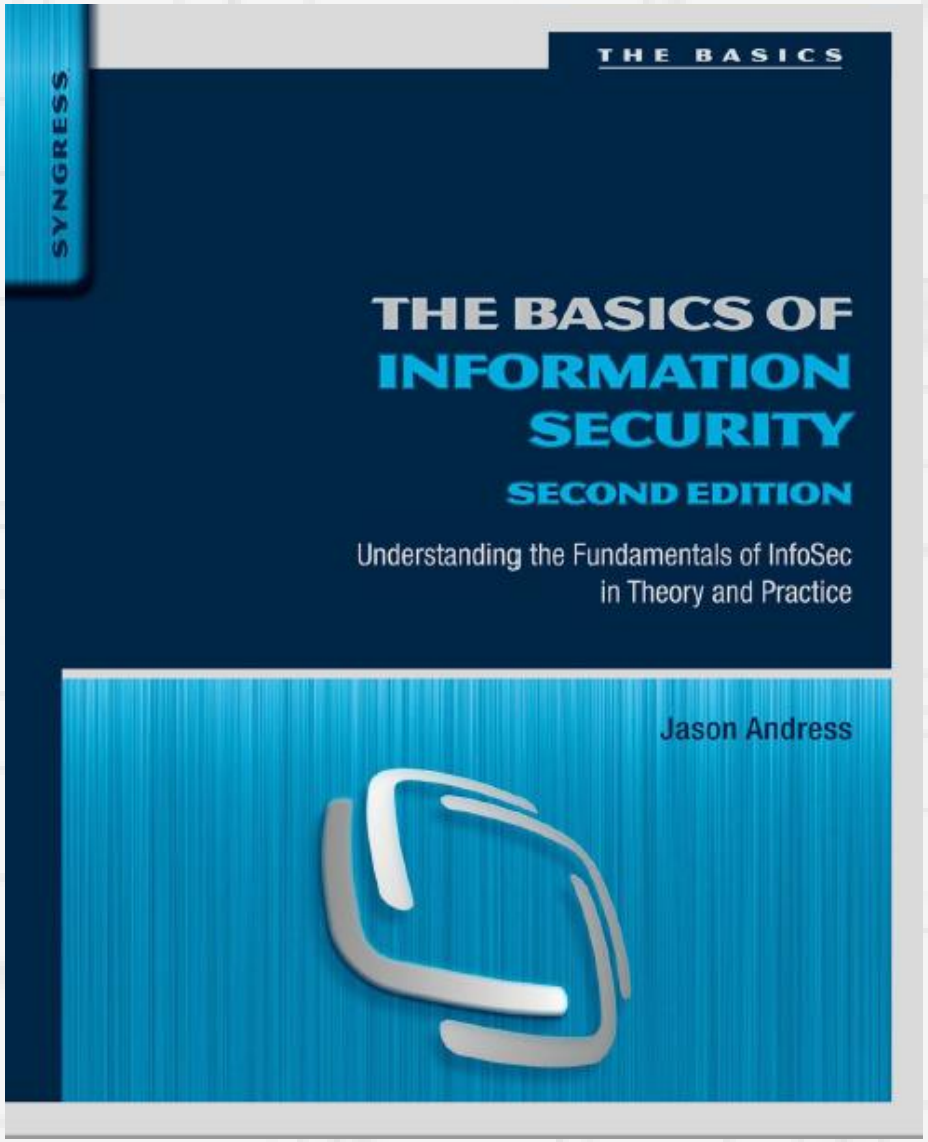
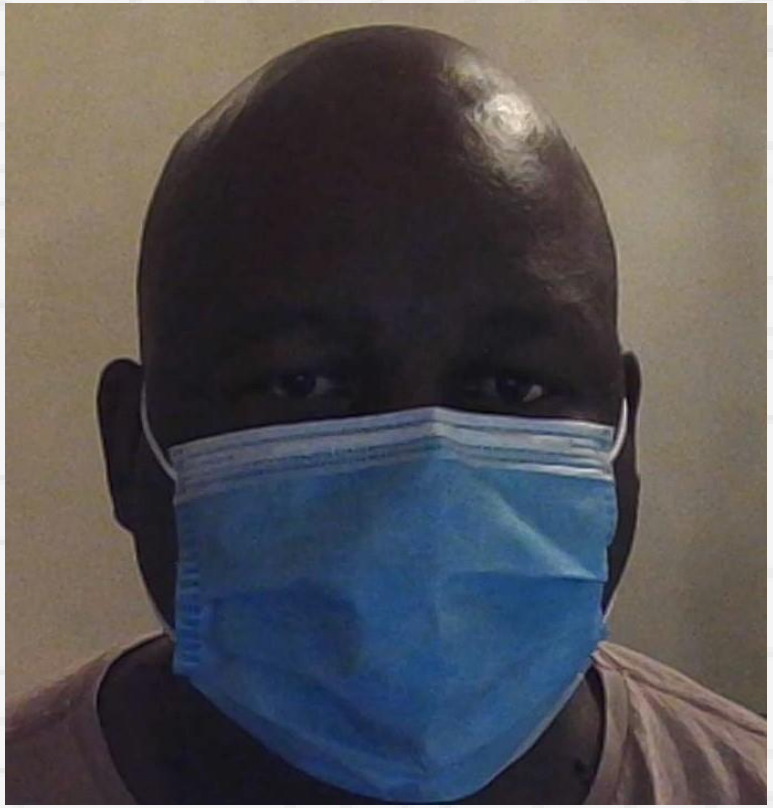


STAY SAFE

WASH HANDS WITH SOAP & WATER
SANITIZE
SOCIAL DISTANCE



CSI454 Information Security Administration

Tallman Nkgau

Administrivia, Overview, Why Information Security Administration

- ❑ Administrivia
- ❑ Overview
- ❑ What is information security?

Administrivia

❑Lectures

- Thur, Fri 1500 - 1600 252-008

❑Lab/Tutorial

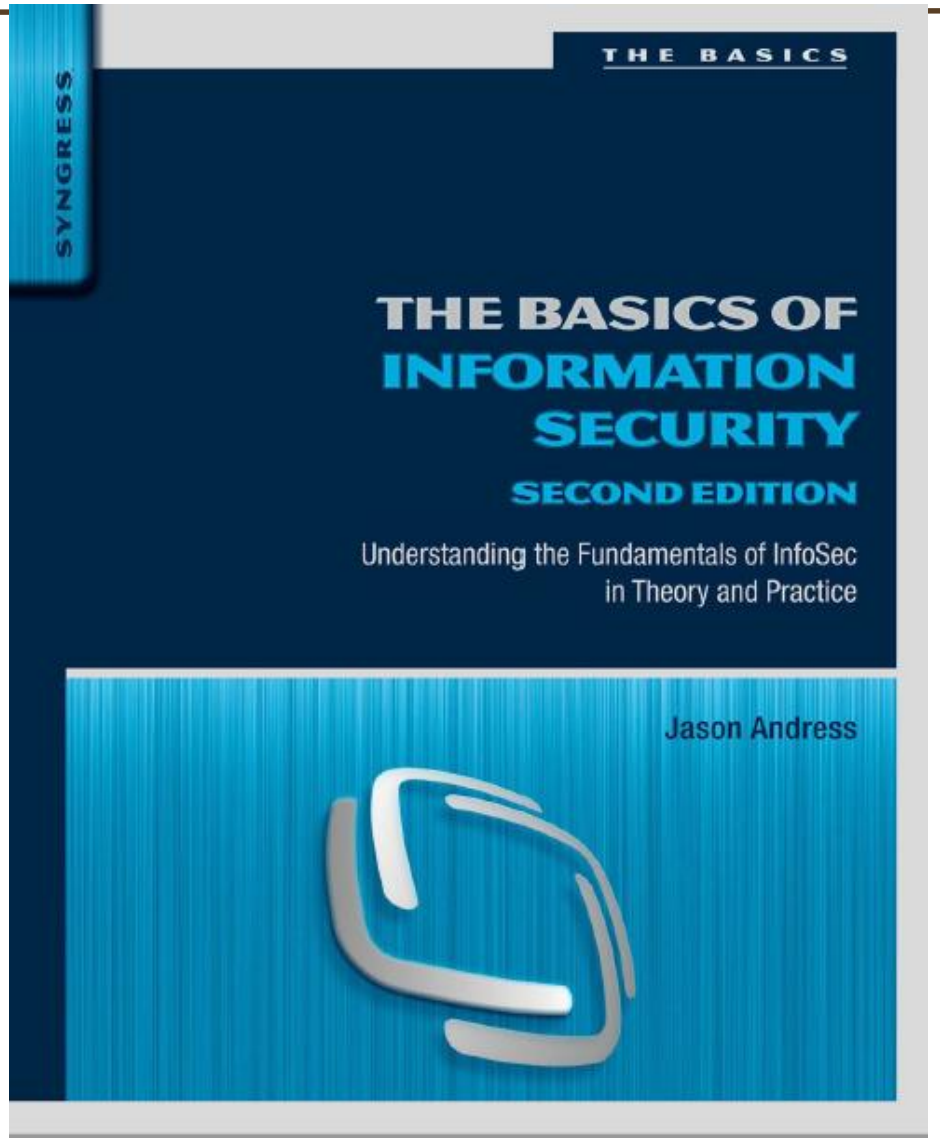
- Tues 0900 - 1100 232 – 112/119/120
- Thur 0900 – 1100 232 – 112/119/120

❑Office Hours

- Communication via your UB email
- Office visits by appointment through email

❑Prerequisite

- CSI374 (>= 50%)



Jason Andress

Grading & Assessments

• 2-Hrs Final Exam	50%
• 2-Hr Midterm Test	10%
• Quizzes	16%
• Assignments	12%
• Labs	12%

- Assignments and Labs may and will probably include Java/python coding.

Labs & Assignments

❑ Assignments:

- Will be in groups of 3-4 students
- Will be submitted on Moodle – ensure your CS Moodle account is operational
- Only 1 member of the group need to submit

❑ Labs:

- Will be in groups of 3-4 students
- Will be submitted on CS Moodle seven days later at 5pm.
- Only 1 member of the group need to submit

In the news…https://www.justice.gov/usao-ndal/pr/irs-employee-sentenced-nine-years-and-two-months-prison-leading-1-million-id-theft-tax

THE UNITED STATES ATTORNEY'S OFFICE
NORTHERN DISTRICT of ALABAMA

HOME ABOUT NEWS MEET THE U.S. ATTORNEY DIVISIONS PROGRAM

U.S. Attorneys » Northern District of Alabama » News

Department of Justice

U.S. Attorney's Office

Northern District of Alabama

SHARE

FOR IMMEDIATE RELEASE Wednesday, August 10, 2016

IRS Employee Sentenced to Nine Years and Two Months in Prison for Leading $1 Million ID Theft Tax Fraud Scheme

BIRMINGHAM – A federal judge today sentenced an IRS employee to nine years and two months in prison for using her access to taxpayer information to lead a complex, multi-year, $1 million stolen identity refund scheme involving hundreds of victims, announced U.S. Attorney Joyce White Vance, IRS Criminal Investigation, St. Louis Field Office, Special Agent in Charge Karl A. Stiften, and Treasury Inspector General for Tax Administration, Mid-States Field Division, Special Agent in Charge Ruben Florez.

NAKEISHA HALL, 40, pleaded guilty in February to theft of government funds, aggravated identity theft, unauthorized access to a protected computer and conspiracy to commit bank fraud and mail fraud

- Employee (insider!)
- Personally Identifiable Information (PII)
- Fraud

In the news…https://www.msspalert.com/cybersecurity-news/solarwinds-orion-vulnerability-investigation/

by Joe Panettieri • Dec 14, 2020

Russian hackers allegedly weaponized SolarWinds Orion business software updates in order to distribute malware called SUNBURST. From there, the Russian hackers allegedly attacked multiple government, consulting, technology, telecom, and oil and gas companies in North America, Europe, Asia and the Middle East, FireEye said in a blog post and The Washington Post further reported.

- Outsider
- Hacking – sophisticated!
- Fraud? Political?

Why?

❑ Use of ICTs is everywhere

- Government
- Businesses (services provision or production)
- Personal (learning, playing, working, communicating)

❑ Benefits of ICTs

- Communication
- Cost effectiveness
- Service availability
- Bridging the cultural gap
- etc

And its use is growing…

https://www.internetworldstats.com/stats1.htm

Internet Users Statistics for Africa

(Africa Internet Usage, 2020 Population Stats and Facebook Subscribers)

AFRICA 2020 POPULATION AND INTERNET USERS STATISTICS						
AFRICA	Population (2020 Est.)	Internet Users 31-Dec-2000	Internet Users 30-SEPT-20	Penetration (% Population)	Internet Growth % 2000 - 2020	Facebook subscribers 30-SEPT-2020
Algeria	43,851,044	50,000	25,428,159	58.0 %	50,756 %	24,730,000
Angola	32,866,272	30,000	8,980,670	27.3 %	29,835 %	2,244,000
Benin	12,123,200	15,000	3,801,758	31.4 %	25,245 %	920,000
Botswana	2,351,627	15,000	1,116,079	47.5 %	7,340 %	830,000
Burkina Faso	20,903,273	10,000	4,594,265	22.0 %	45,842 %	840,000

In the news…

Forbes

11,929 views | Nov 19, 2018, 01:13pm

500,000 Duped Into Downloading Android Malware Posing As Driving Games On Google Play

Thomas Brewster Forbes Staff

Cybersecurity

I cover crime, privacy and security in digital and physical forms.

threatpost

TA505 Crime Gang Debuts Brand-New ServHelper Backdoor

Pre-Installed Android App Impacts Millions with Slew of Malicious Activity

Author:
Tara Seals

January 11, 2019
/ 4:58 pm

2 minute read

Write a comment

Share this article:

The app was developed by legitimate Chinese manufacturing giant TCL.

A pre-installed Android application on Alcatel smartphones has been found surreptitiously siphoning off geolocation data, email addresses and phone identification numbers and sending the data to a server in China.

Analysts with Upstream's Secure-D platform said that the app, Weather Forecast—World Weather Accurate Radar, asks for excessive permissions and sets about subscribing unwitting users to premium services for which the victims are billed via their cell carriers. Further, it also carries out ad fraud, visiting websites and clicking on ads – all in the background, unbeknownst to

Some stats…

- 95% of breached records came from only three industries in 2016 (Government, retail, and technology)
- There is a hacker attack every 39 seconds
- 43% of cyber attacks target small business
- The average cost of a data breach is $3.9 million
- Since COVID-19, the US FBI reported a 300% increase in reported cybercrimes
- 9.7 million health care records were compromised in September 2020
- Approximately $6 trillion is expected to be spent globally on cybersecurity by 2021
- Unfilled cybersecurity jobs worldwide is already over 4 million
- Connected IoT devices will reach 75 billion by 2025
- 95% of cybersecurity breaches are due to human error
- More than 77% of organizations do not have cyber security incidence response plan

Source: https://www.cybintsolutions.com/cyber-security-facts-stats/

Its real!

Key Terminology (Source: CNSSI 4009 *Committee on National Security Systems, 2015*)

Data

- Information in a specific representation, usually as a sequence of symbols that have meaning.

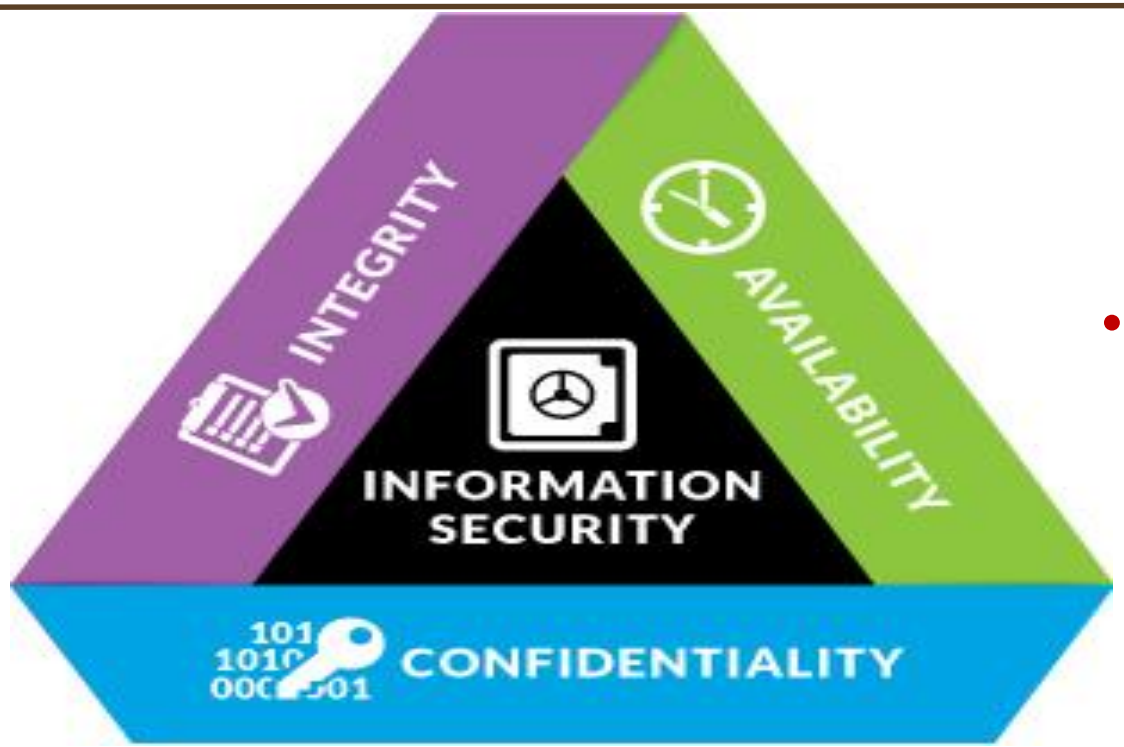
Information

- (1)Facts or ideas, which can be represented (encoded) as various forms of data; (2) Knowledge (e.g., data, instructions) in any medium or form that can be communicated between system entities
  - **is valuable, so can be monetized**
  - **can be measured**
  - **should be accurate, timely, and relevant**

Information security

- The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability

Classic Model – CIA Triad



- **Data/Information states**
  - At rest
  - In transit
  - In use

- **In organizations, this also involves**
  - Hardware, Software, communications
  - Products
  - People
  - Procedures, standards, policies

Key Terminology

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity

- Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity. availability
  - **Data Integrity**

    The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
  - **System Integrity**

    The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Key Terminology

Availability

- Ensuring timely and reliable access to and use of information.

Security controls

- The safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Asset

- Anything of value to an organization. In our context it could be data, information, information systems hardware/software, people, etc.

Threat

- Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Key Terminology

Risk

- A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
- Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems

Vulnerability

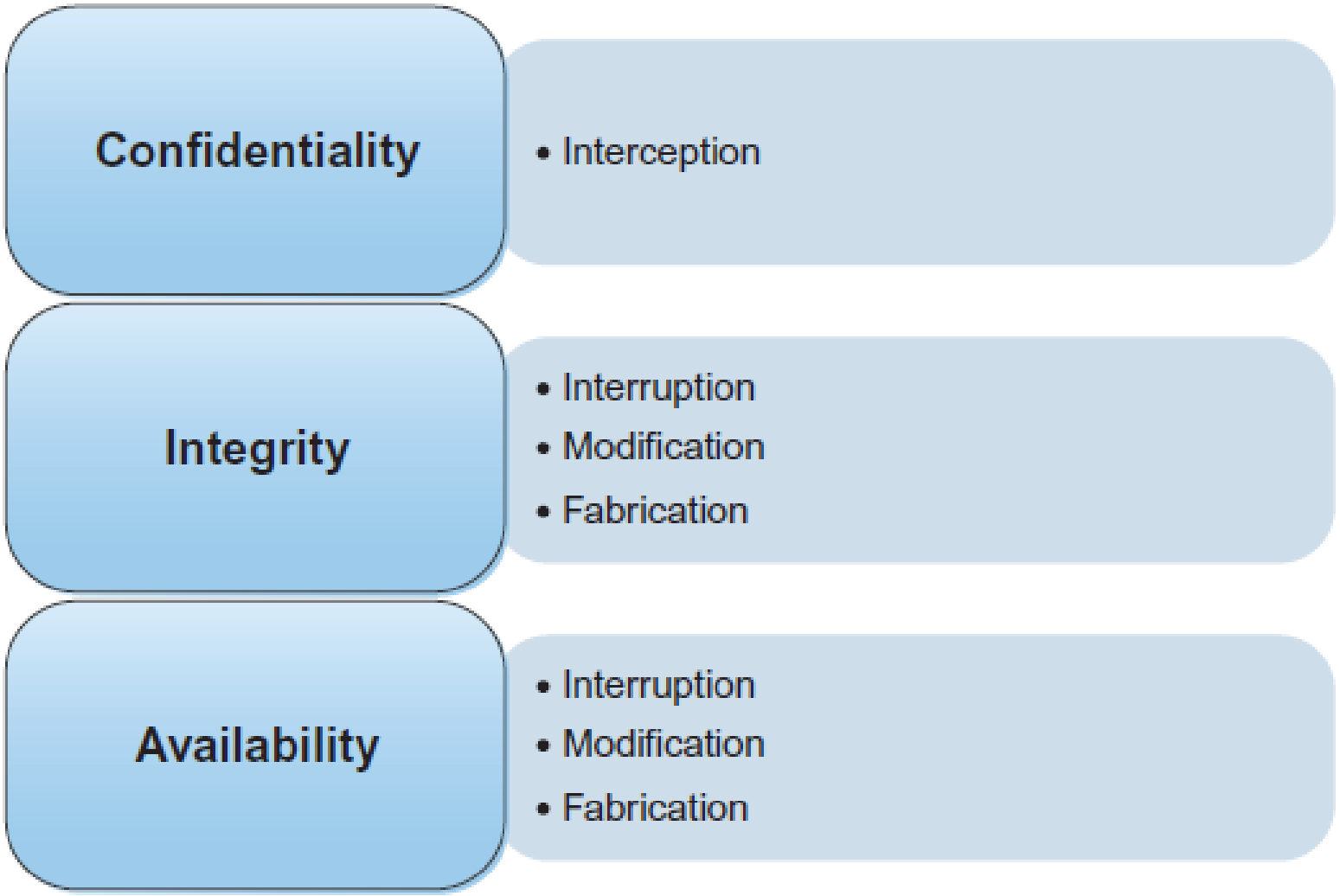
- Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Attacks

- Attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself – compromise information security.

Types of attacks

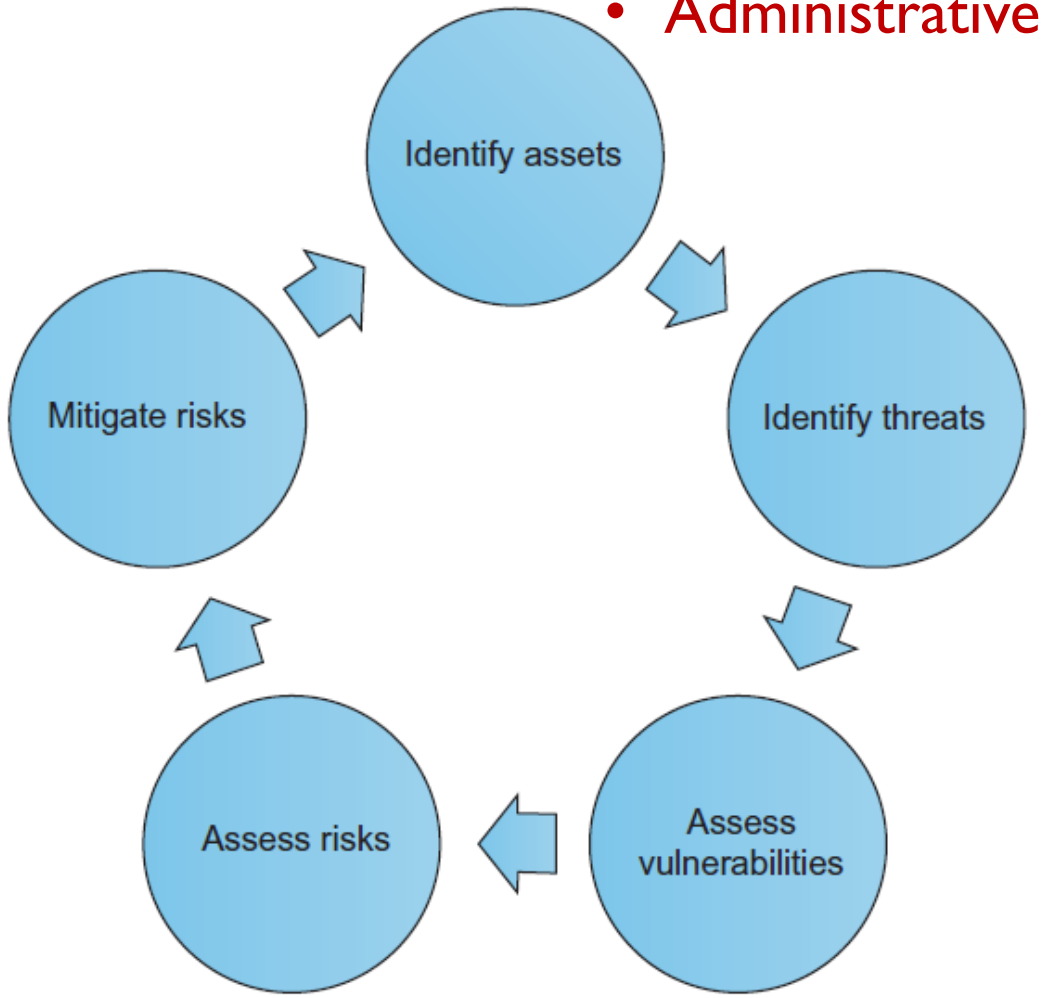
- Interception
- interruption
- modification
- fabrication



Risk

- A vulnerability must have a matching threat to constitute a risk.

- **Mitigating risks**
  - Physical controls
  - Logical/Technical controls
  - Administrative controls



A Threat

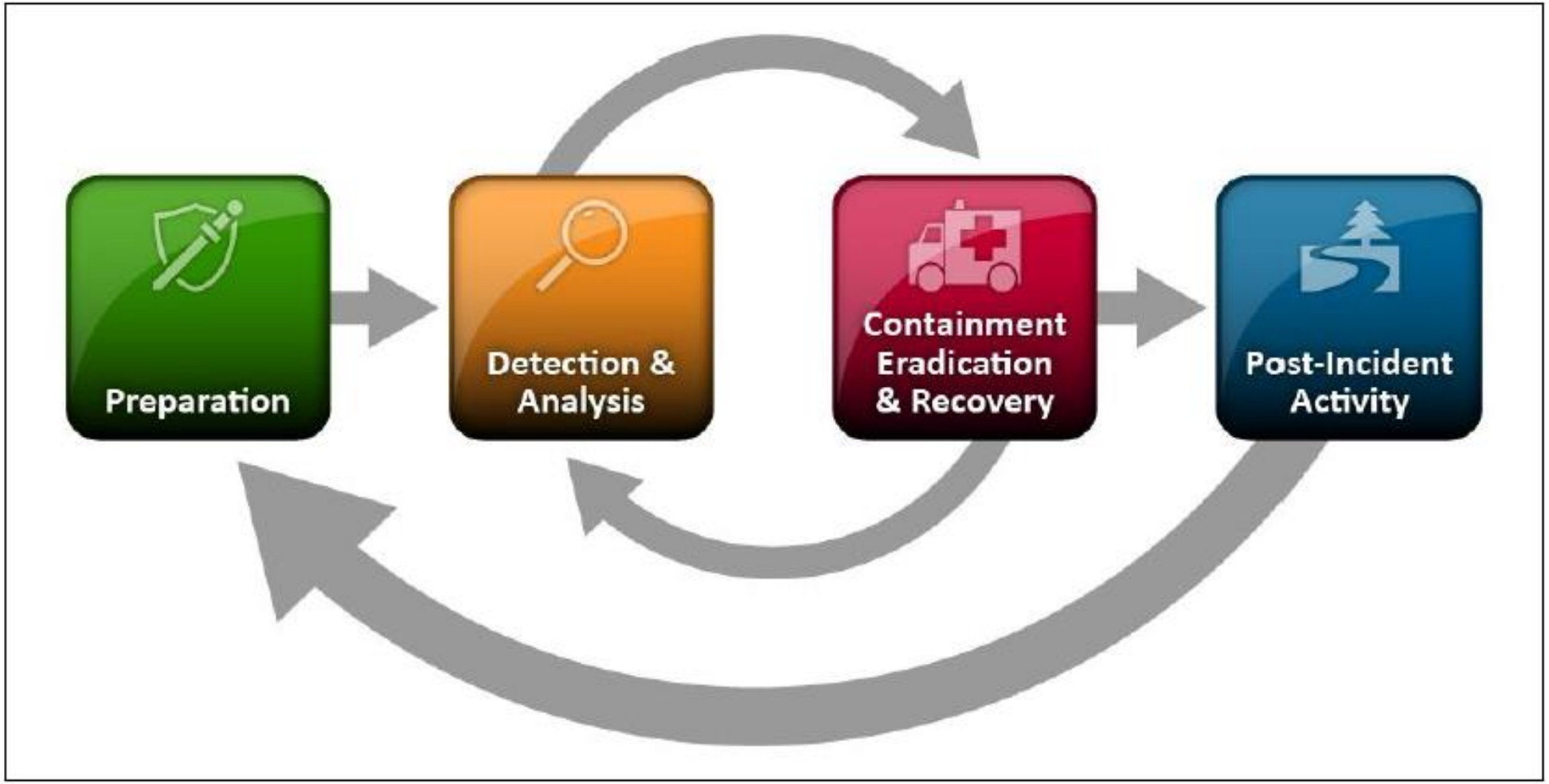
Availability—If the system or application goes down, we cannot process payments

A match vulnerability

We do not have redundancy for the database on the back-end of our payment processing system.

Incident response

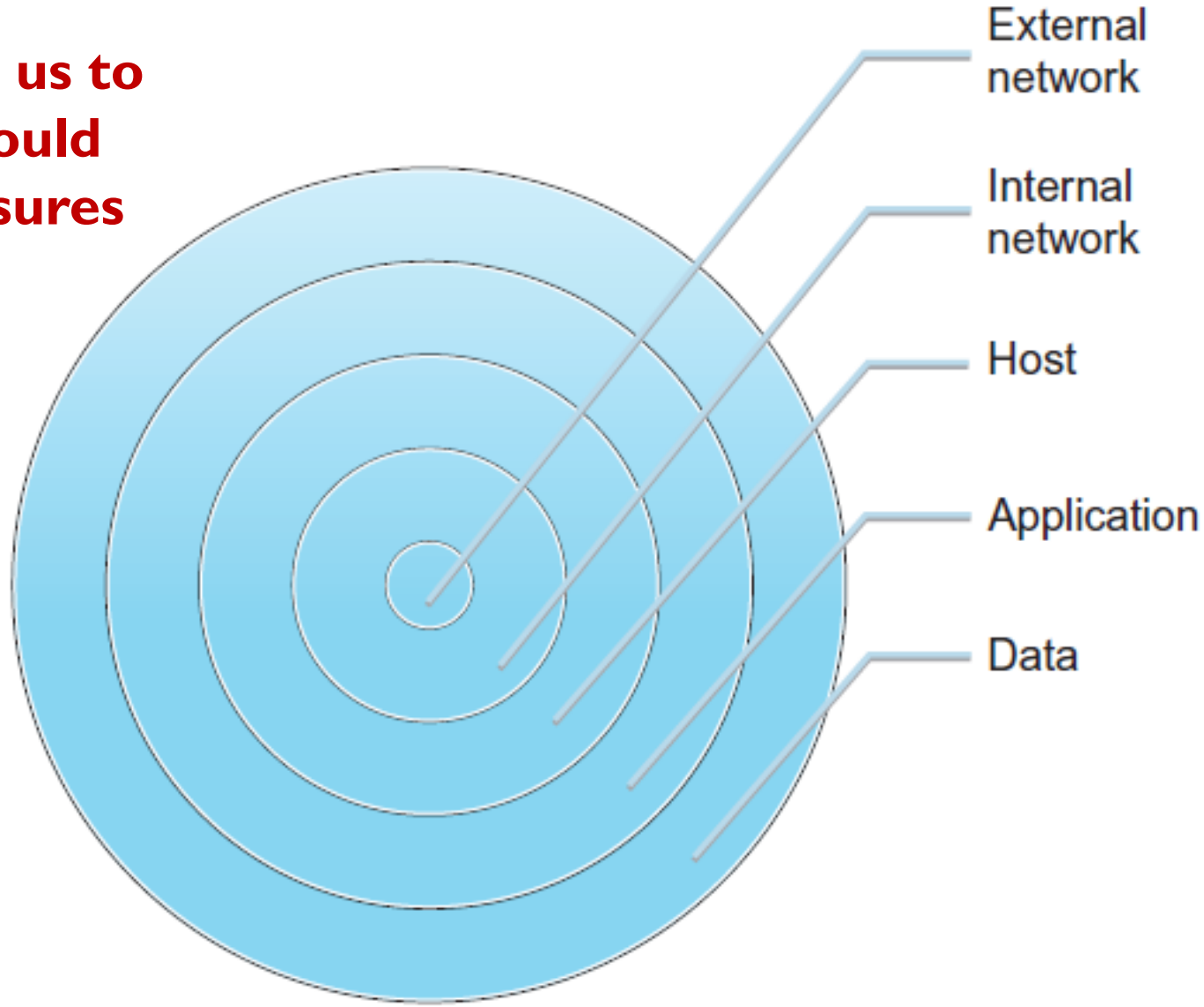
- A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.



Incident Response Life Cycle (source: NIST SP 800-61r2 chap/sec 3)

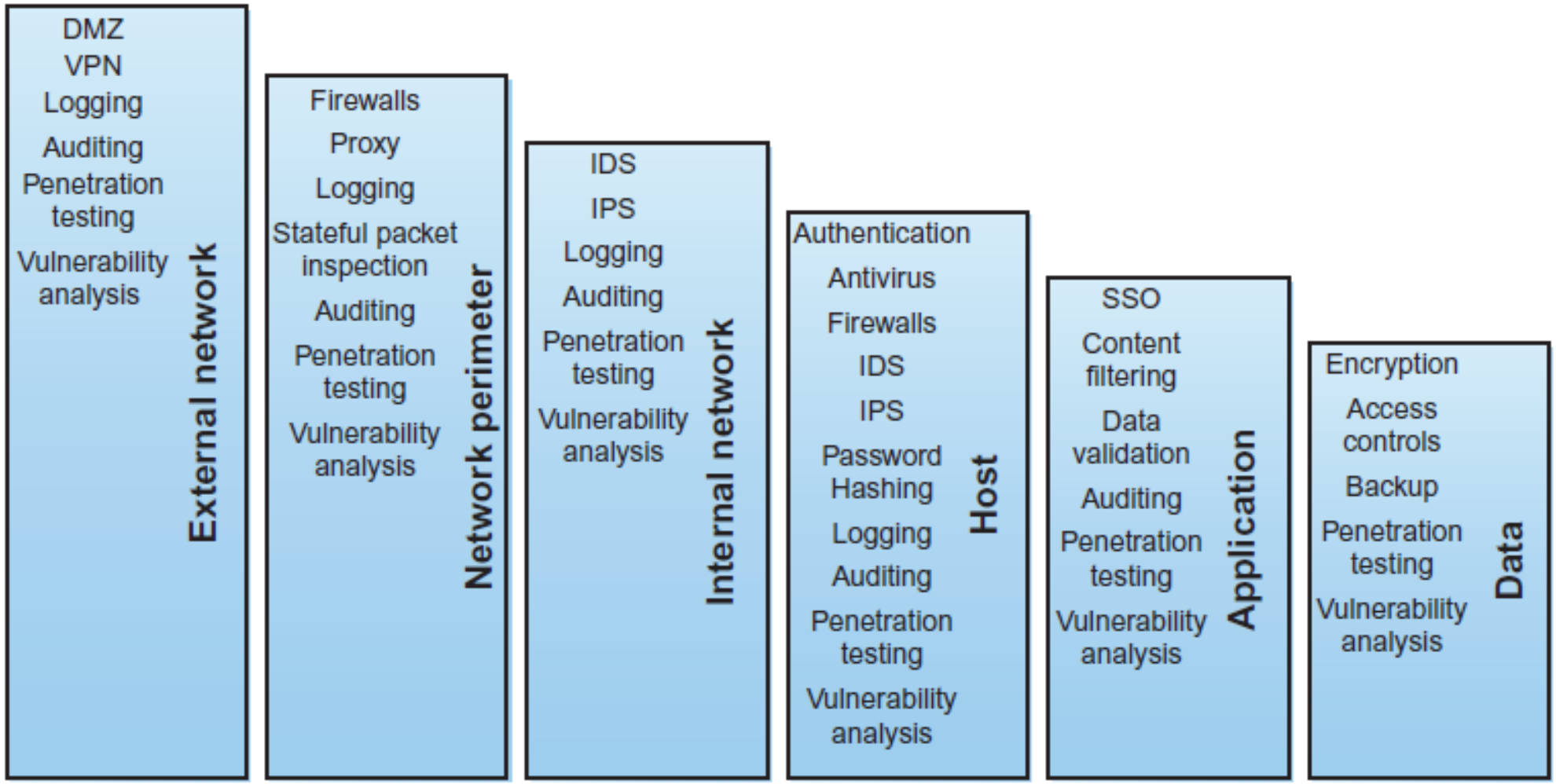
Defense in depth

A multilayered defense that allows us to still mount a successful defense should one or more of our defensive measures fail.



- **Multi-layered approach**
  - A security failure in one layer doesn't lead to a complete security collapse
  - Can facilitate early detection of an attack

Defense in depth



Core Body of Knowledge for Cybersecurity/InfoSec

ACM JTF – CSEC2017	
1	Data Security
2	Software Security
3	Component Security
4	Connection Security
5	System Security
6	Human Security
7	Organizational Security
8	Societal Security

CISSP Knowledge Domains (ISC)2	
1	Security and Risk Management
2	Asset Security
3	Security Engineering
4	Communications & Network Security
5	Identity and Access Management
6	Security Assessment & Testing
7	Security Operations
8	Software Development Security

Cybersecurity/Information Security Organizations

- (ISC)2 – International Information System Security Certification Consortium
- https://www.isc2.org/

"(ISC)² is an international, nonprofit membership association for information security leaders like you. We're committed to helping our members learn, grow and thrive. More than 150,000 certified members strong, we empower professionals who touch every aspect of information security."

Cybersecurity/Information Security Organizations

- The SANS Institute
- https://www.sans.org/

"SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center."

Cybersecurity/Information Security Organizations

- The Open Web Application Security Project (OWASP)
- https://owasp.org/

"The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. Our programming includes:

- Community-led open source software projects
- Over 200+ local chapters worldwide
- Tens of thousands of members
- Industry-leading educational and training conferences

We are an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. All of our projects, tools, documents, forums, and chapters are free and open to anyone interested in improving application security. The OWASP Foundation launched on December 1st, 2001, becoming incorporated as a United States non-profit charity on April 21, 2004."