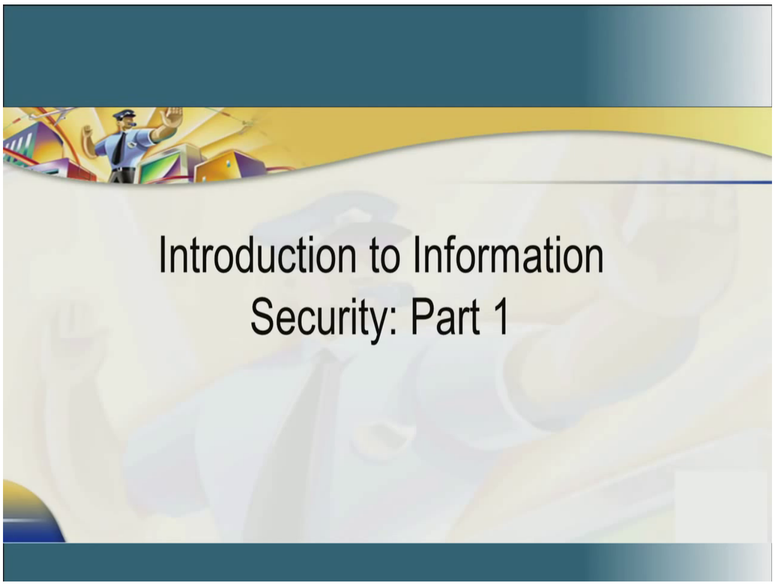
Introduction to Information Security

Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 02
Introduction to Information Security System: Part 1

Brothers and sisters, we will now see module one of the course [FT] part [FT]

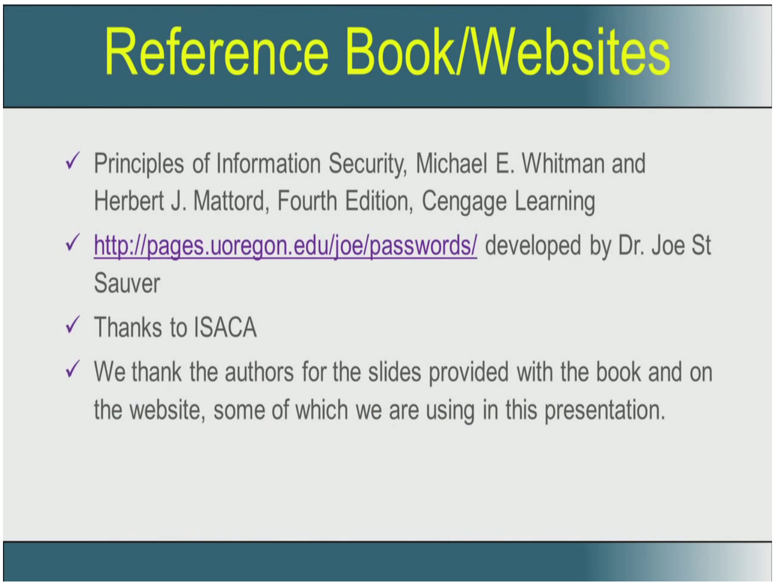
(Refer Slide Time: 00:53)



Introduction to Information Security: Part 1

So, this is the module 1 of the introduction to information security course.

(Refer Slide Time: 01:05)

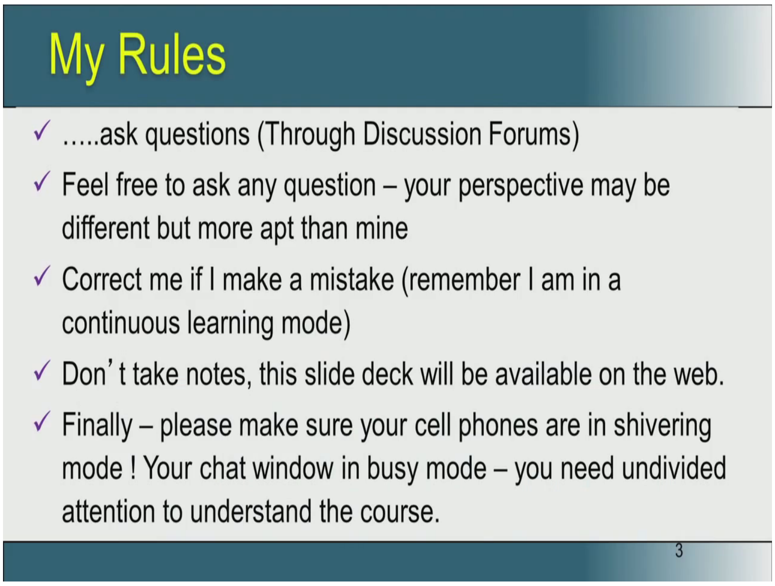


Reference Book/Websites

- ✓ Principles of Information Security, Michael E. Whitman and Herbert J. Mattord, Fourth Edition, Cengage Learning
- ✓ http://pages.uoregon.edu/joe/passwords/ developed by Dr. Joe St Sauver
- ✓ Thanks to ISACA
- ✓ We thank the authors for the slides provided with the book and on the website, some of which we are using in this presentation.

So, these are the reference books and websites. Principles of information security by Whitman et al; and then, we have also used some materials from the university of Oregon; and, thanks to ISACA for the COBIT. And, we thank all the authors for their slides provided with the book and also on the website; some of which we are using in this presentation.

(Refer Slide Time: 01:39)



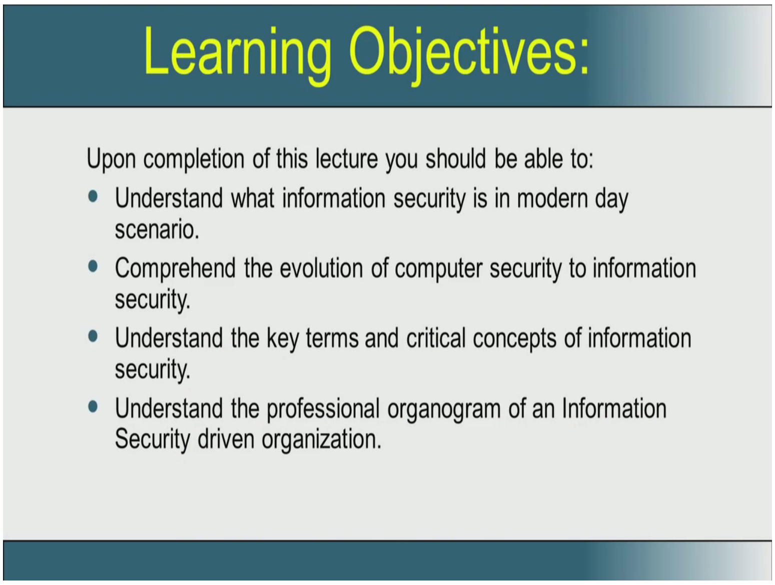
My Rules

- ✓ .....ask questions (Through Discussion Forums)
- ✓ Feel free to ask any question – your perspective may be different but more apt than mine
- ✓ Correct me if I make a mistake (remember I am in a continuous learning mode)
- ✓ Don’t take notes, this slide deck will be available on the web.
- ✓ Finally – please make sure your cell phones are in shivering mode ! Your chat window in busy mode – you need undivided attention to understand the course.

3

The rules of this course – you should ask questions through discussion forums and feel free to ask any question; your perspective may be different or more apt than mine. Correct me if I make a mistake; remember I am in a continuous learning mode. Do not take notes; this slide deck will be available on the web. And finally, please make sure your cell phones are in shivering mode; your chat window in busy mode, so that you give undivided attention to understand the course.

(Refer Slide Time: 02:22)



Learning Objectives:

Upon completion of this lecture you should be able to:

- Understand what information security is in modern day scenario.
- Comprehend the evolution of computer security to information security.
- Understand the key terms and critical concepts of information security.
- Understand the professional organogram of an Information Security driven organization.

Now, we just want to reiterate the learning objectives. Upon completion of this lecture,1) you should be able to understand what information security in the modern day context.

2) And also, in early days, it was called computer security; how it evolved into information security.

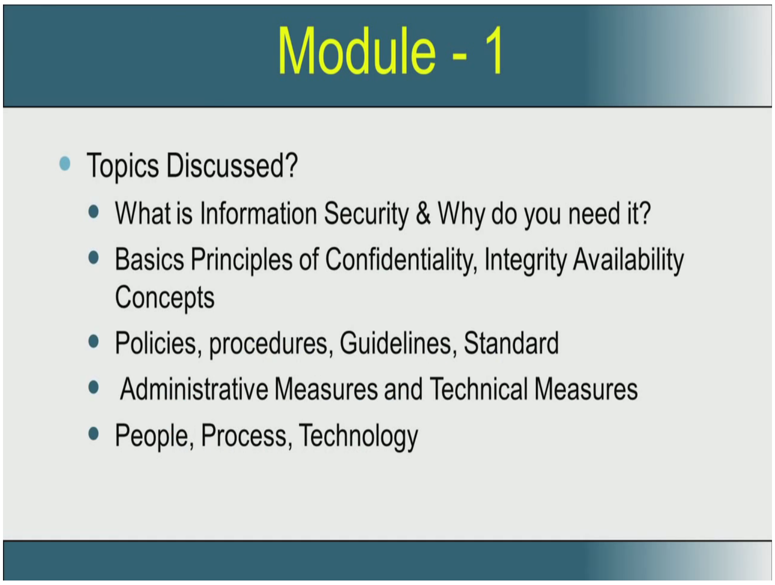
3) Understand many key terms and critical concepts of information security of modern day.

4) And, most importantly, understand the way an organization, which is IT driven – the IT management of an organization; what would be the organogram of that organization; who would be responsible for doing what.

All these four objectives are very important to appreciate information security. And, each of these objectives will have some subtle concepts. I hope many of you know Bertrand Russell.

So, Bertrand Russell came out with a small statement – very very small; he is very much well known for very small jargons or very small statements; is that, obviousness is the enemy of correctness. Many of the things that we will be teaching in this course or we will be debating in this course are obvious things, which are not followed. And, because of that, we land up with issues. So, we will be teaching you the obvious things in… And, what it means if you neglect those things in the global scenario. So, this is what would be our learning objectives.

(Refer Slide Time: 04:04)



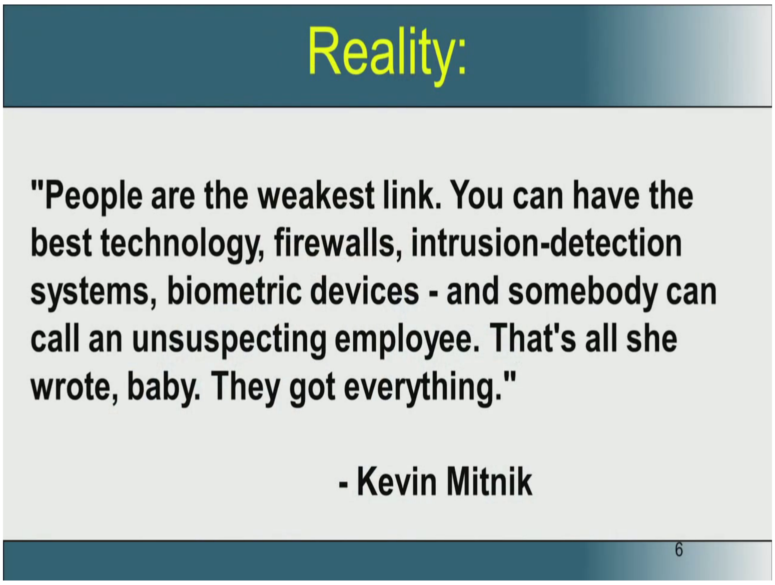
Module - 1

- Topics Discussed?
  - What is Information Security & Why do you need it?
  - Basics Principles of Confidentiality, Integrity Availability Concepts
  - Policies, procedures, Guidelines, Standard
  - Administrative Measures and Technical Measures
  - People, Process, Technology

This course as mentioned earlier has six modules. This is sub-module of module one. And, what we will be discussing in the entire module one would be what is information security; why do you need it; then, CIA is a very very important term in information security; it basically talks about confidentiality, integrity and availability. And, to bring this confidentiality, integrity and availability into the information security system, there are lot of things that need to be done. And, what you see in the three bullet points that follow are those that are necessary to build in confidentiality, integrity and availability into a system. For example, policies, procedures, guidelines, standard from a security perspective; what are all the administrative measures and technical measures needed to enforce these three – the CIA, which are basically the foundations of information security or the goals of information security.

We also look at people, process and technology. People are the ones, who follow a process; and, these processes are implemented by technology. So, security should be addressed at the technology level and the process, which uses this technology, and the people who actually uses these processes. So, there is lot of disciplines and policies and procedures that need to be implemented at each one of these stages namely at the people level, at the process level and technology level. And, this module will talk deeply about that.

(Refer Slide Time: 06:02)



Reality:

"People are the weakest link. You can have the best technology, firewalls, intrusion-detection systems, biometric devices - and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything."

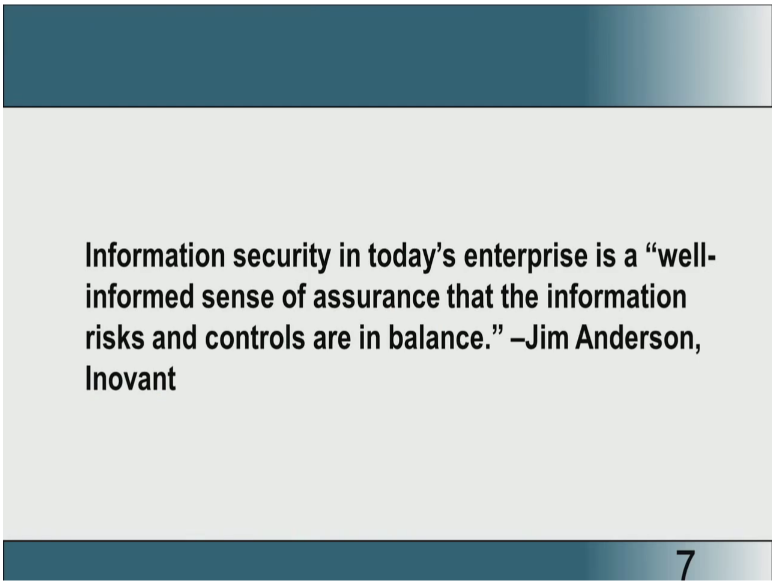
- Kevin Mitnik

6

Now, we are talking about Kevin Mitnik, who is actually a hacker; actually he was a cyber criminal and he was actually captured by – arrested by FBI. he came back and he became one of the world-renowned computer security expert. And, he came out with this very interesting statement; again, it is a very obvious statement – people are the weakest link. This particular phrase is known for decades now that, whenever there is a security lapse, majorly it is going to be because of people's unawareness about certain security measures.

Though we know that people are the weakest link, many many organizations do not actually invest in educating their people on the issues of security. So, this is Kevin Mitnik statement that you read on the screen. You can have the best technology, firewalls, intrusion-detection systems, biometric devices but, somebody can call an unsuspecting employee; but, all is that, if a small leak from the employee side, the human error or human carelessness – that could essentially kill your entire system. And, this is reality.

(Refer Slide Time: 07:50)

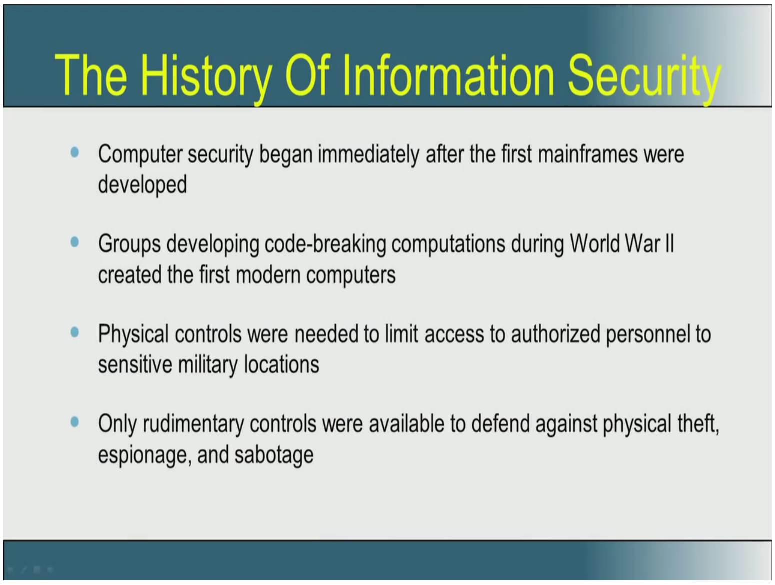


Information security in today's enterprise is a "well-informed sense of assurance that the information risks and controls are in balance." –Jim Anderson, Inovant

7

So, Jim Anderson came out with this very interesting definition of information security. Especially in today's enterprise world, where we have huge data centers, it is nothing but a well-informed sense of assurance that, the information risks and controls are in balance. For every risk, I have a way to control that. I take a risk; I have enough checks and balances to control it. So, if that assurance is given, then your information is actually secured. And, this is the definition that was given by Jim Anderson.

(Refer Slide Time: 08:25)

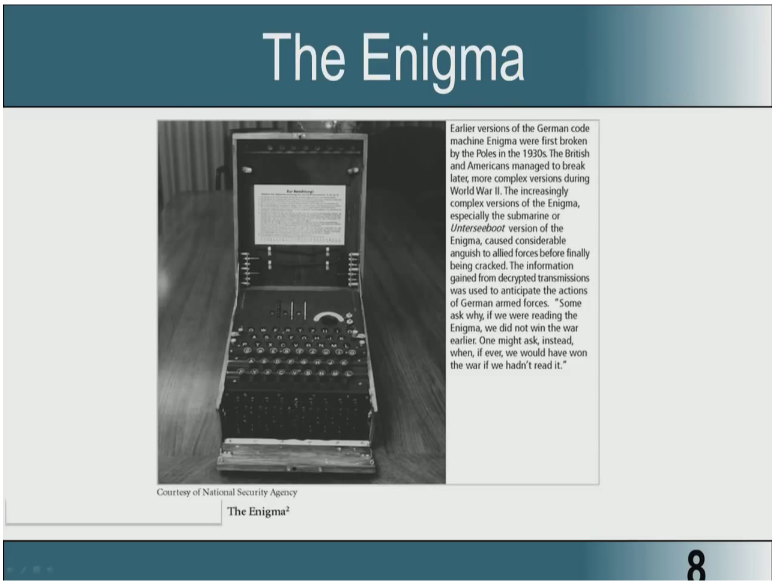


The History Of Information Security

- Computer security began immediately after the first mainframes were developed
- Groups developing code-breaking computations during World War II created the first modern computers
- Physical controls were needed to limit access to authorized personnel to sensitive military locations
- Only rudimentary controls were available to defend against physical theft, espionage, and sabotage

Now, we go into some history of information security, because we have to learn the lessons of the past to go and appreciate the present and the future. The computer security basically began; that time it was computer security; it began immediately after the first mainframes were developed. There were groups developing code breaking computations during World War 2, which created the first modern computers. Physical controls at that point to secure these computing machines, which actually stored some information, which is very sensitive; there were no network, but they had some lot of physical controls; essentially they want to physically secure these system; physically secure means it is should not be broken, manually damaged, it should not be taken out of a place, it should be under lock and key. So, the physical controls were needed to limit access to authorized persons to sensitive memory locations. And, only rudimentary controls were available to defend against this physical theft, espionage and sabotage

(Refer Slide Time: 09:43)



The Enigma

Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."

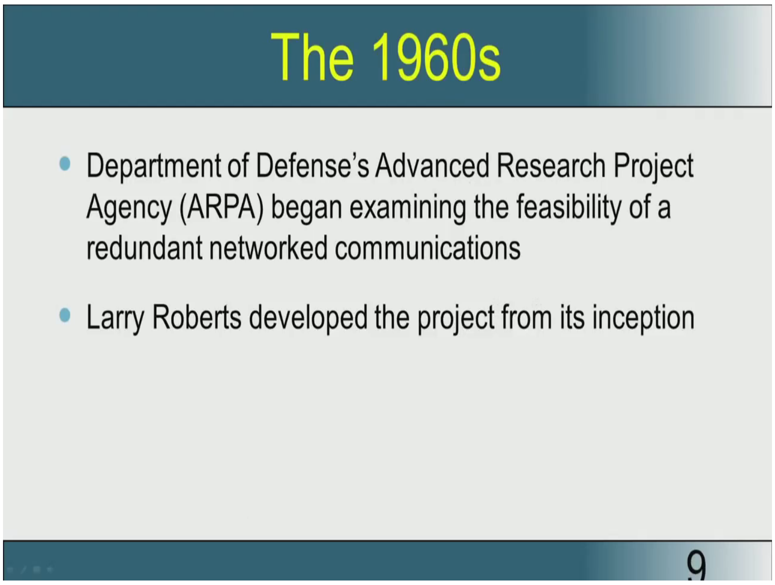
Courtesy of National Security Agency

The Enigma[2]

8

The enigma was the first German computer, which was actually used for sending coded message. So, here is a small description of enigma.

(Refer Slide Time: 09:56)



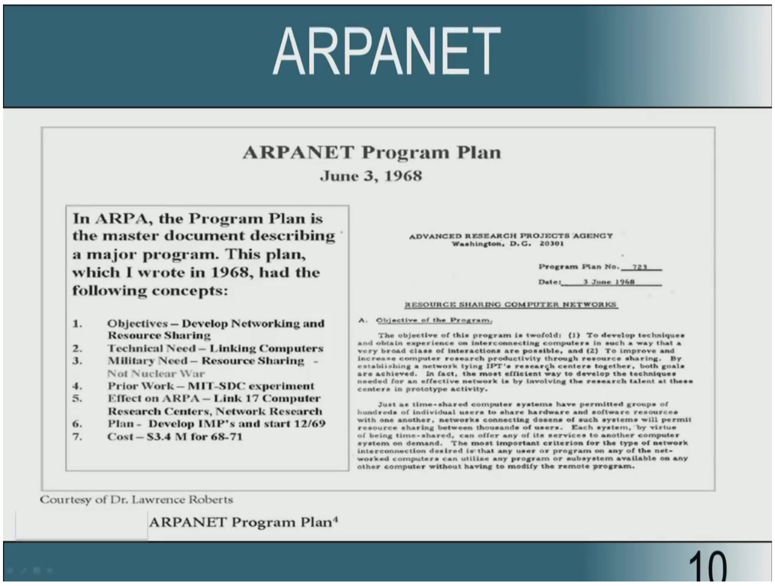
The 1960s

- Department of Defense's Advanced Research Project Agency (ARPA) began examining the feasibility of a redundant networked communications
- Larry Roberts developed the project from its inception

9

So, the entire notion of security started with the Advanced Research Project Agency – ARPA, which began examining the feasibility of a redundant networked communications. This was basically headed by Larry Roberts, who has developed the project from its inception. Larry Roberts is known for his contribution to the internet.

(Refer Slide Time: 10:24)



ARPANET

ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research
6. Plan - Develop IMP's and start 12/69
7. Cost – $3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

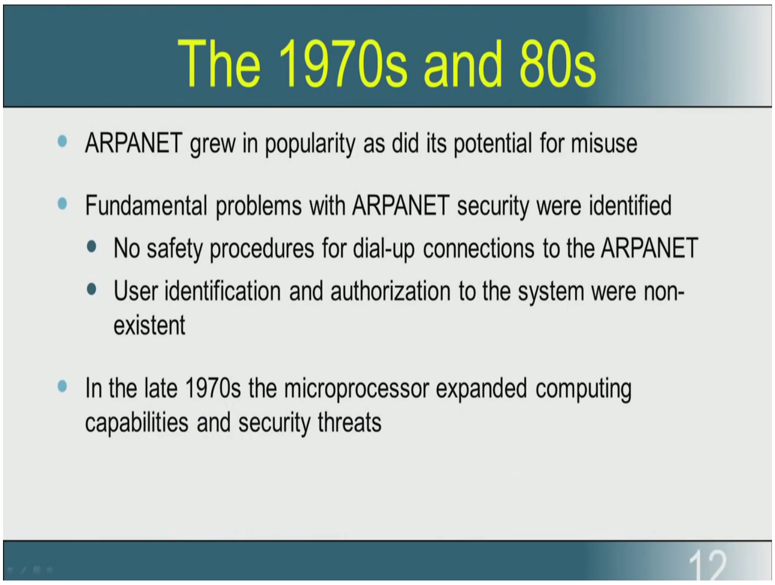
Courtesy of Dr. Lawrence Roberts

ARPANET Program Plan[4]

10

So, if you just look at the ARPANET program plan, the program plan was to basically share. If you carefully look into it, the objective was to develop networking and resource sharing. So,this is the first notion, where computers – where the resources available on multiple computers were shared.

(Refer Slide Time: 10:55)



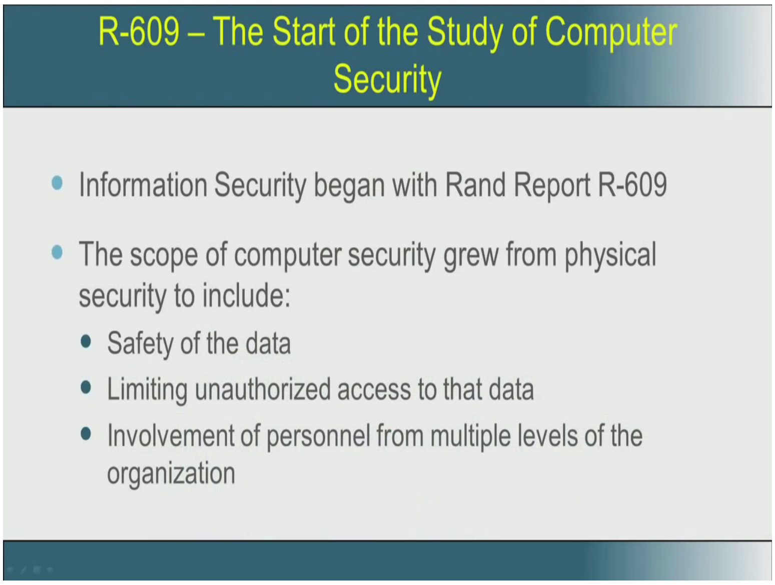
The 1970s and 80s

- ARPANET grew in popularity as did its potential for misuse
- Fundamental problems with ARPANET security were identified
  - No safety procedures for dial-up connections to the ARPANET
  - User identification and authorization to the system were non-existent
- In the late 1970s the microprocessor expanded computing capabilities and security threats

12

The ARPANET actually grew in popularity between the 70s and 80s as and so, were the potentials for misuse. The fundamental problem with ARPANET security were identified at that point. First and foremost, there was no safety procedures for dial-up connections; and, user identification and the authorization to the system were non-existent. So, in the late 1970s, the microprocessor expanded computing capabilities and security threats. So, the ARPANET, which was connecting these microprocessors, essentially brought in a notion of security, wherein somebody dials up a connection, is he an authentic person, is he authorized to dial up the connection. And, if somebody starts using the system, does he have the necessary identification and authorization. And, these are all something, which became issues with the ARPANET. And, this started as early as 1970s and 80s.

(Refer Slide Time: 12:07)

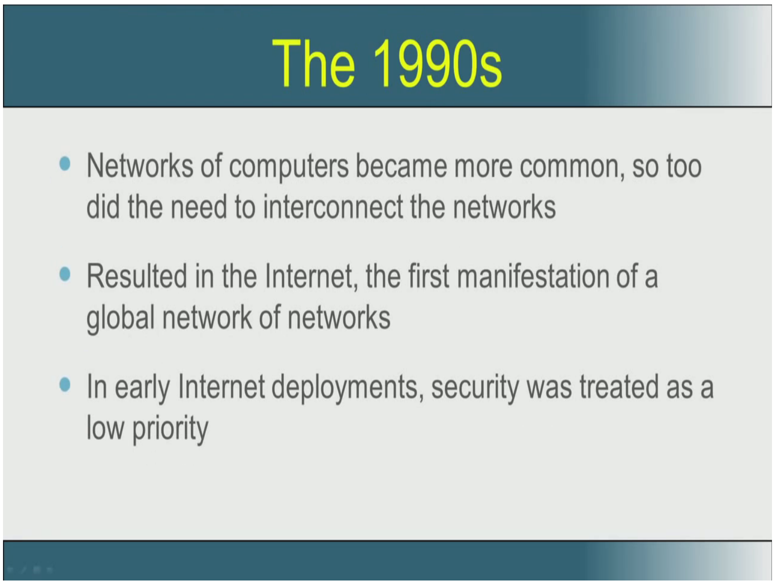


R-609 – The Start of the Study of Computer Security

- Information Security began with Rand Report R-609
- The scope of computer security grew from physical security to include:
  - Safety of the data
  - Limiting unauthorized access to that data
  - Involvement of personnel from multiple levels of the organization

Then, came out the R-609, which called the Rand Report, which formed the first report on computer security; the scope of computer security grew from physical security to include safety of the data, limiting unauthorized access to that data, and also involvement of personnel from multi levels of the organization and each having some specific authorization to use the computers with some level of security. So, if you look at what happened immediately after world war, was that, people were more interested in having the computer a lock and key; there was no notion of sharing the resources between computers; and, slowly came the ARPA, where people started sharing the systems; and, the moment they started sharing, then the issues of – is the correct fellow logging in to the system, is he dialing up, is he you using the data. So, more than the physical security of the computer, people started realizing even in the late 70s and early 80s that, the data in the computer can be stolen without physically accessing the computer. And that, the first notions of that was reflected in this Rand Report R-609.

(Refer Slide Time: 13:40)

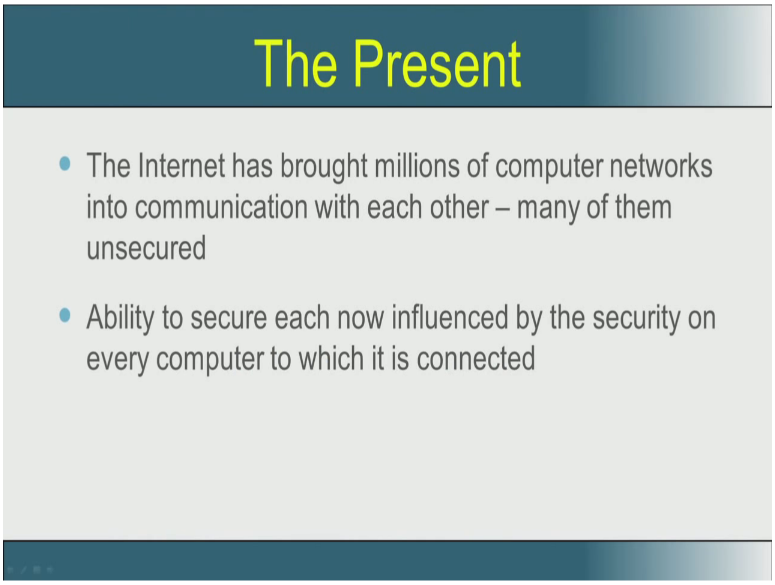


The 1990s

- Networks of computers became more common, so too did the need to interconnect the networks
- Resulted in the Internet, the first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority

In the 1990's, networks of computers became more common in the civilian sector. And so, so did the need to interconnect the networks. So, this resulted in a massive global network, which we today call as the internet. But, in those days still, in this large scale internet deployments, security unfortunately was treated as a low priority, because information that is stored in the computer can be sensitive, is a feel people which did not realize much during those time. They thought a network is basically used for sharing the resources and data also became something that someone can share. And, they wanted to share the data. But, there are going to be unshareable data within a system, is something a realization, which did not immediately occur to the people of the early 1990s. And, that is why, when you look at large scale internet deployments of those days, security was still given a low priority. At present, the internet has brought millions of computer networks into communication with each other and many of them are still unsecure.

(Refer Slide Time: 15:03)



The Present

- The Internet has brought millions of computer networks into communication with each other – many of them unsecured
- Ability to secure each now influenced by the security on every computer to which it is connected

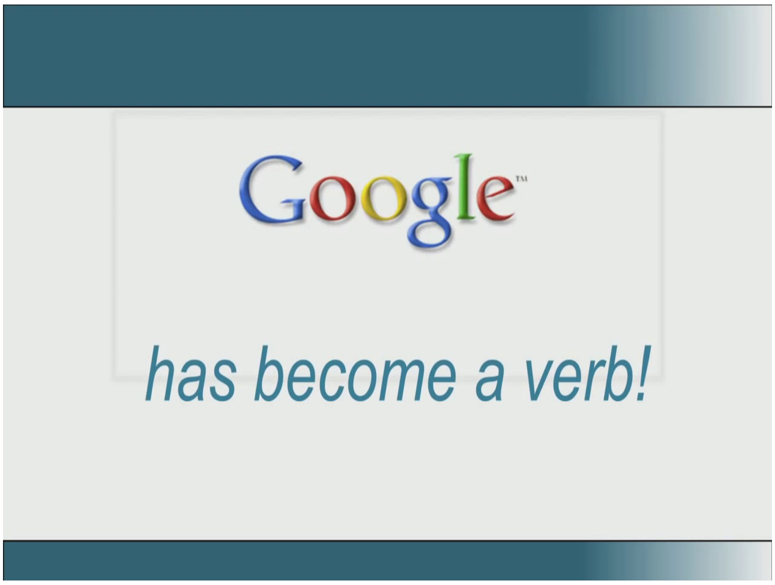
So, the ability to secure each, now, influenced by the security on every computer to which it is connected. As I mentioned in my welcome talk, a mistake done by one system, a vulnerability on one system can launch a massive denial of service attack on the entire LAN. And, this is something that one need to be careful. And so, the present system requires a large scale awareness and discipline in system usage to bring things under control.

(Refer Slide Time: 15:49)

Today’ s Environment

So, what is today's environment? look at all these – Wii, Skype, Ebay, You Tube, Blackberry, Facebook, Amazon, iPhone, LimeWire, iPod, Google.

(Refer Slide Time: 15:56)



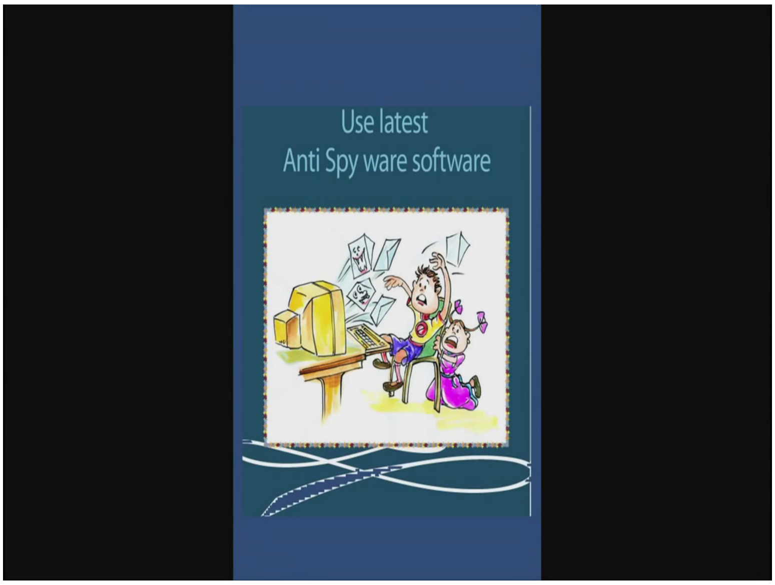
Google™

has become a verb!

The world Google has actually become a verb. Hey, they want something; google it. So, today, so many organizations have trillions and trillions of data and millions and millions of users communicating using this data; and that, everyone wants some level of security and privacy and confidentiality and availability. Now, the entire gamut of information security is to come out with a policy, a process, a procedure, a technology, which will go and enable a major secure feeling and assurance. It will give you a major secure assurance to this millions and millions of users about the privacy availability, confidentiality, integrity of the trillions of trillions of data that they are using.

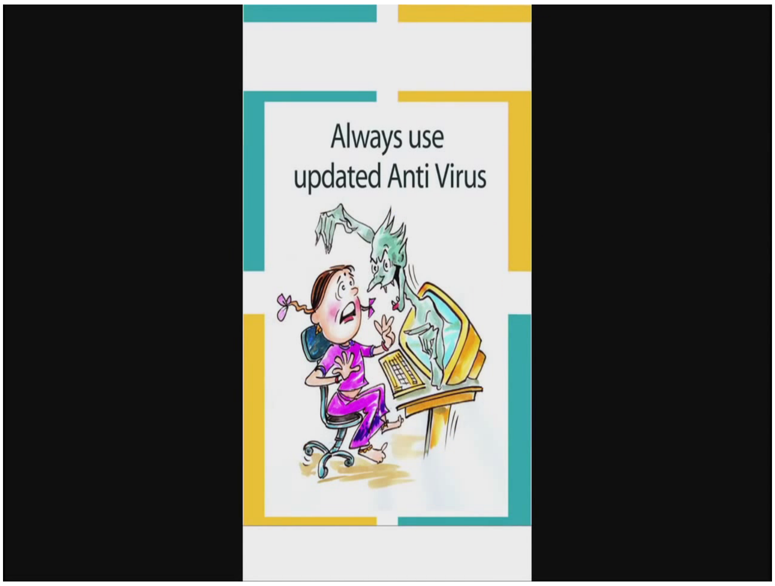
(Refer Slide Time: 17:03)

(Refer Slide Time: 17:06)



Use latest
Anti Spy ware software

(Refer Slide Time: 17:12)



Always use
updated Anti Virus

(Refer Slide Time: 17:17)

CAUTION with e-mail attachments

Don't Slip on the Clip!

Viruses, worms, spyware, and malicious code that can potentially harm your computer are frequently transmitted as e-mail attachments. Use caution when you receive e-mail messages with attached documents, images, programs, and other files. It is a good idea to scan attachments before opening them. Always scan these file types before opening them:

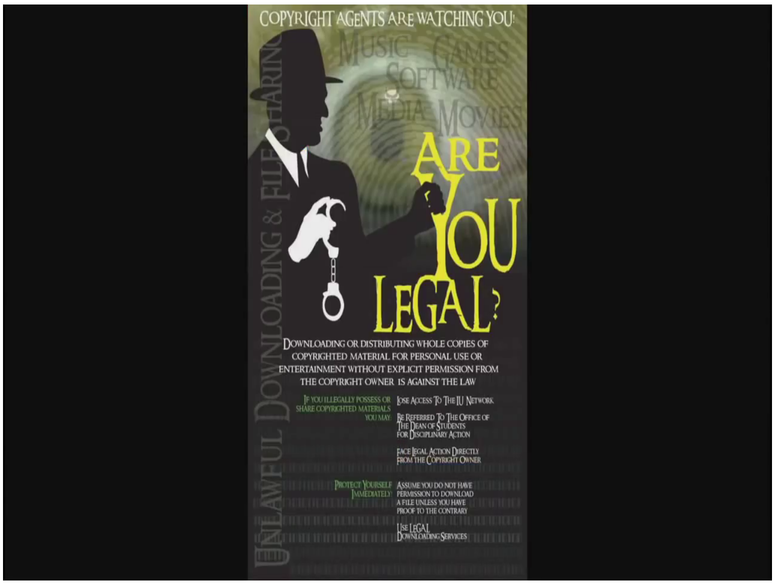
.bat .cmd .exe .inf .ins .js .msi .reg .shs .vbe .wsc .wsf .wsh

The list continues to grow due to new viruses constantly being discovered.

(Refer Slide Time: 17:23)

These days, Web sites, email attachments, and even links in
instant messages can expose you to all sorts of creatures from cyberspace.
Don't let attackers take over your computer.
Tip: Think before you click!
And be sure to scan any files with Antivirus software.

(Refer Slide Time: 17:29)



COPYRIGHT AGENTS ARE WATCHING YOU!
MUSIC GAMES
SOFTWARE
MEDIA MOVIES
ARE YOU LEGAL?
UNLAWFUL DOWNLOADING & FILE SHARING

DOWNLOADING OR DISTRIBUTING WHOLE COPIES OF COPYRIGHTED MATERIAL FOR PERSONAL USE OR ENTERTAINMENT WITHOUT EXPLICIT PERMISSION FROM THE COPYRIGHT OWNER IS AGAINST THE LAW

IF YOU ILLEGALLY POSSESS OR SHARE COPYRIGHTED MATERIALS YOU MAY:

LOSE ACCESS TO THE IU NETWORK

BE REFERRED TO THE OFFICE OF THE DEAN OF STUDENTS FOR DISCIPLINARY ACTION

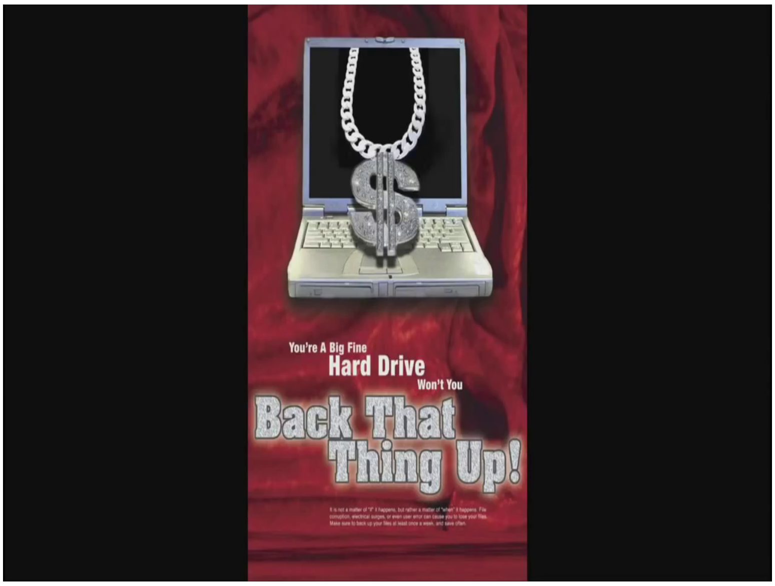
FACE LEGAL ACTION DIRECTLY FROM THE COPYRIGHT OWNER

PROTECT YOURSELF IMMEDIATELY!

ASSUME YOU DO NOT HAVE PERMISSION TO DOWNLOAD A FILE UNLESS YOU HAVE PROOF TO THE CONTRARY

USE LEGAL DOWNLOADING SERVICES

(Refer Slide Time: 17:34)



It is not a matter of "if" it happens, but rather a matter of "when" it happens. File corruption, electrical surges, or even user error can cause you to lose your files. Make sure to back up your files at least once a week, and save often.