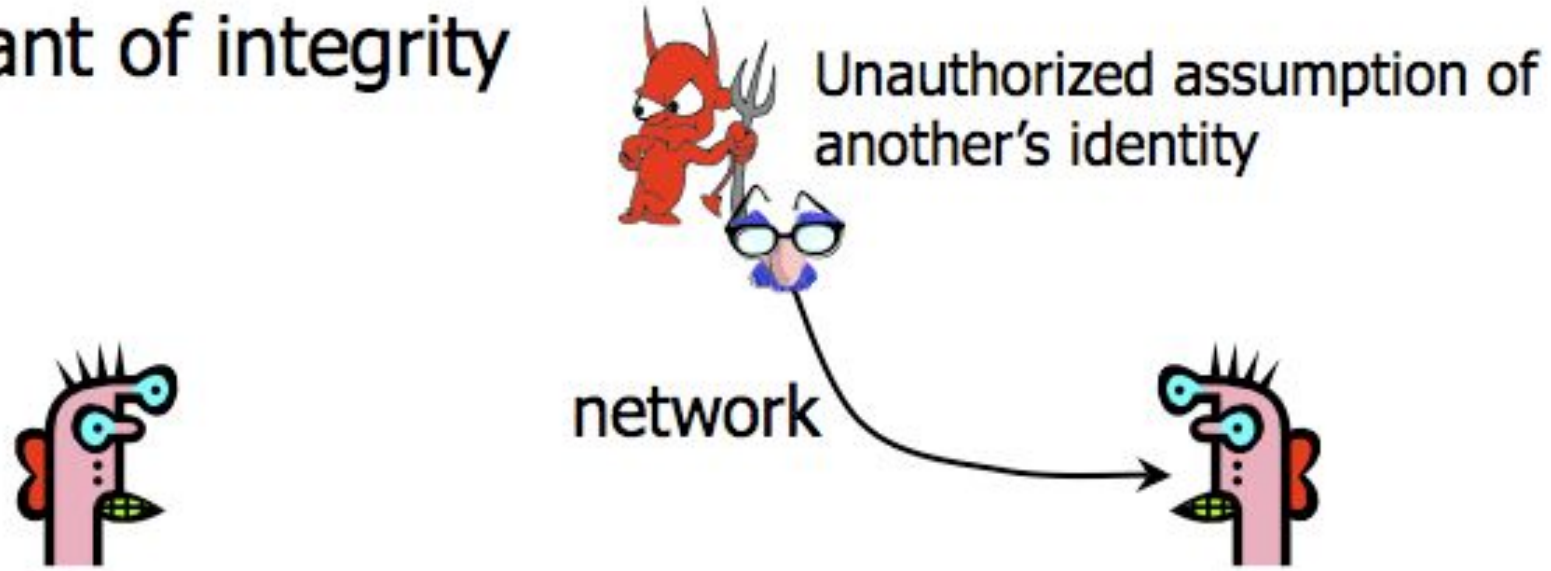
Availability

- Availability is ability to use information or resources desired



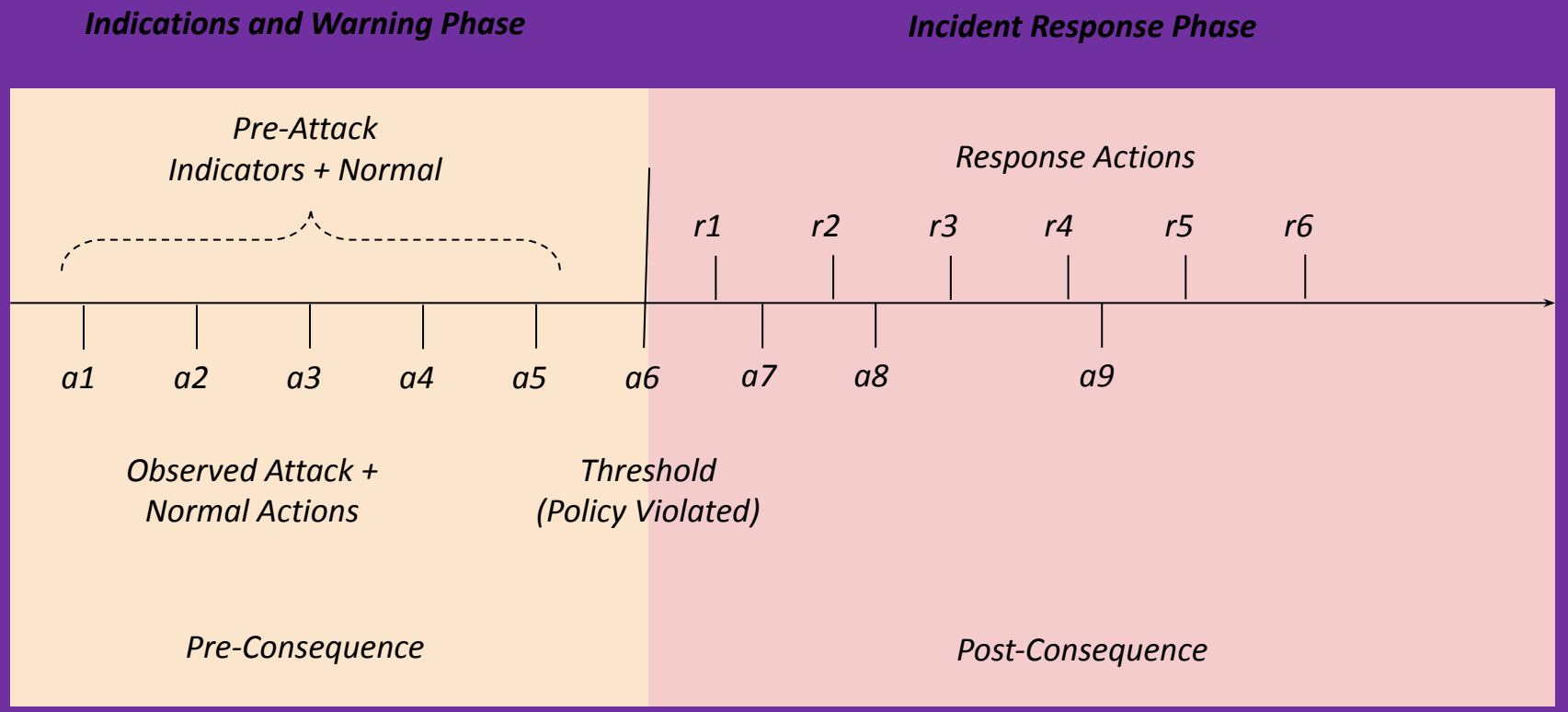
Authenticity

- Authenticity is identification and assurance of origin of information
- Variant of integrity



Week 1

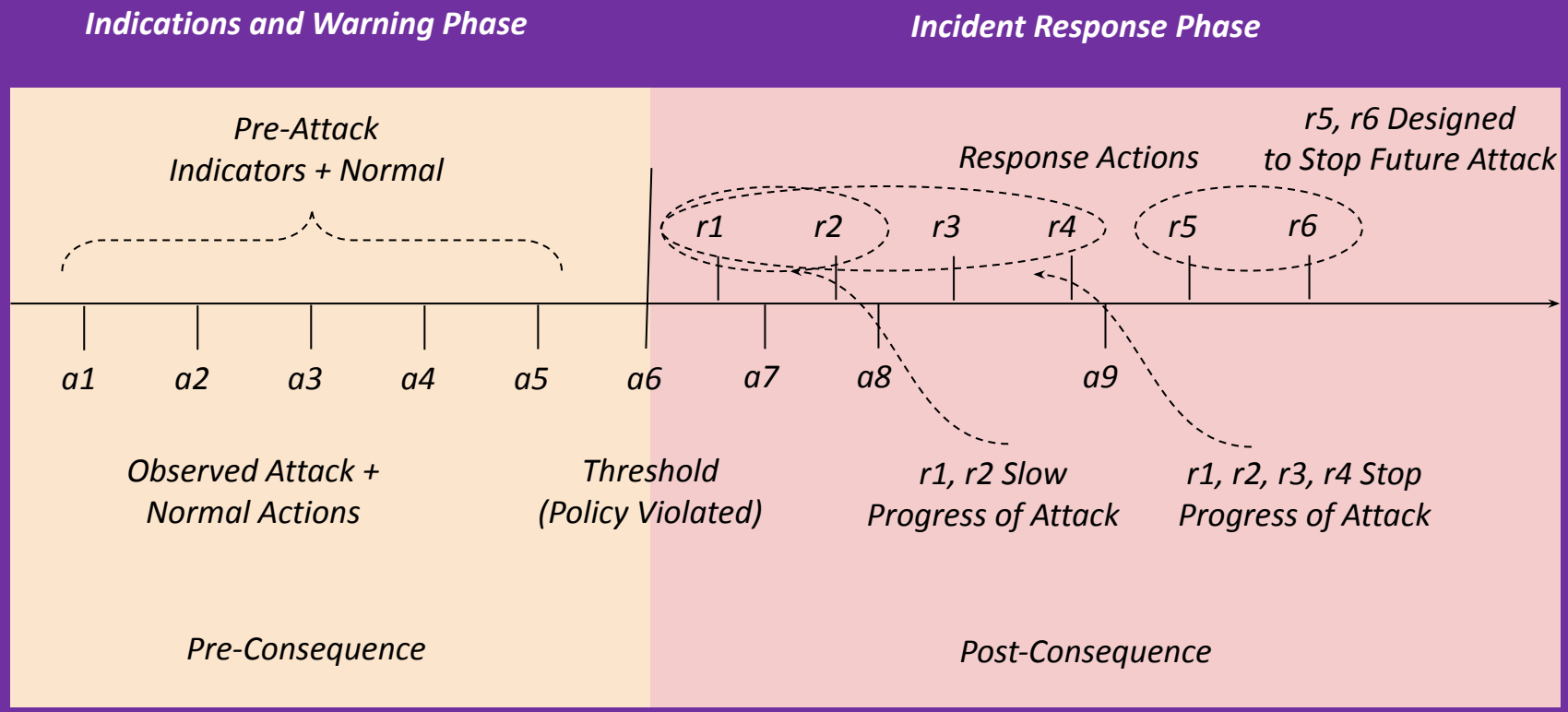
Cyber Security: Attack Lifecycle (Defense View)



- Can have pre-attack indicators, but difficult on defensive side to know when policies are actually violated
- There is a asymmetric nature of cybersecurity with millions of possible attacks

Week 1

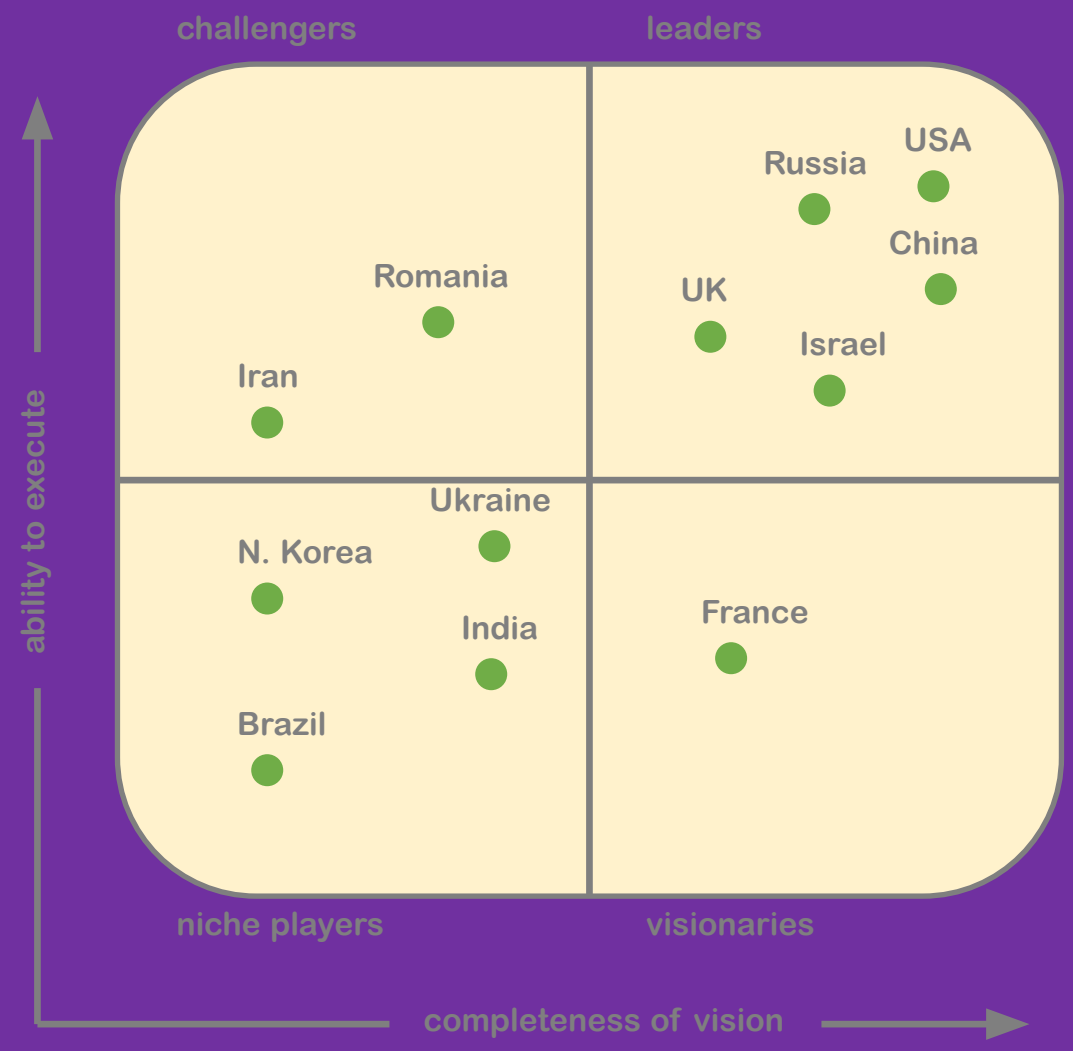
Cyber Security: Attack Lifecycle (Defense View)



- A policy has to be violated for an event to become an incident
- We want to slow down an attack and eventually try and stop it

Week 1

Advanced Persistent Threat (APT) Global Actors



1. USA, Russia, China, Israel, and the UK have ~ 100% success rates on offensive APT cyber operations
   - ➢ If attacks can't be stopped, it's more important to manage risk if it can't be prevented

2. North Korea derives ~100% of its APT cyber operations capability via training and support from China

3. Romania, Iran, and Ukraine have large populations of technically trained, underemployed youth

Week 1

NYU

Break

Week 1

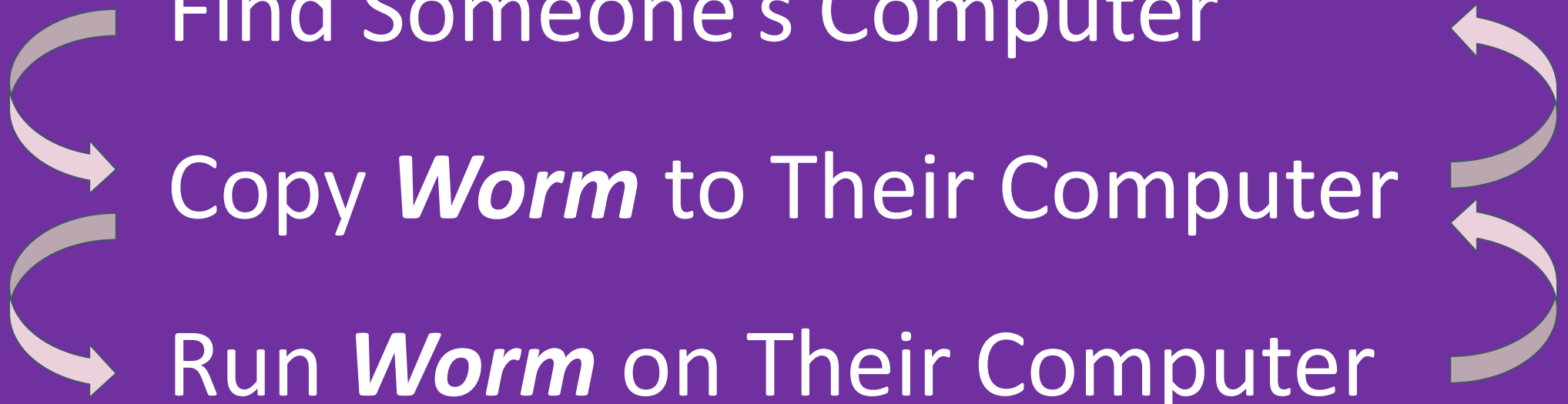
Understanding the Hack: 70's Vintage Vendor Soda Machine

Just because an attack is very simple does not mean it is easy to defend against!

Week 1

Week 1

Worm


Find Someone's Computer
Copy *Worm* to Their Computer
Run *Worm* on Their Computer

Week 1

Can scan IP addresses and copy the worm

Host

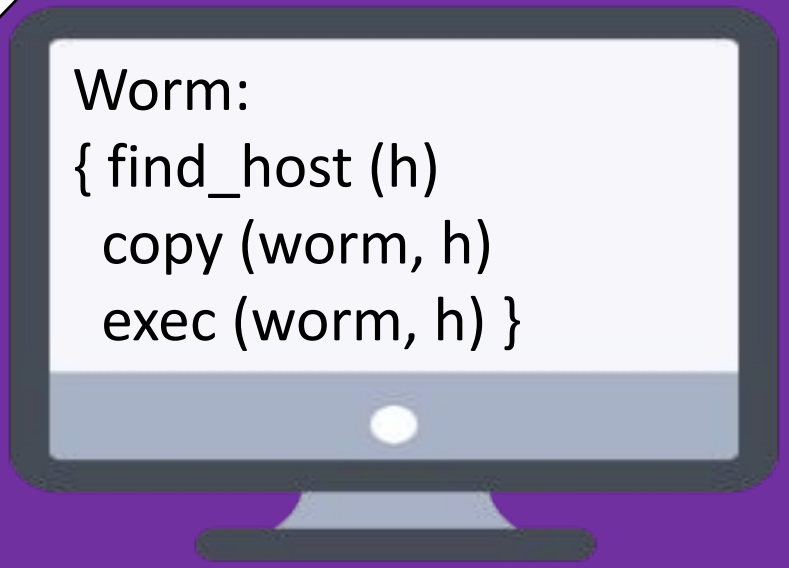
Takes in arguments of worm and h

Run copy function calling itself on h

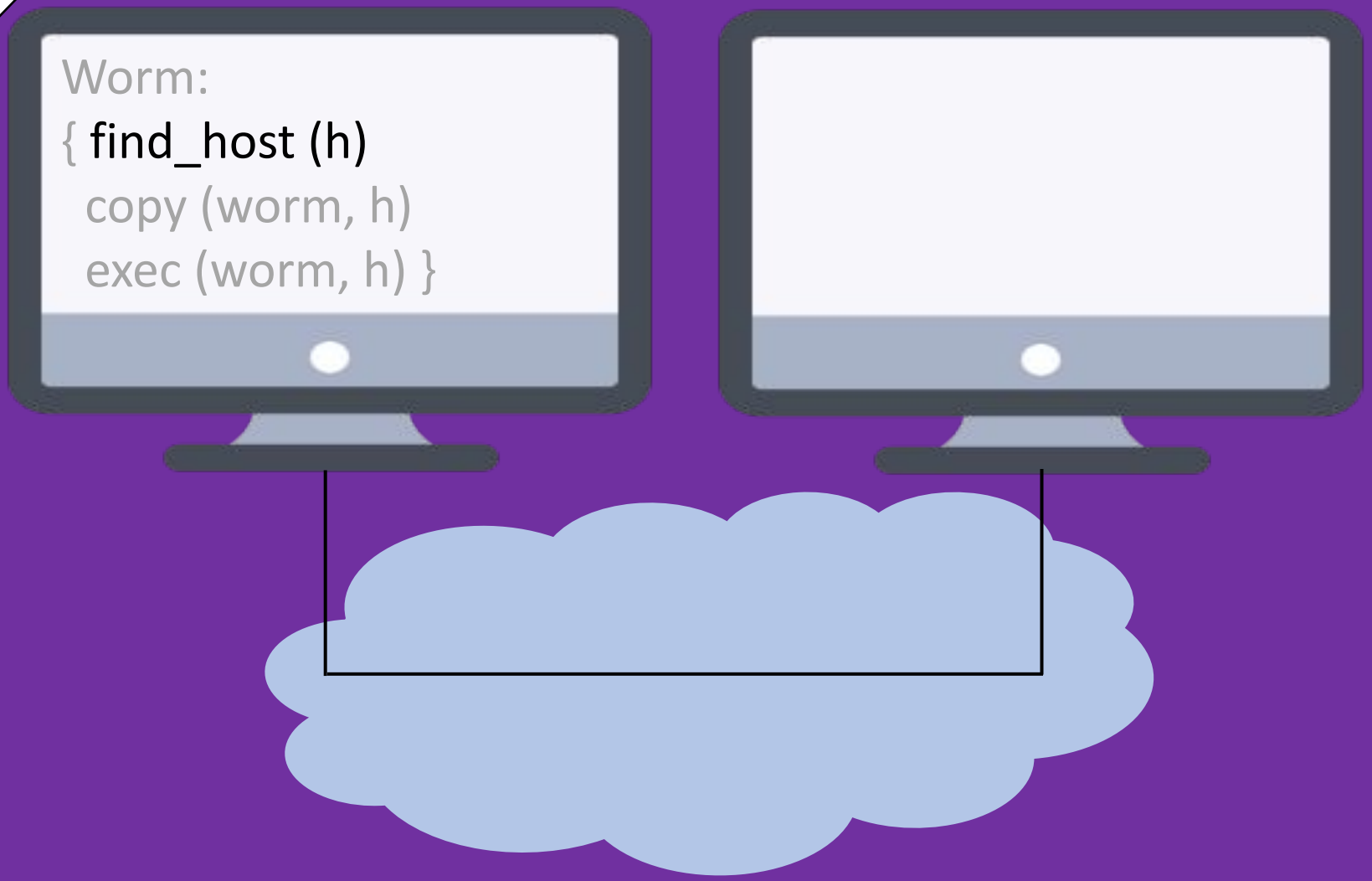
```
Worm:
{ find_host (h)
  copy (worm, h)
  exec (worm, h) }
```

Self propagating

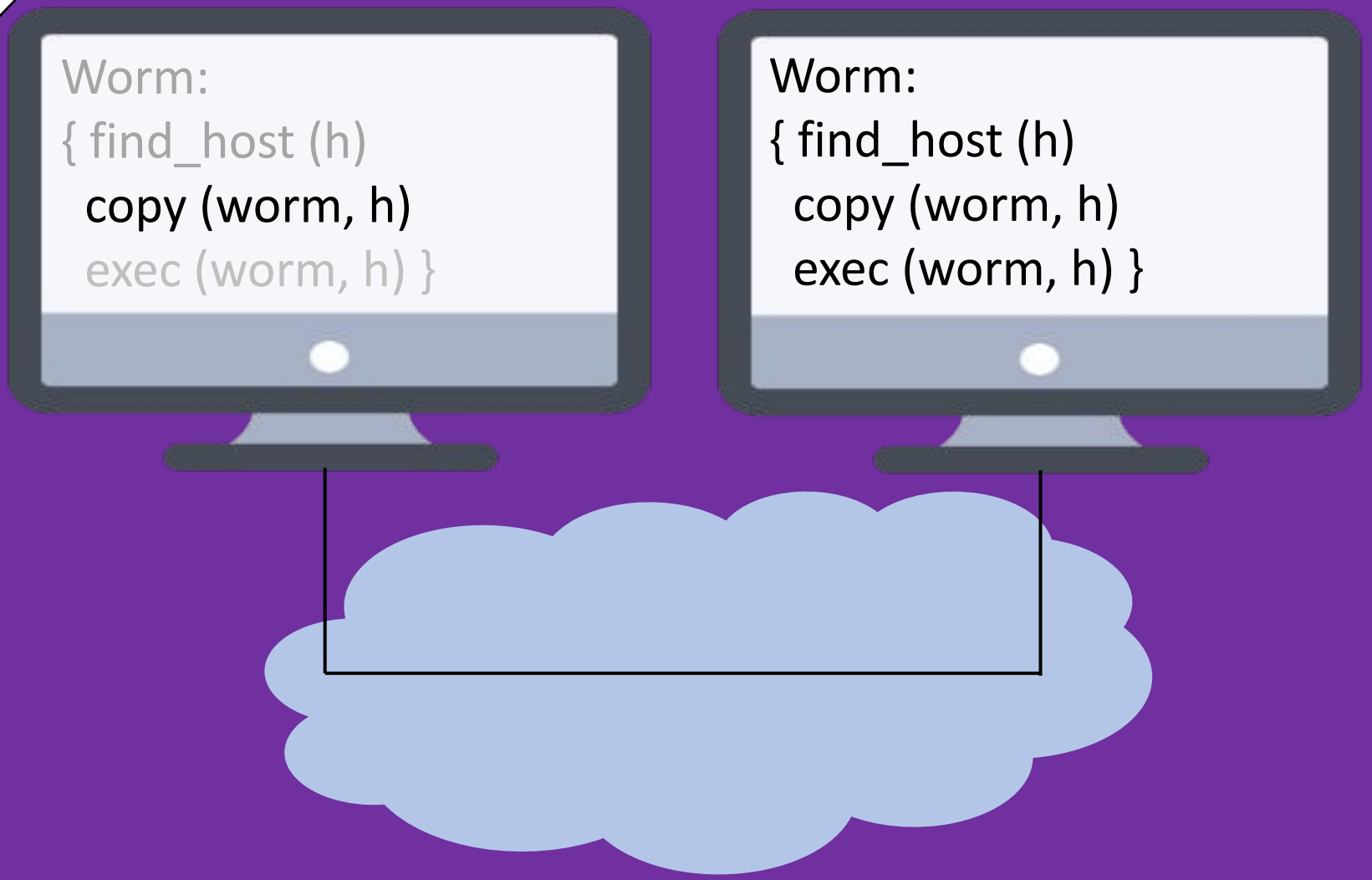
Week 1



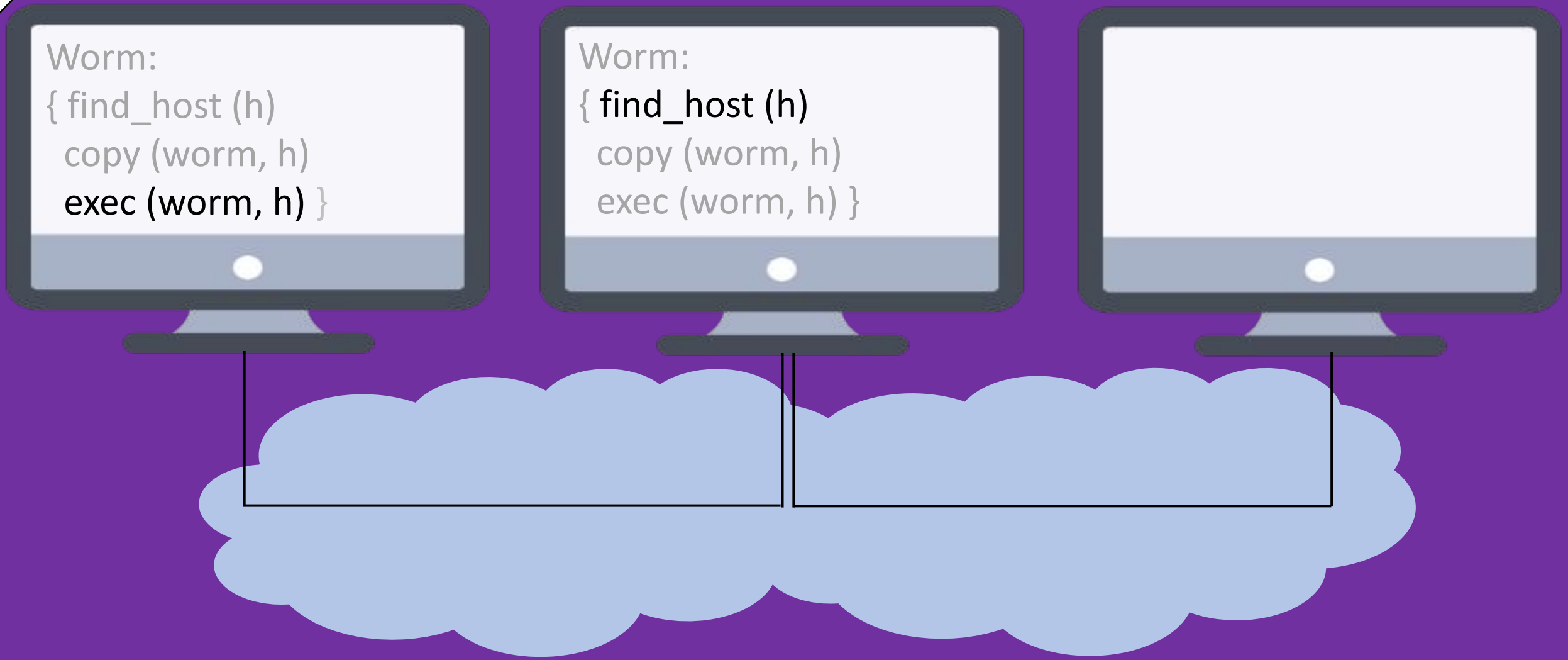
Week 1



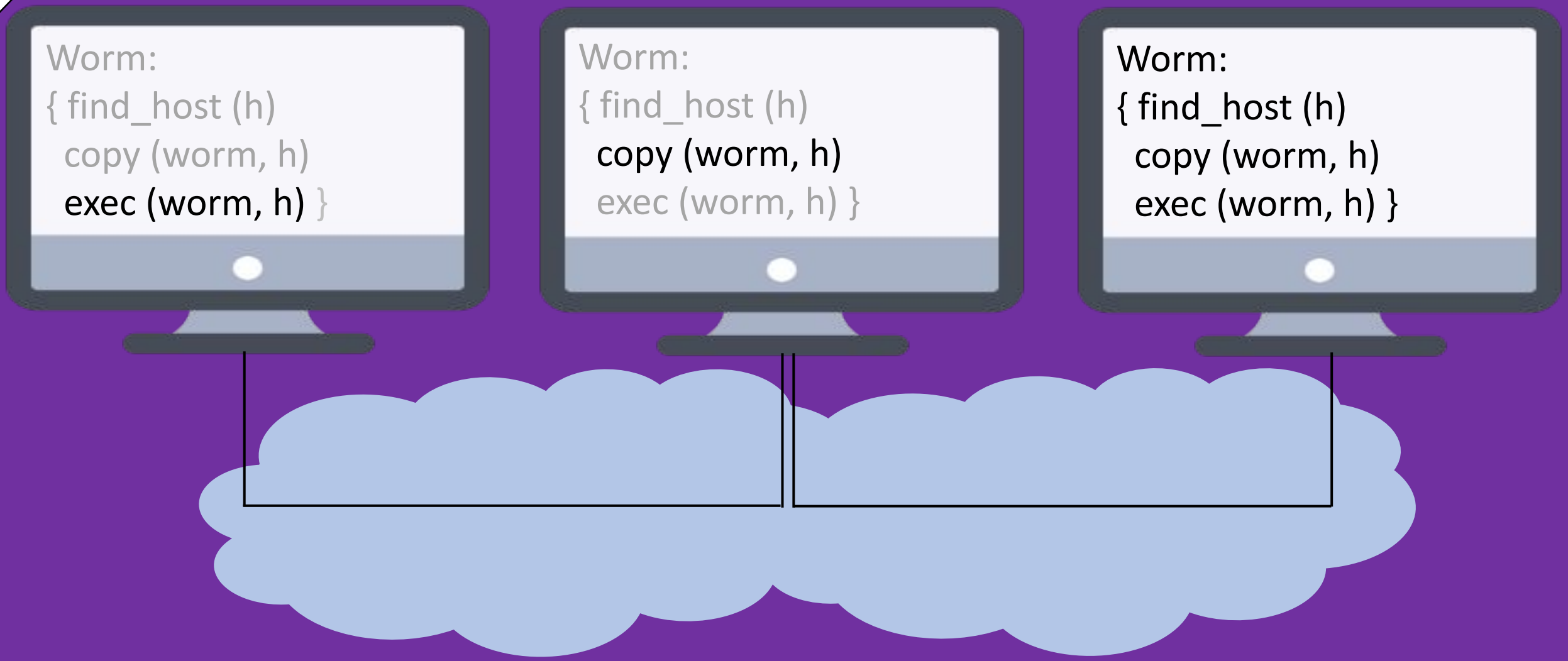
Week 1


Worm:
{ find_host (h)
copy (worm, h)
exec (worm, h) }
Worm:
{ find_host (h)
copy (worm, h)
exec (worm, h) }

Week 1


Worm:
{ find_host (h)
copy (worm, h)
exec (worm, h) }
Worm:
{ find_host (h)
copy (worm, h)
exec (worm, h) }

Week 1


Worm:
{ find_host (h)
copy (worm, h)
exec (worm, h) }
Worm:
{ find_host (h)
copy (worm, h)
exec (worm, h) }
Worm:
{ find_host (h)
copy (worm, h)
exec (worm, h) }

Week 1

The Morris Internet Worm source code

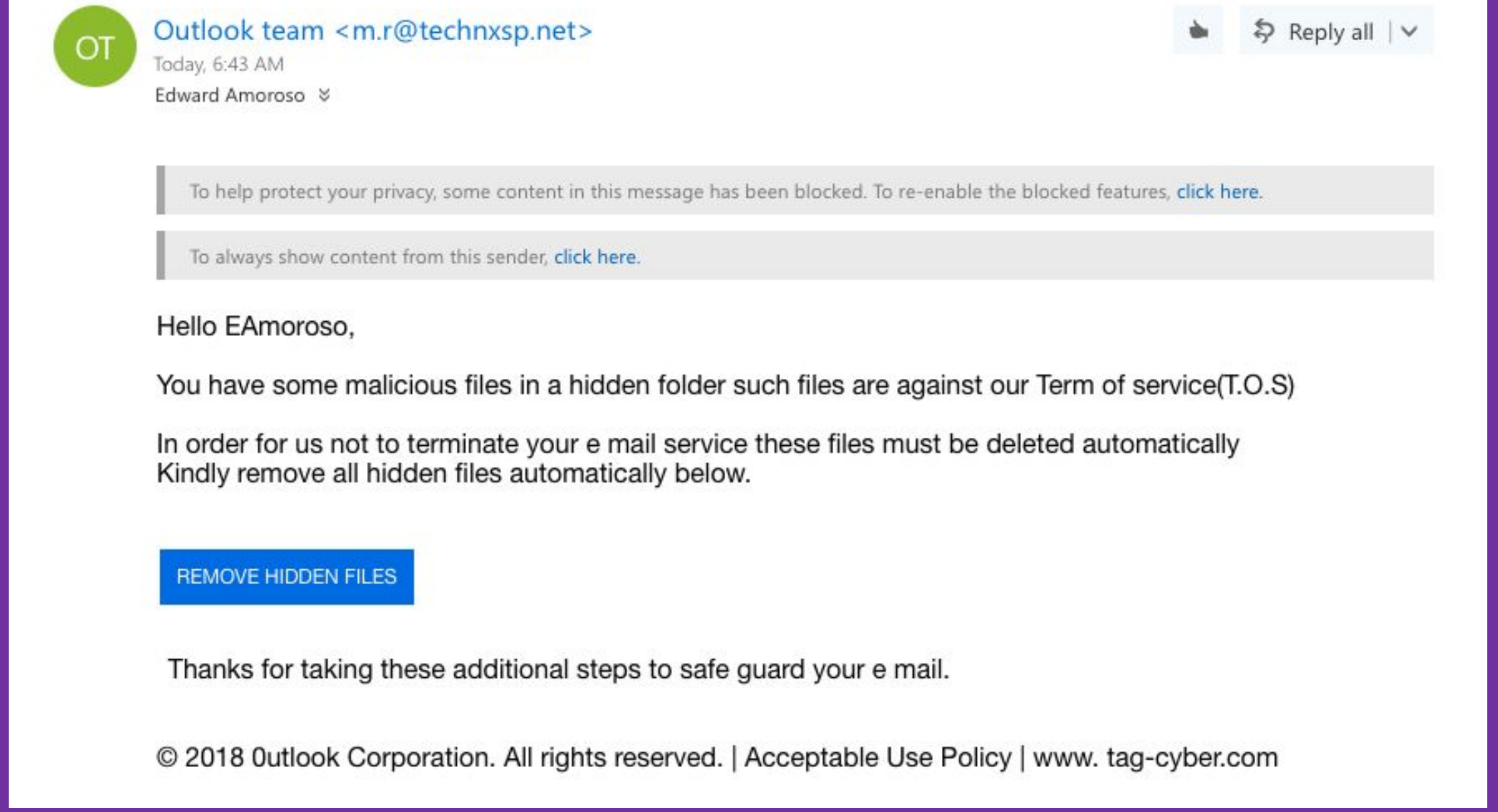
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

The worm was the first of many intrusive programs that use the Internet to spread.

Computer History Museum

Week 1

Most Common Hacking Method



OT

Outlook team <m.r@technxsp.net>

Today, 6:43 AM

Edward Amoroso

Reply all

To help protect your privacy, some content in this message has been blocked. To re-enable the blocked features, click here.

To always show content from this sender, click here.

Hello EAmoroso,

You have some malicious files in a hidden folder such files are against our Term of service(T.O.S)

In order for us not to terminate your e mail service these files must be deleted automatically
Kindly remove all hidden files automatically below.

REMOVE HIDDEN FILES

Thanks for taking these additional steps to safe guard your e mail.

© 2018 0utlook Corporation. All rights reserved. | Acceptable Use Policy | www. tag-cyber.com

Week 1

Computer Security Definitions

Security is the ability of a system to protect information and system resources with respect to *confidentiality, integrity*, and *availability*.

Computer Security deals with the prevention and detection of unauthorized actions by users of a computer system.

Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.

Week 1

Computer Security – other issues

There are other issues that arise in the design of secure systems besides confidentiality, availability and integrity:

- Accountability
- Reliability
- Access Control
- Authentication
- Non-repudiation
- Privacy

NYU

Week 1

Threats, Vulnerabilities and Attacks

A ***threat*** to a system is any potential occurrence, malicious or otherwise, that can have an adverse effect on the assets and resources associated with the system.

A ***vulnerability*** of a system is some characteristic that makes it possible for a threat to occur.

An ***attack*** on a system is some action that involves exploitation of some vulnerability in order to cause an existing threat to occur.

NYU

Week 1

Types of Threats

Can be classified into four broad categories:

Disclosure - unauthorized access to information
Deception - acceptance of false data
Disruption - interruption or prevention of correct operation
Usurpation - unauthorized control of some part of a system

Examples include – snooping, sniffing, spoofing, delay, denial of service, theft of computational resources…

NYU

Week 1

Reading Next Week

Read: Aligning Security and Usability
https://ieeexplore-ieee-org.proxy.library.nyu.edu/document/1341409

Watch DEFCON talk on physical security systems:
http://www.youtube.com/watch?v=vxNymzyEWPQ&feature=related

No-Tech hacking:
http://www.youtube.com/watch?v=5CWrzVJYLWw

Watch a few BlackHat / DefCon videos on YouTube

Purpose: Start to think about security like an attacker

Ethics: https://www.secureworks.com/blog/ethics
http://www.yo\0utube.com/watch?v=Qhfsg_ZBVRY

NYU