Systems Security

Threats, Vulnerabilities, and Risks

Ed Crowley CISSP, NSA-IAM/IEM

Fall '05

1

What is Security?

- How can you tell if you have it?
- How much is enough?
- What are the basic security primitives?
  - How can you evaluate them?
- Who defines them?

2

System Security:
Threats, Risks, and Vulnerabilities

- Who/what wants to break into your computer?
- How do they break into computers?
  - Case Studies
- What can you do?

3

Outline

- Introduction
  - The Big Picture
    - Trends
    - Definitions
- Primitives, Vulnerabilities, Threats, and Risk
  - Attacks and Attackers
- Current Environment
  - Context
- Vulnerabilities
  - Systemic
- Threats
  - Social Engineering
  - Password Guessing
  - Buffer Overflow
  - System Flaws
  - Exploits
- Risk and Risk Management
  - Assessment and evaluation
- Security Models

4

Who am I?

- Certified Information System Security Professional (CISSP)
  - Information System Security Association (ISSA)
  - InfraGard
  - University of Houston Security Council
- NSA Certified INFOSEC Assessment Methodology (IAM), and INFOSEC Evaluation Methodology (IEM)
- Developed NSTISSC Certified IT Security Specialization
  - 4, three credit hour courses, UH, College of Technology
- Former IS Director, Network Admin, Web Master
  - www.tbe.uh.edu
  - ProfessorCrowley.com (coming soon!)
- CompTIA Security +, Net+, Cisco CCNA, Msoft MCSE …
- Graduate Military Police Academy, USARPAC Basic Sentry Dog School, former Security Clearance Holder

5

Trends, *One*

Over time:

- Cyber incidents are increasing in:
  - Number
  - Sophistication
  - Severity
  - Cost.
- The nation's economy is increasingly dependent on cyberspace
  - Unknown interdependencies and single points of failure.
  - A digital disaster strikes some enterprise every day.
- Infrastructure disruptions have cascading impacts, multiplying their cyber and physical effects.

Draft: A National Strategy to Secure Cyberspace

6

Trends, Two

- Fixing vulnerabilities before threats emerge reduces risk.
- It is a mistake to think that past levels of cyber damage are accurate indicators of the future.
  - Much worse can happen.
- Common defense of cyberspace depends on a public-private partnership.
- Everyone must act to secure their parts of cyberspace.

Draft: A National Strategy to Secure Cyberspace

7

Who are the Attackers?

- Here
  - Adrian Lamo
  - Kevin Mitnick
  - Kevin Poulsen
- Later we may also look at:
  - Robert Morris
  - Alexey Ivanov and Vasiliy Gorshkov
  - Others …

8

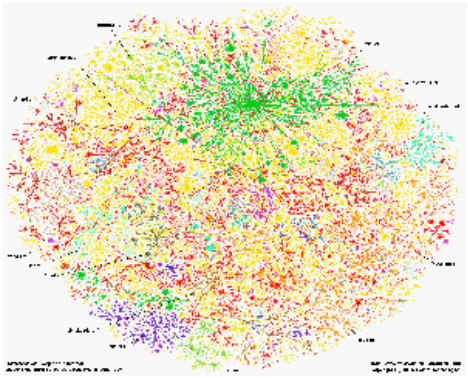
Who are the Defenders?

Last Spring's Security Panel

9

The Big Picture Internet Map

- Internet Traffic Map

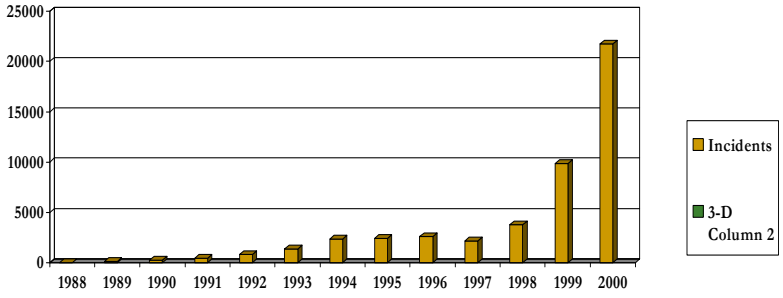


- Where are the national boundaries?
- Where are the police?

10

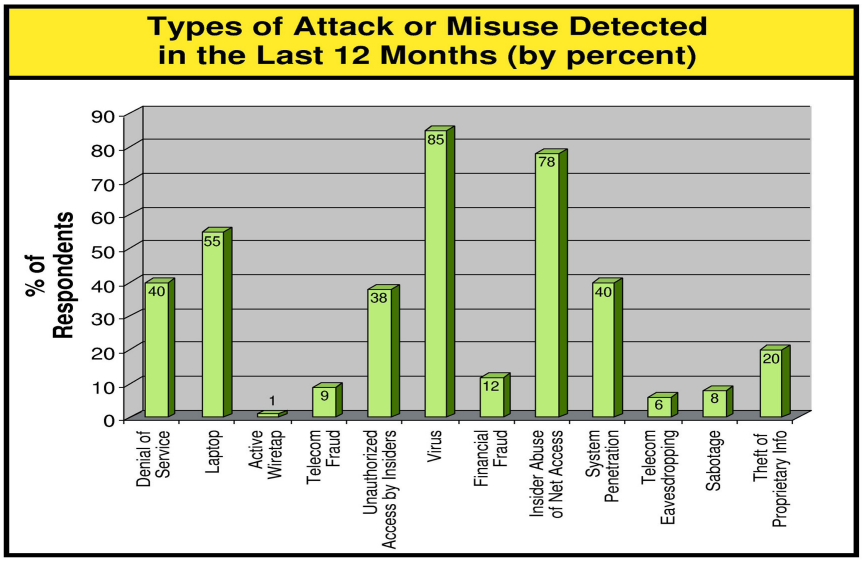
The Big Picture *CERT.org*

- Computer Emergency Reaction Team Incident Statistics



11

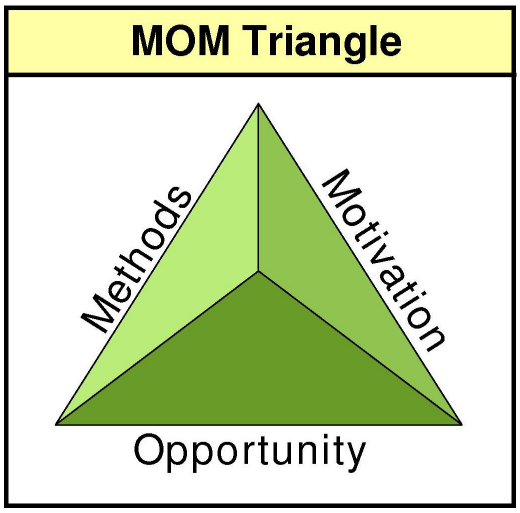
The Big Picture *Computer Security Institute*



12

Opportunity Theft Model

Sometimes described as Desire, Skill, Opportunity.



13

Terms *Definitions One*

- Vulnerability
  - A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security ...
- Threat
  - Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.
- Risk
  - The probability that a particular threat will exploit a particular vulnerability ...
    - *From NCSC-TG-004 Aqua Book*

14

Terms *Definitions Two*

- A threat is a potential violation of security.
  - An attack is defined as an action that might cause a security violation.
    - Those who execute such actions, or cause them to be executed, are called attackers.

Security:

- policy is a statement of what is, and what is not, allowed.
- mechanism is a method, tool, or procedure for enforcing a security policy.

--Bishop

15

Risk Management's Objective

- The objective … is to enable the organization to accomplish its mission(s) by:
  - Better securing the IT systems
    - that store, process, or transmit organizational information
  - Enabling management to make well-informed risk management decisions
    - to justify the expenditures that are part of an IT budget;
  - Assisting management in authorizing (or accrediting) the IT systems
    - on the basis of the supporting documentation resulting from the performance of risk management.

NIST 800-30

16

Vulnerabilities?

- People
- Processes
- Organizations
- Technology (systems, networks, etc…)
  - Workstations and Servers
  - Firewalls
  - IDS
  - Avs
  - VPNs
- Vulnerabilities are Dynamic

17

Vulnerabilities *People*

- People
  - Things people know
  - Relations between people
  - How people they relate to machines
  - Passwords
    - Strong (Yellow Stickies)
    - Over the shoulder acquisition
  - Password Cracking and Password Guessing
    - Morris Worm
    - Rome Labs
  - Do Passwords work?

18

Vulnerabilities *Organizations*

- Organizations
  - Dumpster Diving
    - Identity Theft
    - Sujeet Shenoi – Dumpster Diving
      - Founding member of Tulsa University's Center for Information Security
  - Social Engineering
    - Kevin Mitnick – The Art of Deception
  - Unsecured Web Servers, Unlisted URLs
    - Adrian Lamo
  - Insecure Back up tapes

19

Vulnerabilities *Technology*

- Systems
  - Complexity is the enemy of security
    - In general, security is inversely proportional to the number of Lines of code in a program
      - 30 to 40 Million for Windows 2000
- Firewalls
- Detection Systems, Intrusion and Anti Virus
- Virtual Private Networks
- Local Area Networks
- Internet

20

Vulnerabilities *System*

- "The Mythical Man-Month: Essays on Software Engineering,“
  - Frederick P. Brooks, 1975

Note

- Research indicates that there is a consistent number of bugs per thousand lines of code.
- Often, fixing one bug exposes another in a long cascade of problems that need to be fixed one after another

- More Patches become more problematic
  - Require more labor
  - Less well tested i.e. may break other applications
  - May reopen previously closed or create new vulnerabilities.
- Simplicity is security’s friend, complexity is its enemy!

21

Technology Alone is Not Enough

Technology alone is not enough

22

Technical Solutions

If you think technology can solve your security problems, then:

1. You don't understand the problems and
2. You don't understand the technology.

B. Schneier

23

Vulnerability Trends

- Each day, on the average, 7 new vulnerabilities are discovered.
  - Blue Lance Houston InfraGard Conference
- Since 1972, vulnerabilities have been increasing at a rate of 90% per year.
  - Notes:
    - Not all vulnerabilities are ever exploited
    - It is impossible to predict which new vulnerabilities will ever be exploited.

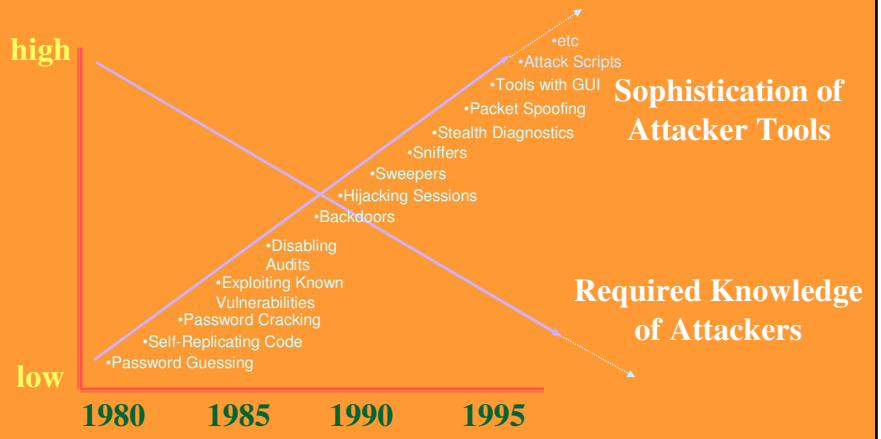
24

Trends

- With time there is an increasing number of :
  - Known vulnerabilities
  - Exploits.
    - Automated exploits can decrease skills required for an exploit.
    - Example ARP poisoning
  - People who employ exploits (threat agents).
  - Internet based ecommerce organizations.
  - People and organizations connecting to the Internet.

25

Required Knowledge Trend

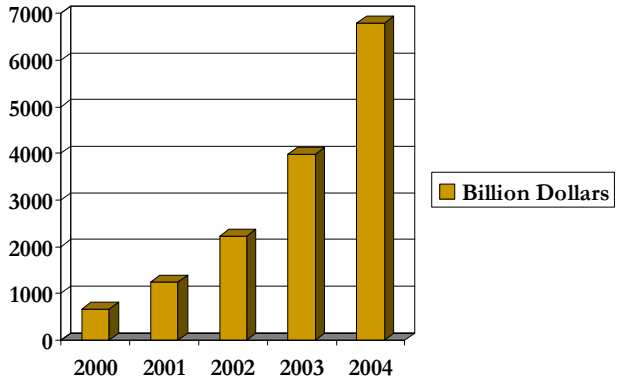


Attackers Require Less Knowledge as Tool Sophistication Increases

26

Trends Money

- Forrester Research predicts that by 2004, online commerce will reach $6.8 trillion.



27

Why Hack?

- That's where the money is!
- Online, I can attack my opponent without exposing myself!
- Online, I can express my political views!
- Because I can!
  - For example, Kevin Mitnick claims to have never directly made money on any of his attacks.
  - He did however use other peoples services.

28

Why Hack the Internet?

- The Cyber Economy is the Economy!
  - Condoleezza Rice
- On the Internet it is difficult to tell where my country's borders stop
  - No one country can police the Internet
  - International LE agencies will forge agreements but it will take time.
- Any system directly connected to the Internet is exposed to about a half billion other users and systems.

29

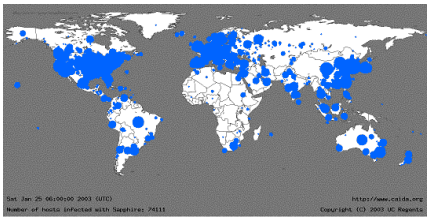
Internet Threat Characteristics, *one*

- Automation
  - Automated infections (Worms and Trojan Horses)
    - Morris Worm, 1988
  - Honey Pot Project Record (17 seconds)
- Speed of Exploit Propagation
  - Negates traditional commerce reaction response
- Distance doesn't matter
  - No International Borders on the Internet
  - Legal jurisdiction scope

30

Threat Characteristics, *two*

- Blue color represents Slammer, 30 minutes after release



- In the first minute, the infected population doubled in size every 8.5 (±1) seconds.
- After approximately three minutes, the worm achieved max scanning rate (over 55 million scans per second)

31

Worms and Viruses

- Robert Morris
  - Internet Worm, 1988
  - First conviction under the 1987 Computer Security Act
  - Father was the chief scientist at NSA's, National Computer Security Center (NCSC)
- Michael Buen & Onel de Guzman
  - I Love You Virus
  - Not in jail (Under Philippines law, hacking not a crime.)

32

Malicious Software

- Trojans
  - Email
    - A virus posing as a photo of Russian tennis player Anna Kournikova. Spread twice as fast as I Love You.
      - Polymorphic
      - Encrypted
  - DDOS
    - Distributed Denial of Service Attack
    - Mafia Boy and Tribal Flood knocked down Yahoo and Ebay.
- Spyware

The computer hacker known as "Mafiaboy," who crippled several major Internet sites, arrives in court Thursday in Montreal, Canada

33

Internet Threat Characteristics *Costs*

- Automated infections (Worms, Viruses, and Trojan Horses)
  - Figures from Computer Economics indicate that the original Code Red cost companies around $1.2 billion.
    - Reflects both expenditures for monitoring and clean-up and losses in productivity.
  - The I LOVEYOU worm and its family of mutations have caused an estimated $6.7 billion in productivity losses and the price tag will go up even more...
    - (Analyst Samir Bhavnanim)

34

Internet Threat Characteristics *Trends*

- Speed of Propagation is increasing.
- For example, NIMDA (ADMIN backwards) went from nonexistent to nationwide in an hour, lasted for days, and attacked 86,000 computers.
  - NIMDA caused significant problems in well-protected industries, forcing firms offline, shutting down customer access, and requiring some firms to rebuild systems entirely.
- Because there is no consistent method to track such damage, the actual financial cost of the NIMDA attack is unknown.
- However, industry sources estimate that the overall financial impact of cyber attacks resulting from malicious code could have been $13 billion in the year 2001.

Draft: A National Strategy to Secure Cyberspace

35

Digital Attack Types

- Criminal
  - Traditional crime facilitated by computers
  - Crimes against computers
- Privacy Violations
  - Increasingly regulated
  - SB 1386
- Publicity Attacks
- Legal Attacks

36

Digital Attacks *Criminal*

- Extortion
  - Alexey Ivanov and Vasiliy Gorshkov (50,000 CC#)
- Fraud & Scams
  - Email from Nigeria
- Intellectual Property Theft
- Identity Theft

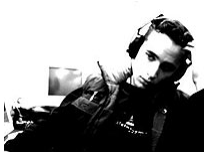
37

Digital Attacks *Privacy Violations*

- (HIPAA) Health Insurance Portability and Accountability Act (1996)
  - aka Kennedy Kassenbaum Health Insurance Portability and Accountability Act
  - Compliance required by April 2003.
  - Standards aim to maintain the right of individuals to keep private information about themselves.
- "A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."
- SB 1386

38

Digital Attacks *Publicity Attacks*



Publicity Attacks

- Publicity seekers don't fall into the same threat model that criminals do …
- Adrian Lamo
  - Used a back door in The New York Times' intranet to obtain home phone numbers of over 3,000 Op-Ed contributors, including Vint Cerf, Warren Beatty, and Rush Limbaugh.
  - Added himself to their roster of experts
- Bumped from NBC telecast after hacking them
  - On camera, demonstrated his techniques for NBC Nightly News. When he cracked the network's own systems, their lawyers killed the story.

39

Digital Attacks *Legal Attacks*

- Don't exploit technical system flaws.
- Aim to persuade a judge or jury that there could be a system flaw.
- When successful, puts doubt in the minds of the judge or jury that the security isn't perfect and a client is innocent.
  - George Mason University lost a 4.3 million dollar court case after a judge refused to allow evidence from their intrusion detection systems into court

40

Potential Attackers

- Common criminals
  - Financial gain
- Industrial spies
  - Competitive advantage
- Hackers
  - People skilled beyond their maturity
- National Intelligence organizations
- Malicious Insiders
- Internet Businesses (Spyware)

41

Threat Attributes

- Attackers may have different :
  - Objectives
  - Skill levels
  - Risk tolerance

42

Hacker

- Person who experiments with the limits of a system out of intellectual curiosity i.e. a person with a particular set of skills not a particular set of morals
  - Some distinguish between a cracker and a hacker with the former being bad and the later being good
- Black, white, or gray hat

43

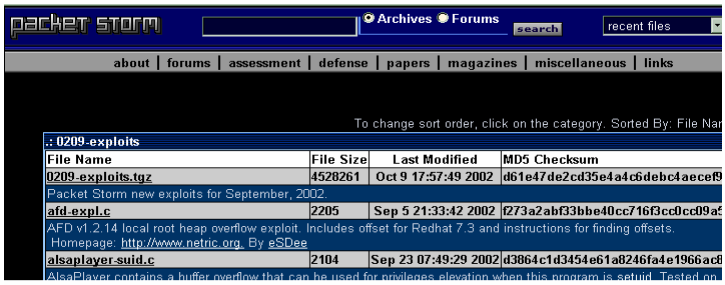
Hacker Hierarchy

- Government funded
- Sophisticated with programming background
- Sophisticated with Network Admin background
- Semi Sophisticate
- Ankle Biter aka Script Kiddie

44

Exploits

- Tools that automate the process of breaking into systems
- Readily available on the Internet



Malicious Insiders

- Not necessarily employees
  - Consultants
  - Contractors
- Not necessarily in the same country as you
- Many security measures firewalls, intrusion detection systems, etc. deal with external threats.
  - Insiders aren't impacted by perimeter security.
  - Certain technologies (VPNs for example) may screen an insider's activities from your ID systems.

Press

- A subspecies of industrial spy with different motivations
- Kevin Lee Poulsen aka Dark Dante
- Can be well funded
- Can tolerate risk

47

Kevin Lee Poulsen

- aka Dark Dante
  - Currently, a well know journalist.
  - Disabled the phone system of KIIS_FM so he could be the102nd caller and win the $50,000 Porsche giveaway.
  - While on under indictment, won four more radio contest grand prizes from L.A.-area Top 40 stations.
  - Usually featured on Security Focus website.

48

Organized Crime

- Hacking supports core competencies
  - Identity Theft
  - Extortion
- What do you get when you combine lone criminals with a money and organization?
  - Russian/East European Mafia

49

Terrorists

- Generally more concerned with causing harm than gathering intelligence
- Infowar
  - Asymmetrical warfare
- Tend to lack funding and skills
  - May change in the future
    - Rome Labs
    - *Datastrean and Kuji*
  - Politically motivated hacking increasing

50

National Intelligence Orgs

- CIA, NSA, DIA, NRO, MI6, MI5, …
  - Federal documents indicate over 100 countries are developing Information Warfare capabilities
- Well funded
- Formidable
- Usually highly risk averse.
- Already engaged in industrial espionage?

51

INFOWar

- A military adversary who tries to undermine his target's ability to wage war by attacking the information or network infrastructure.
- Short term focus of affecting his target's ability to wage war.
- Objects:
  - Military advantage
  - Chaos
- Assymetrical Warfare

52

Security Services

- Confidentiality (Privacy)
  - Privacy and the Government
- Integrity
- Availability
- Authentication
- NonRepudiation

53

Confidentiality and Privacy

- Controls who can read, or access, information
- Different countries have different laws
  - In the US, individuals don't own the data about themselves.
  - The European Union (EU) laws protecting individual privacy.
  - There are legal constraints on companies moving information across national borders.
- Moving privacy information from the EU into the United States where similar protections do not exist is considered illegal

54

Integrity

- Integrity has to do with the data validity.
- The electronic world has no context
- Concerned with trust i.e. how much can you trust a system or data
- Can be divided into system and data domains
  - If you loose system integrity, you will soon loose data integrity

55

Audit and Other Assurance Mechanisms

- Trust but verify
  - Vital whenever security is taken seriously
- Detective security service
  - Enables (facilitates or makes possible) forensics
- Assurance requires more than thinking or believing that you, or your organization, are secure. It requires a mechanism to demonstrate that you have a reason for your belief.
  - i.e. belief based upon external data

56

Authentication

- Authentication is about the continuity of relationships
  - Knowing who to trust and who not to trust…
- Military aircraft have IFF systems to authenticate themselves to allied aircraft and antiaircraft batteries.
  - When this malfunctions, people die. (Iraq war friendly fire.)
  - When it doesn't malfunction, sometimes people die. (Argentine war exocet identification.)
- Session authentication -- IRC
- Transaction authentication – credit card
- Internet is connectionless

57

E-Commerce

Security requirements for e-commerce

- Authentication
- Privacy
- Integrity
- Nonrepudiation
- Audit

58

Security Principles and Models

- Security is a process.
- Needs to be based upon a model.

Some helpful data points:

- Generally Accepted Security Principles (GASSP) (NIST 800-14)
- Layered Security Model (aka DID)
- NSA Security Model
- Risk Management (NIST 800-30)

59

Achieving Security Goals

- Generally Accepted Security Principles (GASSP)
  - Began in mid-1992 in response to the report "Computers at Risk" (CAR), published by the United States National Research Council in 1990.
  - The GASSP Pervasive Principles, based on the Organization of Economic Cooperation and Development (OECD) principles.
  - Developing Linkages with ISC^2

60

GASSP

- Generally Accepted Security Principles
- Security supports an organization's goals
- Information security controls should be proportionate to the risks.
- Risks should be assessed periodically.

61

GASSP

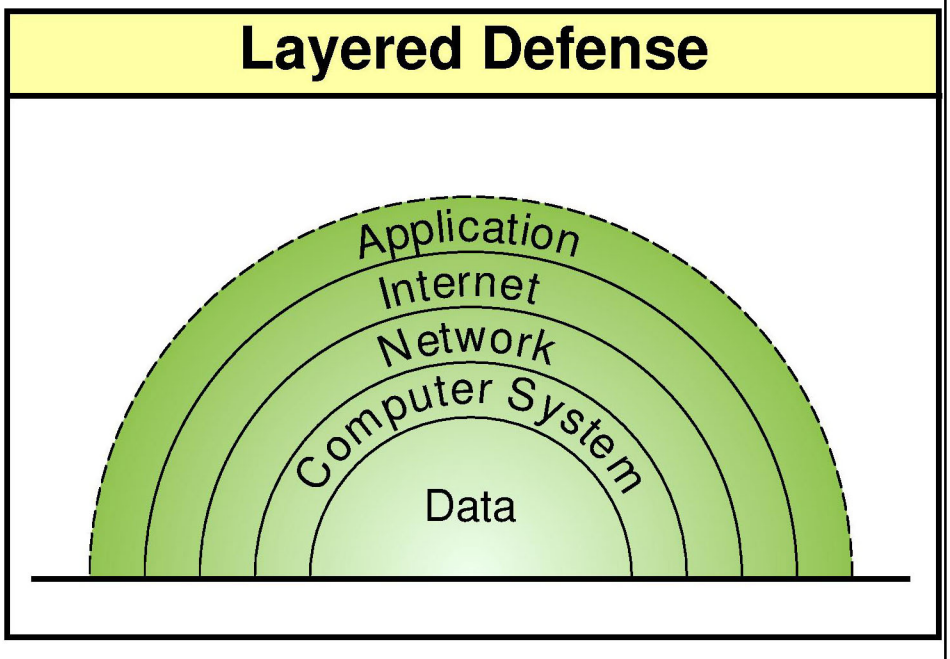
- All parties, with a need to know should have access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems.
- They should also be informed of applicable threats.

62

Systems and Security

- Effective security has to be thought of as a system within larger systems
- Real world issues include design tradeoffs, unseen variables, and imperfect implementations.
- Not a product but a process.
  - Dynamic
- Layered Security Model

63



Security is a Process

- Each layer adds security over existing layers
  - Theoretically, not possible to penetrate multiple layers simultaneously
- Like a chain, security is only as secure as the weakest link
- Security is not a product
  - It can't be bought.
- Like the context that it exists within, information system security is dynamic

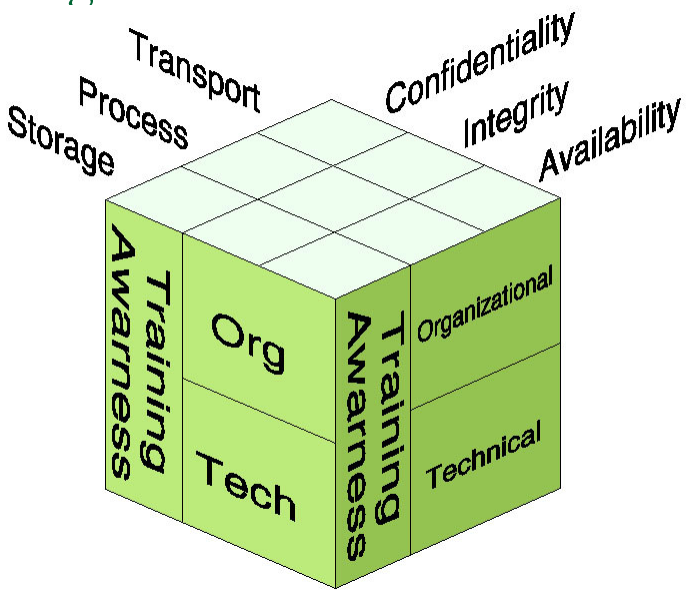
65

Systems Theory

- In order to understand system security of, you need to look at the entire system and its context.
- Viewing any component in isolation is flawed.
- Security should not depend on any particular technology.

66

The Big Picture NSA Model



67

NSA Model

- Developed and modified over time.
- One of its primary authors is Vic Maconachy

68

Proactive Solutions

- The notion of fixing a security flaw after it becomes a problem won't work on the Internet.
- Education and Training are critical components of any security plan.

69

Education

Graduate Program

- MS, Technology Project Management
- Information Systems Security Specialization
  - NSA, CNSS, accredited

70

References, One

- Kevin Mitnick
- http://www.defensivethinking.com/
- Kevin Lee Poulsen
- http://www.well.com/user/fine/journalism/jail.html
- Adrian Lamo
- http://online.securityfocus.com/news/595
- http://online.securityfocus.com/news/358
- Alexey Ivanov and Vasiliy Gorshkov
- http://www.fbi.gov/page2/seattle.htm
- http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=384

71

References Two

- Rome Labs
- http://www.spirit.com/Network/net0598.txt
- http://www.fas.org/irp/congress/1996_hr/s960605b.htm
- Love Bug
- http://www.chguy.net/news/may00/hack.html
- http://www.lloydsoflondon.com/america/library/atlloyds14.10.htm
- http://exn.ca/Stories/2000/05/09/03.asp
- Forrester Research
- http://www.glreach.com/eng/ed/art/2004.ecommerce.php3
- GASSP
- http://web.mit.edu/security/www/gassp1.html
- I Love You
- http://home.planet.nl/~faase009/iloveyou.html
- ISO2

72

Questions?