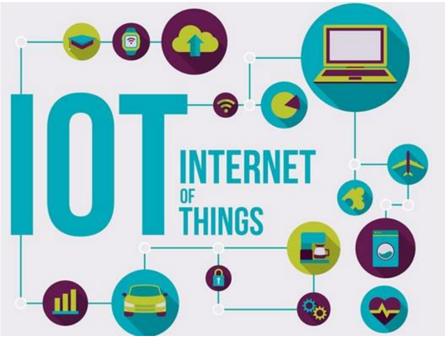
Network Security (CS6500)

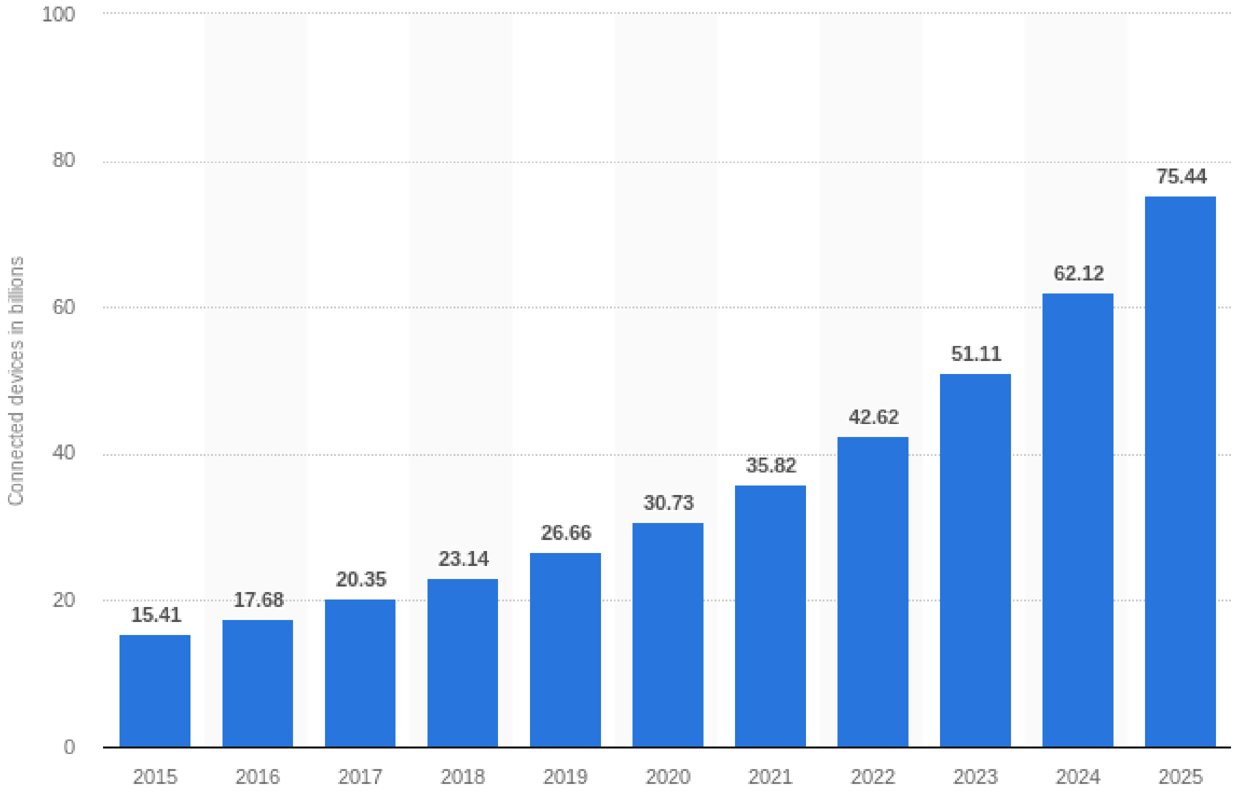
Chester Rebeiro

IIT Madras

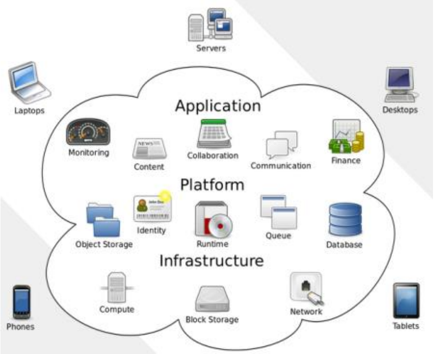
Connected Devices



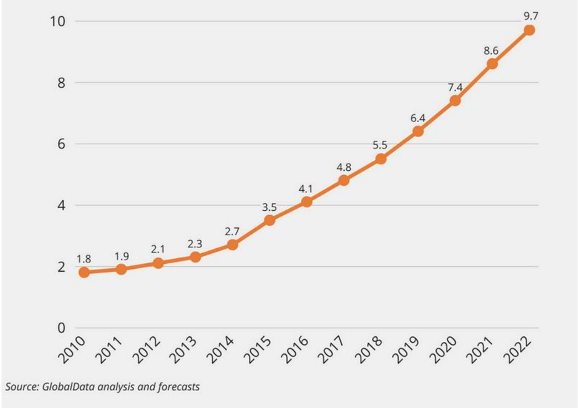
IoT / Smart cities



Critical Infrastructure



Cloud computing



Source: GlobalData analysis and forecasts

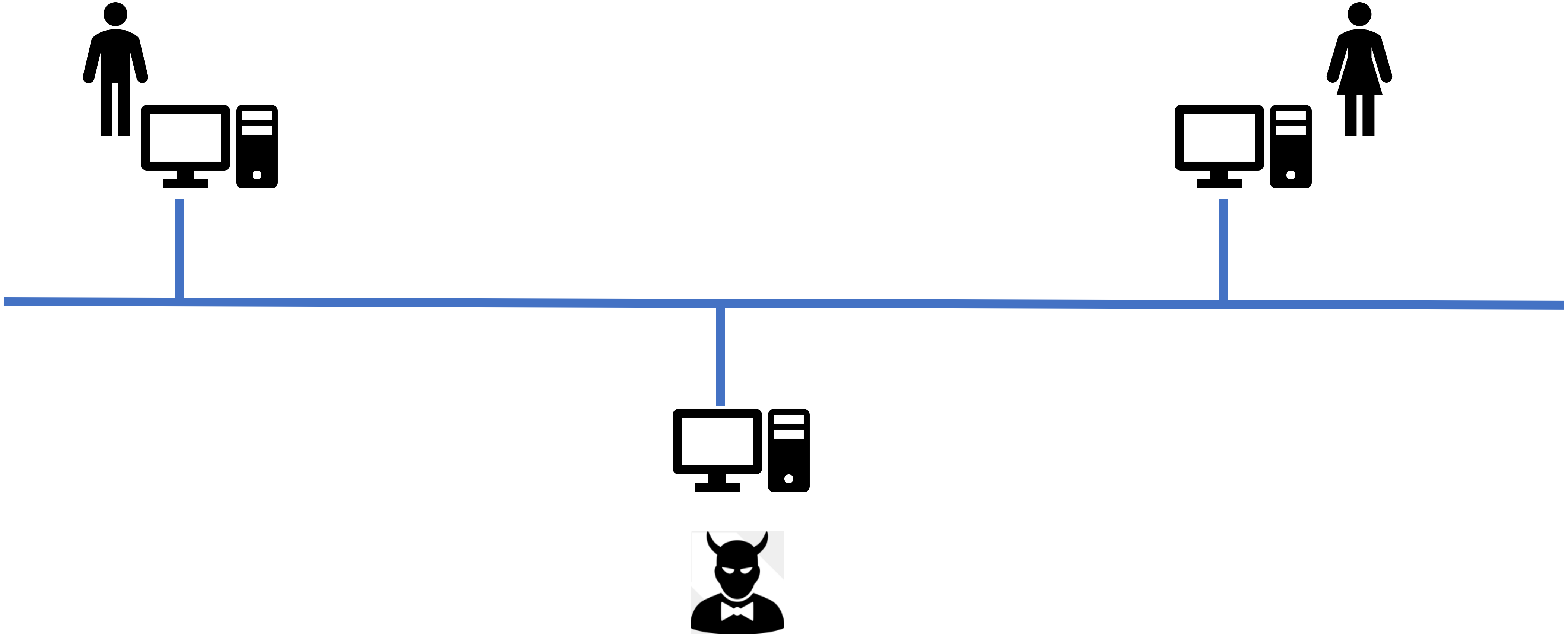
Online Services

PC: Statista 209, Global Data Analysis and Forecasts

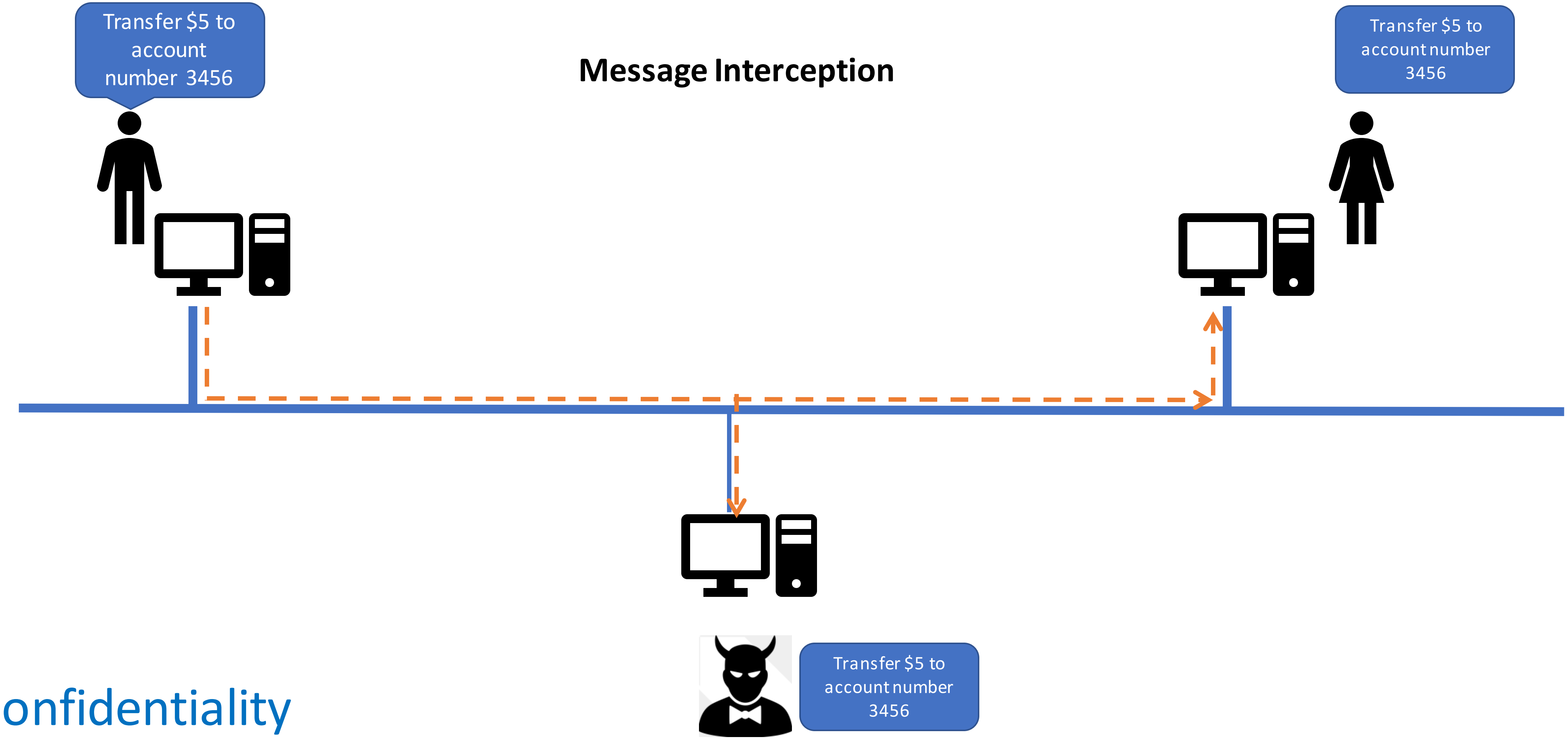
Network Security (Statistics)

- In 2016, the U.S government spent a $28 billion on cyber-security.
- The potential cost of cyber-crime to the global community is $500 billion, and a data breach will cost the average company about $3.8 million (Microsoft).
- Ransomware attacks increased by 36 percent in 2017.
- 1 in 131 emails contains a malware.
- In 2017, 6.5 percent of people are victims of identity fraud resulting in fraudsters defrauding people of about $16 billion.
- **Unfilled cyber security jobs are expected to reach 3.5 million by 2021 — compared to about 1 million in 2016.**

Network Attacks: What is it all about?



Network Attacks: What is it all about?

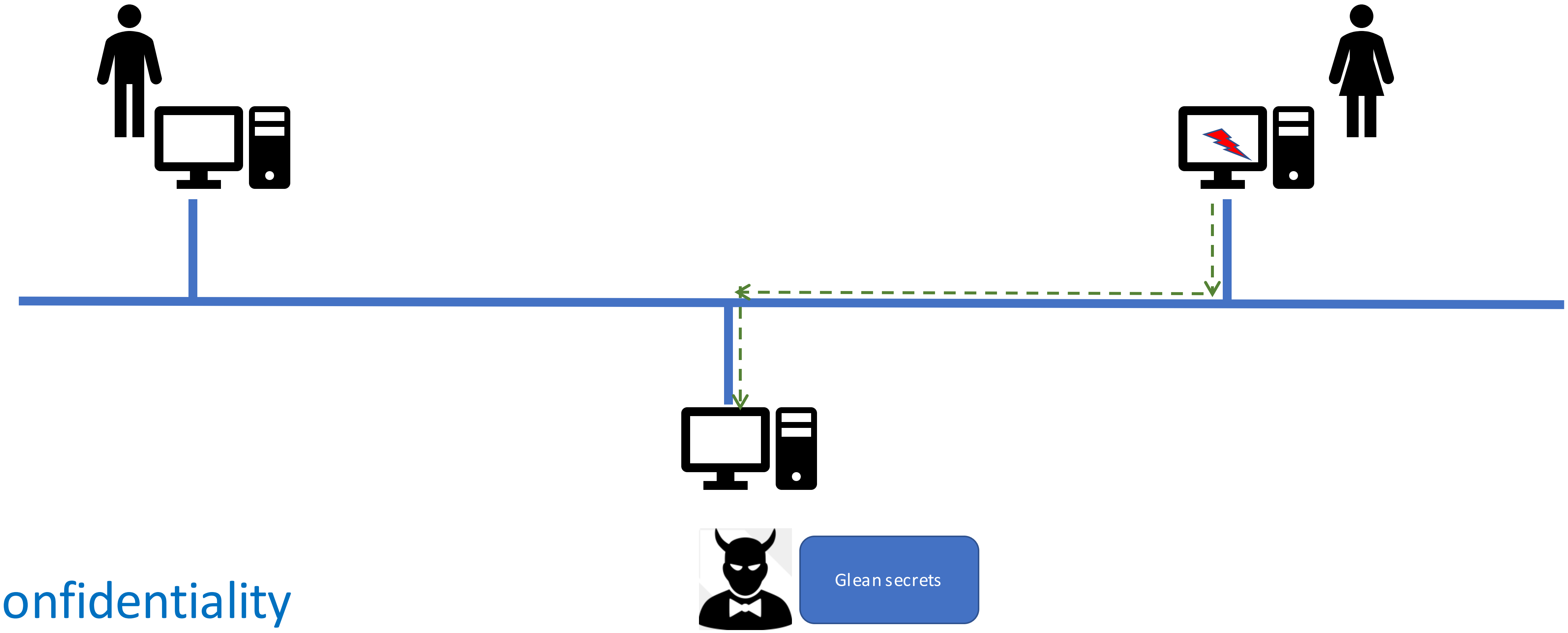


Transfer $5 to account number 3456
Message Interception
Transfer $5 to account number 3456
Transfer $5 to account number 3456

Confidentiality

Network Attacks: What is it all about?

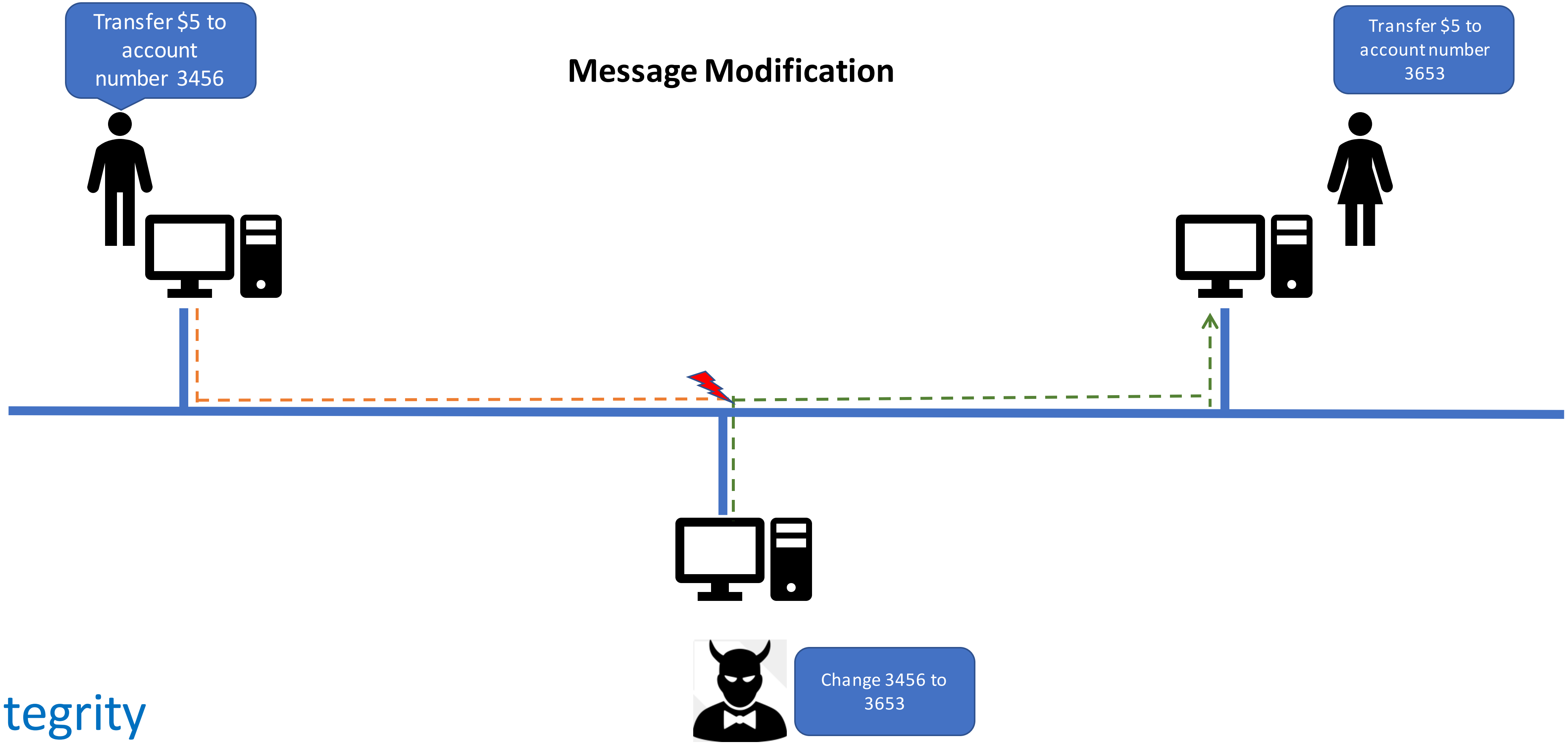
Glean Secrets



Confidentiality

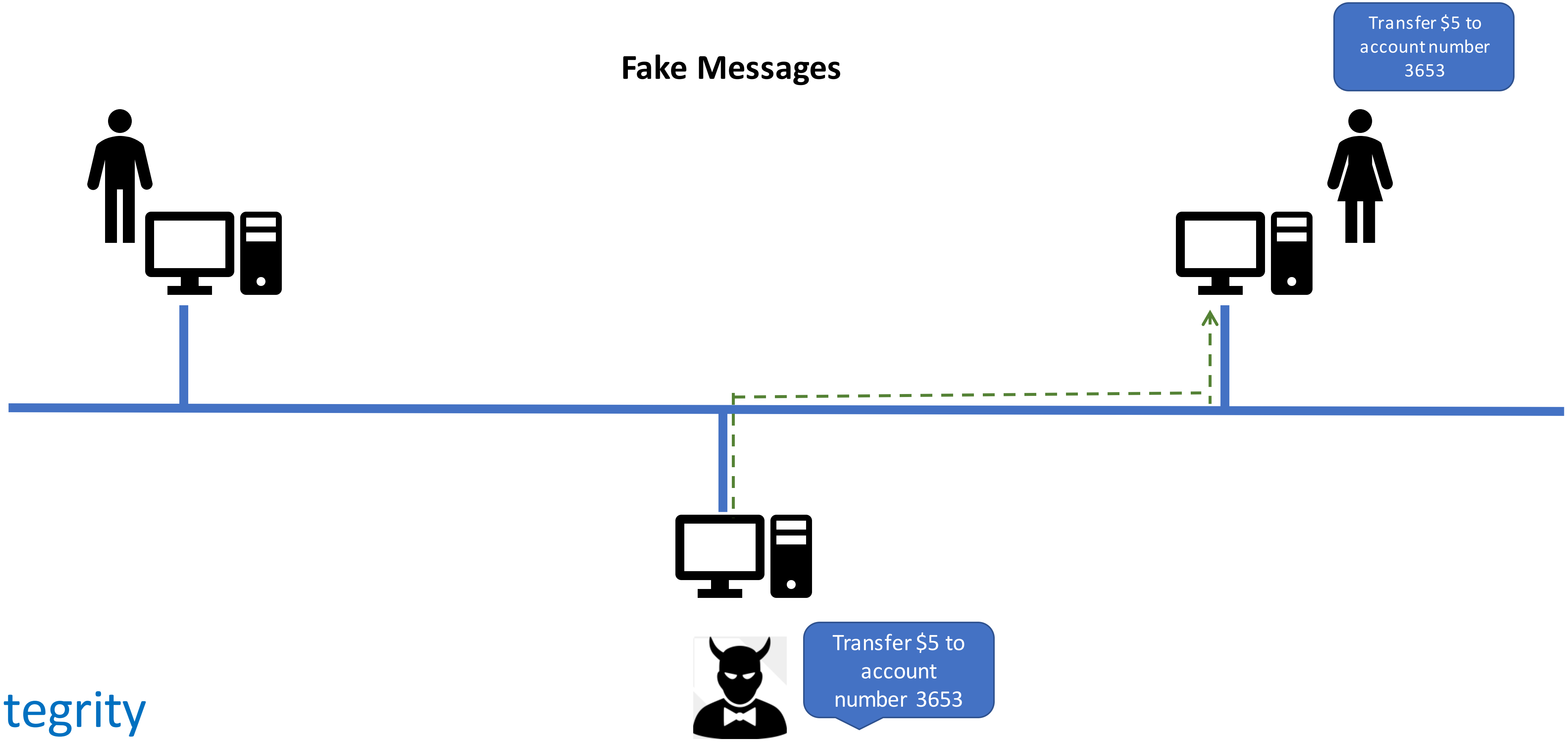
Network Attacks: What is it all about?

Message Modification


Transfer $5 to account number 3456
Transfer $5 to account number 3653
Change 3456 to 3653

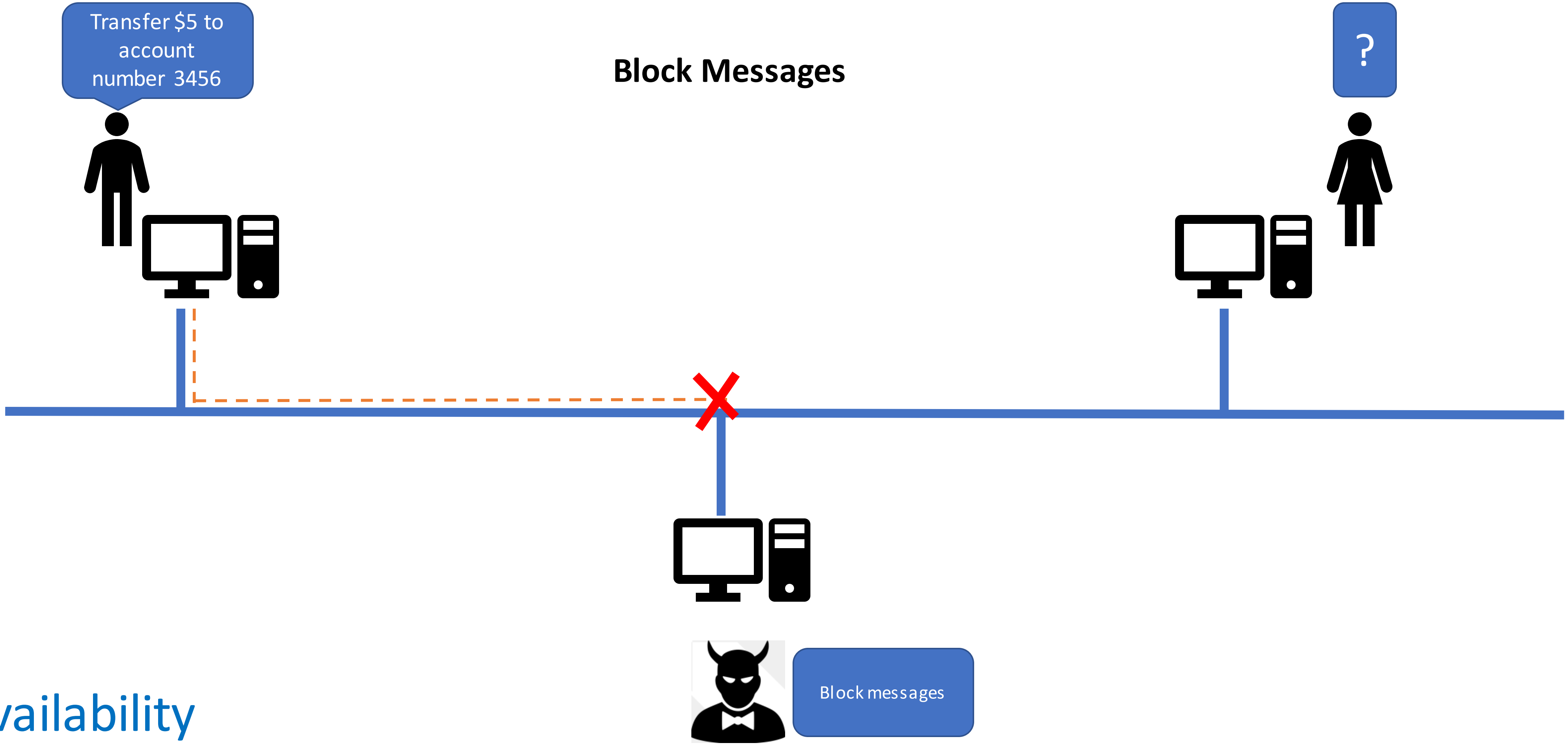
Integrity

Network Attacks: What is it all about?


Transfer $5 to account number 3653
Fake Messages
Transfer $5 to account number 3653

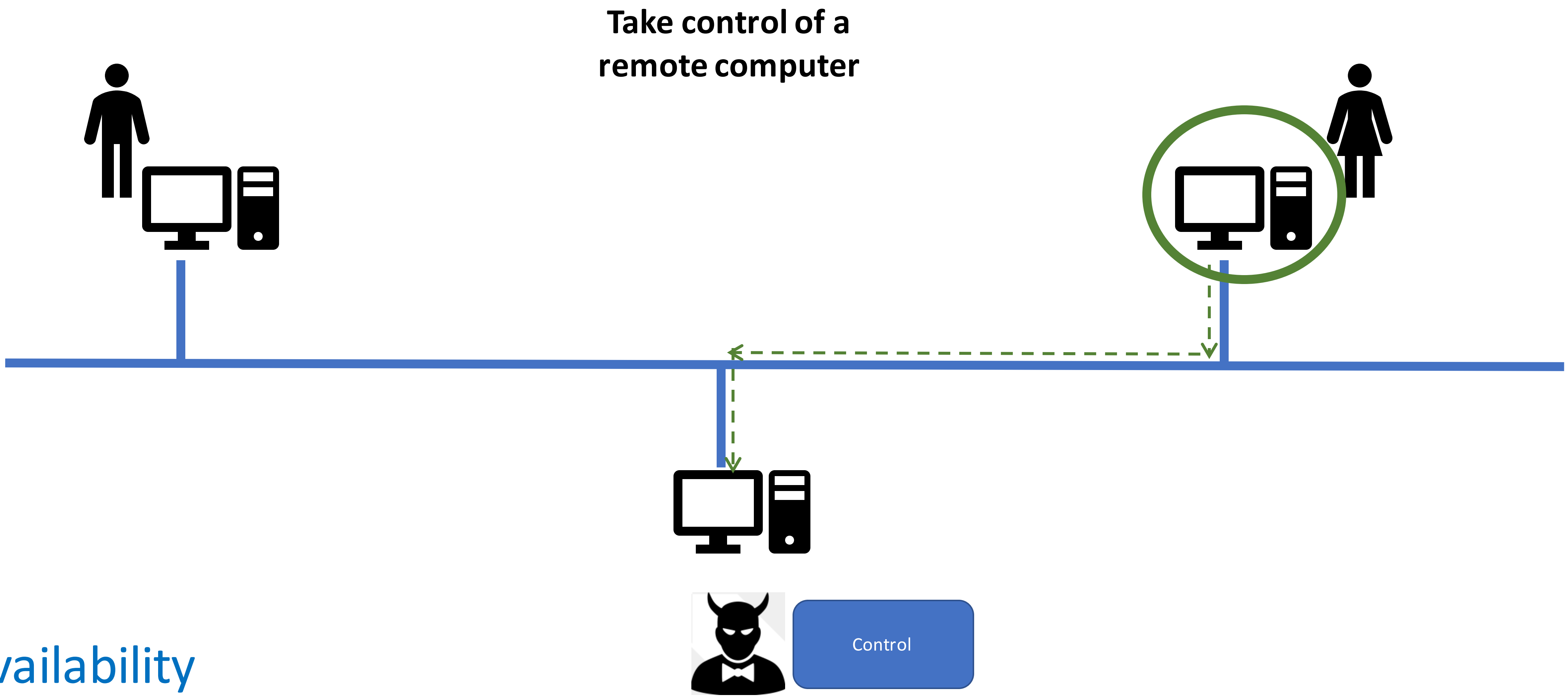
Integrity

Network Attacks: What is it all about?



Availability

Network Attacks: What is it all about?



Availability

Why are there so many threats?

Weakest Link matters!

Several possible weak links

- Shared networks
- Multiple untrusted devices in a network (Hardware Trojans)
- Buggy programs (Heartbleed bug, 2014)
- Design flaws in communication protocols and in applications (WPA2 attack, 2017)

Why are there so many threats?

Weakest Link matters!

Several possible weak links

- Shared networks
- Multiple untrusted devices in a network (Hardware Trojans)
- Buggy programs (Heartbleed bug, 2014)
- Design flaws in communication protocols and in applications (WPA2 attack, 2017)
- User ignorance (not all users have taken CS6500)

Cryptography

It is not the panacea for all network security problems

- but provides tools to achieve confidentiality and integrity

This Course (contents)

Part 1

Network Protocol Attacks
(Sniffing/Spoofing, TCP Attacks, DNS attacks, firewalls, and IDS)

Part 2

Cryptography (basics)
Public key and private key algorithms

Part 3

Using Cryptography to achieve secure communication

Key distribution and management
Virtual Private Network
Public Key Infrastructure
Transport Layer Security

Part 4

Tools for ethical hacking

(if time permits)

Anonymous Routing and Dark Web

This Course (What to expect?)

- **Loads of Assignments (50%)**
  - Capture the flag contests (roughly once every 3 to 4 weeks)
  - Programming assignments (around 6 to 7 of them)
- **Quizzes**
  - Mid semester exam (20%)
  - End semester exam (20%)
- **Reading Assignment** (10%)

This Course (Expected Learning)

- Appreciate and recreate various network security attacks
- Be able to apply cryptography to achieve security
- Be aware of various research problems in the area of network and cyber security

Textbooks

- **Computer Security: A Hands-on Approach**

  Author: Wenliang Du, Syracuse University

  First Printing: October 2017

  Publisher: CreateSpace

- **Cryptography Theory and Practice**

  Author: Douglas R. Stinson

  Publisher: CRC Press

Schedule

- **Three theory classes a week**
  - Monday (10:00 to 10:50AM)
  - Tuesday (9:00 to 9:50AM)
  - Wednesday (8:00 to 8:50AM)
- **Tutorials**
  - Friday (12:00 to 12:50PM)
  - Capture the flags contests will be mostly on Friday (evening) or Saturdays and announced in the class at-least 2 weeks early

Website and Communication

- **Website**

  http://www.cse.iitm.ac.in/~chester/courses/19e_ns/index.html

- **Communication**

  Google groups (link will be posted on IITM moodle)

- **Assignment Submissions**

  IITM moodle