Threats, Vulnerabilities, and Risks

Ed Crowley CISSP, NSA-IAM/IEM

Spring '05

1

Threats, Risks, and Vulnerabilities

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

2

Outline

- Introduction
  - The Big Picture
    - Trends
    - Definitions
- Threats
  - Threat Agents
- Current Environment
  - Context
- Vulnerabilities
  - Systemic
- Attacks
  - Social Engineering
  - Password Guessing
  - Buffer Overflow
  - System Flaws
  - Exploits
- Security,what is it?
- Security Models

3

Who am I?

- Certified Information System Security Professional (CISSP)
  - Information System Security Association (ISSA)
  - InfraGard
- 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

4

Current Themes, Part One

- Cyber incidents are increasing in number, sophistication, severity, and 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

5

Current Themes, Part 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

6

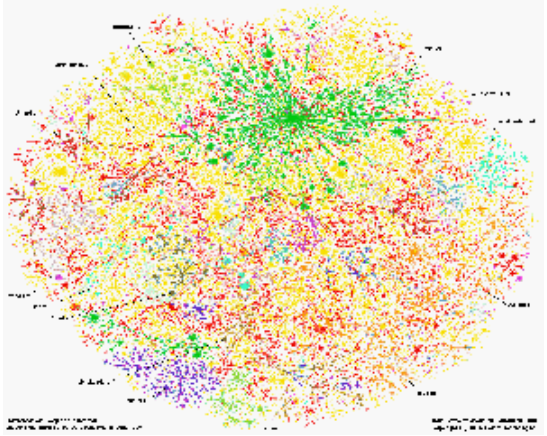
Threat Agents, Who are They?

- Here
  - Adrian Lamo
  - Kevin Mitnick
  - Kevin Poulsen
- Later we will look at:
  - Robert Morris
  - Alexey Ivanov and Vasiliy Gorshkov
  - And others …

7

The Big Picture Internet Map

- Internet Traffic Map

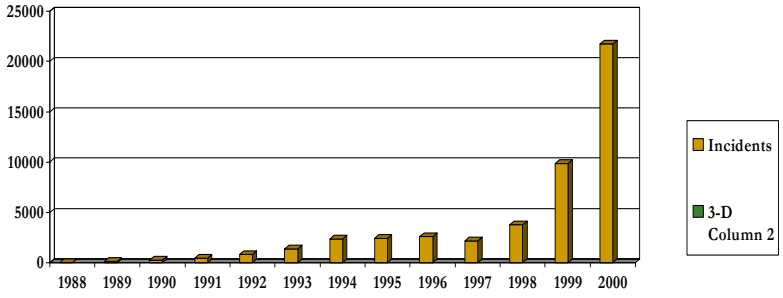


- Where are the national boundaries?

8

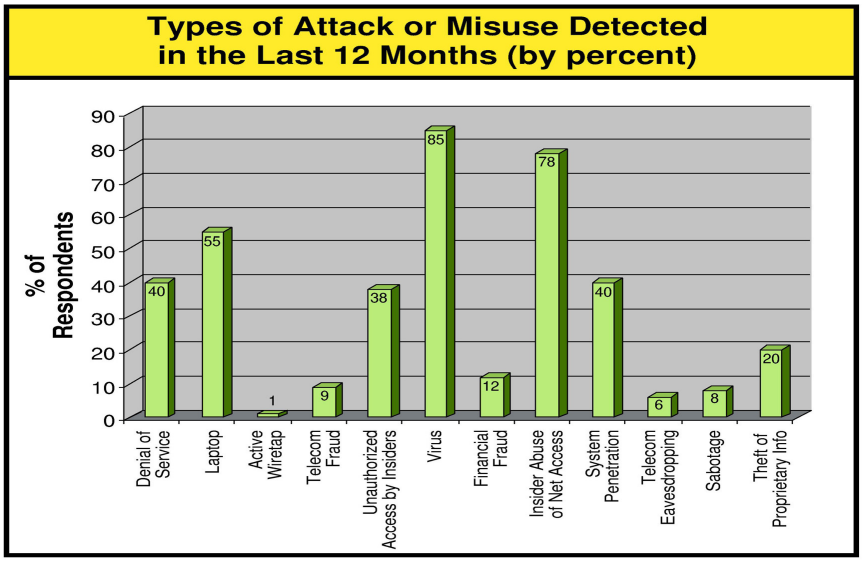
The Big Picture *CERT.org*

- Computer Emergency Reaction Team Incident Statistics



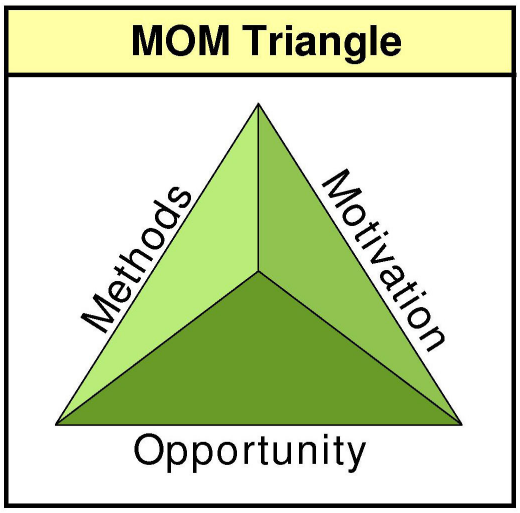
9

The Big Picture *Computer Security Institute*



10

Method Opportunity Means



11

The Big Picture Definitions

- 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.
  - Here we use the term “threat agent” to denote a person capable of creating the above represented circumstance.
- Risk
  - The probability that a particular threat will exploit a particular vulnerability ...
    - *From NCSC-TG-004 Aqua Book*

12

Where are Vulnerabilities?

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

13

Vulnerabilities People

- People
  - Things people know, relations between people
  - People and how they relate to machines
  - Passwords
    - Strong (Yellow Stickies)
    - Over the shoulder acquisition
  - Password Cracking and Password Guessing
    - Morris Worm
    - Rome Labs

14

Vulnerabilities Organizations

- Organizations
  - Dumpster Diving
    - Identity Theft
    - Sujeet Shenoi – Dumpster Diving assignment
      - 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

15

Where are Vulnerabilities Found?

- Systems
  - Number of Lines of Code
  - 30 to 40 Million for Windows 2000
- Firewalls
- Detection Systems, Intrusion and Anti Virus
- Virtual Private Networks
- Local Area Networks
- Internet

16

System Vulnerabilities

- "The Mythical Man-Month: Essays on Software Engineering,“
  - Frederick P. Brooks, 1975
- **Note**
  - Constant number of bugs per thousand lines of code.
  - What often happens is that fixing one bug exposes another in a long cascade of problems that need to be fixed one after another
- More Patches become more problematic
  - Requires more labor
  - Less well tested i.e. may break other applications
  - May reopen previously closed vulnerabilities.
  - May create new vulnerabilities.
- No substitute for simplicity

17

Technology Alone is Not Enough

Technology alone is not enough

18

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**

19

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.

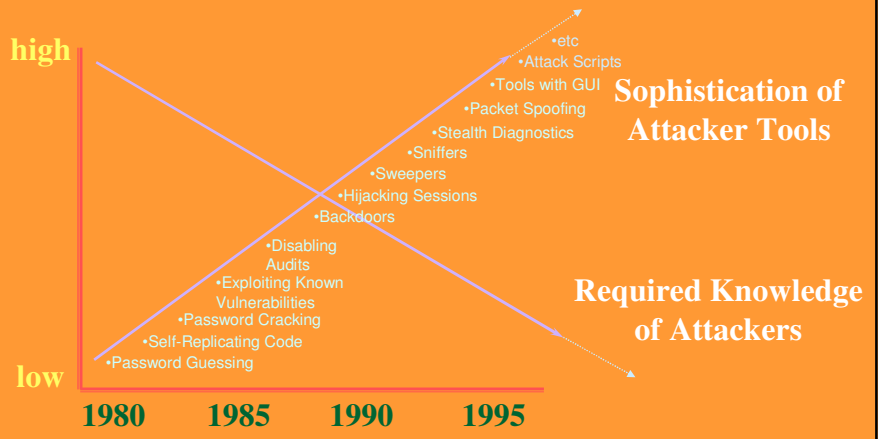
20

Trends

- Increasing with time, 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.

21

Required Knowledge Trend

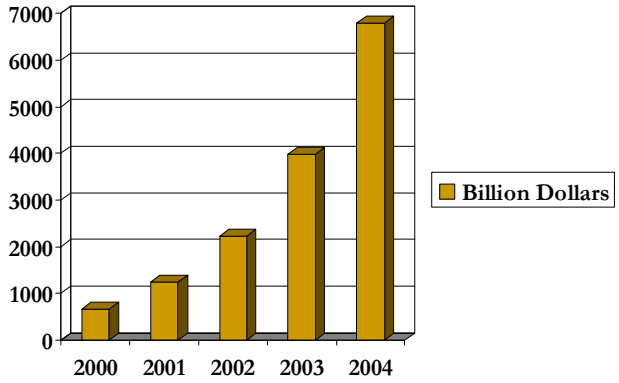


Attackers Require Less Knowledge as Tool Sophistication Increases

22

Trends Money

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



23

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!
  - Kevin Mitnick never directly made money on any of his attacks.
  - He did however use other peoples services.

24

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.

25

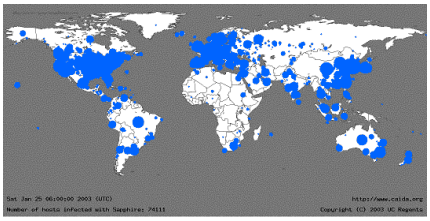
Internet Threat Characteristics, *one*

- 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

26

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)

27

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.)

28

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.

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

29

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)

30

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

31

Digital Attacks

- Criminal
  - Traditional crime facilitated by computers
  - Crimes against computers
- Privacy Violations
- Publicity Attacks
- Legal Attacks

32

Digital Attacks Criminal

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

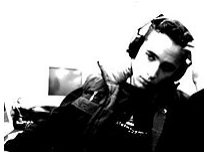
33

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."

34

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.

35

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

36

Potential Threat Agents

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

37

Threat Properties

- Threat agents may have:
  - Different objectives
  - Different skill levels
  - Different risk tolerance

38

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

39

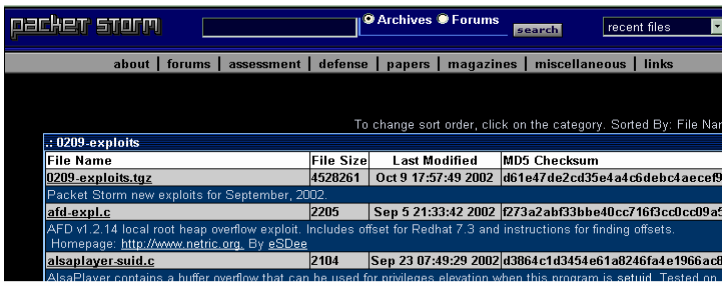
Hacker Hierarchy

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

40

Exploits

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



41

Hacker Properties

- Stereotypically, young, male, on the fringe
  - Lots of time
  - Little finances
- Currently, the bulk of computer related crimes appear to be caused by lone criminals

42

Malicious Insiders

- Not necessarily employees
  - Consultants
  - Contractors
- Many security measures firewalls, intrusion detection systems, etc. deal with external threats.
  - These methodologies are useless versus an insider

43

Press

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

44

Press

- Kevin Lee Poulsen aka Dark Dant
  - 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.

45

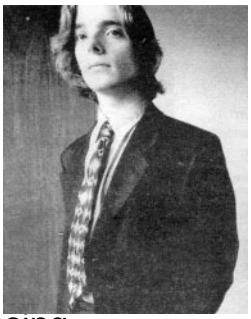
Organized Crime

- 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

46

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



47

National Intelligence Orgs

- CIA, NSA, DIA, NRO, M16, MI5, …
  - Federal documents indicate over 100 countries are developing Information Warfare capabilities
- Well funded
- Formidable
- Usually highly risk averse.
- Already engaged in industrial espionage?

48

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

49

Security Goals

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

50

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

51

Integrity

- Integrity has to do with the data validity.
- The electronic world has no context

52

Audit and Other Assurance Mechanisms

- Vital whenever security is taken seriously
- Detective security service
- Designed to aid 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.

53

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.)
  - Sometimes people die when it doesn't malfunction. (Argentine war exocet identification.)
- Session authentication -- IRC
- Transaction authentication – credit card

54

E-Commerce

Security requirements for e-commerce

- Authentication
- Privacy
- Integrity
- Nonrepudiation
- Audit

55

Security Principles and Models

How to achieve security

- Generally Accepted Security Principles (GASSP)
- Layered Security Model (aka DID)
- NSA Security Model

56

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 ISC²

57

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.

58

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.

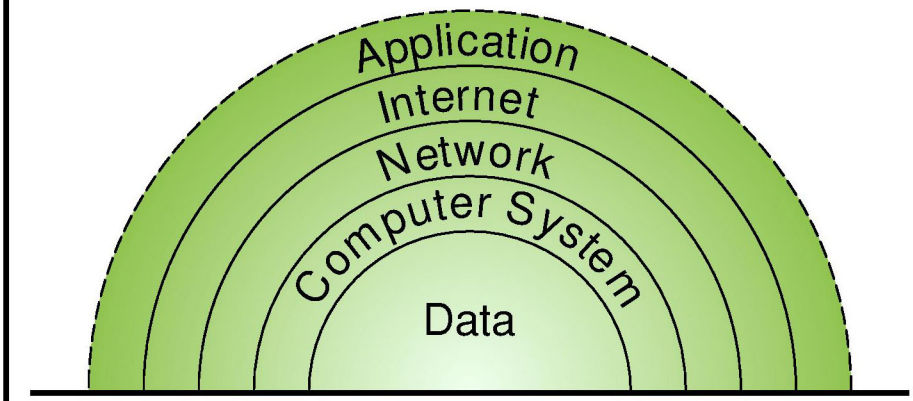
59

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

60

Layered Defense



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

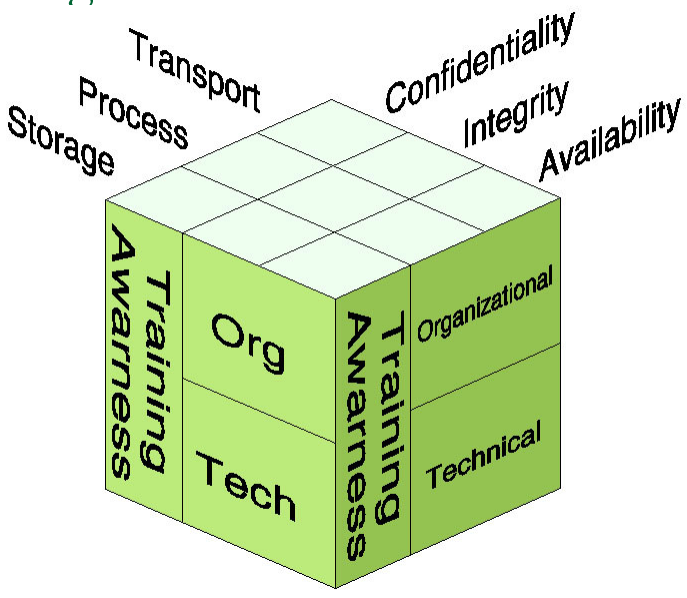
62

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.

63

The Big Picture NSA Model



64

NSA Model

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

65

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.

66

Education

Applied Security Classes

- Introduction to Security
- Security Foundations
- Together the two courses cover ISC^2 Common Body of Knowledge
  - University of Houston Downtown, Applied Business and Technology Center
    - Phone: 713.221.8032, Fax: 713.221.8166
    - E-mail: abtc@dt.uh.edu
- Review for the CISSP exam!

67

Education

Graduate Program

- MS, Technology Project Management
- Information Systems Security Specialization
  - 713-743-4098

68

Questions?

69

References, Partial Listing

- 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
- Rome Labs
- http://www.spirit.com/Network/net0598.txt
- http://www.fas.org/irp/congress/1996_hr/s960605b.htm

70