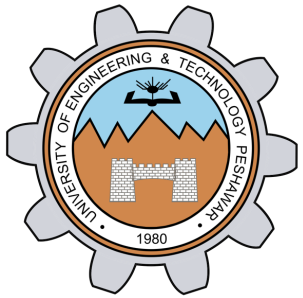
Computer Security

Lecture 1: Introduction

Prof. Dr. Sadeeq Jan

Department of Computer Systems Engineering

University of Engineering and Technology Peshawar



Instructor

Prof. Dr. Sadeeq Jan

- Director, National Centre for Cyber Security
- Professor, DCSE

Qualification:

- *PhD (Security Testing) with Excellent grade – University of Luxembourg*
- *MS (Info/Comm System Security) with Excellent grade - KTH Sweden*
- *BSc Engg (Computer Systems Engineering) - UET Peshawar*
- ***IZAZ-E-SABQAT** (Presidential Award), **Gold Medalist**, CGPA **3.98/4.00***

Contact:

sadeeqjan@uetpeshawar.edu.pk

sadeeqjan@yahoo.com

Venue

Lecture room:

- Lab 1, DSP Lab

Day:

- Tuesday, Thursday

Timing:

- Tuesday 11 to 2.00
- Thursday 8 to 11.00

Books

Course Books

- Cryptography and Network Security By William Stallings
- Introduction to Computer Security By Matt bishop

Reference Books

- Network Security Essentials By William Stallings
- Computer Security Art and Science by Matt. Bishop

Grading Criteria

Exams

- Midterm: 25%
- Final Term: 50%

Sessional

- Attendance: 5%
- Assignments: 10%
- Quizzes: 10%

Course Objective

- Learn about the most important concepts in computer security
- Analyze cryptographic algorithms, their use & issues of strengths
- Understand computer security techniques, e.g., authentication, Firewalls, IDS, etc.
- Basics of Ethical Hacking/Penetration Testing

Course Content

Weekly Schedule		
Week	Course Contents	Assignments (A)/Quiz (Q)
Week 01	Introduction to Computer Security	
Week 02	Key Concepts of Computer Security	
Week 03	Security Policies/Mechanisms and Risk Management	
Week 04	Cryptography (Classical Encryption Systems)	Assignment#1
Week 05	Cryptanalysis of Classical Encryption Systems	Q#01
Week 06	Modern Ciphers & Data Encryption Standard (DES)	Assignment#02
Week 07	Double & Triple DES, Meet-in-the-Middle Attack	
	Midterm Examination	
Week 8	Advanced Encryption Standard (AES)	Q#02
Week 9	Key Management	Assignment#03
Week 10	RSA Asymmetric Key Exchange Algorithm	Q#03
Week 11	Diffie-Hellman Key Exchange Algorithm	
Week 12	Message Authentication & Hash Functions	
Week 13	Malicious Code, Virus, Trojan, Trapdoors etc.	Assignment#04
Week 14	Web Security	Q#04
Week 15	Ethical Hacking/Penetration Testing	
	Final Term Examination	

CLOs-PLOs Mapping

CLO #	Course Learning Outcomes (CLOs)	Level of Learning (Bloom's Taxonomy)	Program Learning Outcomes (PLOs)
1	Explain the key concepts and importance of computer security in today's computer-driven world.	Cog-2 (Comprehension)	PLO:1 Engineering Knowledge
2	Analyze the classical and modern cryptographic algorithms, their weaknesses and strengths.	Cog-4 (Analysis)	PLO 4 (Investigation)
3	Illustrate security policies/mechanisms and strategies for protection/testing of systems against malware attacks	Cog-3 (Application)	PLO:1 Engineering Knowledge

CLOs-Assessment Tools Mapping

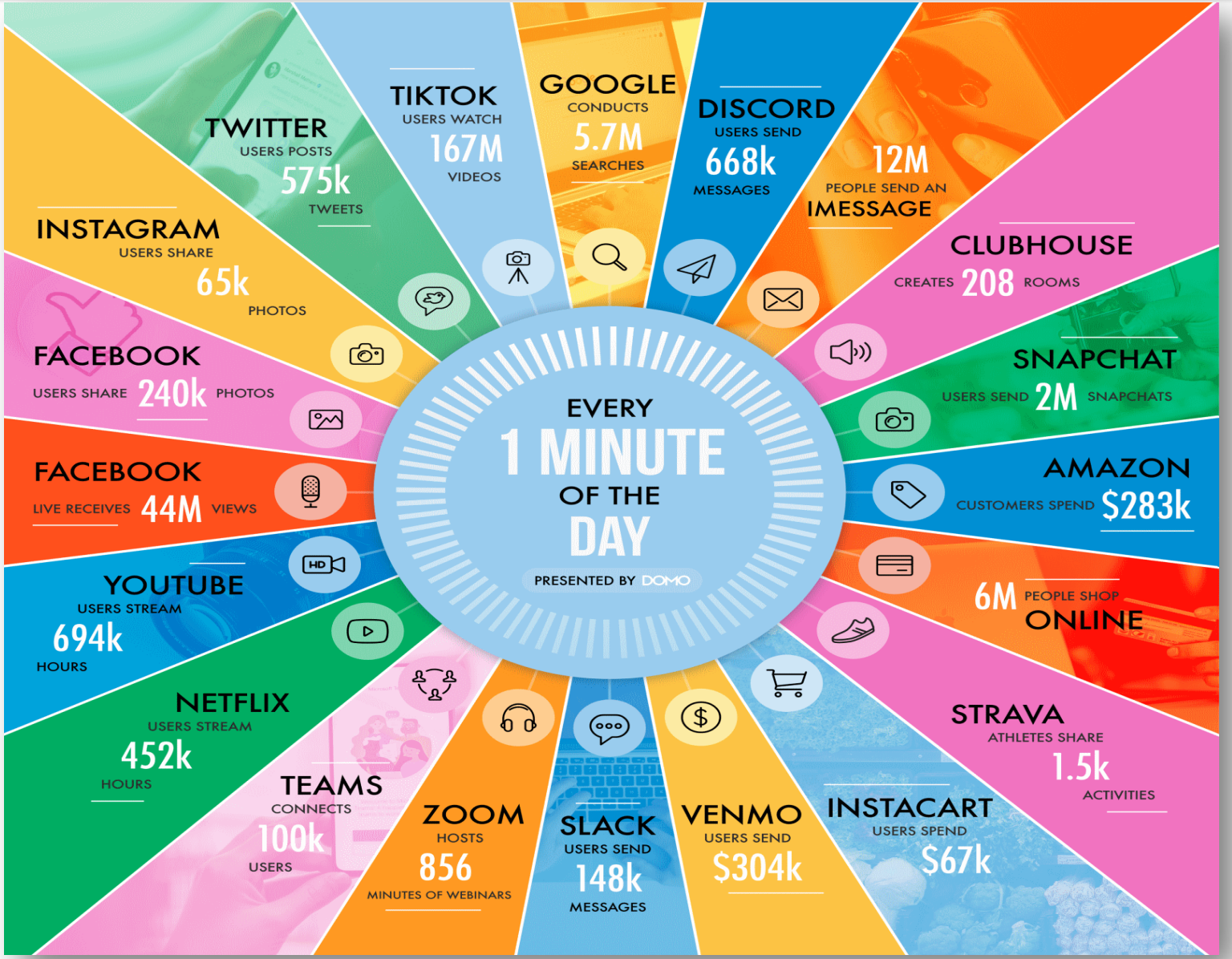
Course Assessment Tools	CLOs		
	CLO 1	CLO 2	CLO 3
Assignments		✓	
Quizzes		✓	
Midterm Exam	✓	✓	
Final Exam		✓	✓

Lecture Outline

- 60 seconds of Internet
- Data Breaches
- Vulnerability
- Introduction to Security and Network Security
- Basic Definitions
- Why Is Security Necessary?
- History of the Security Problem
- Computer Security and History
- Do We Really Need Computer Security?
- Why Aren't All Computer Systems Secure?
- Problems With Patching
- Attacks are developed more quickly
- Why do we need Network Security?
- Internet Evolution

Seconds of Internet

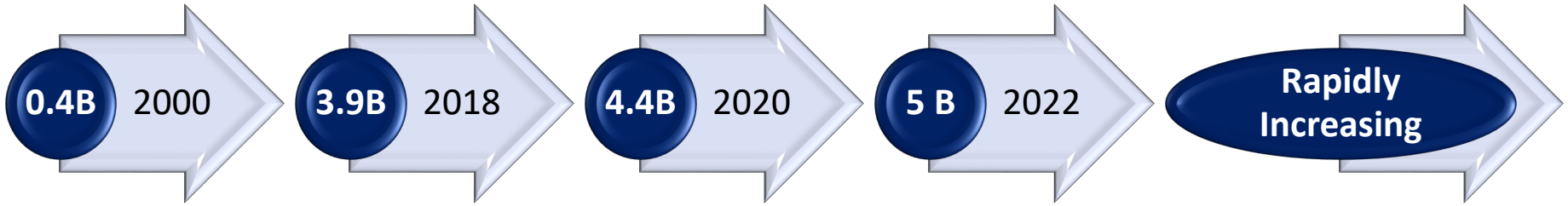
Seconds of Internet



Source: https://www.smartinsights.com/internet-marketing-statistics/happens-online-60-seconds/

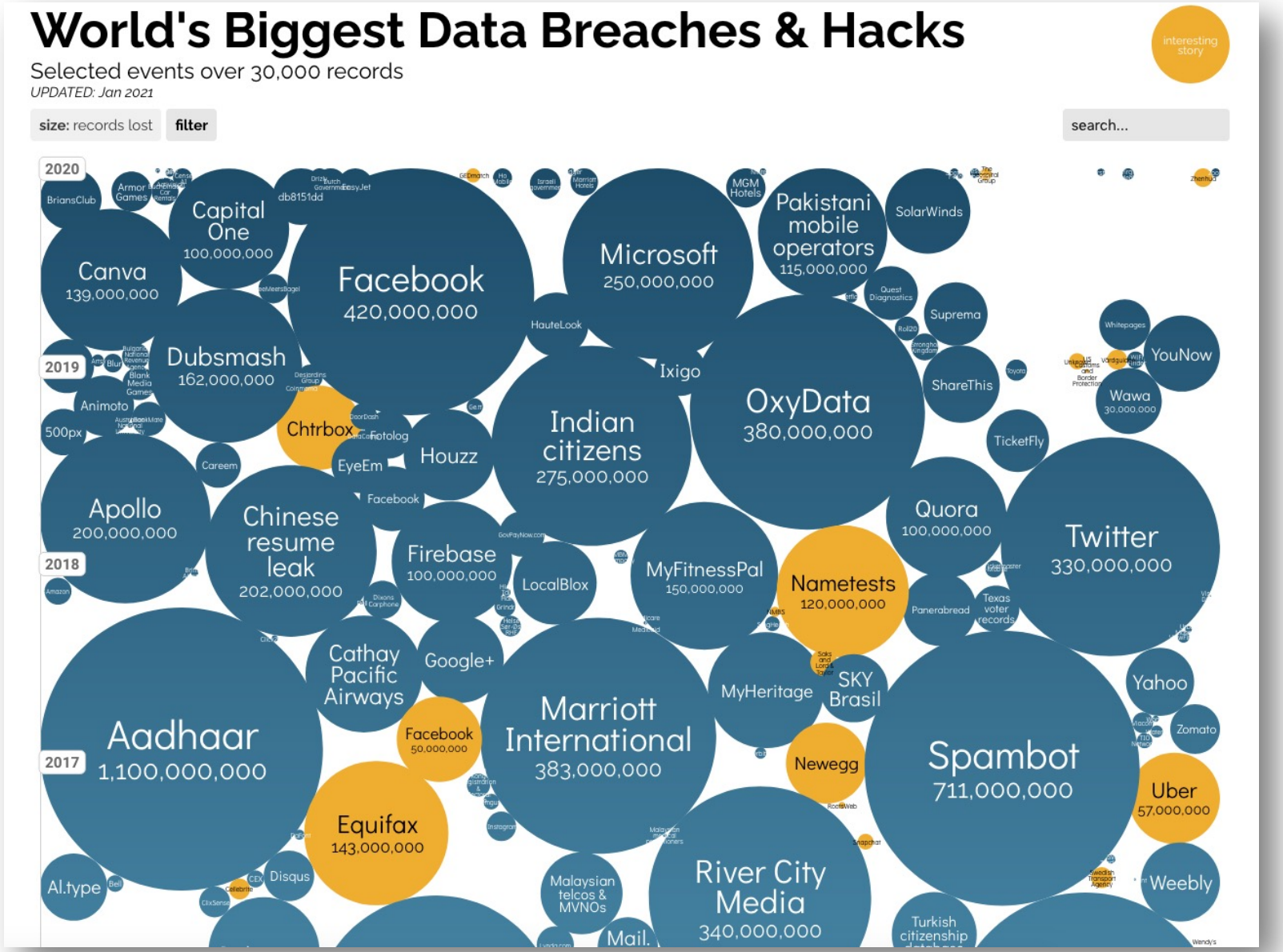
Global Internet Population Growth (in Billions)

- As of July 2022, the internet reaches 63% of the world's popultation and now represents around 5 billion people.
  - 92.6 percent accessed the internet via mobile devices.
- The total amount of data consumed globally in 2021 was 79 zettabytes, and annual number projected to over 180 zettabytes by 2025.



Source statista

Data Breaches are Extremely Common



Security Breaches

- 3.96 million records are stolen or lost per day (≈ 2750/minute)
- 5912 million data records stolen/lost approximately, since 2013

Source: Breach Level Index

Current Internet Threat Trends

- **Symantec Internet Security Threat Report**
  - produced by Symantec on a regular basis
  - gathers information from over 175 million hosts in over 150 countries

- **Global trends**
  - release of devastating ransomware attacks
  - coin-mining on compromised computers is significant
  - mobile malware continues to surge
  - attacks against IoT devices significantly increase
  - attacks are increasingly diversified

Source

Symantec

Cybersecurity Ventures

- According to Cybersecurity Ventures, cybercrime will cost the world $ 10.5 trillion annually by 2025.
- Cybercrime is estimated to cost the world $10.5 trillion annually by 2025
- By 2023, hacking statistics will register another 33 billion stolen records. While the number sounds frightening, it is easily achievable.
- Americans lose $15 billion annually due to identity theft.
- It takes 196 days on average to identify a data breach.

Source

The Cost of Cybercrime Per Minute

Average cost of a breach

$7.2

Source

RISKIQ®

The Cost of Cybercrime Per Minute

Average cost of a breach in the healthcare industry

$13.3

E-commerce losses to online payment fraud

$38,052

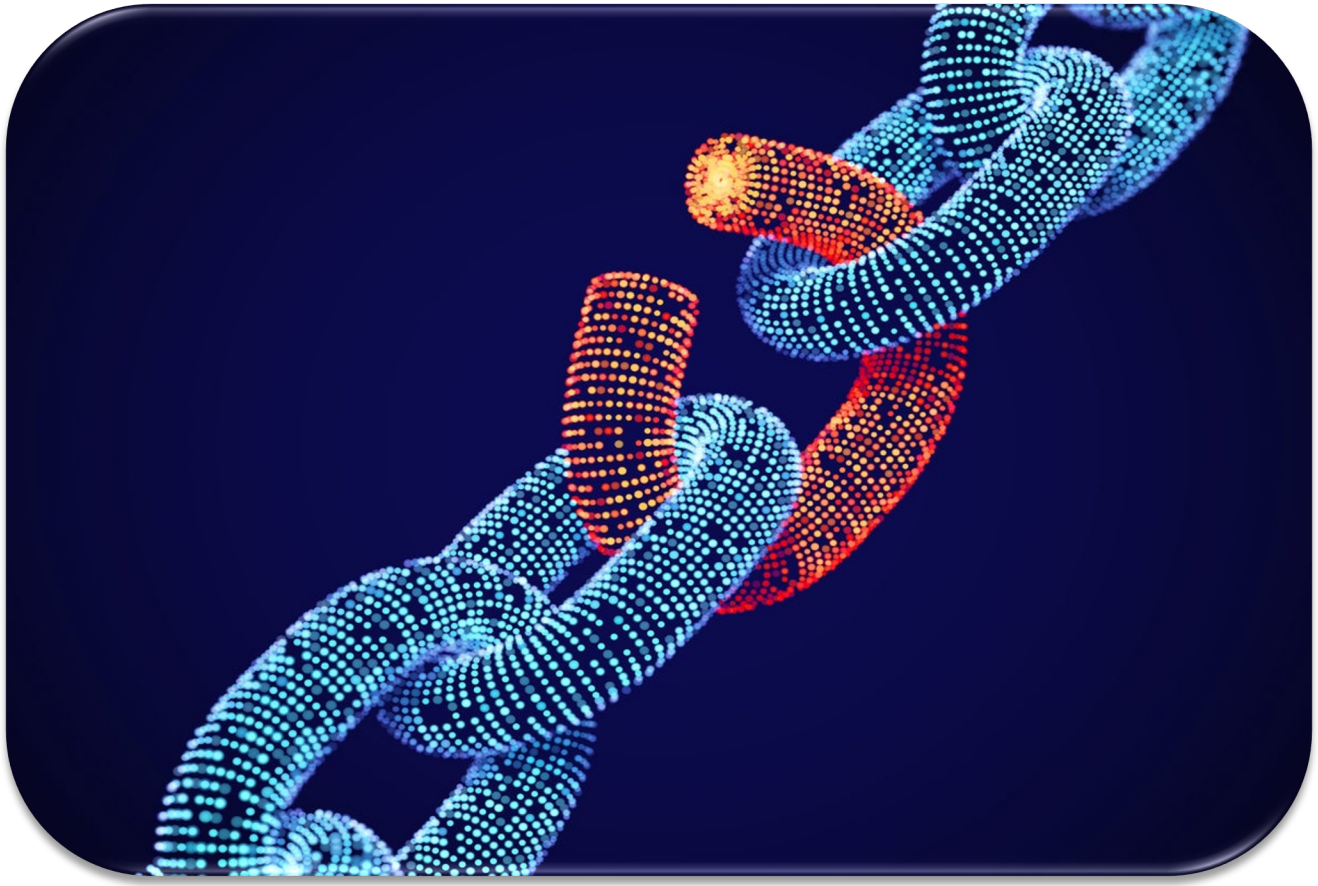
Amount lost to cryptocurrency scams

$3,615

Source

RISKIQ®

What is Vulnerability?



What is Vulnerability?

A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy

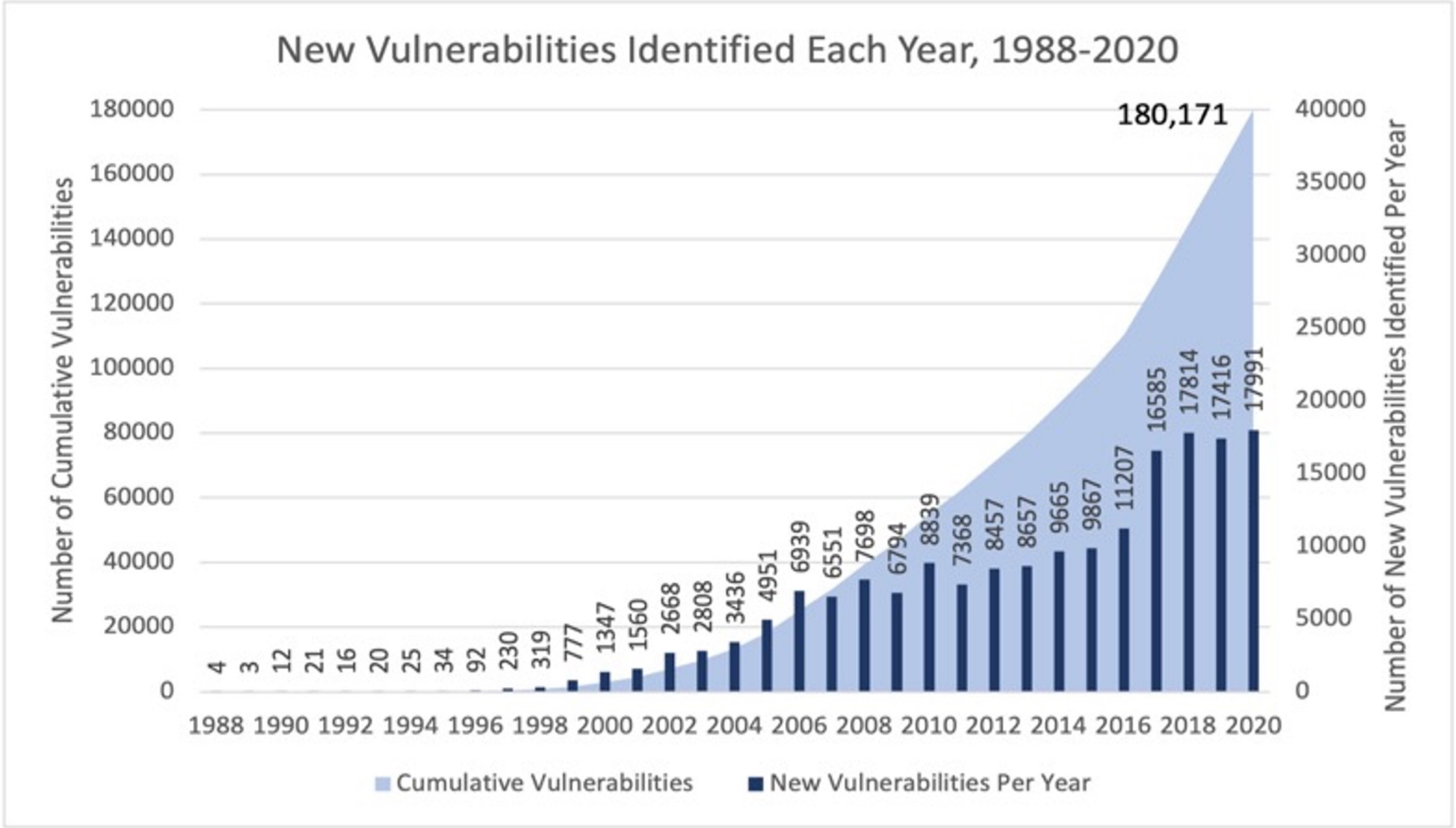
- ✓ Software bugs
- ✓ Configuration mistakes
- ✓ Network design flaw
- ✓ Lack of encryption

Exploit

- Taking advantage of a vulnerability

Vulnerabilities Over the Past 32 Years

- Number of vulnerabilities have significantly increased over time



Source: Data obtained from securityintelligence.com on March 10, 2021

Examples of Largest Cyber Breaches

2016 to 2022

The Carbanak Attack (The Great Bank Robbery)

- *Approximately 1$ billion stolen from financial institutions worldwide over a period of 2 years*

How the attack works?

Sending Carbanak backdoor to Bank Employees via Phishing emails

2. Harvesting Intelligence

Interception of the clerk's screen by hackers

3. Mimicking the staff (stealing $)

- Using Online-banking, E-payment systems to transfer money
- Inflating account balances
  - Increasing customer's account balance and transferring extra funds their (hackers) account
- Controlling ATMs
  - Orders to dispense cash at certain times

Bangladesh Bank Heist - 2016

- One of the biggest cyber attacks- $81 Million stolen
- Hackers obtained credentials of an operator at Bangladesh Bank and installed several malware.
- Sent requests from Bangladesh Bank to Federal Reserve Bank of New York via SWIFT network.
- Money transferred to hackers' accounts in Sri Lanka and Philippines.
- Also tampered bank's printing system to hide the SWIFT acknowledgement receipts.

Equifax - 2017

- Equifax, one of the largest credit bureaus in the US.
- In 2017 said that an application vulnerability in one of their websites led to a data breach that exposed about 147.9 million consumers.
- The breach compromised the PII (including Social Security numbers, birth dates, addresses, and in some cases drivers' license numbers) of 143 million consumers.
- 209,000 consumers also had their credit card data exposed. That number was raised to 147.9 million in October 2017.
- At least $575 Million fined were paid by the company.

Marriott International - 2018

- Marriott International announced in November 2018 that attackers had stolen data on approximately 500 million customers.
- The credit card numbers and expiration dates of more than 100 million customers were believed to be stolen.
- The publicized breach potentially cause $23.7 million in fines, 18.4 million were paid in 2020.

Capital One - 2019

- In March 2019, Paige Thompson – former software engineer at Amazon Web Services) hacked into Capital One's customer databases.
- Thompson was able to gain access to nearly 106 million bank clients and applicants. She extracted the personal information of both customers and applicants from 2005 to the early months of 2019.
- The publicized breach potentially cause the bank between $100 million to $500 million in fines.
- Aside from that, the bank's chief Information Security Officer, Michael Johnson, was demoted from his position four months following the incident.

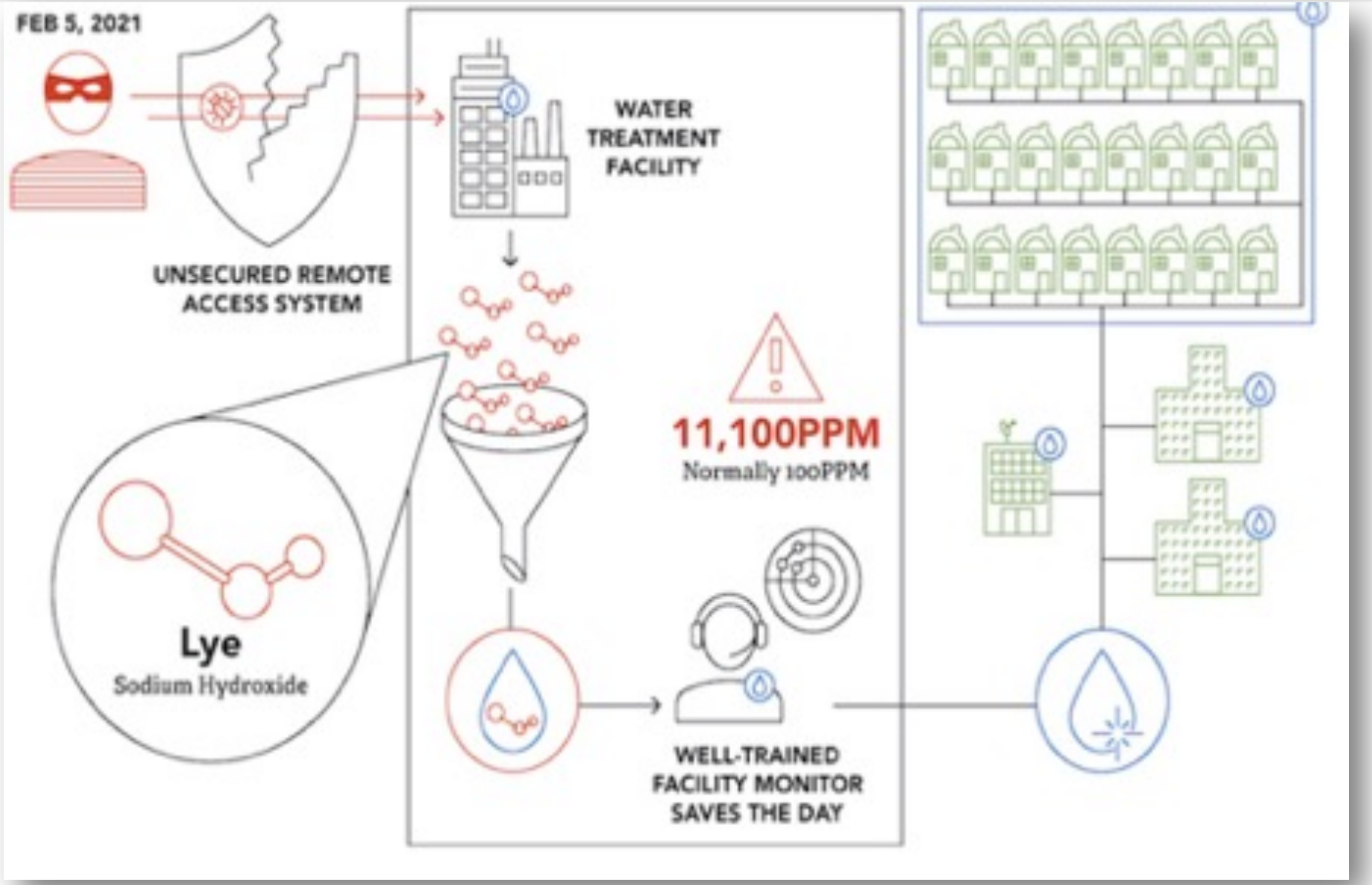
Pakistani Mobile Users - 2020

- Pakistani Mobile suffered a major breach spread across two separate incidents.
- Hackers put 55 million user accounts up for sale in April 2020.
- A month later, in May of 2020, hackers leaked another 44 million user accounts.

Florida Water System - 2021

- On February 5, 2021 hacker tried to poison the water supply by using a remote access software "Teamviewer".
- The malicious hacker increased the level of sodium hydroxide/Lye to over 100 times its normal level.
- The level got back to the normal range as soon as there was an alert of a cyberattack from an employee to avoid a significant consequence to the Florida citizens.

Florida Water System - 2021



Russia and Ukraine Cyberwar - 2022

- Cyberattack on the KA-SAT satellite broadband network, owned by Viasat , and is believed to have caused severe communications disruptions in Ukraine and the surrounding areas. Feb 24, 2021

- Ukraine releases details of a hack on news agencies. Reportedly, the hack was performed by "Russian Federation's hackers" and appears to be a defacement operation that included placing symbols banned in Ukraine on the agencies' front pages. CIP mentioned no data was compromised as a result. March 18, 2022

Russia and Ukraine Cyberwar - 2022

- The Russian Civil Aviation Authority Rosaviatsiya was attacked by unnamed threat actors, erasing 65 TB of data and collapsing the government agency's network. It was reported that at least some of the data had no backups and could not be restored. The attack was initially attributed to Anonymous. March 30, 2022

- The Anonymous-affiliated group NB65 claimed they hacked the All-Russia State Television and Radio Broadcasting Company (VGTRK), accusing them of spreading Putin's propaganda. In addition, the hackers allegedly stole 870 GB of data from the company to be released soon. March 28, 2022

Basic Definitions

Definitions

- **Information Security**
  - Keeping data secure in any form (whether digital or on paper)
  - Broader than Cyber Security
- **Cyber Security**
  - Protecting data found in electronic form
  - A subset of Information Security

Definitions

- **Computer Security**
  - ✓ Generic name for the collection of tools designed to protect data and to defeat hackers
- **Network Security**
  - ✓ Measures to protect data during their transmission
- **Internet Security**
  - ✓ Measures to protect data during their transmission over a collection of interconnected networks

Why Is Security Necessary?

Why Is Security Necessary?

- **Fundamental aspects of information must be protected**
  - ✓ Confidential data
  - ✓ Employee information
  - ✓ Business models
  - ✓ Protect identity and resources

History of the Security Problem

- In the beginning, there was no computer security problem
- Later, there was a problem, but nobody cared
- Now, there's a big problem and people care
  - Only a matter of time before a real disaster
  - At least one company went out of business due to a DDoS attack
  - Identity theft and phishing claim vast number of victims
  - Ransomware attacks are spreading rapidly and in many different ways
  - Increased industry spending on cybersecurity

Computer Security and History

- Much of our computer infrastructure is constrained by legacy issues
  - Core Internet design
  - Popular programming languages
  - Lack of security awareness by programmers
  - Lack of Security Testing
- All developed before security was a concern
  - Generally, with little or no attention to security

Do We Really Need Computer Security?

- The preceding examples suggest we must have it
- Yet many computers are highly insecure
- Why?
- Ultimately, because many people don't think they need security
  - Or don't understand what they need to do to get it

Why Aren't All Computer Systems Secure?

- Partly due to hard technical problems
- But also due to cost/benefit issues
- Security costs
- Security usually only pays off when there's trouble
- Many users perceive no personal threat to themselves
  - "I don't have anything valuable on my computer"
- Ignorance also plays a role
  - Increasing numbers of users are unsophisticated

Retrofitting Security

- Since security not built into these systems, we try to add it later
- Retrofitting security is known to be a bad idea
- Much easier to design in from beginning
- Patching security problems has a pretty dismal history

Problems With Patching

- Usually done under pressure
  - So generally quick and dirty
- Tends to deal with obvious and immediate problem
  - Not with underlying cause
- Hard (sometimes impossible) to get patch to everyone
- Since it's not organic security, patches sometimes introduce new security problems

Attacks are developed more quickly

- Attacks are developed more quickly
  - Often easier to adapt attack than defense to counter it
- Malware spreads faster
  - Slammer infected 75,000 nodes in 30 minutes
  - According to Microsoft, nearly 97% of all ransomware infections take less than 4 hours to successfully infiltrate their target. The fastest can take over systems in less than 45 minutes.

Why do we need Network Security?

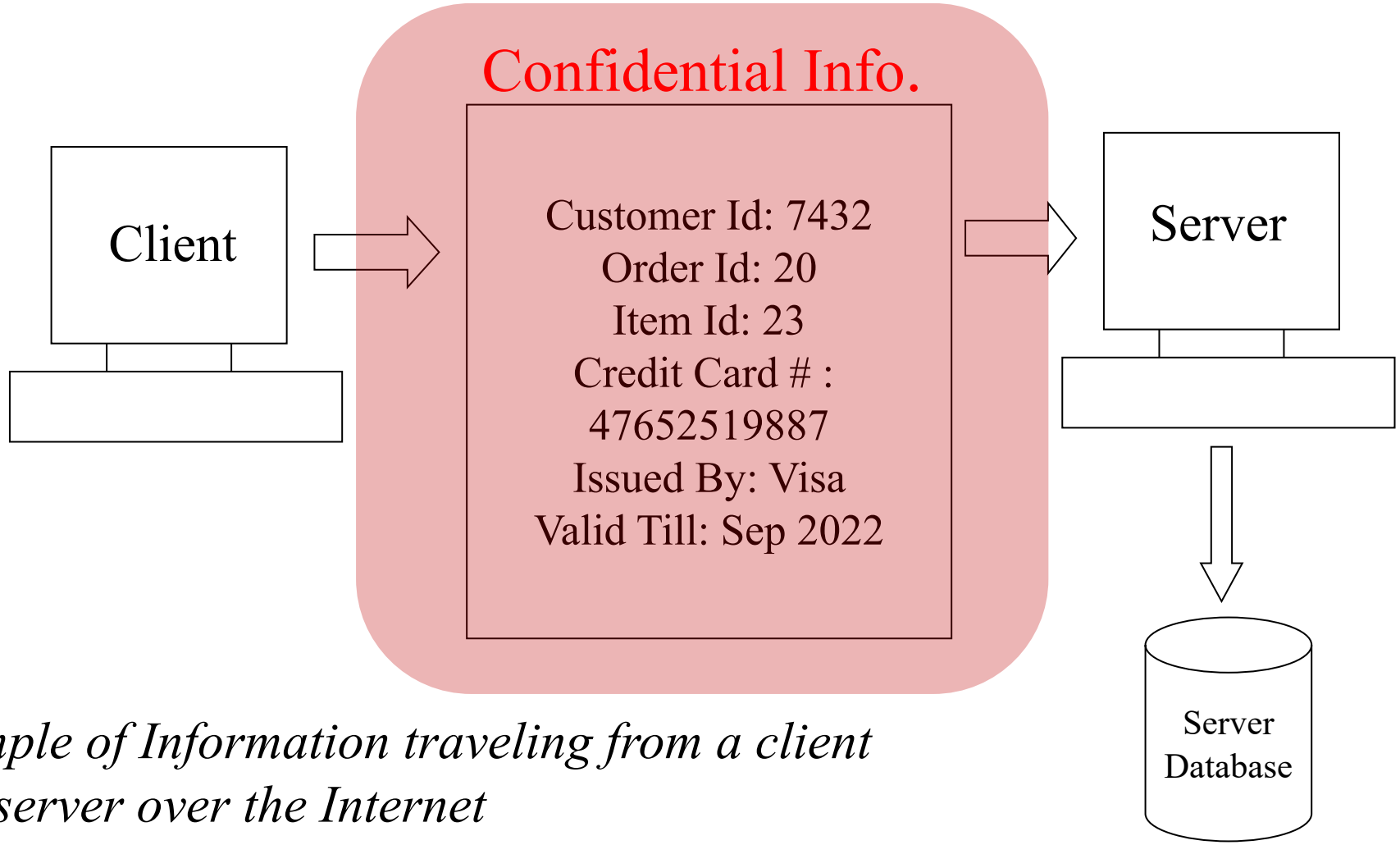
Why Network Security?

- **The Internet was initially designed for connectivity**
  - ✓ Trust assumed
  - ✓ We do more with the Internet nowadays
  - ✓ Security protocols are added on top of the TCP/IP

Why Network Security?

- **We can't keep ourselves isolated from the Internet**
  - ✓ Most business communications are done online
  - ✓ We provide online services
  - ✓ We get services from third-party organizations online

Need for Network Security - Example



Example of Information traveling from a client
To a server over the Internet

Internet Evolution

LAN connectivity

Application-specific
More online content

Cloud computing
Application/data hosted
in the cloud environment

Different ways to handle security as the Internet evolves

Well, What About Tomorrow?

- Will security become more important?
- Yes!
- Why?
  - More money on the network
  - More sophisticated criminals
  - More leverage from computer attacks
  - More complex systems

END