

# Module 8: Software Issues: Risks and Liabilities

1

Chapter 8

# Module 8: Software Issues: Risks and Liabilities

- Definitions
- Causes of Software Failures
- Risks
- Consumer Protection
- Improving Software Quality
- Producer Protection

# Definitions

- Software- computer programs made up of a logical sequence of commands to perform a task.
- The software producer/developer creates computer programs to meet either general or specific needs of the consumer
- A buyer gets the benefits of a computer program to solve a specific task/problem.
- Whenever there is a software there are producers and consumers.

# Definitions...

- There is, therefore, a relationship between software producers and users made up of: **user expectations** and **developer limits**
- For a healthy relationship all the following must be agreed on:
  - (1) Standards – universally accepted level of confidence

# Definitions...

- Standards depend on:
  - Development testing
  - Verification and Validation
- (2) Reliability – software reliability does not depend on **age** and **wear and tear** like hardware
- Software reliability - is the probability that the software does not encounter an input sequence resulting into failure.

# Definitions...

- (3) **security**- software is secure if it does not contain trapdoors through which an intruder can access the system.
- (4) **Safety** – the safety of a software product means the absence of a likelihood of an accident, a hazard, or a risk
  - A number of life critical systems depend on software, therefore, software safety is important.
- (5) **Quality**- a software product has quality if it maintains a high degree of excellence in standards, security, safety, and dependability.

# Causes of Software Failures

- There are factors that contribute to software failures:
  - Human factors
    - Memory lapses and attentional failures, Rush to finish, Overconfidence and use of nonstandard or untested algorithms, Malice, Complacency
  - Nature of software
    - Complexity, Difficult testing, Ease of programming, Misunderstanding of basic design specifications
- Safety critical systems – these are software systems with real-time control components that can have a direct life-threatening impact
- Examples of critical systems:
  - Nuclear reactors
  - Missile systems
  - Aircraft and air control systems

# Causes of Software Failures...

- Examples of safety-critical failures:
  - The Indian Union Carbide - Bhopal
  - The Therac-25.
  - The Chernobyl Nuclear Power Accident



# Consumer Protection and the Law

- Buyer's rights:
  - Replacement
  - Refunds
  - Updates
- Understanding software complexity-software as:
  - Product
  - Service
  - Mix

# Consumer Protection and the Law...

- Costumer protection tools:
  - (1) contract (used with products):
    - Express warranties
    - Implied warranties
    - Third-party beneficiary
    - Disclaimers
    - Breach of contract – lack of compliance
  - (2) Tort (used with services):
    - Intentional
    - Unintentional

# Consumer Protection and the Law...

- Torts include:
  - Negligence – careless, lack of competence, etc..
  - Malpractice
  - Strict liability
  - Misrepresentation

# Improving Software Quality

- The safety and reliability of a software product defines the quality of that software
- Software quality can only be improved during the development cycle
- The following techniques done during the software development phase can improve software quality (see page 122):
  - Final review
  - Inspection
  - Walk-throughs
  - Phased-inspection

# Producer Protection and the Law

- Protection against:
  - Piracy
  - Illegal copying/downloading of copyrighted software
  - Fraudulent lawsuits by customers
- Seek protection from the courts



# Computer Crimes

Chapter 9

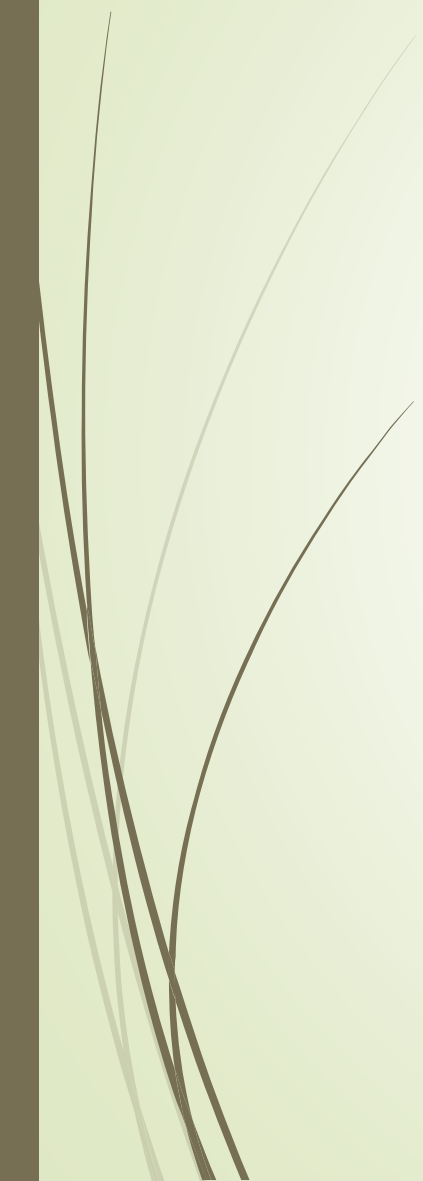


# Definition

- Illegal act that involves a computer system or computer-related system
  - Telephone, microwave, satellite telecommunications system
- That connect one or more computers or computer-related systems
- A computer crime is a crime like any other crime, except that in this case, the illegal act must involve a computer system either as an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime.



# Three Categories

- Natural or inadvertent attack
  - Human blunders, errors and omissions
  - Intentional threats
- 





# History of Computer Crimes

- Cohen, then a graduate student at the University of Southern California, associated the term with a real-world computer program, and he wrote for a class demonstration
- Hacking, as a computer attack technique, utilizes the internetworking between computers and communication devices. **As long as computers are not interconnected in a network, hacking cannot take place**
- The history of hacking begins with the invention of the telephone in 1876 by Alexander Graham Bell which has made internetworking possible.



# Two Types of Attacks

- Penetration
  - Insider threats
  - Hackers
  - Criminal Groups
- Denial of Service Attacks
  - Inside
  - Outside

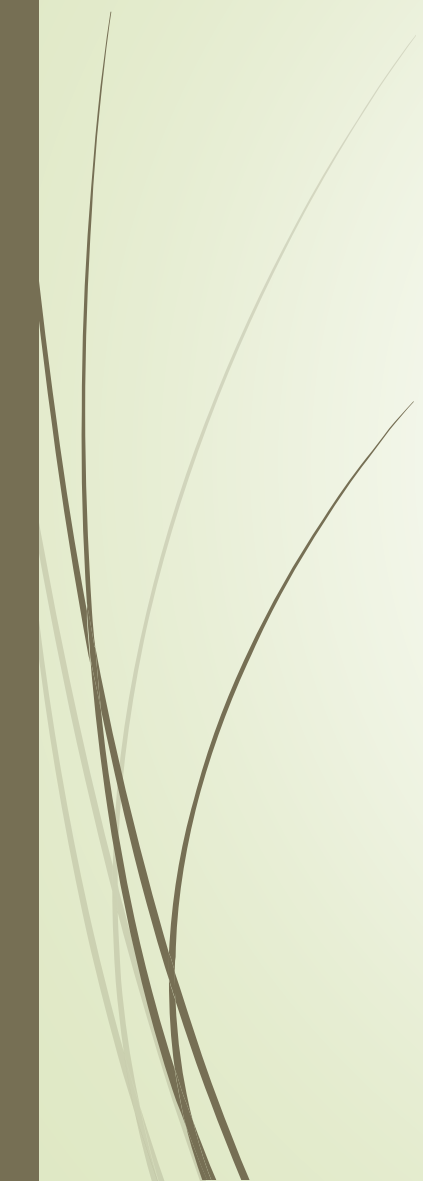


# Motivation of Attacks

- Business and Industrial Espionage
  - Joke/Hoax
  - Political Activism
  - Political and Military Espionage
  - Terrorism/Extortion
  - Vendetta
  - Personal Gain/Fame/Fun
- 



# Reasons for No Information

- Lack of reporting requirements
  - Public sector – fear of market reaction to news
  - Lack of enforcement of existing reporting mechanisms
  - Detection of insider attacks
  - Lack of security agencies or trained security agencies
- 



# Reason for Growth in Cyber Crimes

- Rapid technology growth
- Easy availability of hacker tools
- Anonymity
- Cut-and-past programming technology
- Communication speed
- High degree of internetworking
- Increasing dependency on computers



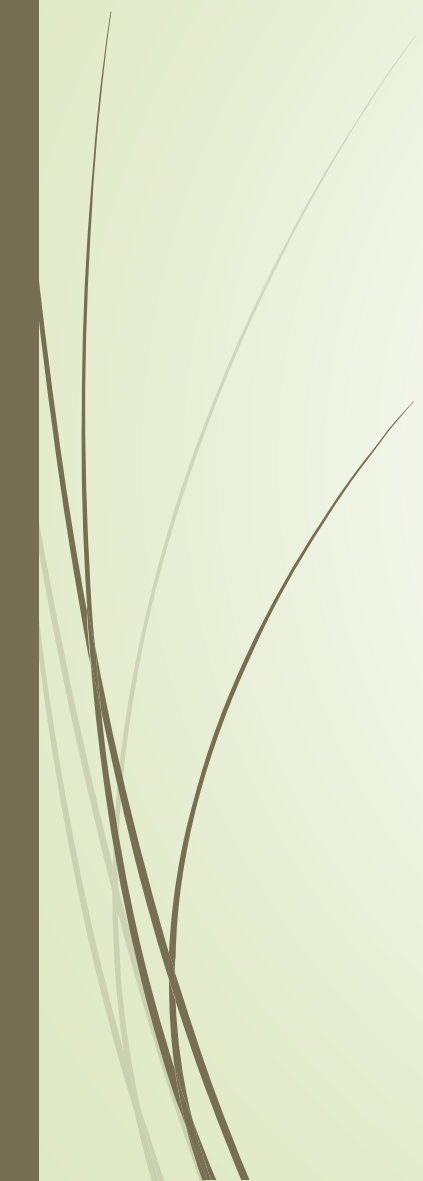
# How Much Does It Cost? Who Knows?

- Difficult to quantify the number of attacks
- No baseline
- Not reporting insider attacks
- Lack of cooperation between emergency and computer crime reporting centers

Continued ➤




# How Much Does It Cost? Who Knows?

- Unpredictable types of attacks
  - Virus mutation
  - Not enough trained system administrators
  - Primitive monitoring technology
- 



# Social and Ethical Consequences

- Psychological effects – hate and bigotry
  - Acceptance of the norm and resulting moral decay
  - Loss of privacy
  - Trust
  - Others?
- 





# Educating the Computer User

Just as we did with the computer criminal, we need to educate the user to be aware of possible sources of computer crime and what to do if and when one becomes a victim of a computer crime



# Questions

Are we prepared for a cyber attack?

What are the consequences?

## Chapter 10

New Frontiers for Ethical Considerations:  
Artificial Intelligence and Virtual Reality

# Artificial Intelligence

- AI – is a field of learning that emulates human intelligence
- Advances in human intelligence:
  - Machine intelligence has led to Robotics
  - Space exploration
  - Medicine
  - Advanced research

# Intelligent Agents

- Personal assistants
- Meeting scheduling
- Email handling
- Filtering
- Entertainment

## Weizerburm Theory

“it is immoral to use a computer system to replace human functions involving interpersonal respect, understanding and love”

# Question

- Will human beings let intelligent “creatures” keep on getting more and more intelligent even though they are aware the ultimate end result would be to surpass human intelligence?

# Question

- ▶ How much power and autonomy should we give these creatures, and will these agents eventually take away human autonomy and consequently take control of human destiny?



# Two School of Thought

- All AI activities are research gone wrong or “mad scientist”
- AI is very beneficial to humanity

# Artificial Intelligence...

- Limitations of AI:
  - Lack of credible science safeguards
  - Fear of a superhuman
  - Abdication of individual responsibilities
- AI and ethics:
  - AI agents and user responsibilities
  - User accountability

# Cyberspace

## ➤ The Internet:

- Opened up new frontiers in almost all spheres of human life
- The WWW revolutionarized indexing and delivery of information
- E-commerce transformed global economies, changed lives.

# Virtual Reality

- VR – is a stimulation of a real or imaginary phenomena in three-dimensional environments
- Is revolutionalizing the study of science
- Ethics in Virtual Reality:
  - Lack of being in control
  - Safety and security of users
  - Human-agent interactions
  - Intentions of the actor
  - Accountability of the actor
  - Responsibility of the actor
  - Psychological effects on the actor and community

# Point of discussion.

- The Future of AI: How Artificial Intelligence Will Change the World
- Why is Artificial Intelligence important?



# Virtualization



# Virtualization

- Virtualization is a process through which one can create something that is there in effect and performance but, not there—that is, virtual. It is a physical abstraction of reality, real phenomena such as a company's computing resources like storage, network servers, memory, and others.



# Different Aspects of Virtualization

- The immersion aspects of virtualization process of its participants and the autonomy accorded to them give the virtualization process a wide range of the different aspects of real life that can be virtualized. These may include gaming, computing, and life itself.





# Virtualization of Computing Resources

- VMware.com, a software developer and a global leader in the computing virtualization market, defines virtualization of computing resources as a process in which software creates virtual machines (VMs), including a virtual machine monitor called hypervisor, that allocate hardware resources dynamically and transparently so that multiple operating systems, called guest operating systems, can run concurrently on a single physical computer without even knowing it.



# History of Computing Virtualization

- The history of computing virtualization is as amazing as the concept itself. Since computers of the 1960s could do only one task at a time and depended on human operators, increasing system performance was bottlenecked at two points: at job submission and at the computation stage. One way to improve the submission stage was to use a batch, where jobs were submitted into a queue and the system picked them from there, thus reducing human intervention and errors.



# Computing Virtualization Terminologies

- **Host CPU/Guest CPU** - When a virtualization software is creating a new VM upon which the virtual OS runs, it creates a virtual CPU, known as a guest CPU, best on the time slices allowed on the underlying physical, now called a host CPU on the host machine.
- **Host OS/Guest OS** - During the virtualization process, the virtualization software creates complete VMs based on the underlying physical machine. These VMs have all the functionalities of the underlying physical/host machine.
- **Hypervisor** - A hypervisor, as a virtual machine manager, is a software program that allows multiple operating systems to share a single physical hardware host.
- **Emulation** - An emulation is a process of making an exact copy of all the functionalities of an entity like a hardware resource of a computing system, like a CPU and operating system, I/O devices and drivers, and others.

# Types of Computing System Virtualization

- **Platform Virtualization** - Platform virtualization is the use of server hardware by the virtualization software to host multiple VMs as guest VMs
- **Workstation Virtualization** - This is also referred to as desktop virtualization. It is the abstraction of the traditional workstation with its operating system, by moving it to a remote server system, accessed via a smart or dumb terminal.
- **Server Virtualization** - Server virtualization is the process of having a physical server runs a server-based virtualization software called a hypervisor to divide the physical server into multiple isolated virtual environments
- **Network Virtualization** - Like storage virtualization, network virtualization pools the resources, like files, folders, storage, and I/O devices, of separate and different networks into one network.
- **Storage Virtualization** - The process of pooling together of resources of many different network storage devices such as hard drives to create what looks like one big storage managed from a single console is referred to as storage virtualization.
- **Application Virtualization** - In application virtualization, the software package allows the bytecode of an application package to be portably run on many different computer architectures and operating systems.

# The Benefits of Computing Virtualization


- Reduction of Server Sprawl
- Conservation of Energy
- Reduced IT Management Costs
- Better Disaster Recovery Management
- Software Development Testing and Verification
- Isolation of Legacy Applications
- Cross-Platform Support
- Minimizing Hardware Costs
- Faster Server Provisioning
- Better Load Balancing
- Reduce the Data Center Footprint
- Increase Uptime
- Extend the Life of Older Applications



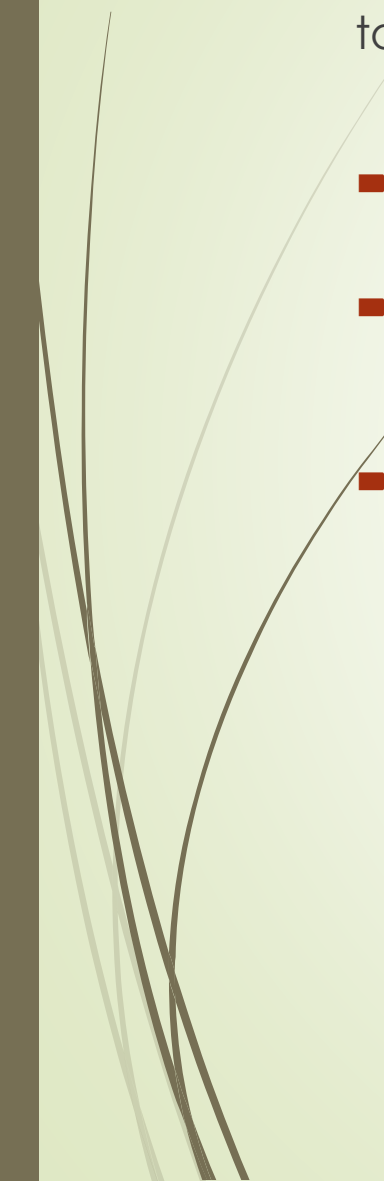


# Virtualization and Ethics

- To many, the image evoked by the word frontier rekindles a sense of free adventurism, unregulated and pure. The virtualization environment brings the user closer to this romantic vision. But illusion is illusion, and it brings forth two major social and ethical themes.
  - The Emotional Relationship and the Feeling of Being in Control
  - Safety and Security
  - Human-Agent Interaction
  - The Intentions of the Creator



This responsibility should be based on sound ethical and moral principles relating to VR. Collins Beardon outlines three traditional principles by famous philosophers quite relevant to VR:

- One should not do things with computers for which one should not accept responsibility without computers.
  - Continuous exposure to VR will impoverish those aspects of life that determine social development, interpersonal insights, and emotional judgment.
  - Computers should be used in applications where computation and symbol manipulation are adequate ways of dealing with reality.
- 



# Cyberspace and Cyberbullying





# Cyberspace and the Concepts of Telepresence and Immersion

- Cyberspace is a global artificial reality environment based on a global mesh of interconnected computer networks. This mesh allows and makes it possible for anyone using a point-of-entry device like a computer, smartphone, or any other Internet-enabled electronic device to reach anyone else, with the potential to access the mesh, through a one-on-one, one-to-many, and many-to-one communication capabilities or through broadcasting via the World Wide Web.
- Cyberspace, because of its immense capabilities and global reach, is used either in real time or otherwise simultaneously by millions if not billions of people around the world.



# Securing Cyberspace



- Keeping cyberspace users secure is a daunting job that requires advanced detection techniques and prevention methods. Both the detection and prevention techniques are changing very fast.
- A detection system deployed around a computer system, or a computer network is a 24-h monitoring system to alert the owner or system manager whenever something unusual—something with a nonnormal pattern, different from the usual pattern of life in and around the system—occurs.



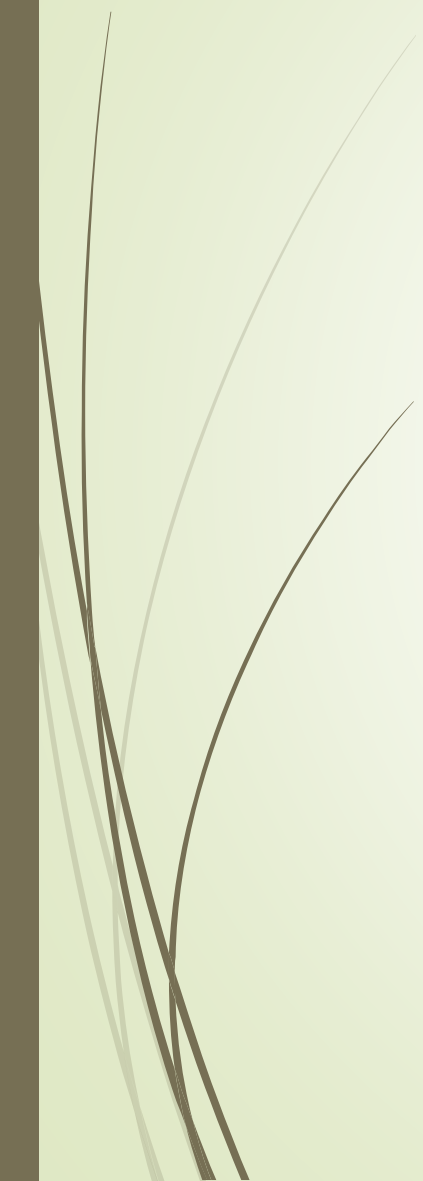
# Cyberspace Forensics



- An investigative process that studies the computer network environments in cyberspace to provide information on all issues of a healthy working network. It seeks to capture network information on:
  - Network traffic and the changing traffic patterns.
  - The trends of individual network packet traffic.
  - The density of traffic at specific times of the day as traffic patterns is traced; their sources and entry points in the network must be noted.

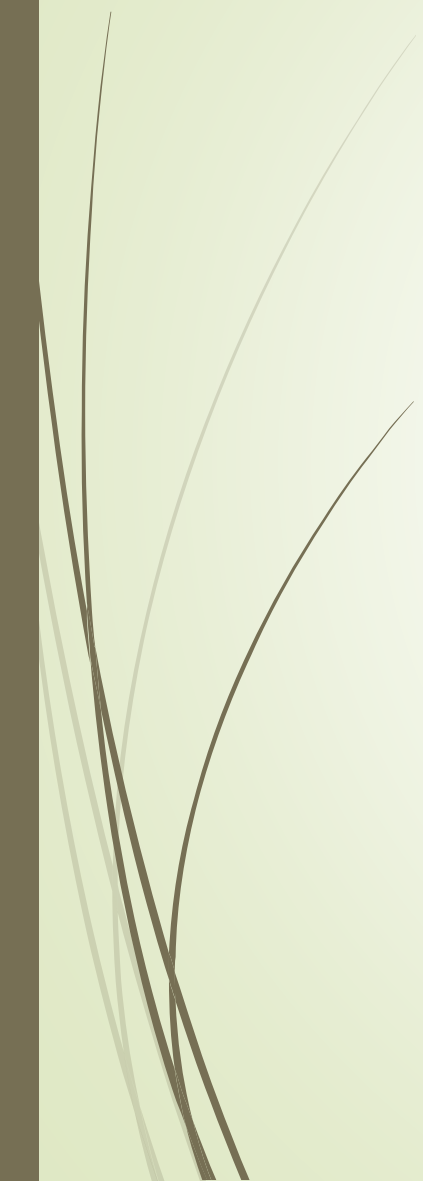


# Intrusion Detection in Cyberspace

- A new technology because software used in all cyber-attacks often leaves a characteristic signature. This signature is used by the detection software, and the information gathered is used to determine the nature of the attack
- 



# Vulnerability Scanning in Cyberspace

- System and network scanning for the vulnerability is an automated process where a scanning program sends network traffic to all computers or selected computers in the network and expects receiving return traffic that will indicate whether those computers have known vulnerabilities.
- 

# Cyberspace Systems Survivability

- In the new networked computer environments, system survivability is the ability of a computing system, whether networked or not, to provide essential services in the presence of attacks and failures and gracefully recover full services in a timely manner.
- System survivability requirements that are based on distributed services should include the following:
  - Distributed logic
  - Distributed code
  - Distributed hardware
  - Shared communications
  - Routing infrastructure
  - Diminished trust
  - Lack of unified administrative control.
- Intrusion requirements to demonstrate the correct performance of essential and nonessential system services as well as the survivability of essential services during the intrusion.




# Cyberspace Systems Survivability

- Development requirements to make sure that there are sound development and testing practices during the development of the system, especially software systems.
- Operations requirements to define channels of communicating survivability policies, monitoring system use, responding to intrusions, and evolving system functions as needed to ensure survivability as usage environments and intrusion patterns change over time.
- Evolution requirements to be able to quickly respond to user requirements for new functions and be able to determine and counter increasing intruder knowledge of system behavior and structure.



# Intellectual Property Rights in Cyberspace

- Anonymity
  - Internet paradox
  - Browsing rights
  - Lack of control on cyberspace services
  - Distributed liability
- 





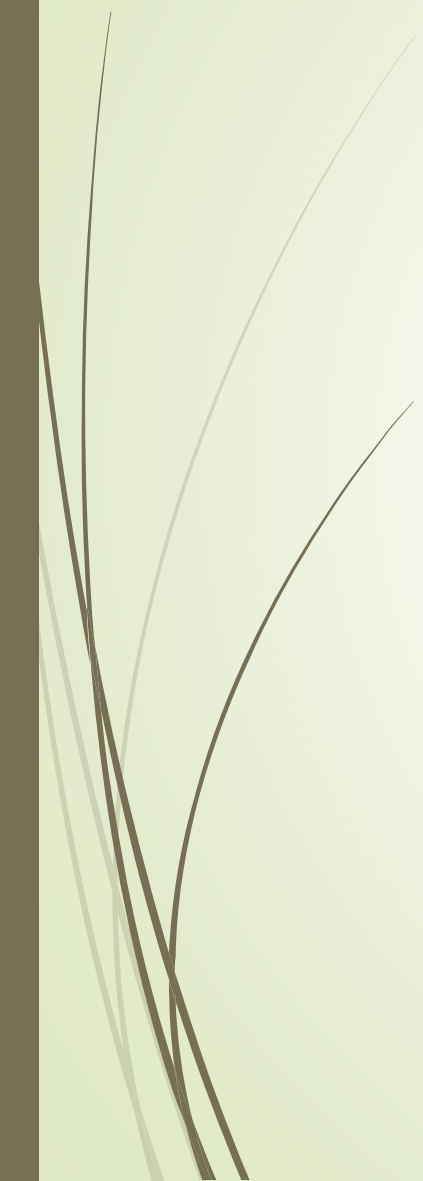
# Cyberbullying



- Actions that use information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group that is intended to harm another or others.
- Use of communication technologies for the intention of harming another person.
- Use of Internet service and mobile technologies such as Web pages and discussion groups as well as instant messaging or SMS text messaging with the intention of harming another person.



# Cyberstalking

- Stalking, a cousin of bullying, is defined as an unwanted and/or obsessive attention given to an individual or group by a perpetrator or perpetrators. Cyberstalking, a cousin of cyberbullying then, is digital stalking, usually using online media.
- 



# Cyber Harassment

- To harass is to annoy continuously and persistently someone: to create an unpleasant or hostile environment for an individual, especially by uninvited and unwelcome verbal or physical conduct and to make repeated attacks against a victim.



# Types of Cyberbullying

- Harassment
  - Flaming
  - Exclusion
  - Outing
  - Masquerading
- 



# Areas of Society Most Affected by Cyberbullying

- Schools
  - Cyberbullying in the Workplace
- 

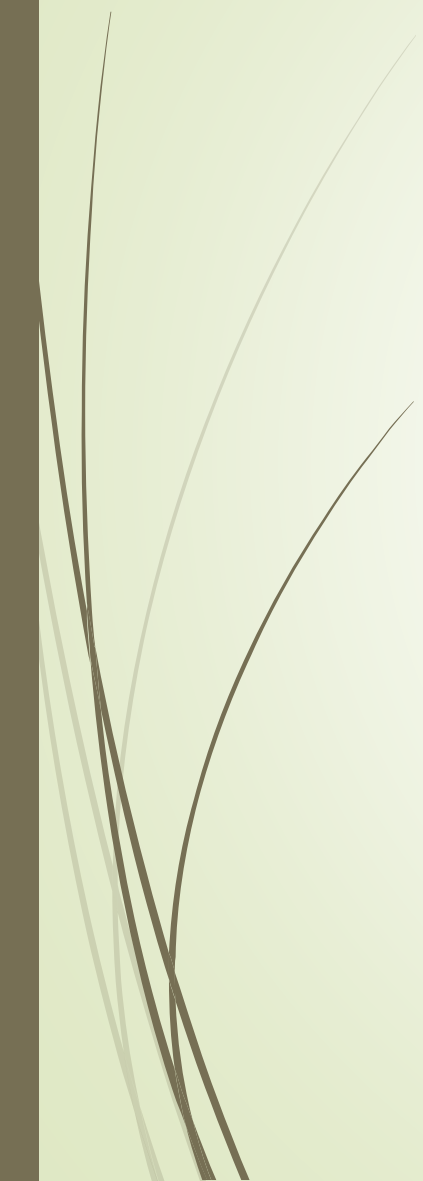


# Effects of Cyberbullying

- Statistics from different countries are showing that the vice is growing, hampered only by massive awareness campaigns, hence affecting more and more people. Like all forms of bullying, cyberbullying affects everyone, the bully, the victim, and the bystanders, though in different ways.

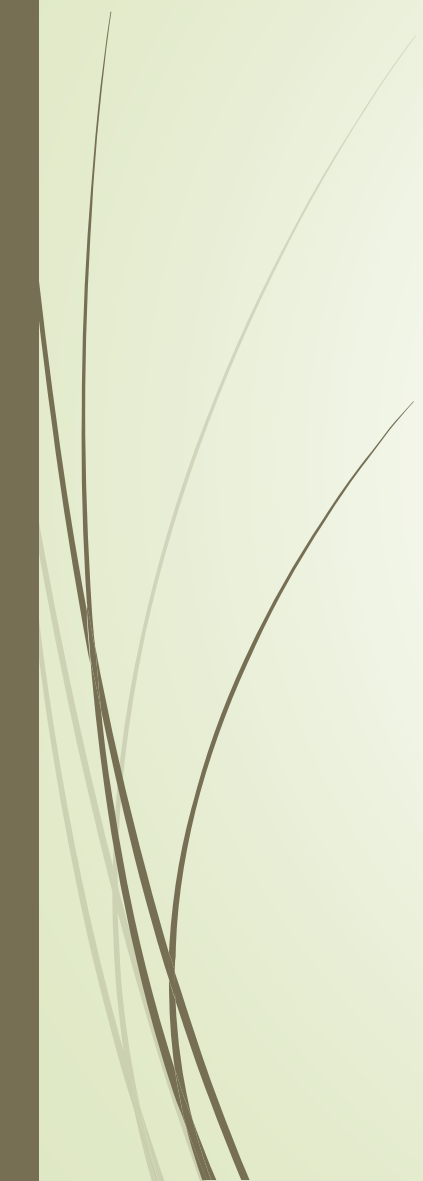


# Kids Who are Bullied

- Depression and anxiety, increased feelings of sadness and loneliness, changes in sleep and eating patterns, and loss of interest in activities they used to enjoy.
  - Health complaints
  - Decreased academic achievement—GPA and standardized test scores—and school participation.
- 



# Kids Who Bully Others

- Abuse alcohol and other drugs in adolescence and as adults
  - Get into fights, vandalize property, and drop out of school
  - Engage in early sexual activity
  - Have criminal convictions and traffic citations as adults
  - Be abusive toward their romantic partners, spouses, or children as adults.
- 





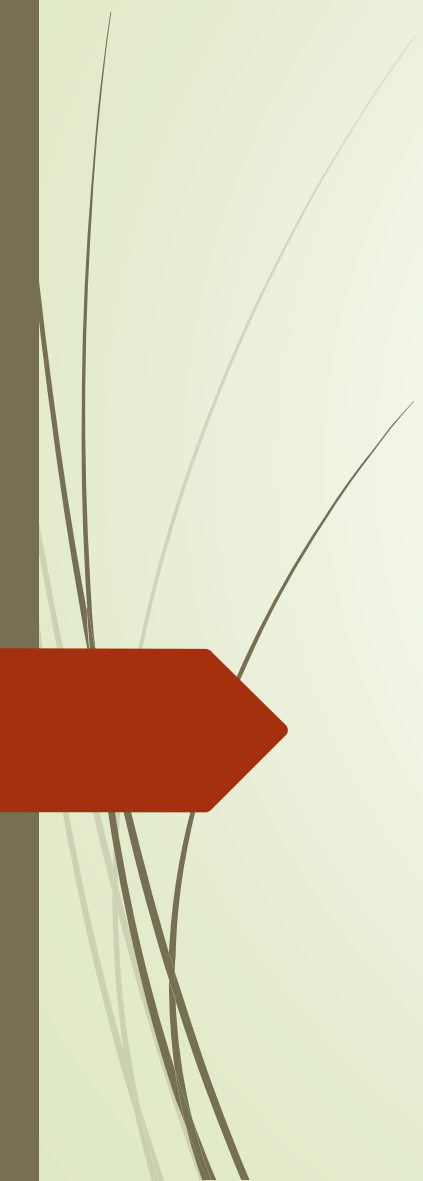
# Bystanders

- Have increased use of tobacco, alcohol, or other drugs
- Have increased mental health problems, including depression and anxiety
- Miss or skip school.



# Dealing with Cyberbullying

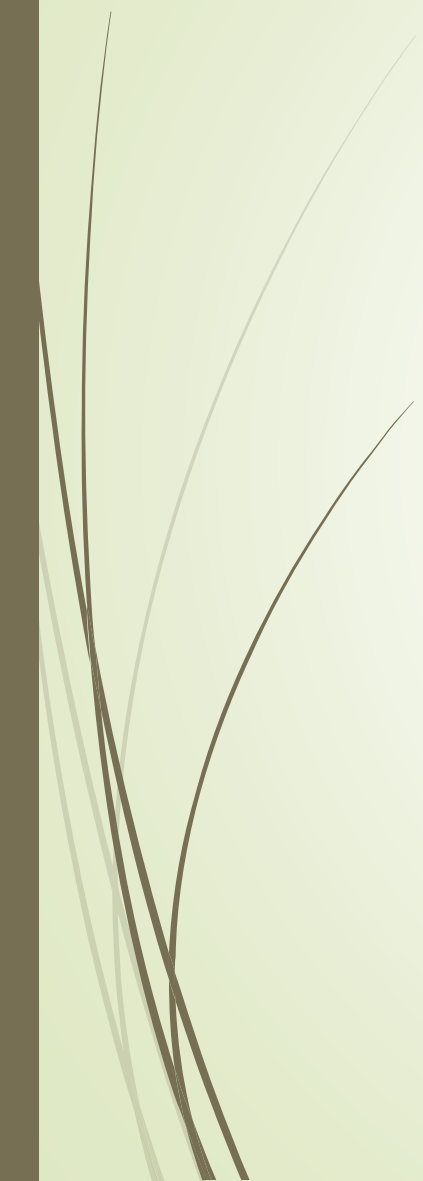
- Cyberbullying comes in many forms including pretense, masquerading, hacking into the victim's online account, invading, and bracketing of social media, and a lot more others.
- However, since most of its effects are based on psychological, emotional, and physical stress, there are underlying and broad approaches that we can take that will cover the major source of cyberbullying and will deal with the different reactions to its effects.
  - Awareness
  - Legislations
  - Community Support



# Internet of Things (IoT): Growth, Challenges, and Security



# Learning Objectives

- 1. Understand the nature and the technology driving the Internet of Things (IoT).
  - 2. Learn about the changing landscape of evasive technology as it comes to the home front.
  - 3. Learn about the security issues surrounding the advent of smart technology in the home
- 



# Introduction

- The Internet of Things (IoT)
- Initially proposed by Kevin Ashton in 1998
- Back then, the idea was often called “embedded internet” or “pervasive computing”.



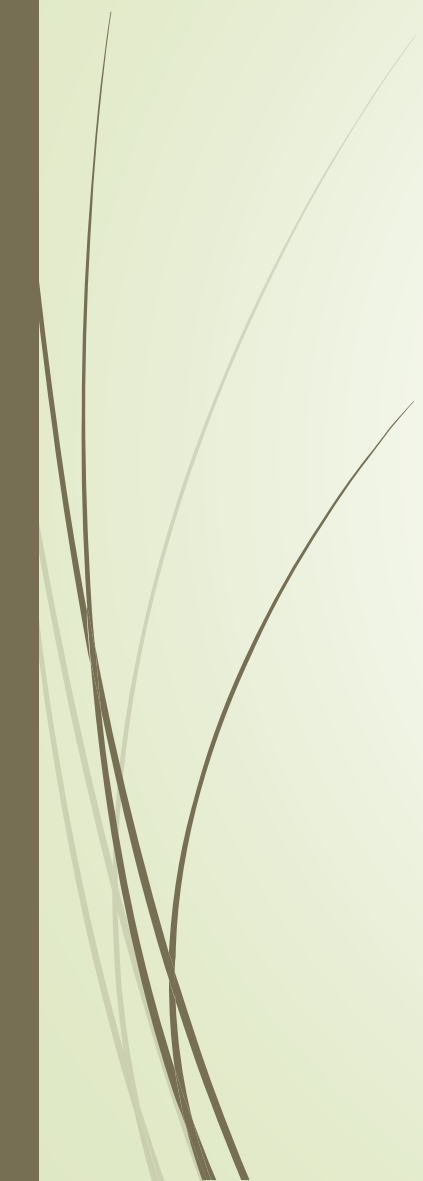
# Internet of Things



- Gubbia et al. - A smart environment that is made up of an interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications
- Some well-known examples for Internet of Things applications today are:
  - Wearable devices/fitness trackers (e.g., Jawbone Up, Fitbit, Pebble)
  - Home Automation (Examples: Nest, 4Control, Lix)
  - Industrial asset monitoring (GE, AGT Intl.)
  - Smart energy meters



# IoT cntd.

- Morgan also sees it an environmental ecosystem that “allows for virtually endless opportunities and connections to take place, many of which we cannot even think of or fully understand the impact of today.”
  - With billions of devices being connected together, what can people do to make sure that their information stays secure?
- 



# Overview and Growth of Internet of Things

- ▶ With the expected continued growth of the Internet, there is unanimous expectation of an enormous growth of the Internet of Things.
- ▶ John Greenough and Jonathan Camhi both of Business Intelligence (BI) look at IoT in terms of business growth predicting that IoT is the next Industrial Revolution or the Next Internet

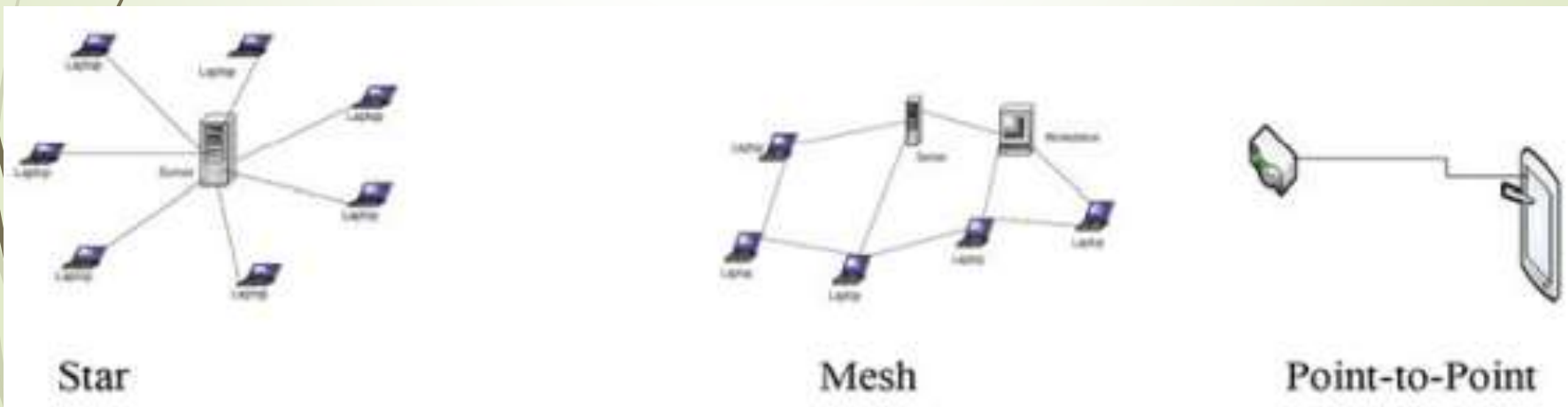




# Architecture and Networking of IoT

- For the IoT ecosystem to function and support intended applications and accommodate the heterogeneity of devices and applications in the ecosystem, the IoT had to adopt the open standards of TCP/IP protocol suite.
- However, the open standards of TCP/IP protocol suite were initially developed for the wired global Internet several decades ago, as the networking solution.

- The networking technology standard currently being used in the IoT fall into three categories:
- (i) point-to-point, for example, an end device to a gateway;
- (ii) star—with a gateway connected to several end-devices by one hop links, and
- (iii) a mesh—with one or more gateways connecting to several end devices and one or more hop links away as demonstrated



# IoT Governance, Privacy, and Security Challenges

- Governance and Privacy Concerns
- As the IoT grows, it presents us with several challenges including global governance, individual privacy, ethics, and of course security. These are the most critical issues in the growth of IoT.
- Globally, governance is mostly understood to refer to the rules, processes, and behavior that affect the way in which powers are exercised, particularly as regards openness, participation, accountability, effectiveness, and coherence - *five principles of good governance*
- Have been already applied to the Internet for specific aspects, and there are already organizations like IETF, ICANN, RIRs, ISOC, IEEE, IGF, W3C, which are each responsible and dealing with every specific area
- But currently, this is not the case with the IoT.

# Security Challenges

- 
- 
- Security is critical to IoT applications due to their close interaction with the physical world.
  - Insufficient authentication/authorization
  - Lack of transport encryption
  - Insecure web/mobile interface



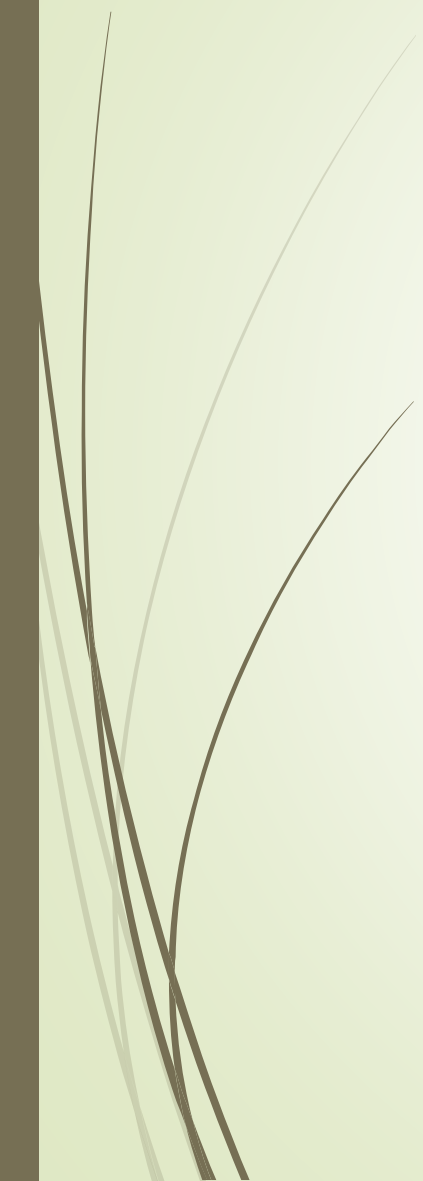
# Autonomy



- High heterogeneity and complexity and lack of dynamic and scalable management schemes in the IoT due to its plethora of sometimes constrained devices, with different data communication capabilities, create a challenge in the manual maintenance of a large number of devices becomes inefficient and demands the presence of intelligent and dynamic management schemes.
- Self-managing systems



# Computational Constraints

- ▶ Low-level devices on the fringes can be of limited power sometimes of less than 10 kBs of RAM, which is sometimes orders of magnitude lower than an ordinary desktop computer with GIGs of RAM.
- 



# Trust Relationships



- We have already seen and discussed the connectivity and heterogeneity of the IoT.
- We know that IoT connects to billions of devices with high connectivity complexities and challenges.
- These human-IoT relationships create a relationship-trust mesh in the IOT which result into a multitude of questions of a social, ethical, and legal nature. Questions such as
  - What threats are caused by delegating fundamental aspects of humanness?
  - How can we preserve the human capability to freely act and make choices in the IoT?
- A lot more issues are and will continue to be raised as the IoT grows.





Thank you!