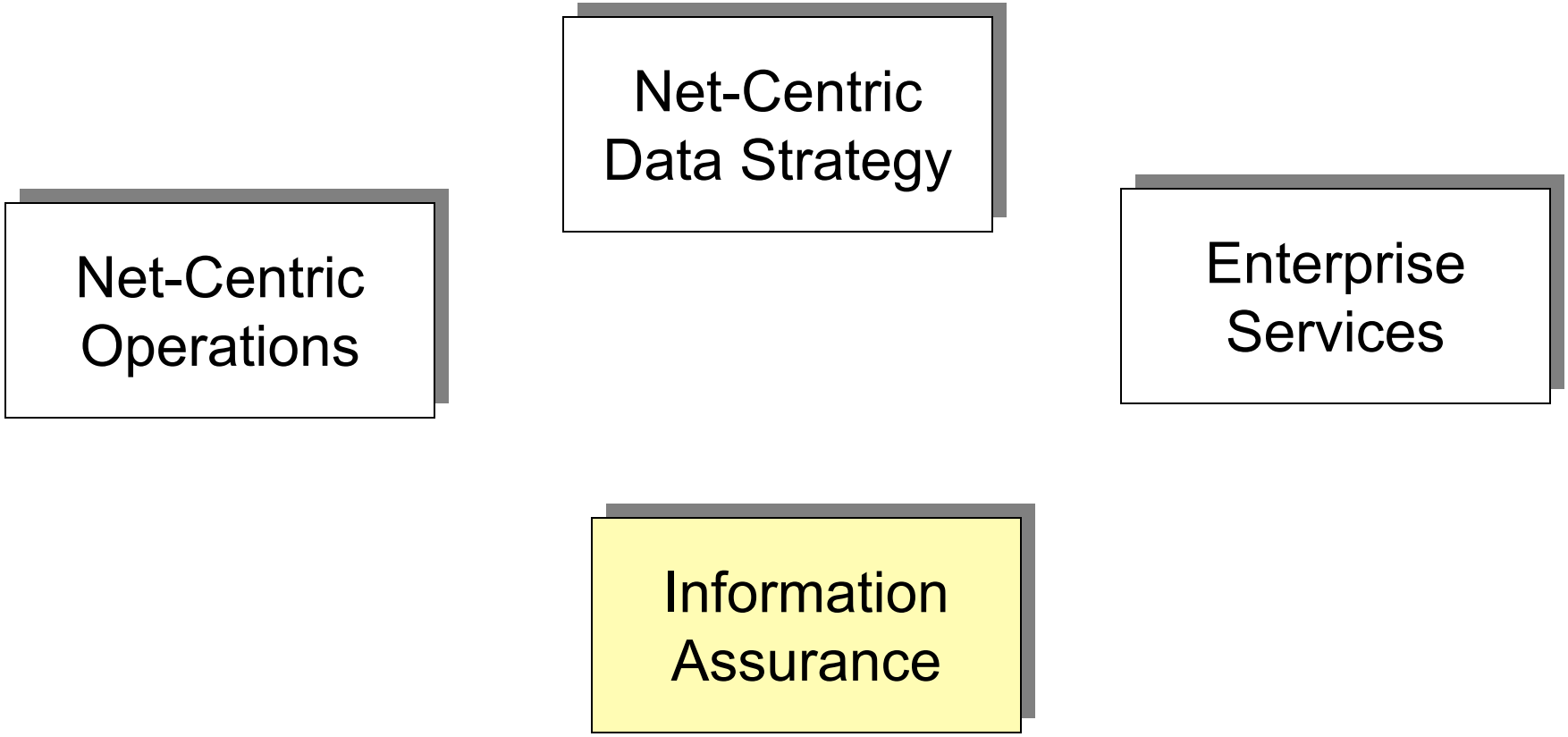
Information Assurance for Defense Security

Prof. Paul A. Strassmann
George Mason University, March 27, 2007

Elements of Information Transformation in DoD



Information Assurance Requirements

Definition of Information Assurance

- Information Assurance (IA) are the methods for managing the risks of information assets.
- IA practitioners seek to protect the confidentiality, integrity, and availability of data and their delivery systems, whether the data are in storage, processing, or transit, and whether threatened by malice or accident.

IA is More than Information Security

- IA's includes reliability and emphasizes risk management over tools and tactics.
- IA includes privacy, regulatory compliance, audits, business continuity, and disaster recovery.
- IA draws from fraud examination, forensic science, military science, systems engineering, security engineering, and criminology in addition to computer science.
- IA is a superset of information security.

Responsibilities

- CIO responsibilities include:
  - Monitoring the reliability of cyber-security;
  - Robustness of cyber-crime protection;
  - Up-time availability of network services;
  - Installation of trusted backup capabilities;
  - Designs for systems redundancy;
  - Capacity for recovery from extreme failures.

Federal Information Security Management Act of 2002 - "FISMA"

- FISMA imposes processes that must be followed by information systems used by US Government.
- Must follow Federal Information Processing standards (FIPS) issued by NIST (National Institute of Standards & Technology).

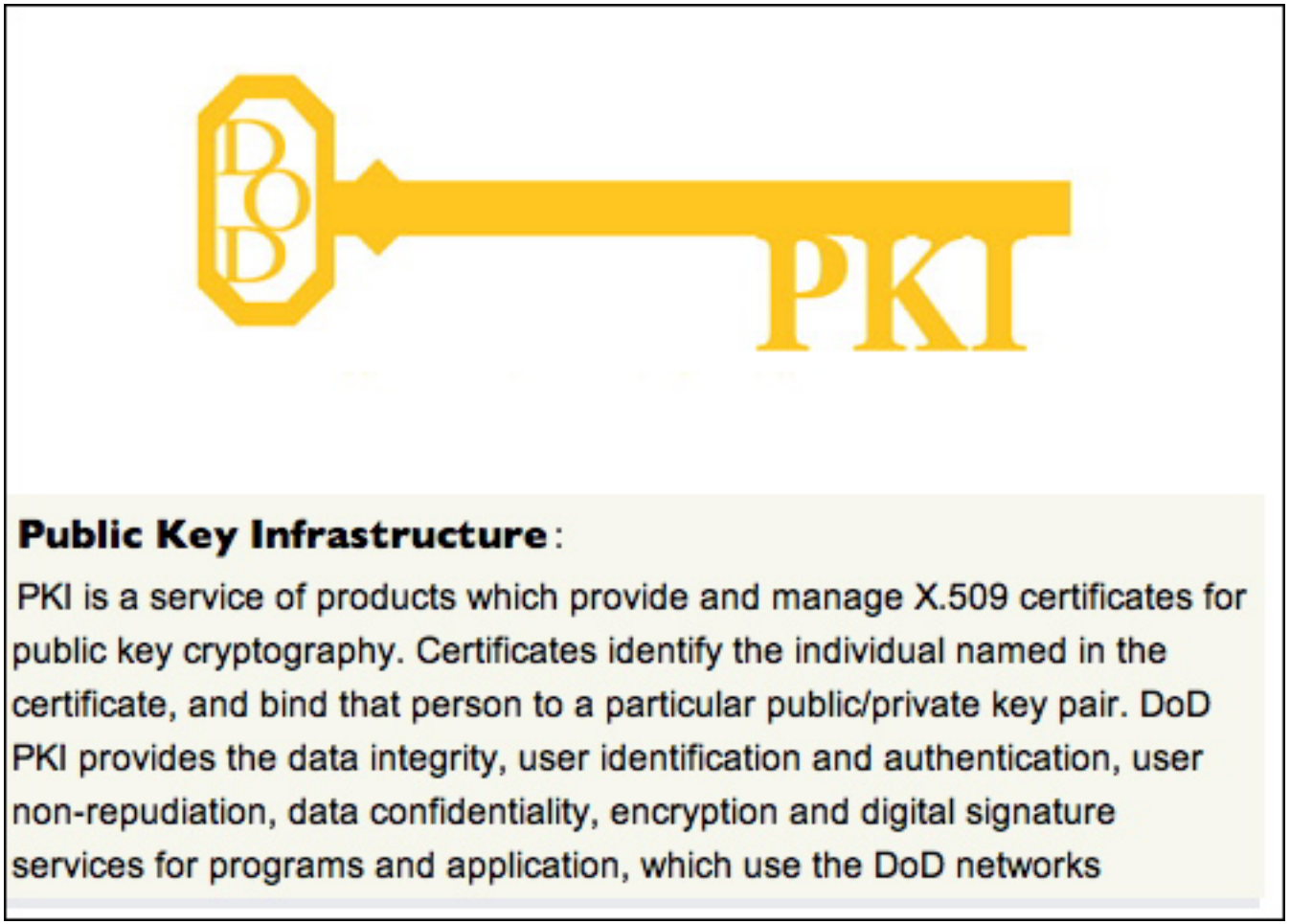
FISMA Requirements

- Security controls must be incorporated into system.
- Must meet the security requirements of NIST 800-53.
- Security controls must contain the management, operational, and technical safeguards or countermeasures.
- The controls must be documented in the security plan.

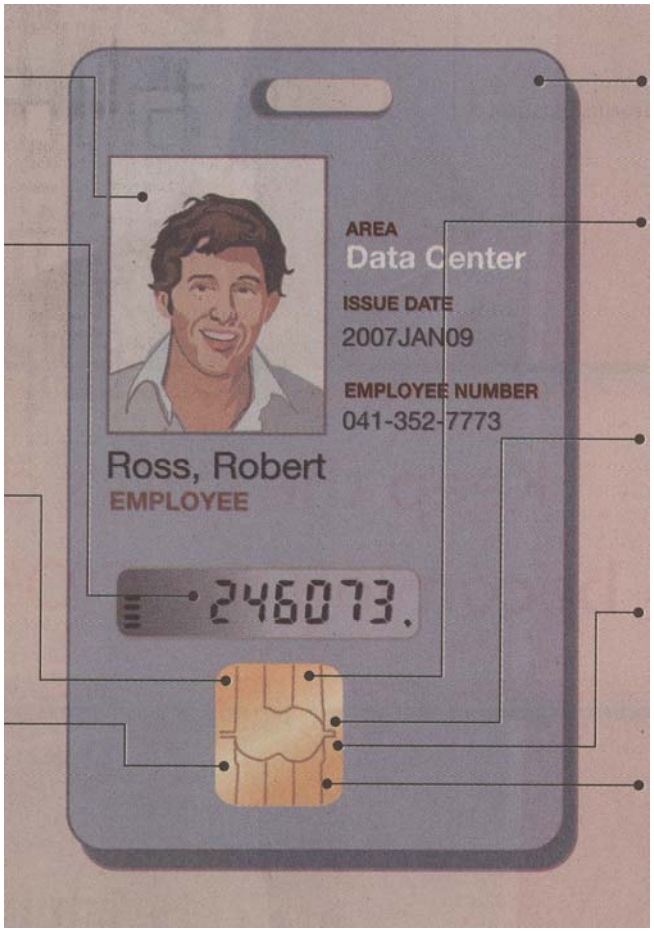
Homeland Security Presidential Directive HSPD-12

- Defines the Federal standard for secure and reliable forms of identification;
- Executive departments and agencies shall have a program to ensure that identification meets the standard;
- Executive departments and agencies shall identify information systems that are important for security.

Required: Public Key Encryption



A Secure Identity Card



Digital Photo

One-Time Password

Physical Access Control

Biometrics

Radio Frequency Antenna

Heavy Duty Password

Electronic Wallet

Digital Identify Certificate

Encryption Key

Encryption Policy

- Unclassified data on mobile computing devices and removable storage media shall be encrypted.
- Encryption is achieved by means of the Trusted Platform Module (TPM). It is a microcontroller that can organize and store secured information.
- TPM offers facilities for secure generation of cryptographic keys

What is TPM

- The TPM is a microcontroller that stores keys, passwords and digital certificates.
- It is affixed to the motherboard.
- Silicon ensures that the information stored is made secure from external software attack and physical theft.
- Security processes, such as digital signature and key exchange are protected.
- Critical applications such as secure email, secure web access and local protection of data are assured.

MS VISTA Necessary for TPM

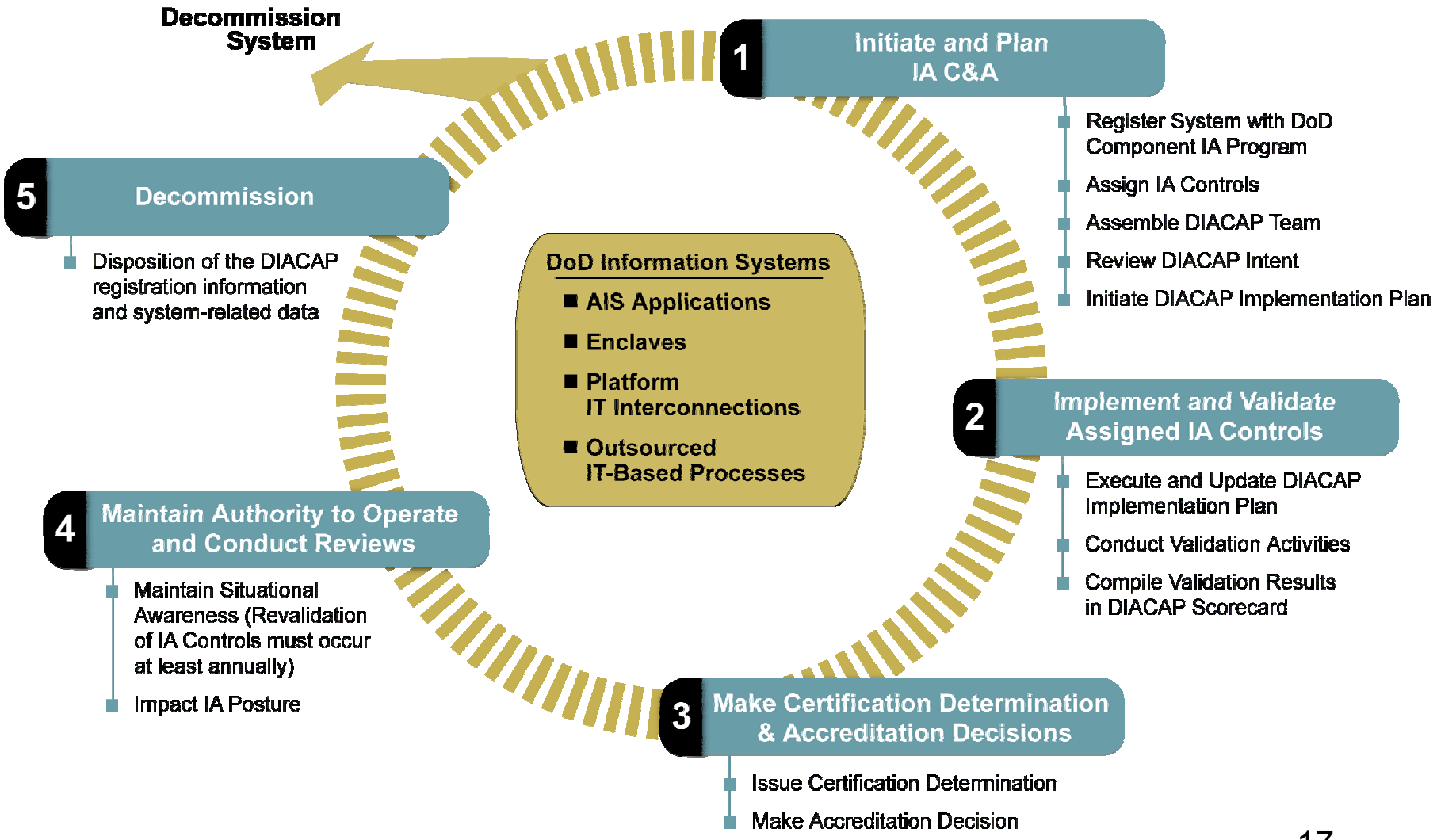
Spending on Information Assurance

Federal Information Assurance Spending ($B)	FY 06	FY 07
Defense Department	$3.15	$3.31
All Others	$2.31	$2.45
Total I.T. Security Spending	$5.46	$5.76
Total IT Spending on Training and Reporting	$1.38	$1.43
DoD IA Spending/Total I.T. Spending	10.3%	10.5%

Information Assurance Certification & Accreditation Program (DIACAP)

- E-Government Act
  - Title III of the E-Government Act, Federal Information Security Management Act (FISMA), requires Federal departments and agencies to develop, document, and implement an organization-wide program to provide information assurance. DIACAP ensures DoD Certification and Accreditation (C&A) is consistent with FISMA, DoDD 8500.1 and DoDI 8500.2
- Global Information Grid (GIG)
  - The DIACAP is a central component of GIG IA C&A Strategy. DIACAP satisfies the need for a dynamic C&A process for the GIG and net-centric applications

DIACAP Activities

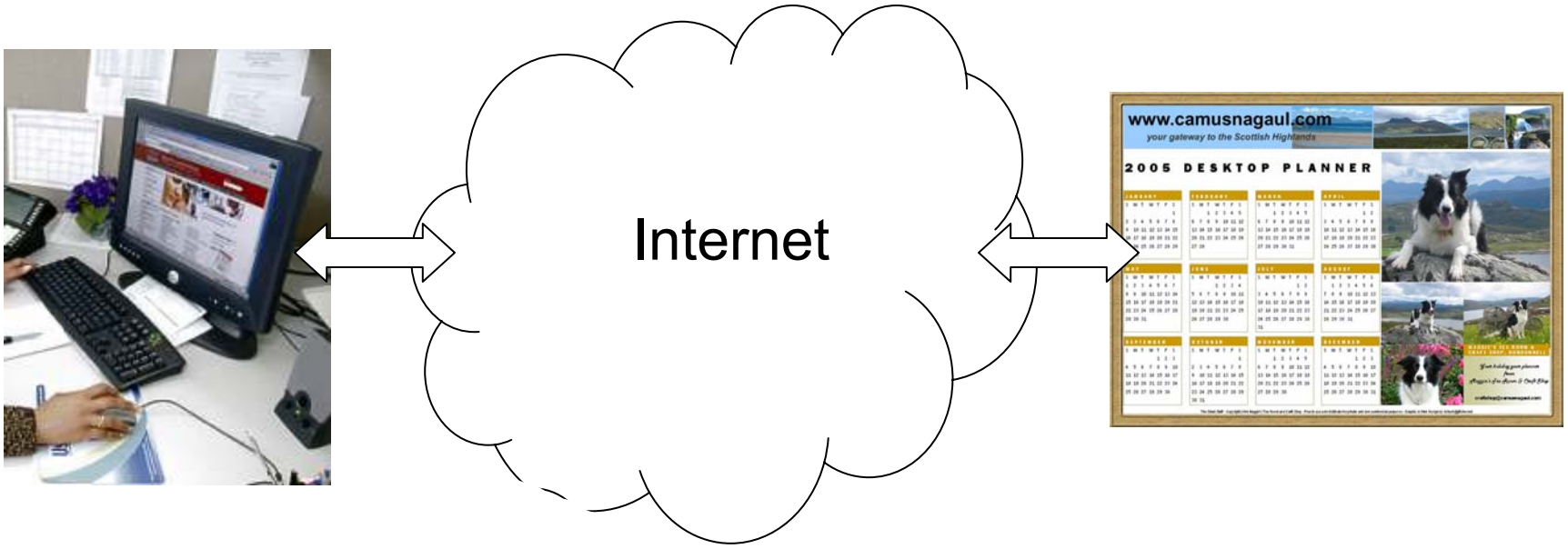


Designated Approving Authority (DAA)

- Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk.

The Internet

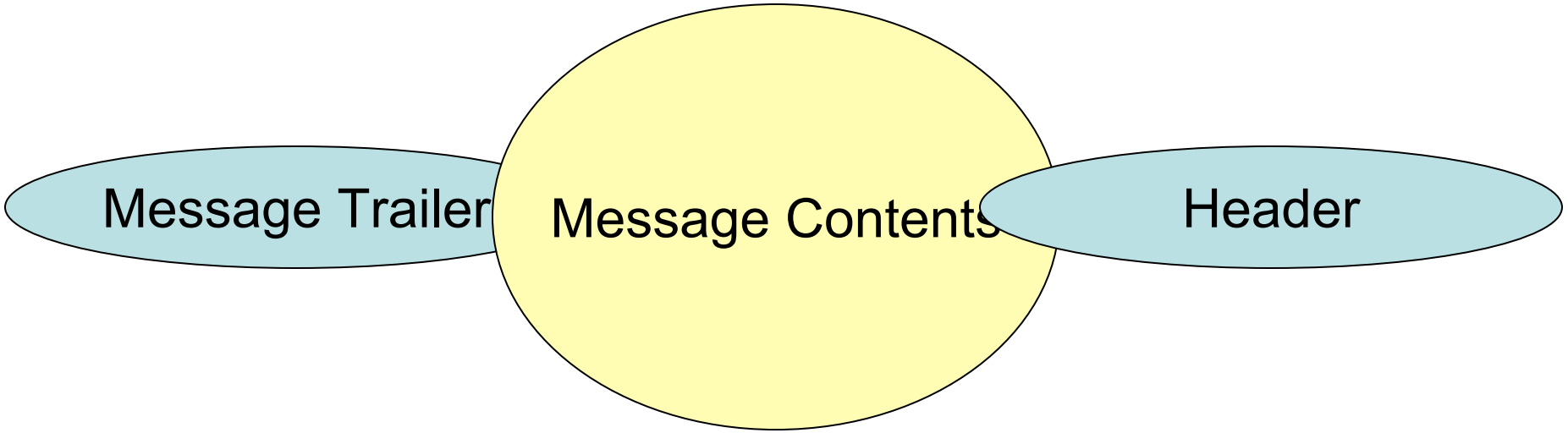
Web Looks Simple to the User



Internet Advantage

- Any properly configured computer can act as a host for a personal web-page.
- Any of several hundred million other computers can view that personal web-page.
- Any of several hundred million other computers can connect to another computer capable of delivering an information processing service.

Internet Protocols: For Identification of Message "Packets"



What is in an Internet Packet Header

- 4 bits that contain the version, that specifies IPv4 or IPv6 packet,
- 4 bits that contain the length of the header,
- 8 bits that contain the Type of Service - Quality of Service (QoS),
- 16 bits that contain the length of the packet,
- 16 bits identification tag to reconstruct the packet from fragments,
- 3 bits flag that says if the packet is allowed to be fragmented or not,
- 13 bits identify which fragment this packet is attached to,
- 8 bits that contain the Time to live (TTL) number of hops allowed
- 8 bits that contain the protocol (TCP, UDP, ICMP, etc..)
- 16 bits that contain the Header Checksum,,
- 32 bits that contain the source IP address,
- 32 bits that contain the destination address.

Problems with Nets and Servers

- Capacity limitations for peak loads;
- Congestion in access to data sources;
- Excessive delays for global access;
- Expensive to scale capacity for growth;
- Problem not in bandwidth, but mostly in switching;
- Depends on reliability and capacity of ISP “peers” to forward data to the destination;
- Conflicting economic interests among “peers” can inhibit growth and performance.

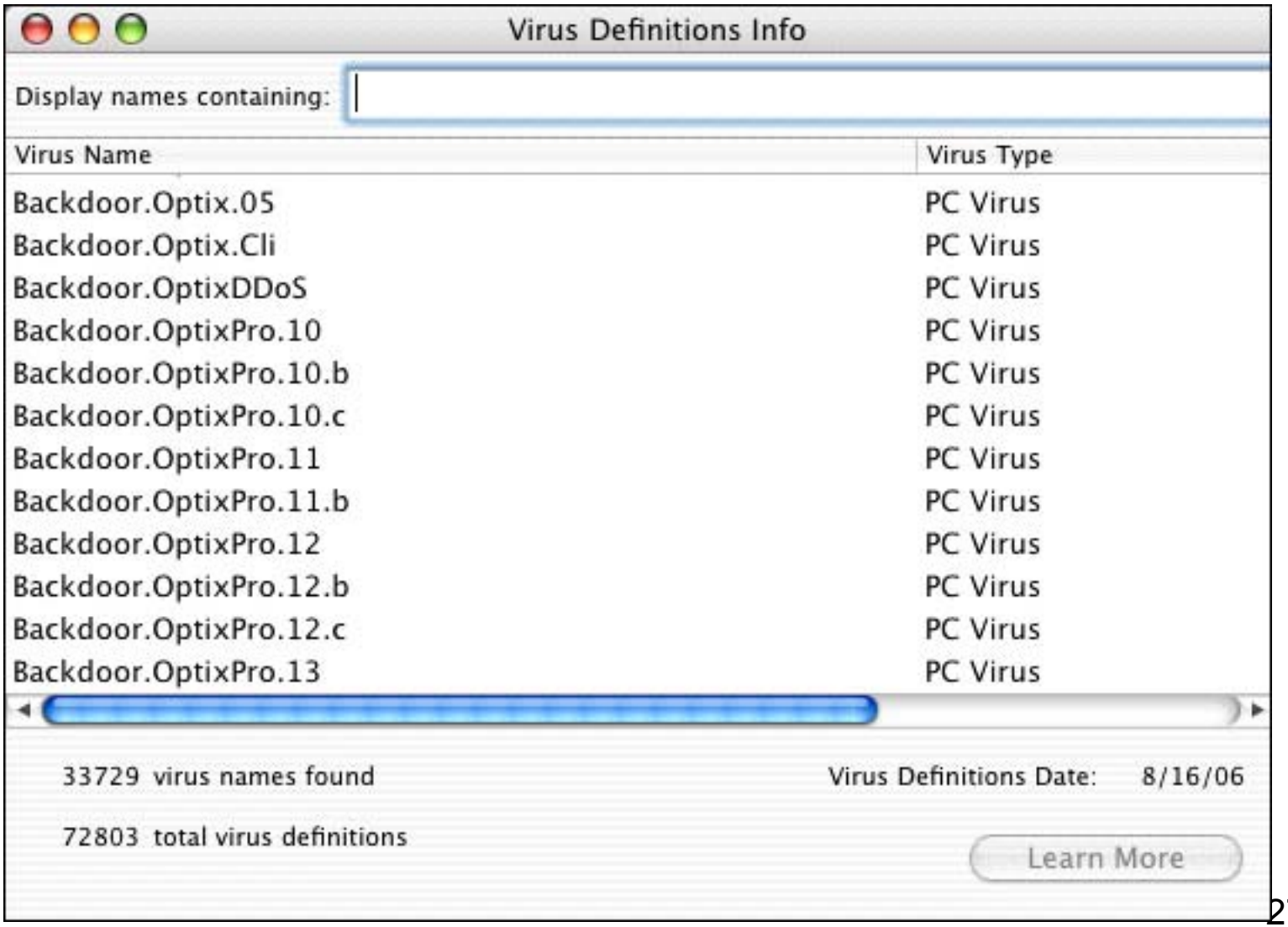
Internet Liabilities

- 17,000+ partially secure, poorly connected networks with practically unlimited number of unverifiable points of access;
- The most frequently used security protocol (SSL- Secure Socket Layer authenticates destination servers, but not the sending sources);
- Networks are mostly small, with large ISP's managing less than 10% of network traffic;
- Performance of the network depends on "peering relationships" between ISP (Information Service Providers), each providing network capacity and router switching capacity ;
- Delivery of packets cannot be guaranteed because network performance determined by routers that may not have sufficient capacity to handle traffic spikes.

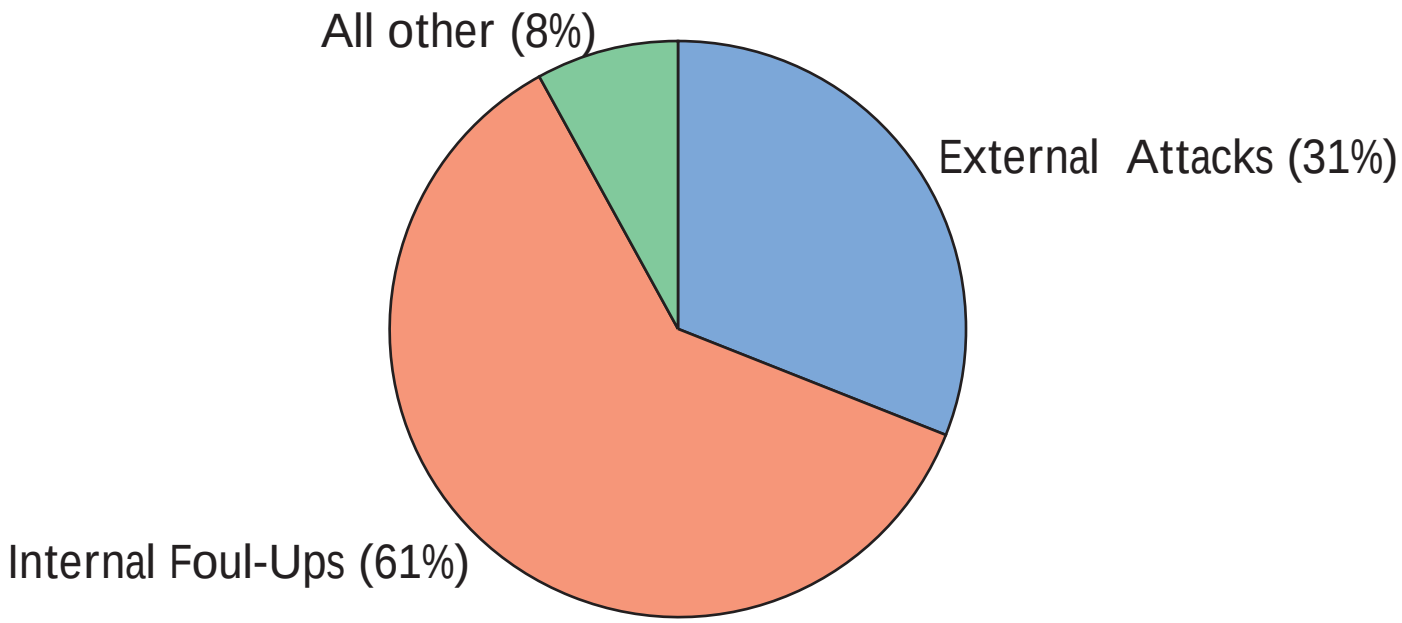
Internet Liabilities - Cont'd.

- The (BGP) Border Gateway Protocol are ISP instructions for forwarding packets from one network link to another. BGP is unreliable if router tables are in error;
- Average broad-band web-page download time to LAN can be well over 0.5 seconds, if message "packet" traverses several "hops";
- (DNS) Domain Name System can be compromised, by diversion of communications;
- Software robots (Botnets) can automatically proliferate and convey destructive software such as "worms", "rootkits" or parasitic "malware" such as "Trojans" for finding "backdoors" into computers.
- Denial of service attacks can be launched.

My Computer Scanned for 72,803 Viruses



Internal SNAFUs Cause Most Breaches of Security



SOURCE: Study of 550 security breaches, University of Washington, Computerworld 3/19/07

Security Management Issues

Types of Cyber-Threats

* Denial of service (DoS)
* Malicious software: Viruses; Worms; Trojans; Logic bombs
* Password crackers
* Spoofing / masquerading
* Sniffers
* Back door/trap door
* Emanation detection
* Unauthorized targeted data mining
* Dumpster diving
* Eavesdropping and tapping
* Social engineering
* Phishing
* Theft

Information Operations > Information Assurance

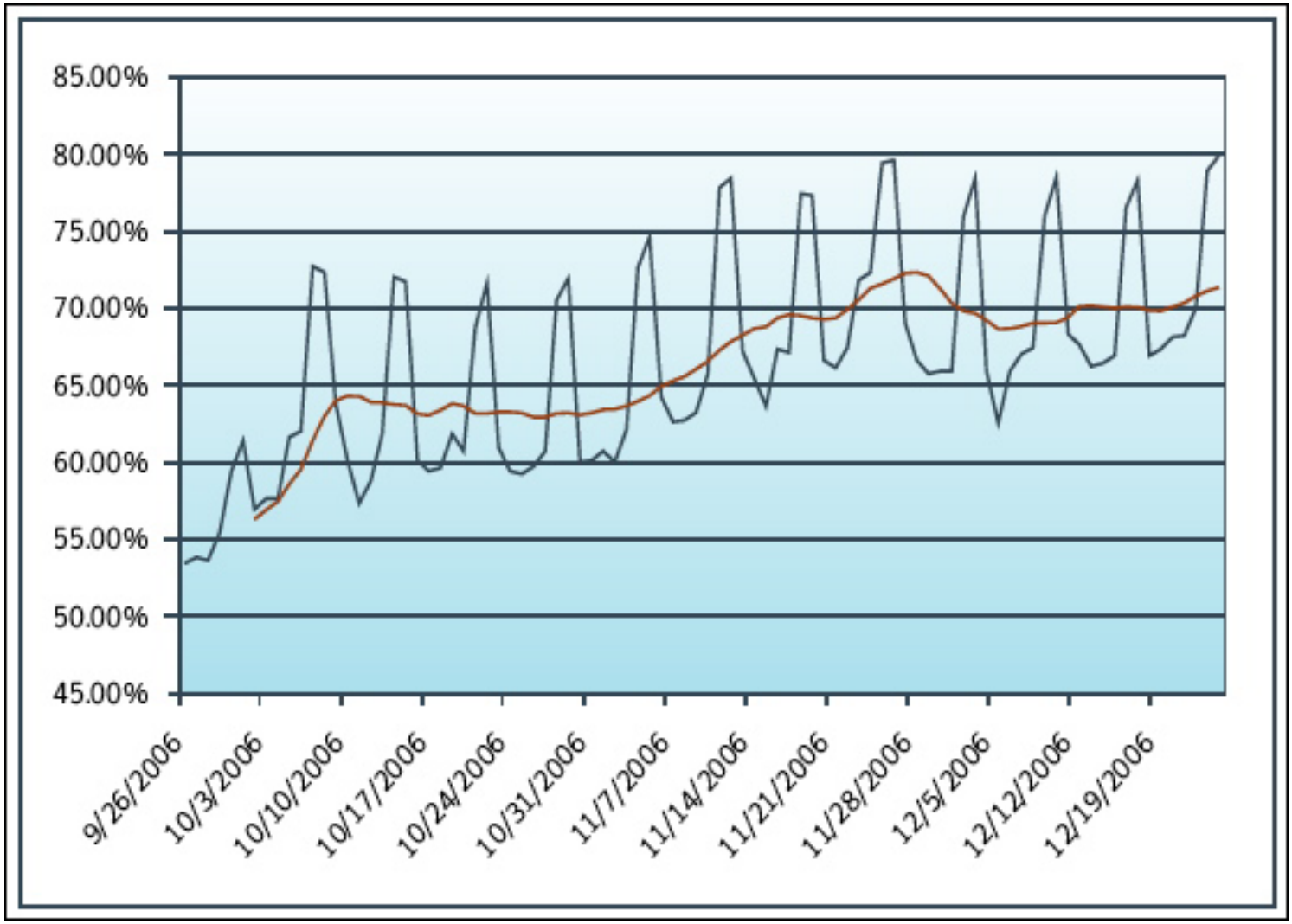
INFORMATION OPERATIONS	ACTIVITIES	OBJECTIVES
Electronic warfare	Electronic attack	Destroy, disrupt, delay
	Electronic warfare support	Identify and locate threats
	Electronic protection	Protect the use of electromagnetic spectrum
Computer network operations	Computer network attack	Destroy, disrupt, delay
	Computer network defense	Protect computer networks
	Computer network exploitation	Gain information about computer networks
Psychological operations	Psychological operations	Influence
Military deception	Military deception	Mislead
Operations security	Operations security	Deny
Supporting capabilities	Information assurance	Protect information and information systems
	Physical security	Secure information and information infrastructure
	Physical attack	Destroy, disrupt
	Counterintelligence	Mislead
	Combat camera	Inform, document
Source: Joint Pub 3-13, Information Operations		

E-Mail Filtering

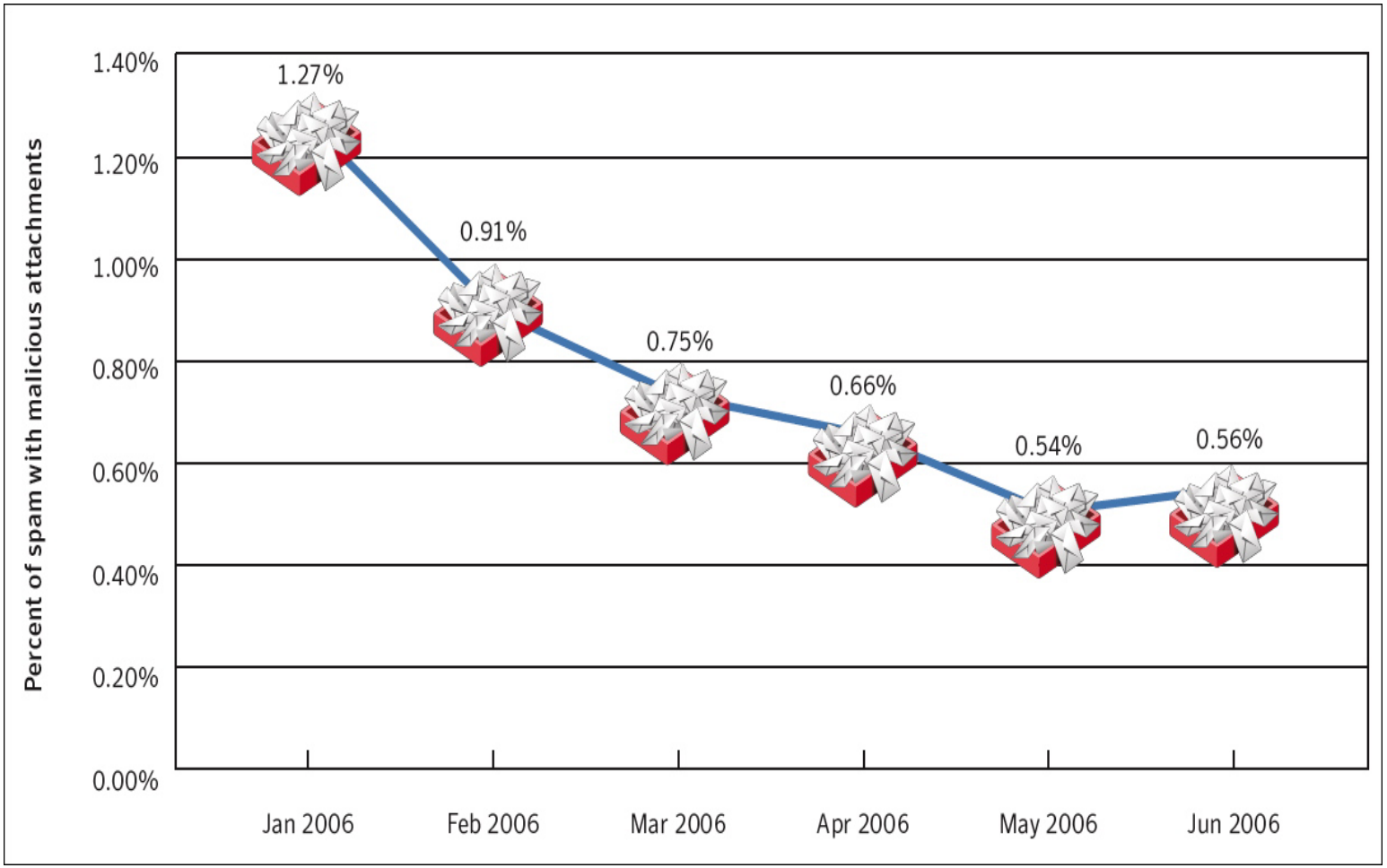
Email sent to: pstrassm@gmu.edu Visit Junk Box

	From	Subject	Reason
Unjunk | View	vecterpxfk@buytrucksineurop...	MS Office 2007 Enterprise ready to download	Likely Spam
Unjunk | View	tdcefkj@clientlogic.com	Billing report changes	Likely Spam
Unjunk | View	kozsclwu@mtu-net.ru	Download notification	Likely Spam
Unjunk | View	nwyulwklob@benidorm.org	Download notification	Likely Spam
Unjunk | View	aw-confirm@eBay.com	Urgently Respond Now	Phishing
Unjunk | View	aw-confirm@eBay.com	Urgently Respond Now	Phishing
Unjunk | View	service@paypal.com	Your payment has been sent to sales@wholesaleipod.com	Phishing

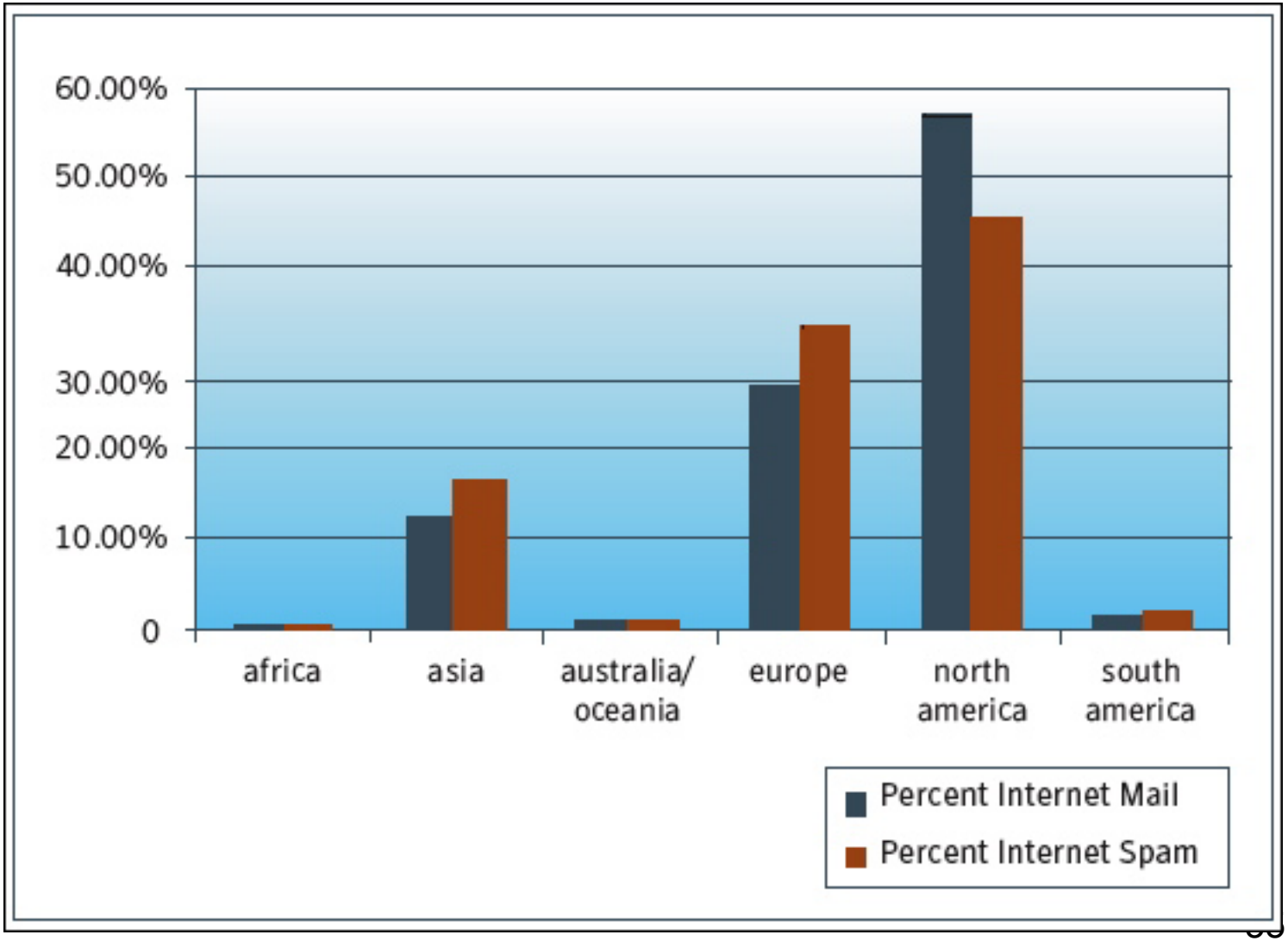
Internet SPAM % of Total E-mail



Percent of Spam with Malicious Attachments



Distribution of E-Mail and Spam



Buffer of 256 bytes Gets Loaded with 512 bytes

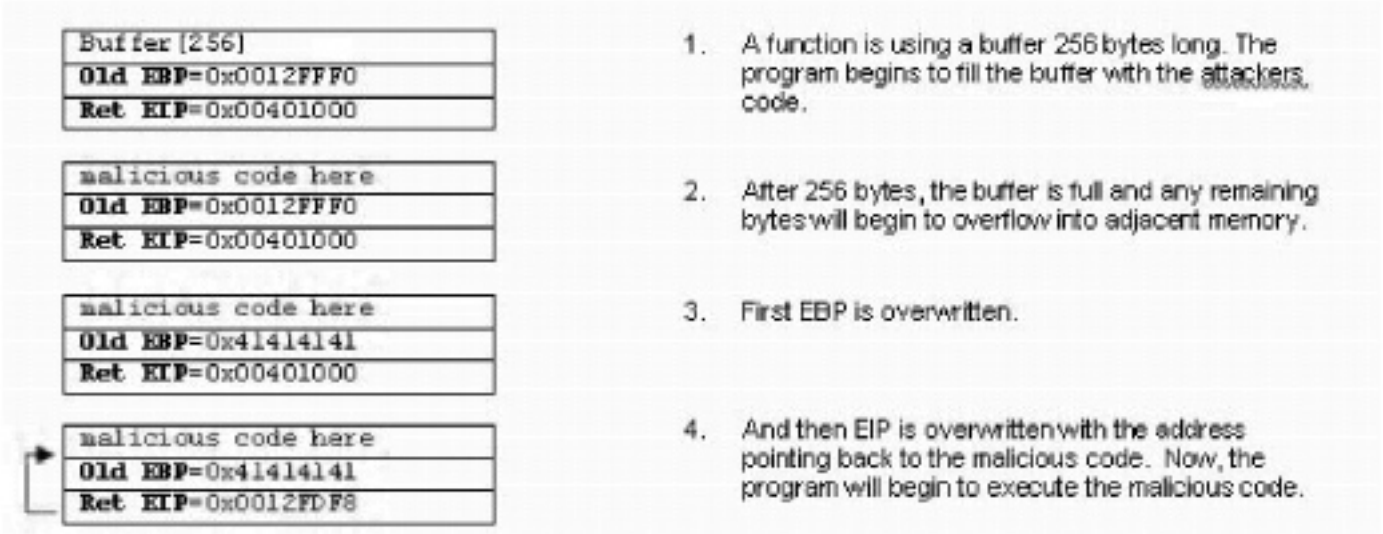
For example, the following program declares a buffer that is 256 bytes long. However, the program attempts to fill it with 512 bytes of the letter "A" (0x41).

```
int i;
void function(void)
{
char buffer[256]; // create a buffer

for(i=0;i<512;i++)              // iterate 512 times
        buffer[i]='A';          // copy the letter A
}
```

Placement of Malicious Code in Overflow Buffer

Overflow Instead of filling the buffer full of As, a classic exploit will fill the buffer with its own malicious code. Also, instead of overwriting the return EIP (where the program will execute next) with random bytes, the exploit will overwrite EIP with the address to the buffer, which is now filled with malicious code. This causes the execution path to change and causes the program to execute injected malicious code.



1. A function is using a buffer 256 bytes long. The program begins to fill the buffer with the attackers code.
2. After 256 bytes, the buffer is full and any remaining bytes will begin to overflow into adjacent memory.
3. First EBP is overwritten.
4. And then EIP is overwritten with the address pointing back to the malicious code. Now, the program will begin to execute the malicious code.

Losses from Virus Attacks

Financial Losses From Specific Virus Attacks in 2004 (Stated in Billions of US Dollars)	
Bagle	$ 1.50B
NetSky	$ 2.75B
Sasser	$ 3.50B
MyDoom	$ 4.75B

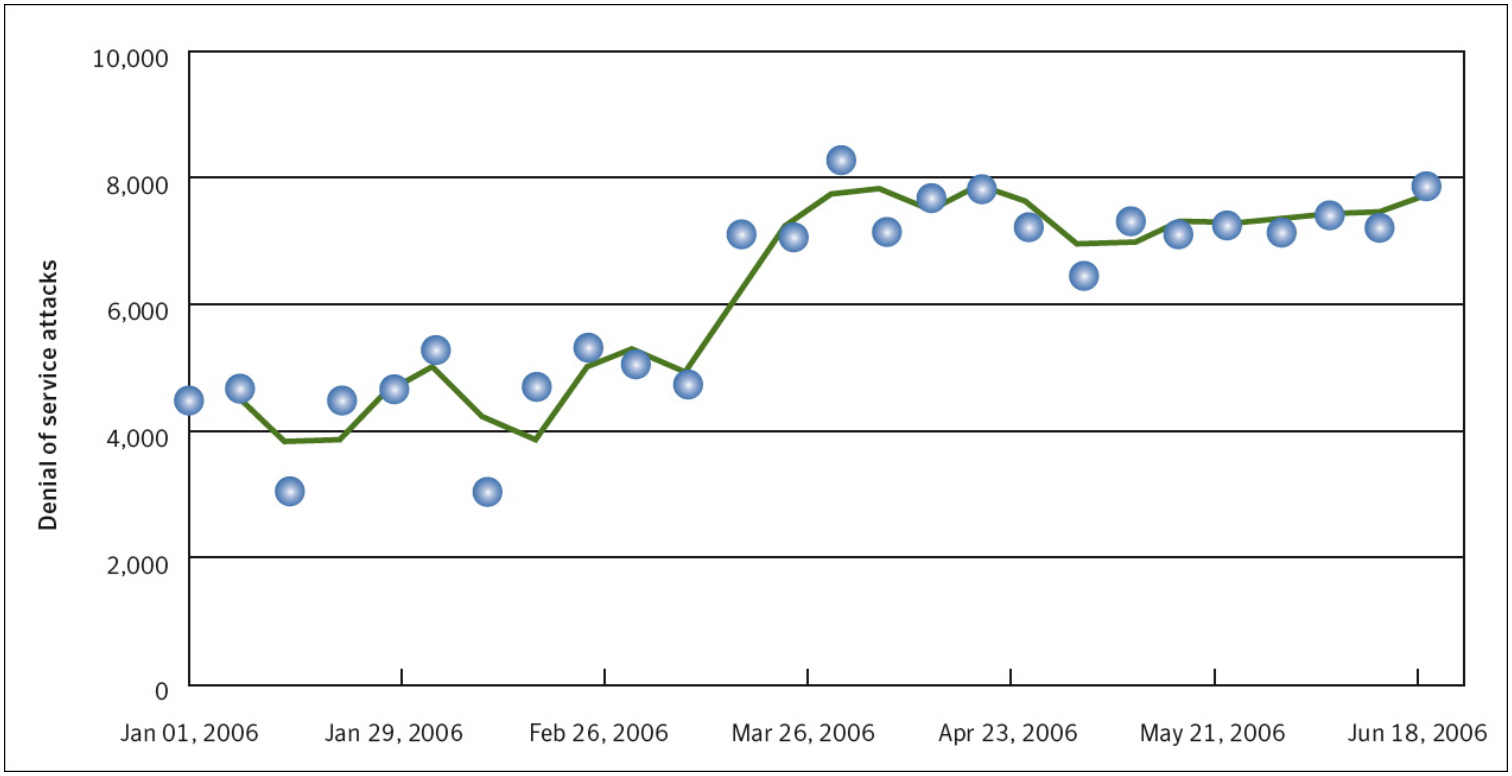
Classes of Malware

- A computer virus attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels.
- Worms spread from computer to computer, but unlike a virus, it has the capability to travel without any help from a person.
- A Trojan Horse tricks users into opening them because they appear to be receiving legitimate software or files from a legitimate source.

Pathology of Virus Types

Rank	Sample	Type	Vectors	Impact
1	Polip	Virus	File sharing, P2P	Lowers security settings
2	Bomka	Trojan, Backdoor	Spam	Drops other malcode
3	Gobrena	Trojan	Spam	Downloads Goldun Trojan
4	Detnat	Virus	Filesharing	Downloads Lineage Trojan
5	Ecup	Worm	P2P	
6	Rajump	Backdoor	N/A	Allows remote access
7	Nebuler	Trojan	N/A	Sends information to remote sites, downloads other threats
8	Awax	Trojan	N/A	Downloads and installs other threats
9	Yamanner	Worm	Yahoo! Web mail	Sends email addresses from contact list to a remote host
10	TopFox	Trojan	N/A	Logs keystrokes

Trends in Denial of Service Attacks



Concentration of Denial of Service Attacks

Rank	Sector	Proportion of attacks
1	Internet Service Provider	38%
2	Government	32%
3	Telecommunications	8%
4	Transportation	4%
5	Education	3%
6	Accounting	3%
7	Utilities / Energy	3%
8	Insurance	3%
9	Financial Services	2%
10	Information Technology	2%

Characteristics of Browser-Based Attacks

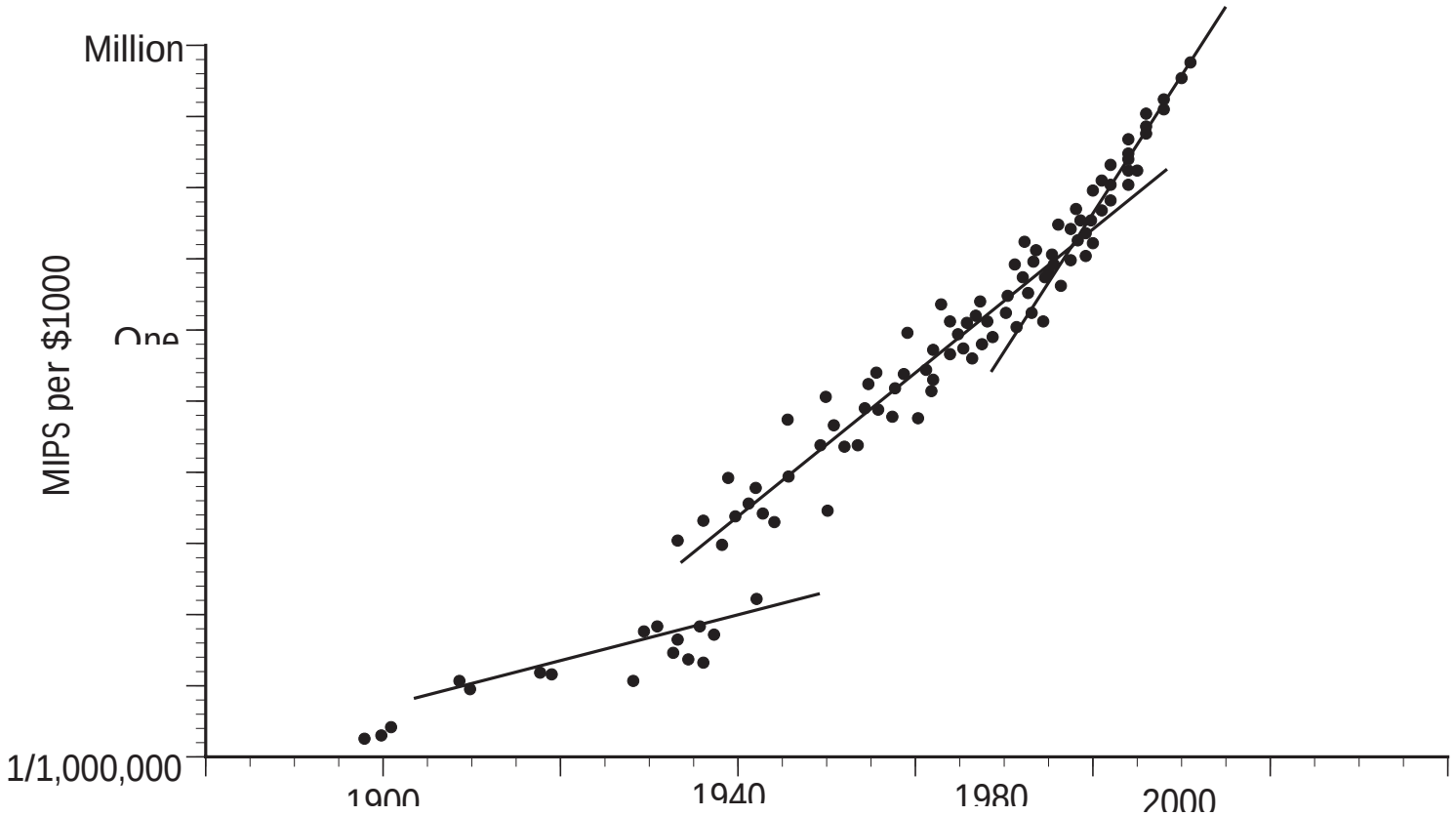
Jan–June 2006 rank	Attack	Jan–June 2006 percent of attackers
1	Multiple Browser Zero Width GIF Image Memory Corruption Attack	31%
2	Microsoft Internet Explorer DHTML Object Race Condition Memory Corruption Attack	19%
3	Microsoft Internet Explorer Remote URLMON.DLL Buffer Overflow Attack	17%
4	Mozilla JavaScript URL Host Spoofing Arbitrary Cookie Access Attack	8%
5	Mozilla Browser BMP Image Decoding Multiple Integer Overflow Attack	7%
6	Microsoft Internet Explorer Bitmap Processing Integer Overflow Attack	3%
7	Mozilla Browser Non-ASCII Hostname Heap Overflow Attack	3%
8	Microsoft Internet Explorer Drag and Drop Attack	3%
9	Mozilla Multiple URI Processing Heap Based Buffer Overflow Attack	2%
10	Microsoft Internet Explorer HTML Document Directive Buffer Overflow Attack	2%

Attack on Wireless Devices

Current rank	Threat	Proportion of total threats
1	Device Probing for an Access Point	30%
2	Spoofed MAC Address	17%
3	Unauthorized NetStumbler Client	16%
4	Rogue Wireless Access Point	8%
5	Unauthentication Association Denial of Service Attack	6%
6	Radio Frequency Jamming Denial of Service Attack	4%
7	CTS Flood Denial of Service Attack	3%
8	Illegal 802.11 Packet	2%
9	Potential Honeypot Access Point	2%
10	Authentication Flood Denial of Service Attack	2%

Future Prospects

Power of Microprocessors



Projected Development of Machine Intelligence

Organism	Number of Neurons	Equivalent MIPS	Computer Processing Available	MIPS/ $1000	Computing Costs
Bacterium	1	0.001	1975	0.001	$1,000
Worm	300	1	1990	1	$1,000
Guppy	100,000	100	1996	1,000	$100
Lizard	2,000,000	10,000	2000	10,000	$1,000
Mouse	60,000,000	100,000	2005 - 2010	100,000	$1,000
Monkey	3 Billion	1,000,000	2010 - 2020	Million	$1,000
Human	100 Billion	100,000,00	2020 - Beyond	Billion	$100

Implications of "Smart" Attackers

- Viruses are sufficiently smart to learn about defenses and reconfigure attacks accordingly.
- Static defenses will not work any more.
- Vulnerability is in software and almost none in hardware.
- Networks must the capability to actively intercept and neutralize the attackers.
- Protection must move from devices (clients) and servers to the network.

Summary

- Information Assurance is now the primary requirement for designing of government networks.
- The virulence of attacks is rising faster than the capabilities of defenses.
- Information Assurance will have to migrate from defending desktops, laptops and PDAs to protecting the network.
- Information Assurance offers attractive career opportunities.