Network Programming and Security

TNM031

Pierangelo Dell'Acqua

www.itn.liu.se/~piede

Background

- Information Security requirements have changed
  - Traditionally provided by physical and administrative mechanisms
  - Nowadays the use of networks and communications links requires:
    - measures to protect data during transmission
    - automated tools to protect files and other stored information

Aim of the course

- Computer Security
  - generic name for the collection of tools designed to protect data
- Network Security
  - consists of measures to protect data during transmission
- This course focuses on network security

Lec1: Outline

1. Attack trends 2015
2. Types of Attacks
3. Security Goals
4. Plan-Protect-Respond Cycle
5. Password Cracking

1. Attack Trends 2015

Security Surveys

- Symantec
  - Internet Security Threat Report
- Microsoft
  - Security Intelligence Report
- F-secure
  - Threat Report

Attack Trends

- Growing Randomness in Victim Selection
  - In the past, large firms were targeted
  - Now, targeting is increasingly random
- Growing Malevolence
  - Most early attacks were not malicious
  - Malicious attacks are becoming the norm
- Targeted attacks continue to evolve

- In 2015, the number of Zero-Day vulnerabilities more than doubled from 2014
- Four of the five most exploited zero-day vulnerabilities in 2015 were Adobe Flash
- Over half a billion personal records were stolen or lost in 2015
- Over one million web attacks in 2015
- Ransomware increased 35 Percent in 2015
- Symantec blocked 100 million fake technical support scams in 2015

Attackers trick people with pop-ups that alert them to a serious error or problem, thus steering the victim to call a technical support representative that attempts to sell the victim worthless services

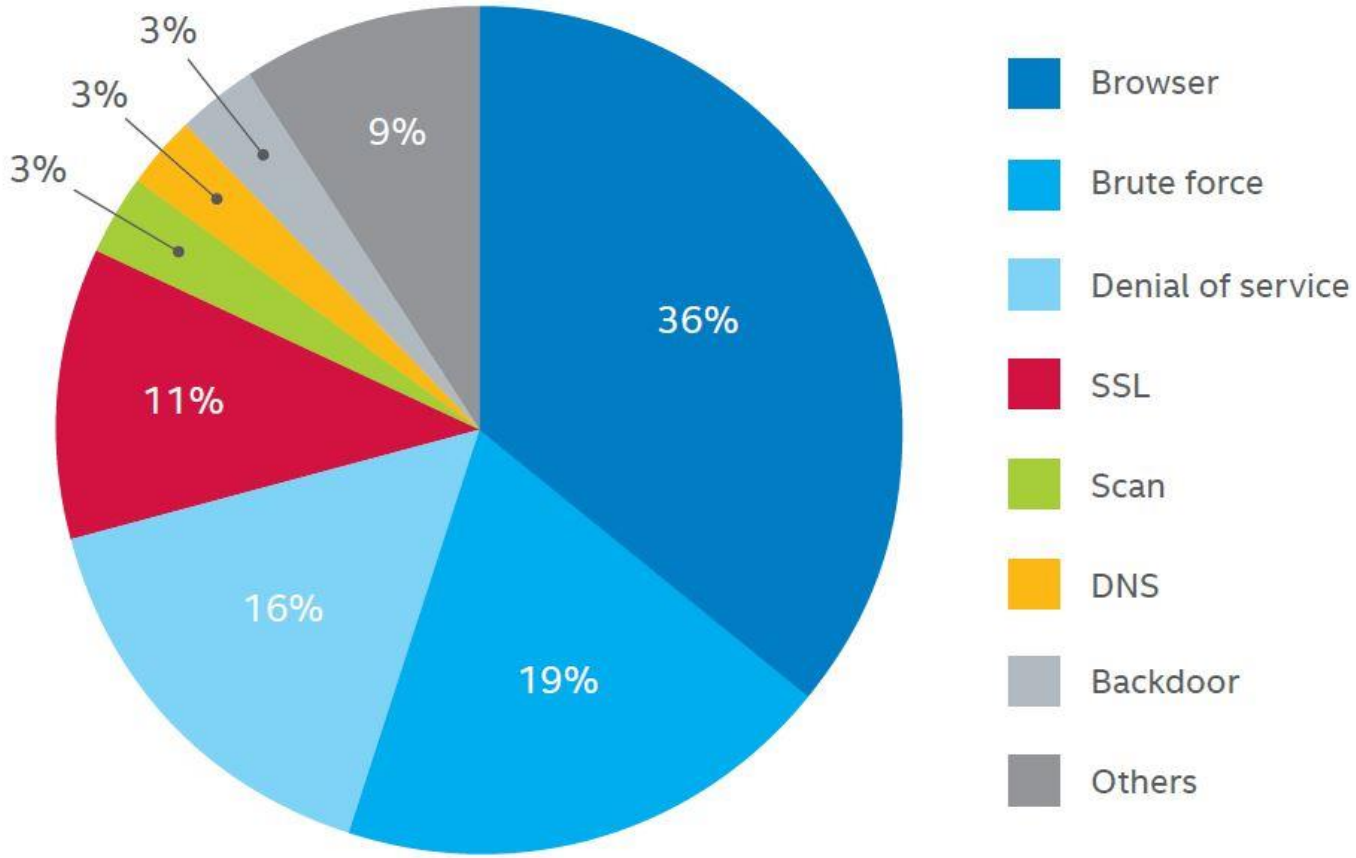

Top 10 Sub-Sectors Breached
by Number of Incidents
Healthcare 120
Business 20
Education 20
Insurance 17
Hotels 14
Wholesale Trade 10
Eating and Drinking Places 9
Executive, Legislative, & General 9
Depository Institutions 8
Social Services 6

Top 10 Types of Information Exposed

- *Financial information includes stolen credit card details and other financial credentials.*

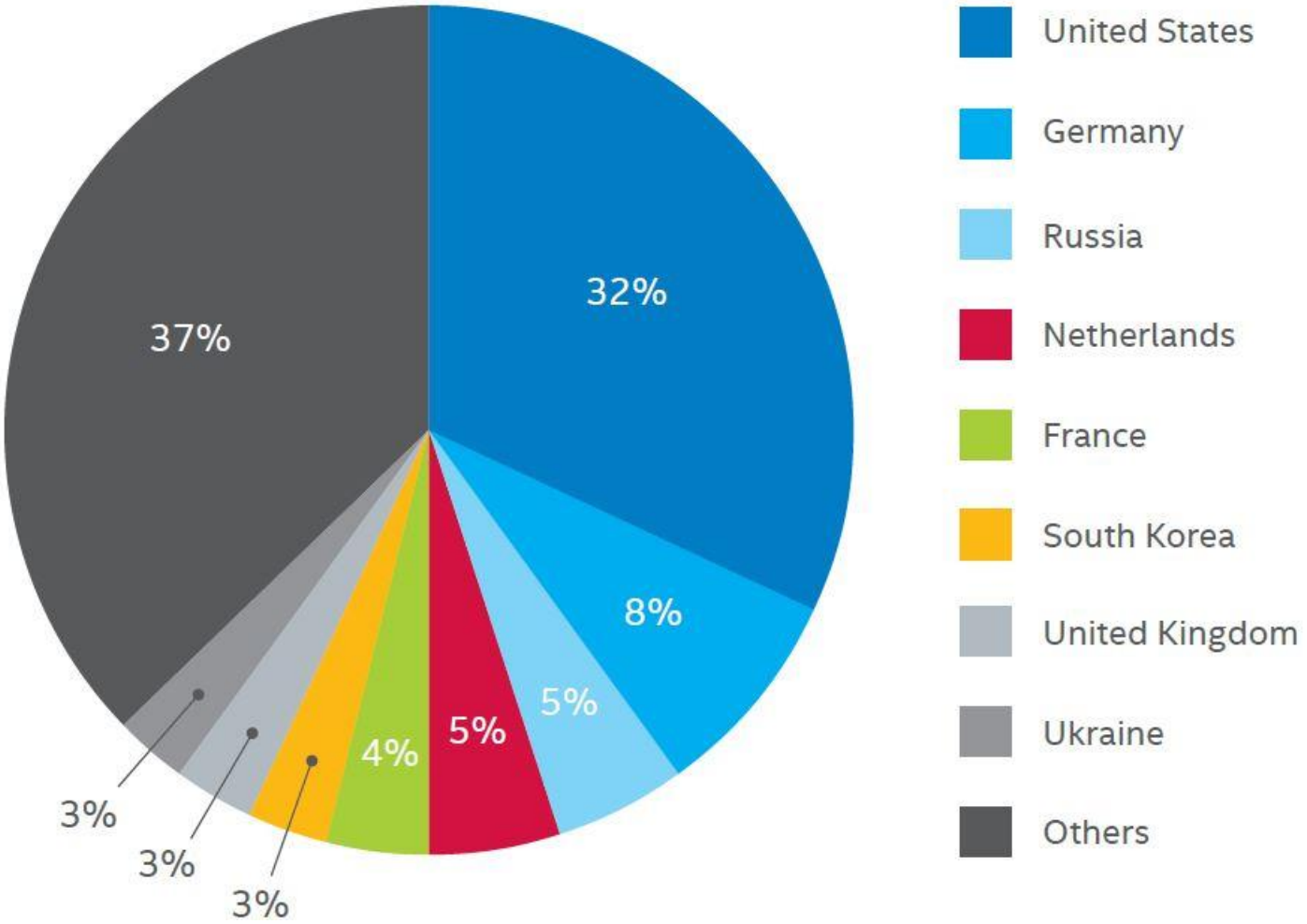
	2015 Type	2015 %	2014 Type	2014 %
1	Real Names	78%	Real Names	69%
2	Home Addresses	44%	Gov. ID Numbers (e.g., SSN)	45%
3	Birth Dates	41%	Home Addresses	43%
4	Gov. ID Numbers (e.g., SSN)	38%	Financial Information	36%
5	Medical Records	36%	Birth Dates	35%
6	Financial Information	33%	Medical Records	34%
7	Email Addresses	21%	Phone Numbers	21%
8	Phone Numbers	19%	Email Addresses	20%
9	Insurance	13%	User Names & Passwords	13%
10	User Names & Passwords	11%	Insurance	11%

Network attacks, 2015

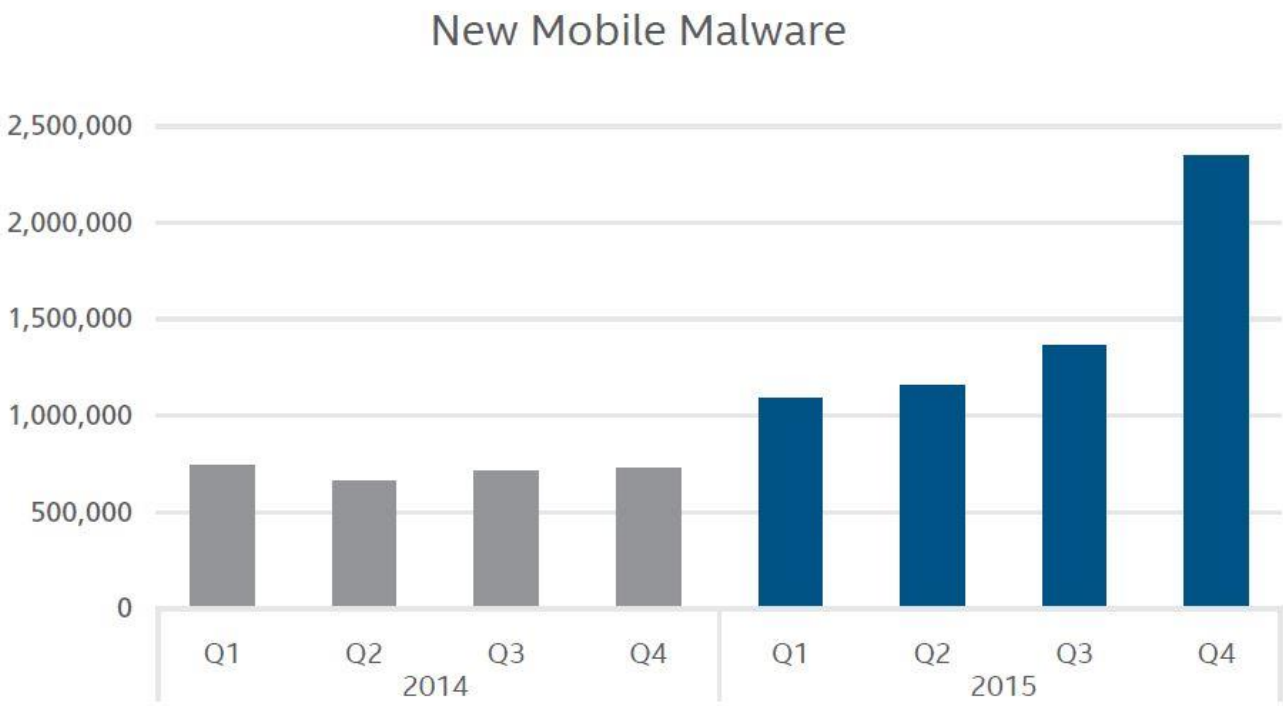


McAfee

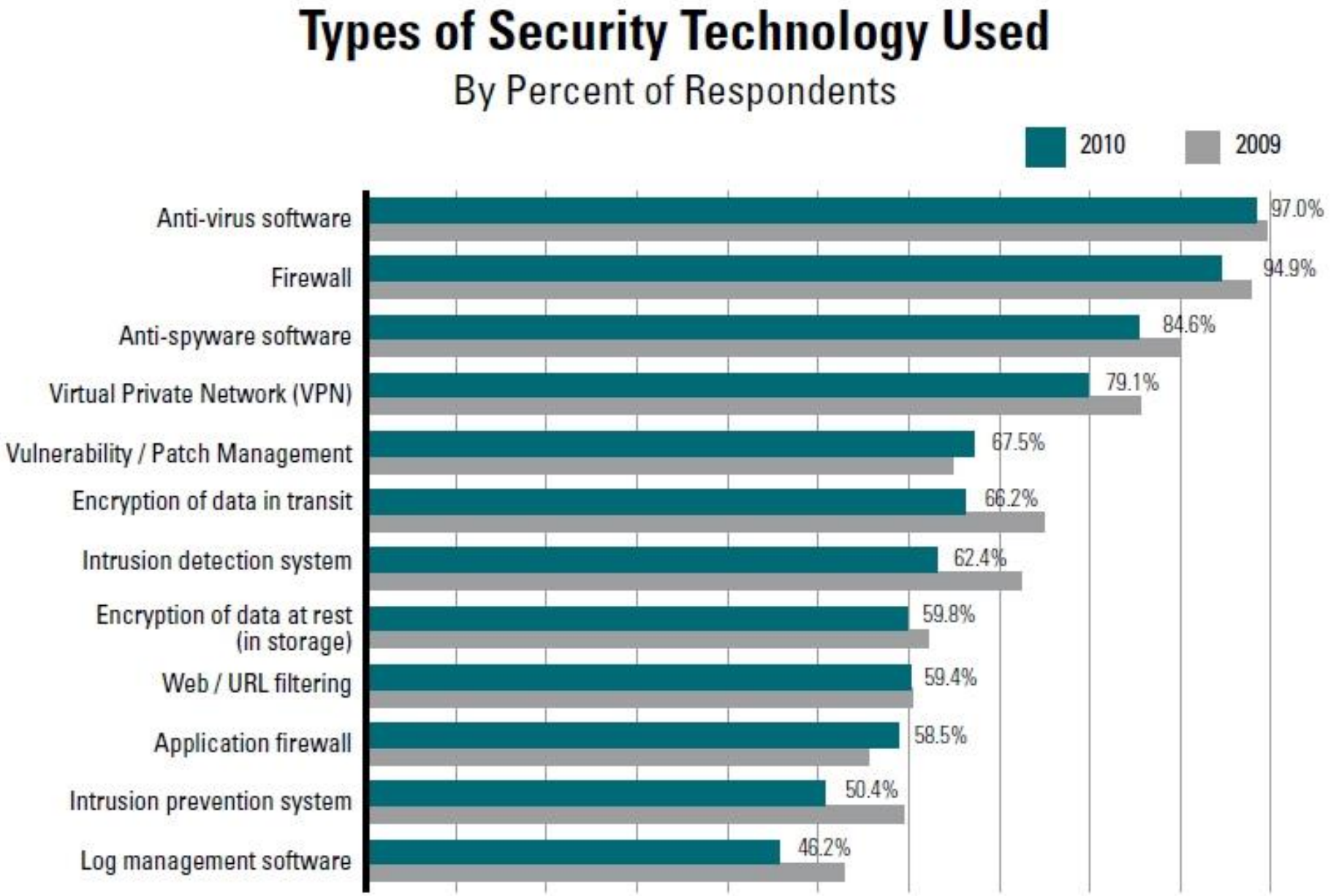
Top Countries Hosting Botnet Control Servers



This quarter we recorded a 72% increase in new mobile malware samples. We believe that Google's August 2015 notification that it would release monthly updates to its Android mobile operating system forced malware authors to develop new malware more frequently in response to the enhanced security in each monthly release of the operating system. The detection of newly developed mobile malware is reflected in our Q4 statistics.




Peek into the Future:
The Risk of Things
Internet-connected things
Numbers in billions
20.8 billion
(predicted)
The insecurity of things
Medical devices. Researchers have found potentially deadly vulnerabilities in dozens of devices such as insulin pumps and implantable defibrillators.
Smart TVs. Hundreds of millions of Internet-connected TVs are potentially vulnerable to click fraud, botnets, data theft and even ransomware, according to Symantec research.
Cars. Fiat Chrysler recalled 1.4 million vehicles after researchers demonstrated a proof-of-concept attack where they managed to take control of the vehicle remotely. In the UK, thieves hacked keyless entry systems to steal cars.
Today in the USA, there are
25 connected devices per 100 inhabitants
6.4 billion
4.9 billion
3.9 billion
20
19
18
17
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
2014
2015
2016
2020


Types of Security Technology Used
By Percent of Respondents
2010
2009
Anti-virus software
97.0%
Firewall
94.9%
Anti-spyware software
84.6%
Virtual Private Network (VPN)
79.1%
Vulnerability / Patch Management
67.5%
Encryption of data in transit
66.2%
Intrusion detection system
62.4%
Encryption of data at rest (in storage)
59.8%
Web / URL filtering
59.4%
Application firewall
58.5%
Intrusion prevention system
50.4%
Log management software
46.2%

2. Types of Attacks

Types of Attacks

Social Engineering Attacks
- Opening Attachments
- Password Theft
- Information Theft

Dialog Attacks
- Eavesdropping
- Impersonation
- Message Alteration

Penetration Attacks
- Scanning
- Break-in
- Denial of Service
- Malware

Social Engineering Attacks

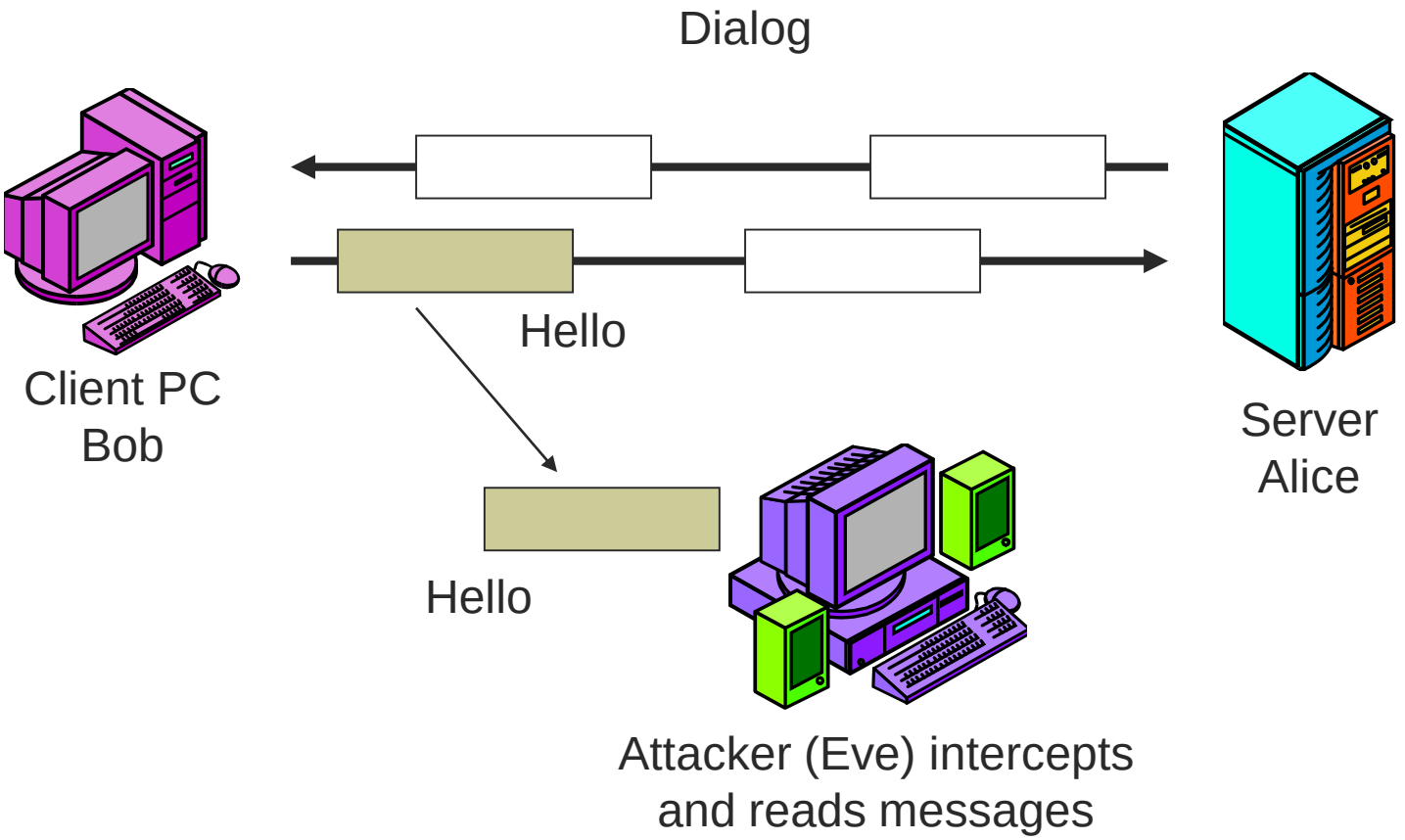
- Social Engineering is tricking someone to give out information
  - Asking for a file to be sent to you
  - Asking for a password claiming to be someone with rights to know it
  - Tricking someone to open an e-mail attachment that may contain a virus

Social Engineering Attacks

- Social Engineering Defenses
  - Training
  - Enforcement through sanctions (punishment)

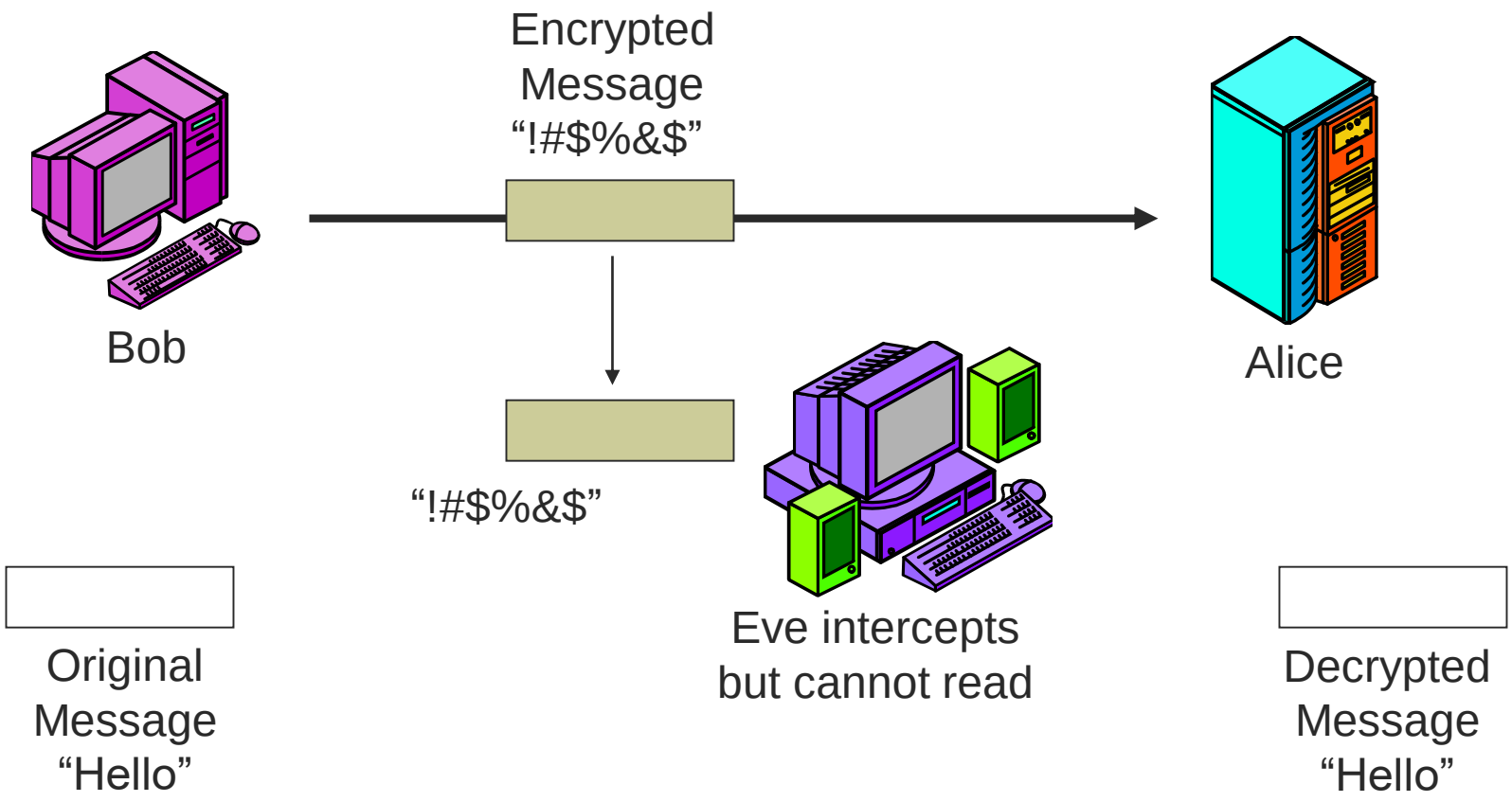
Dialog Attacks

Eavesdropping = to listen secretly to a private communication



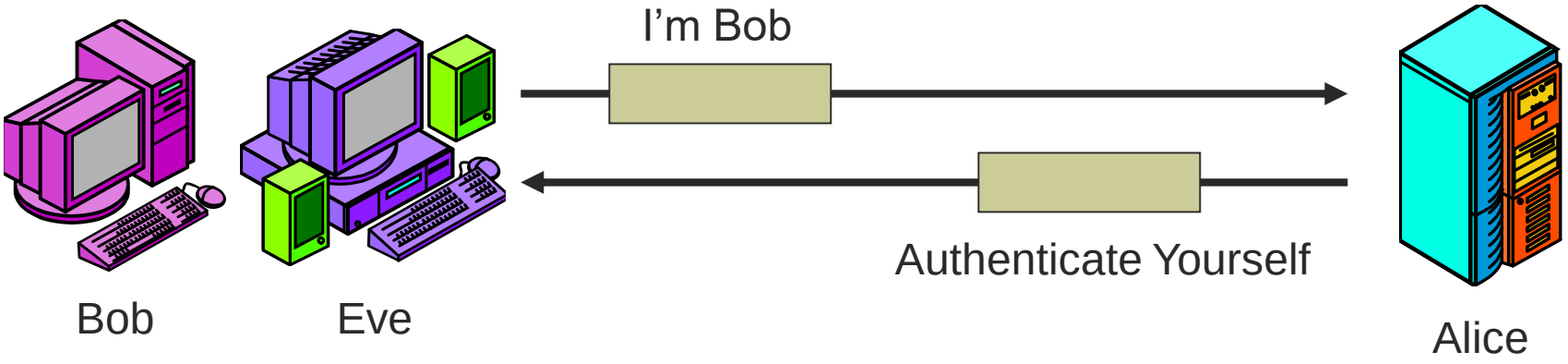
Dialog Attacks

Eavesdropping Defense: Encryption for Confidentiality



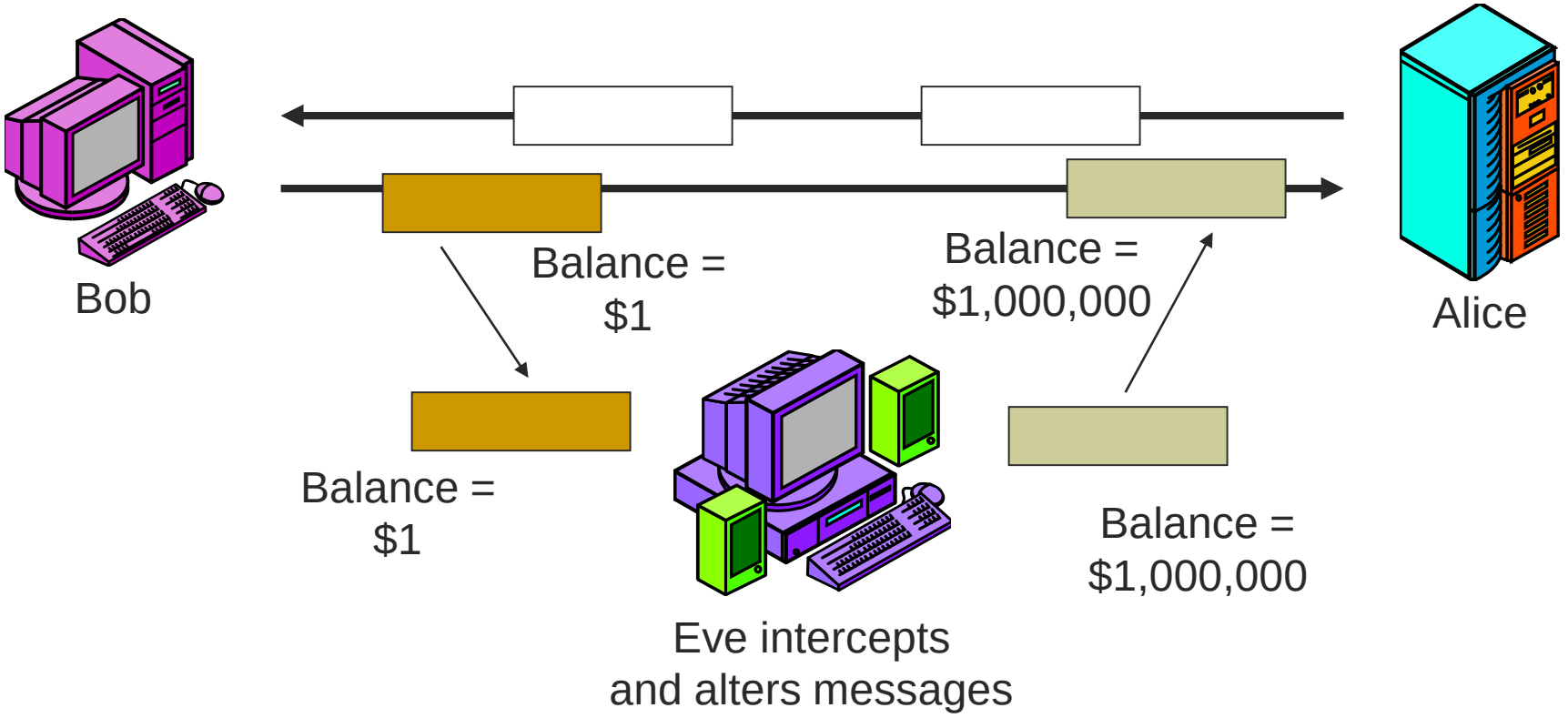
Dialog Attacks

Impersonation



Dialog Attacks

Message Alteration

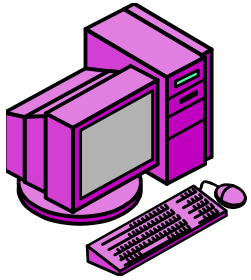


Dialog Attacks

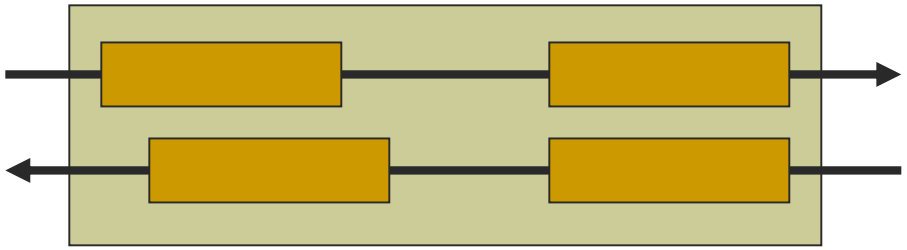
encryption	defeats eavesdropping
authentication	defeats impersonation
encryption + authentication	gives data integrity

Dialog Attacks

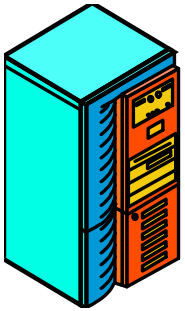
Secure Dialog System



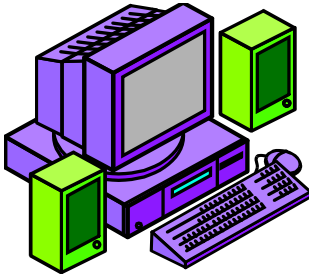
Bob



Automatically Handles:
Encryption
Authentication
Data Integrity



Alice



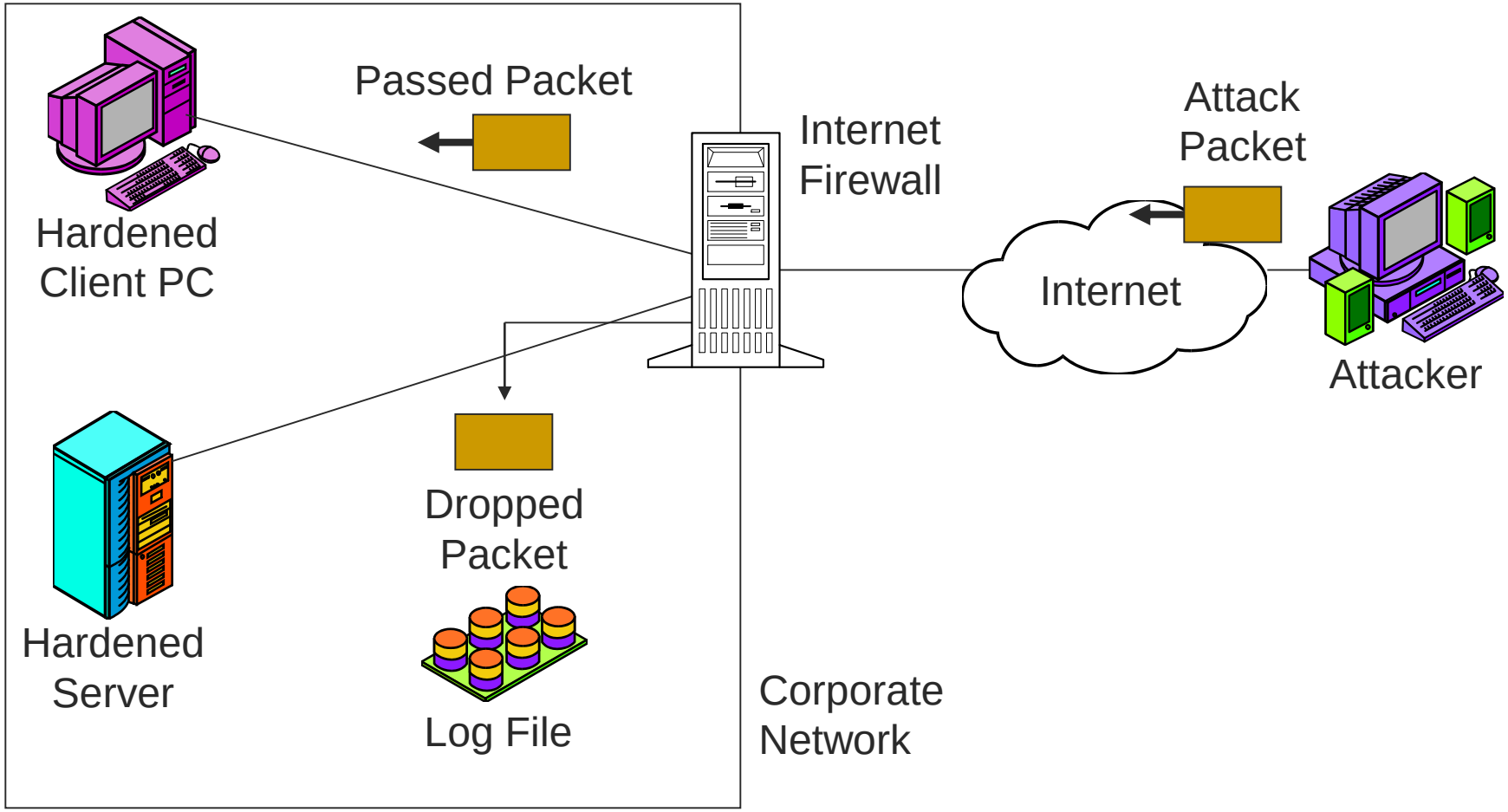
Eve cannot
read messages, alter
messages, or impersonate

Penetration Attacks

- One or many messages (packets) are sent to an internal network of a corporation
  - to explore its defenses
  - to do damage

Penetration Attacks

Internal Network and Firewalls

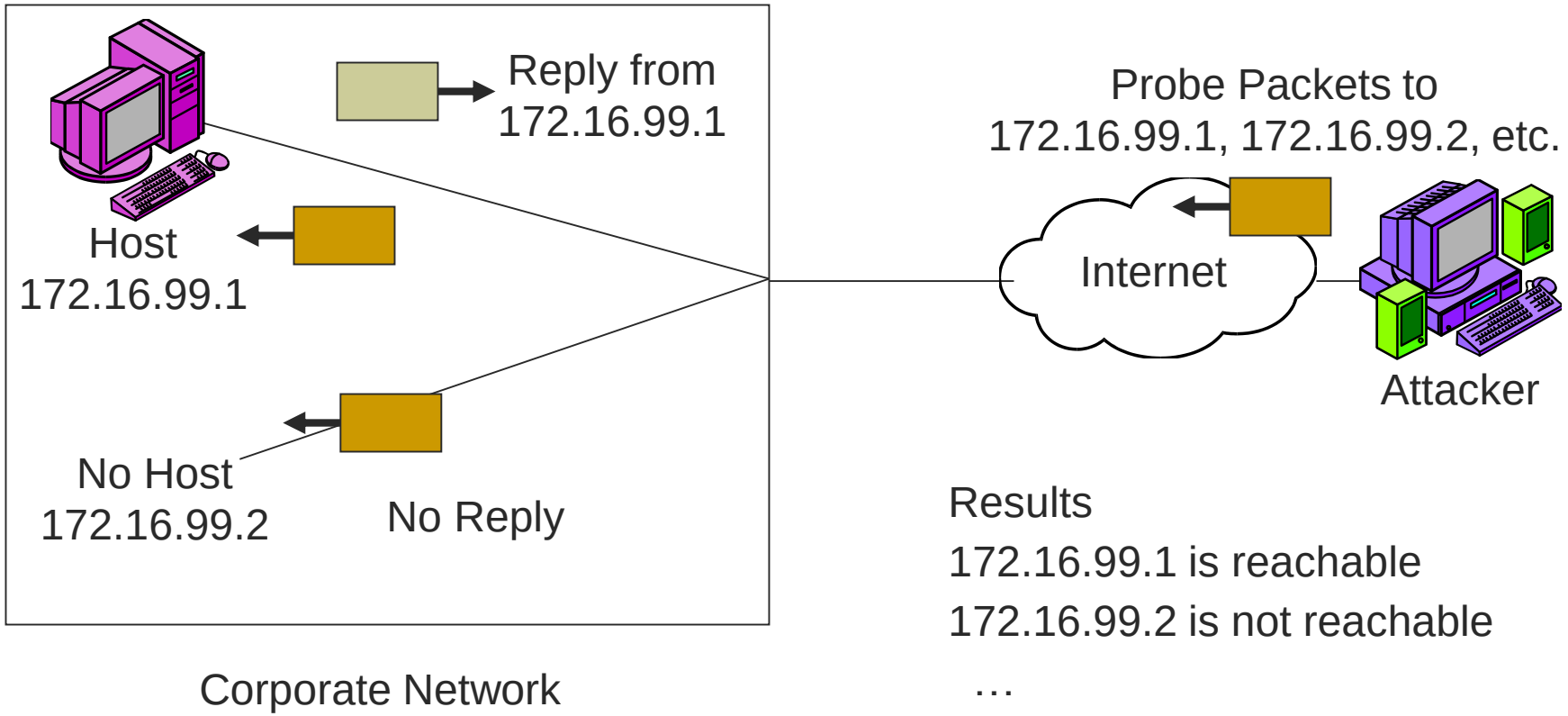


Hardening = process of securing a system

Penetration Attacks

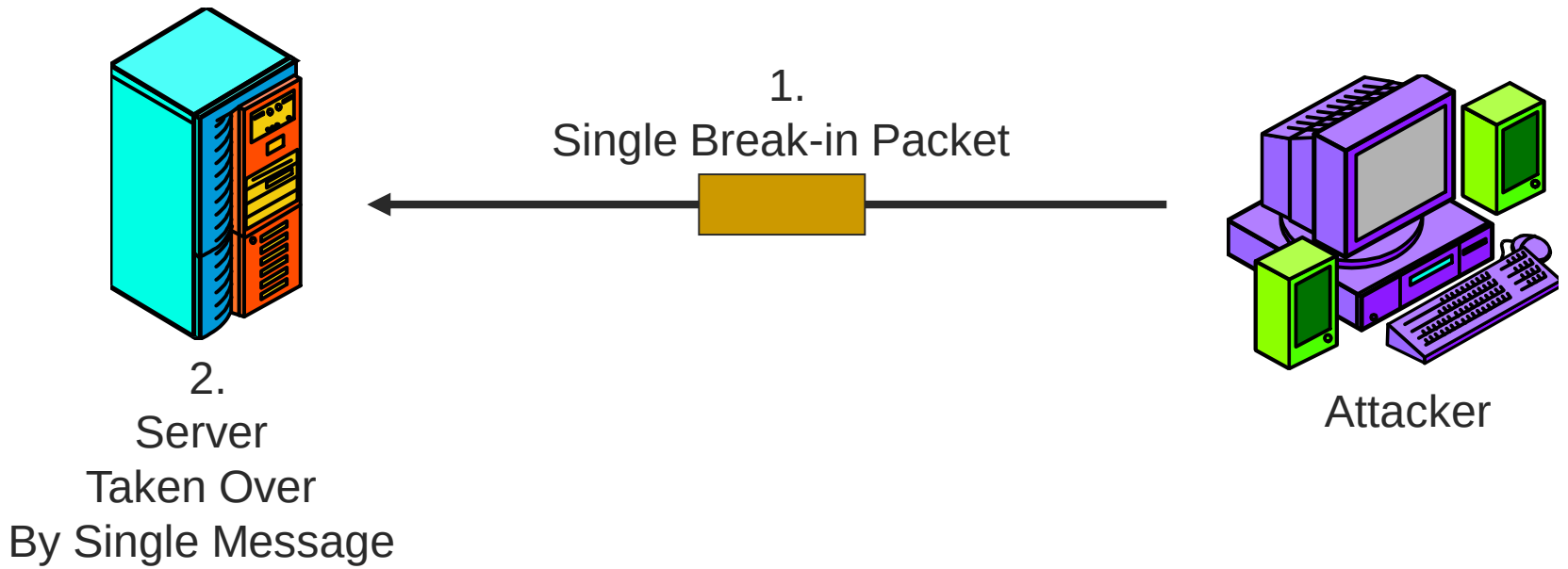
Scanning (Probing)

Probing = to make a critical exploration



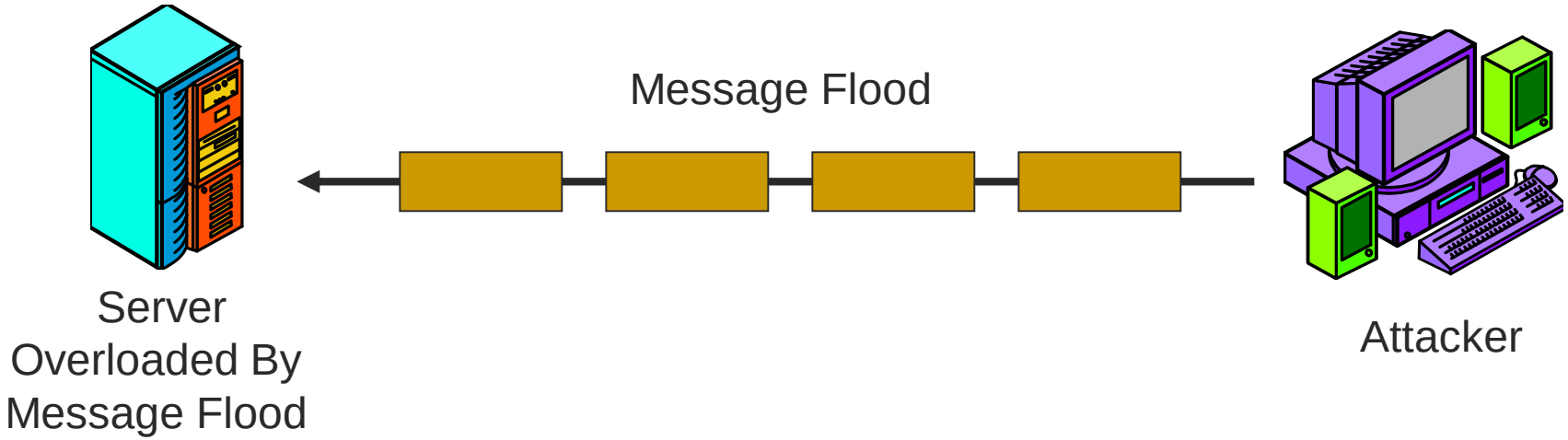
Penetration Attacks

Break-in



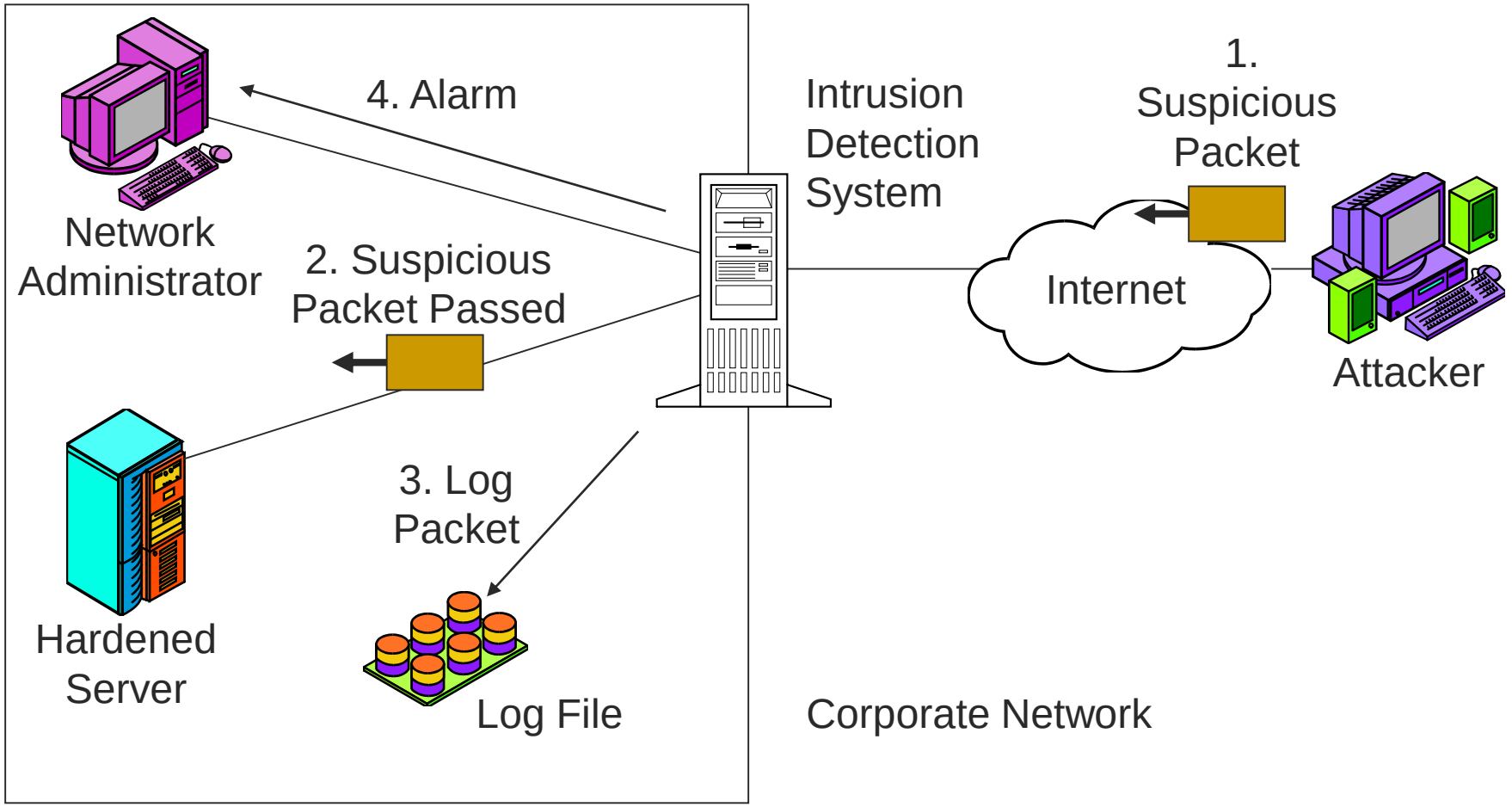
Penetration Attacks

Denial-of-Service (DoS)



Penetration Attacks

Intrusion Detection System (IDS)



Penetration Attacks

Malware

- Essentially, a category of attacks consisting of virus and worms
  - The attacker releases them, and they spread to their victims autonomously
  - Virus are spread via the opening of e-mail attachments, drive-by downloads, etc

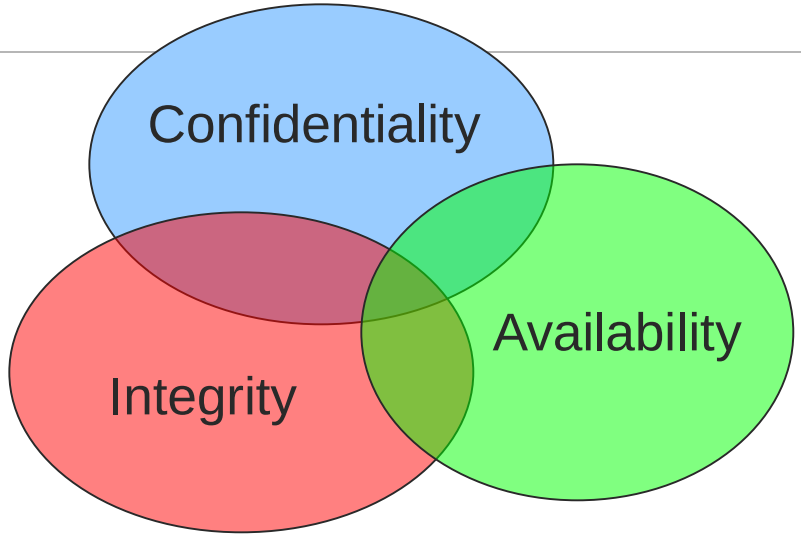
    Executing an infected file infects other files
  - Worms spread autonomously using scanning and break-in attacks

Summary

- Penetration Attacks
  - Scanning
  - Break-in attacks
  - Denial-of-Service attacks
  - Malware
- Defenses
  - Firewall (actually drops attack packets)
  - Intrusion detection system (only gives warnings)
  - Anti-virus

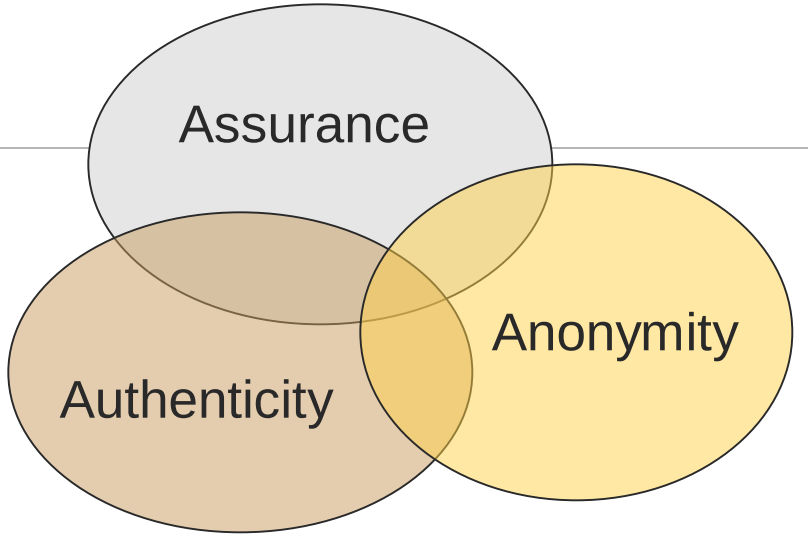
3. Security Goals

Security Goals: CIA



- Confidentiality
  - Attackers cannot read messages
- Integrity
  - If attackers change messages, this will be detected
- Availability
  - System is able to serve users

Other Security Goals: AAA



- Assurance
  - Refers to how trust is provided and managed in computer systems
- Authenticity
  - Ability to determine that statements, policies, and permissions issued by persons or systems are genuine
  - Provides non-repudiation
- Anonymity
  - Property that certain records or transactions cannot be attributed to any individual

4. Plan-Protect-Respond Cycle

Planning

- Need for comprehensive security (no gaps)
- Risk analysis
  - Enumerating threats
  - Threat severity = estimated cost of attack * probability of attack
  - Value of protection = threat severity – cost of countermeasure
  - Prioritize countermeasures by value of protection

Threat Severity Analysis

	Threat	A	B	C	D
1	Cost if attack succeeds	$500,000	$10,000	$100,000	$10,000
2	Probability of occurrence	80%	20%	5%	70%
3	Threat severity	$400,000	$2,000	$5,000	$7,000
4	Countermeasure cost	$100,000	$3,000	$2,000	$20,000
5	Value of protection	$300,000	- $1,000	$3,000	- $13,000
6	Apply countermeasure?	Yes	No	Yes	No
7	Priority	1	-	2	-

Protecting

- Installing protections: firewalls, IDSs, host hardening, etc.
- Updating protections as the threat environment changes
- Testing protections: security audits

Security audit = examination and review of a system to identify security weaknesses

Responding

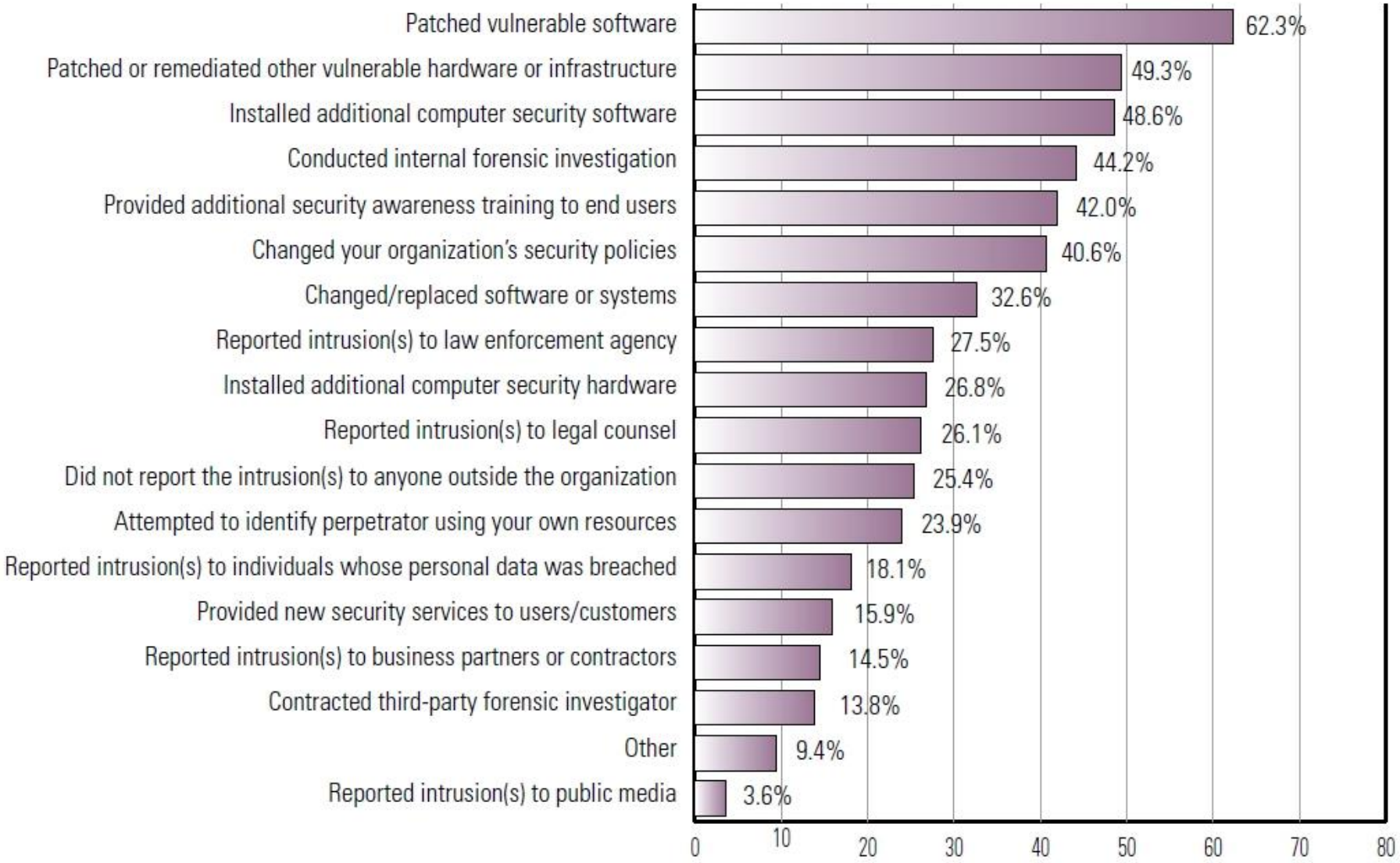
- Incident detection and determination
  - Procedures for reporting suspicious situations
  - Determination that an attack really is occurring
  - Description of the attack

Responding

- Recovery
  - Stop the attack
  - Repair the damage
- Punishment
  - Prosecution
  - Employee Punishment
- Fixing the vulnerability that allowed the attack

Actions Taken After an Incident

By Percent of Respondents



5. Password Cracking

Reusable Passwords

- Reusable Passwords
  - A password you use repeatedly to get access to a resource on several occasions
  - Bad because attacker will have time to learn it
- Difficulty of cracking passwords by guessing remotely
  - Usually cut off after a few attempts
  - However, if attacker can steal the password file, he/she can crack passwords

Password Cracking Programs

- l0phtcrack
  - Spelled: lower-case L, zero, phtcrack
  - Password cracking program
  - Run on a server (need physical access)
  - Or copy password file and run l0phtcrack on another machine

Brute-force Password Cracking

- Try all possible character combination
- Longer passwords take longer time to crack
- Using more characters also takes longer time
  - Alphabetic, no case sensitive (26 possibilities)
  - Alphabetic, case sensitive (52)
  - Alphanumeric (letters and numbers) (62)
  - All keyboard characters (~80)

Password Length

Password Length In Characters	Alphabetic, No Case (N=26)	Alphabetic, Case (N=52)	Alphanumeric: Letters & Digits (N=62)	All Keyboard Characters (N=~80)
1	26	52	62	80
2	26^2=676	2,704	3,844	6,400
4	26^4=456,976	7,311,616	14,776,336	40,960,000
6	308,915,776	19,770,609,664	56,800,235,584	2.62144E+11
8	2.08827E+11	5.34597E+13	2.1834E+14	1.67772E+15
10	1.41167E+14	1.44555E+17	8.39299E+17	1.07374E+19

Password Length

Password Length In Characters	Alphabetic, No Case (N=26)	Alphabetic, Case (N=52)	Alphanumeric: Letters & Digits (N=62)	All Keyboard Characters (N=~80)
1	< 1sec	< 1sec	< 1sec	< 1sec
2	< 1sec	< 1sec	< 1sec	< 1sec
4	< 5 sec	< 2 min	< 3 min	< 7 min
6	< 52 min	< 55 hours	158 hours	8420 years

Suppose your PC can process 100.000 keys/sec

Password Cracking Methods

- Guess
- Brute Force Attacks
  - Try all possible character combinations
  - Slow with long passwords length
- Dictionary attacks
  - Try common words (“123456”, “password”, etc.)
  - There are only a few thousand of these
  - Cracked very rapidly

Password Cracking Methods

- Malware
  - A key logger can be installed by malware which records everything you type
- Offline cracking
  - Often the target was compromised
  - This provides access to the system servers and user password hash files
- Social engineering

Password Cracking Defenses

- Good passwords
  - At least 6 characters long
  - Change of case not at beginning
  - Digit (0 through 9) not at end
  - Example: triV6#ial
  - Other keyboard character not at end
  - Password checker available
- Change your password frequently