NETWORK SECURITY

Ch. 1: Introduction

PTIIK
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER

Networking… at a glance

Discrete Mathematics	Advance Networking
Operating Systems	Network Analysis
Computer Networks	Multimedia Networking
Network Security	Network Programming

Distributed Systems

System Administrations

PTIIK

Course Design

- Classes
  - 2 Credits
- Exercises (assistant required)
  - 1 Credits
- Evaluation
  - 2 Structured Task (25 %)
  - 4 Quiz (25 %) *all of a sudden
  - 1 Midterm Test (25 %)
  - 1 Final Test (25 %)

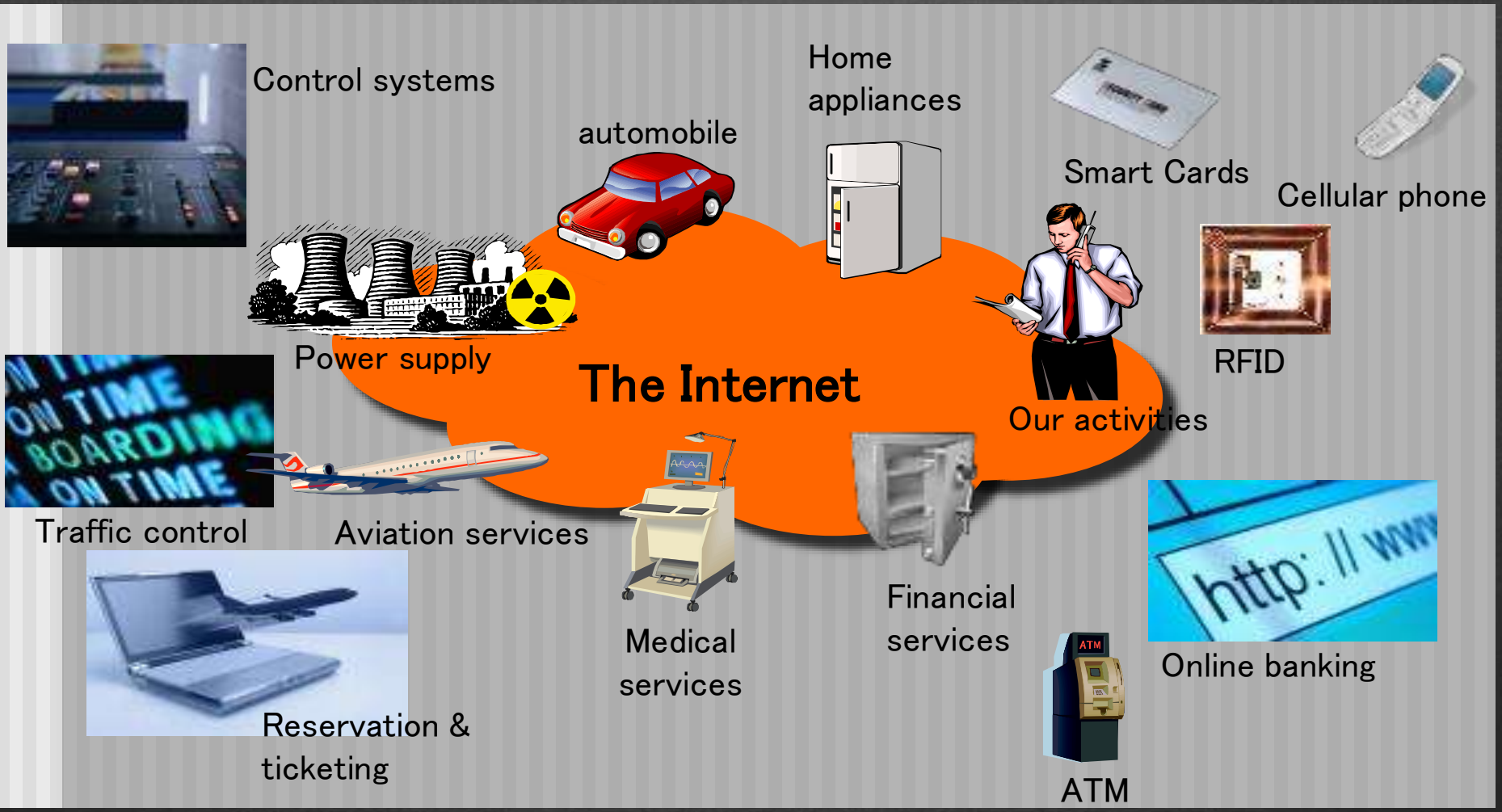
References

- *Douligeris, Christos : "Network Security : Current Status and Features Directions" , John Wiley & Sons , 2007*
- *Kizza, Joseph Migga: "Computer Network Security" , Springer, 2005*
- *Canavan, John E : "Fundamentals of Network Security" , Artech House , 2001*
- *Cole, Eric : "Network Security Bible" , John Wiley & Sons , 2005*

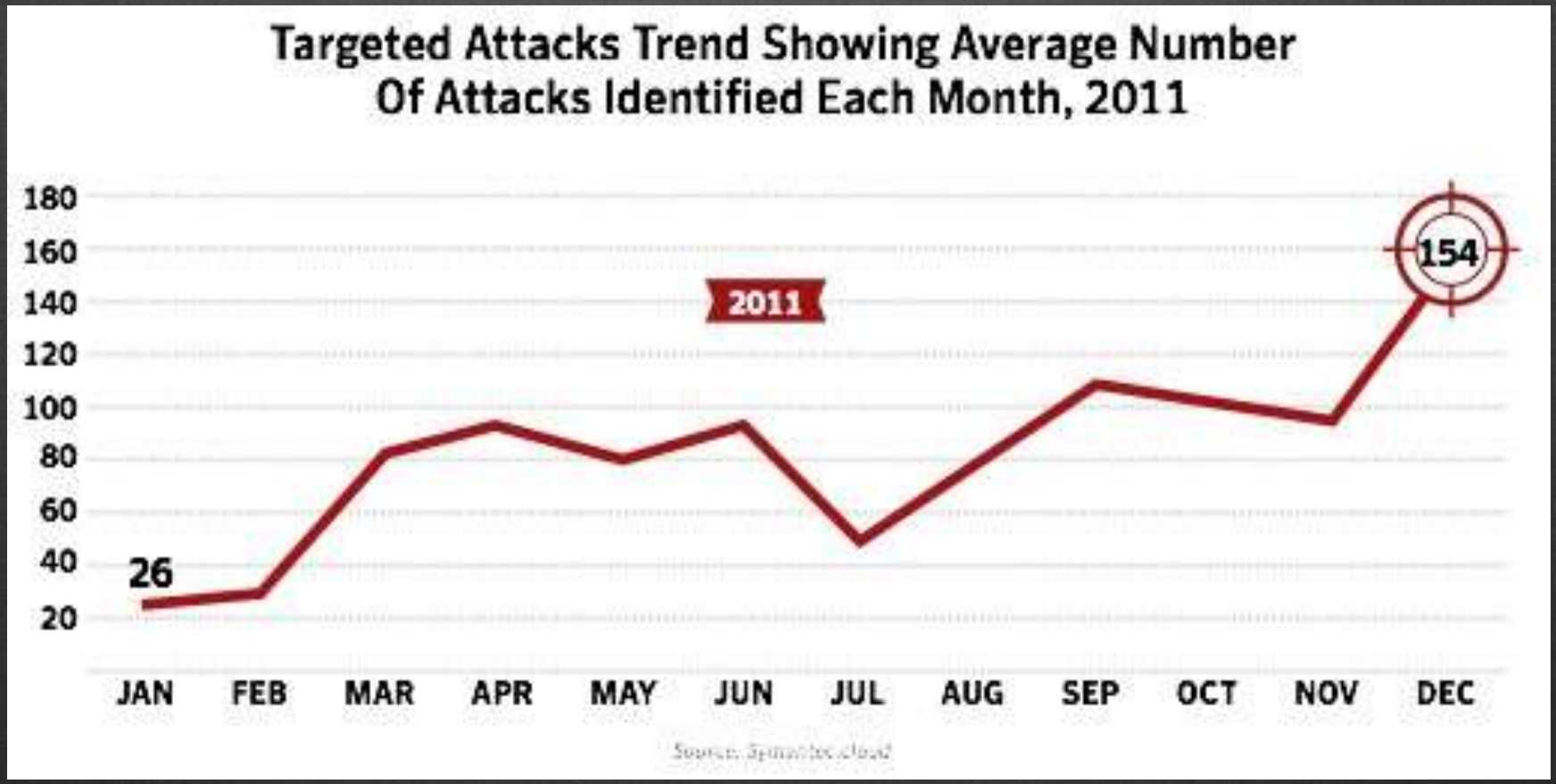
Course Content

- 01 Introduction
- 1.1 Some Terminology
- 1.2 Network Security Attacks
- 1.3 Sources of Security Threats
- 1.4 Security Threat
  - 1.4.1 Motives
  - 1.4.2 Management
  - 1.4.3 Correlation
  - 1.4.4 Awareness

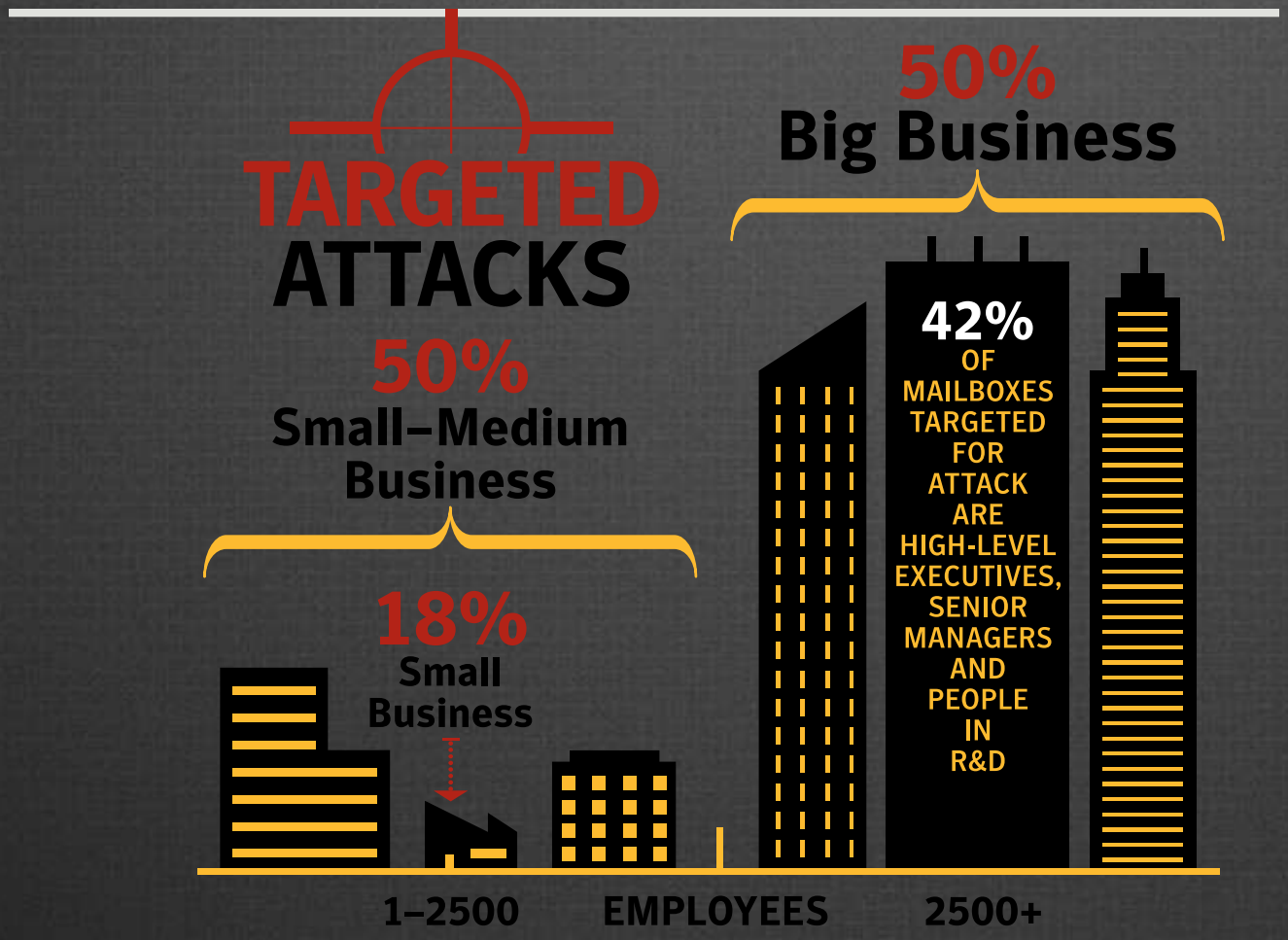
Current State

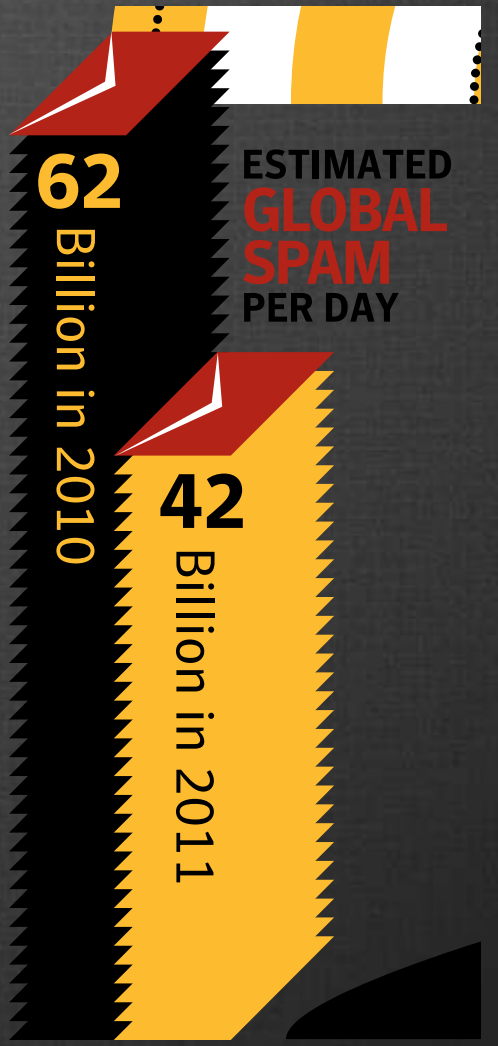


Current State



Current State





Current State

Figure 7

Top-Ten Sectors By Number Of Data Breaches, 2011

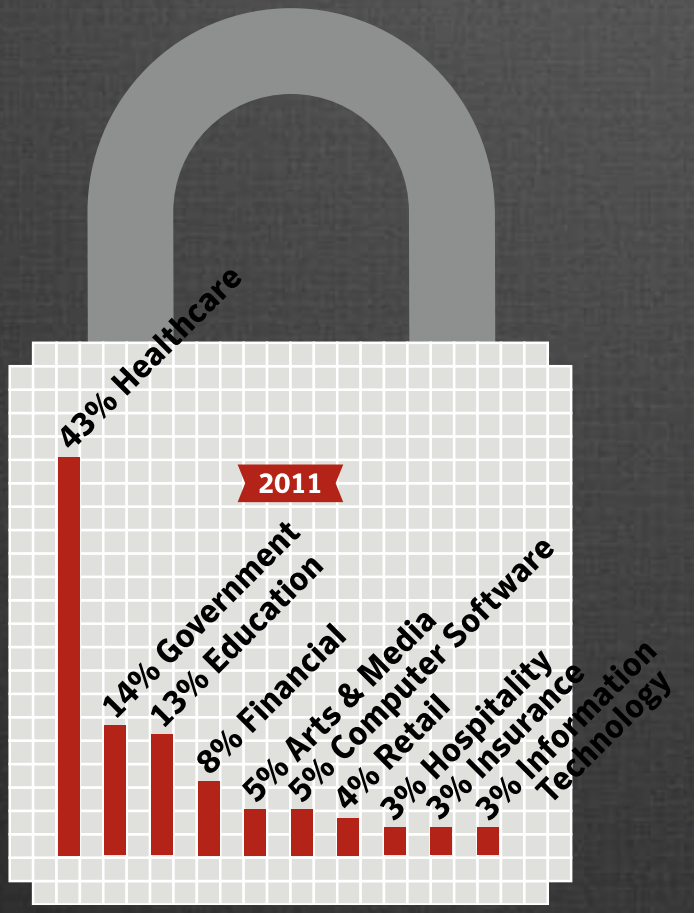
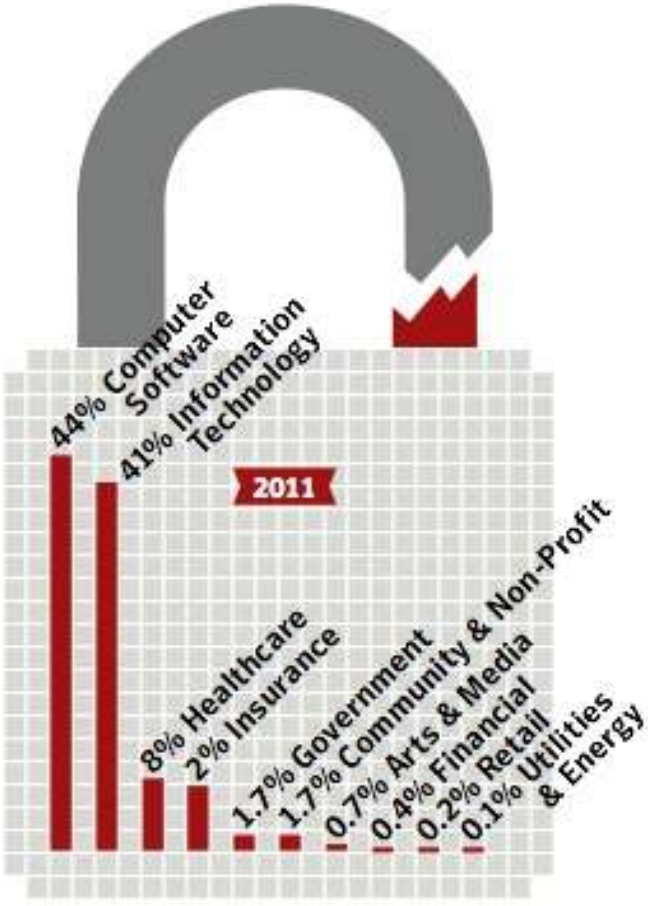


Figure 8

Top-Ten Sectors By Number Of Identities Exposed, 2011

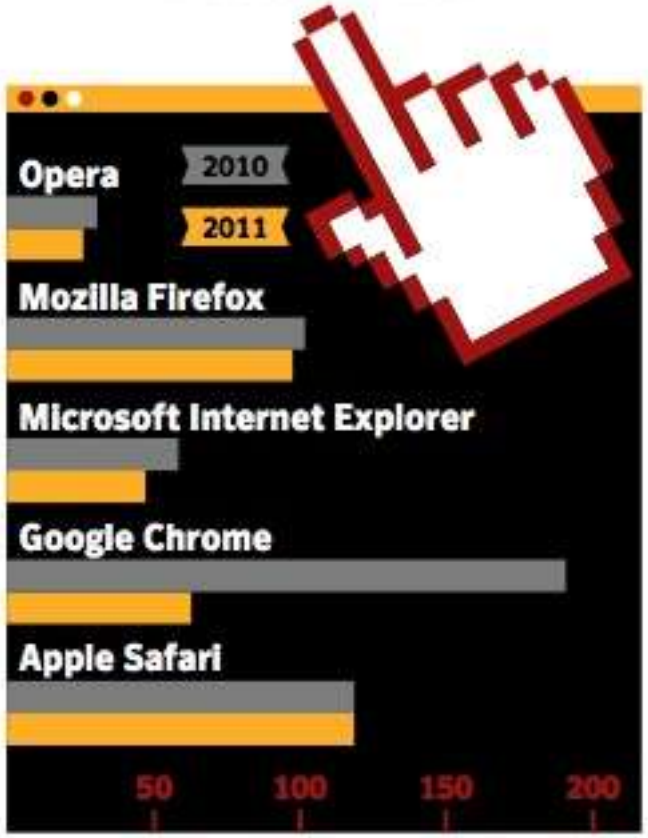


Source: Symantec

Current State

Figure 19

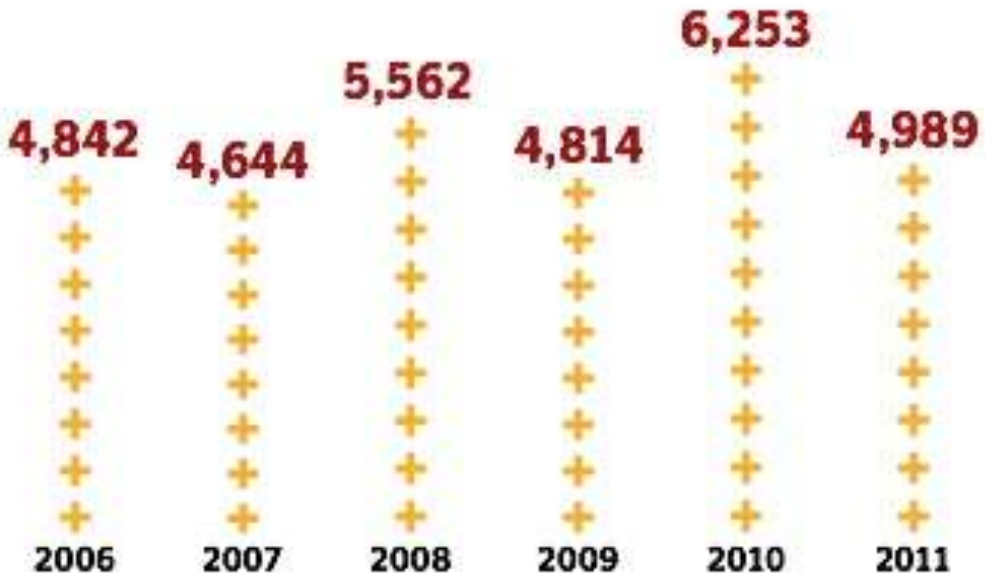
Browser Vulnerabilities In 2010 And 2011



Source: Symantec

Figure 18

Total Number Of Vulnerabilities Identified, 2006-2011



Source: Symantec

Current State

- Top-5 Most Infected Websites
  - Blogs and Web communications.
  - Hosting/Personal hosted sites.
  - Business/Economy.
  - Shopping.
  - Education and Reference.

Current State

- Web based attacks increased by 36% with over 4,500 new attacks each day.
- 403 million new variants of malware were created in 2011, a 41% increase of 2010.
- SPAM volumes dropped by 13% in 2011 over rates in 2010.
- 39% of malware attacks via email used a link to a web page.
- Mobile vulnerabilities continued to rise, with 315 discovered in 2011.

Total notifications: **119** of which **36** single ip and **83** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2012/02/27	JEMBER HACKER TEAM	H	M				www.fathimiah.com	Linux	mirror
2012/02/27	JEMBER HACKER TEAM	H	M				www.amperanews.com	Linux	mirror
2011/12/15	Jember Hacker Team	H					www.glocalsuppliesservices.com	Linux	mirror
2011/12/14	Jember Hacker Team	H					mykawin.com	Linux	mirror
2011/12/14	Jember Hacker Team	H					www.myberita.com	Linux	mirror
2011/12/14	Jember Hacker Team	H					www.carpos.com.my	Linux	mirror
2011/12/13	Jember Hacker Team	H	M				okeslip.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				birumalam.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				ehsempoi.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				tanyaft17.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				solehahworks.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				gempakcyber.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				visioncare-optometry.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				xpert.com.my	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				rumorslogy.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				segalanyadisini.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				hfmohd.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				atmajujaya.com	Linux	mirror
2011/12/11	Jember Hacker Team	H					heshroon.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				www.dropshipbabyproducts.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				www.yusufultraman.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				jikebiotechgroup.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				www.kiddolegacy.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				www.kedaiemas2u.com	Linux	mirror
2011/12/11	Jember Hacker Team	H	M				www.shafeeqphotography.com	Linux	mirror

Mirror saved on: 2011-12-09 05:31:19

Notified by: Jember Hacker Team **Domain:** http://omahmoesik.com **IP address:** 116.213.48.131
System: Linux **Web server:** Apache Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2011-12-09 05:31:19

HAC ED Y J MBE HA KER TEA

STATUS : CLOSED
DEFACER : Jember Hacker Team
NOTICE : Nothing Secure ..
TEAM : JEMBER HACKER TEAM
GREETS : -=- Unwanted -=- d'ZheNwaY -=- iBox -=- anarchy666 -=- chengcheng -=- MJL007 -=- 4Ng3L~5kY -=- newbie-herbet -=- vbenk -=- And YOU -=-


http://rakernas.mahkamahaghttp://bappeda.bireuenkab.gchttp://outreacher.depsos.go.i

#tangodown

Berikut KabarKampus tampilkan beberapa screenshot website yang diretas oleh hacker anonymous dan kawan-kawan. Para hacker tidak terima, peretas situs www.presidensby.info diancam dengan hukuman penjara selama 12 tahun. Perlu diketahui peretas situs SBY berasal dari Jember lulusan SMK dengan nama Jember Hacker Team. Kini si peretas telah diamankan oleh Mabes Polri.

What Wildan Did?

PTIIK
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER

1.1 Some Terminology

- Definition of network security can be constructed by defining its two components, security and networks.
- Security can be defined as follows:
  - A situation with no risk, with no sense of threat.
  - The prevention of risk or threat.
  - The assurance of a sense of confidence and certainty.

1.1 Some Terminology

- Security, is described through the accomplishment of some basic security properties, namely confidentiality, integrity, and availability of information.
- Confidentiality is the property of protecting information from all non-intended or unauthorized users.
- Integrity is the property of protecting the content of information from alteration by unauthorized users.

1.1 Some Terminology

- Availability is the property of protecting information from non authorized temporary or permanent withholding of information.
- Other basic properties of security is authentication and nonrepudiation.
- Authentication is divided into peer-entity authentication and data origin authentication.

1.1 Some Terminology

- Nonrepudiation is the property of ensuring that principals that have committed to an action cannot deny that commitment at a latter time.
- In practical approach, security involves the protection of information assets.

1.1 Some Terminology

- The protection of assets can be achieved through several security mechanisms, that is, aimed at the prevention, detection, or recovery of assets from security threats and vulnerabilities.
- Threat is any event that may harm an asset. When it is realized, system is under attack.
- Vulnerability is any characteristic in a system which makes an asset more vulnerable to threats.

1.1 Some Terminology

- The combination of threats, vulnerabilities, and assets provides a quantified and/or qualified measure, that known as risk.
- Network security can be considered through the achievement of two security goals:
  - computer system security, to protect information assets; and
  - communication security, to protect information during its transmission against unauthorized or malicious use as well as disclosure, modification, or destruction.

1.2 Network Security Attack

- Eavesdropping, an unauthorized interception of network communication and the disclosure of the exchanged information by:
  - Sniffing, in the network layer, or
  - Wiretapping, in physical layer.

- Logon Abuse, bypass the authentication and access control mechanisms and allow a user to obtain access with more privileges than authorized.

1.2 Network Security Attack

- Spoofing, is the act of a subject asserting an identity that the subject has no right to use. For example: IP Spoofing.
- Intrusion Attacks, focus on unauthorized users gaining access to a vulnerable system through the network.
- Hijacking Attacks, attempts to gain unauthorized access to a system by using a legitimate entity's existing connection.

1.2 Network Security Attack

- Denial-of-Service (DoS) Attacks, attempts to exhaust the network or server resources in order to render it useless for legitimate hosts and users. Some well known DoS attacks:
  - SYN Attack. In a SYN attack, the attacker exploits the inability of a server process to handle unfinished connection requests.
  - Ping of Death. An early DoS attack in which an attacker sends a ping request that is larger than 64Kb, which is the maximum allowed size for the IP, causing the system to crash or restart.

1.2 Network Security Attack

- Application-Level Attacks. These attacks are concerned with the exploitation of weaknesses in the application layer and really focus on intrusion attacks in most cases. Examples of these attacks include:
  - malicious software attacks (viruses, Trojans, etc.),
  - Web server attacks,
  - remote command execution,
  - Structured Query Language (SQL) injection, and
  - cross-site scripting (XSS).

1.3 Sources of Security Threats

- The security threat to computer systems springs from a number of factors that include:
  - weaknesses in the network infrastructure and communication protocols,
  - the growth of the hacker community,
  - the vulnerability in operating system protocols,
  - the insider effect resulting from workers who steal and sell data of the company,
  - social engineering,
  - physical theft, etc.

1.4 Security Threats

1.4.1 Motives

- Terrorism, electronic terrorism is used to attack military installations, banking, and many other targets of interest.
- Espionage, gaining access to highly classified commercial information.
- Vendetta or revenge.
- Notoriety, proving hacking competencies.
- Greed, Many intruders into company systems do so to gain financially from their acts.

1.4 Security Threats

1.4.2 Management

Security threat management is a technique used to monitor security systems in real-time to review reports from the monitoring sensors such as the intrusion detection systems, firewall, and other scanning sensors.

It is important for the response team to study the risks as sensor data come in and decide which threat to deal with first.

Forensic analysis is done after a threat has been identified and contained.

1.4 Security Threats

1.4.3 Correlation

- Security teams have to reduce the turnaround time, the time between the start of an incident and the receipt of the first reports of the incident.
- Threat correlation, therefore, is the technique designed to reduce the turnaround time by monitoring all network sensor data.
- In fact threat correlation helps in:
  - reducing false positives,
  - reducing false negatives,
  - verifying sensor performance and availability.

1.4 Security Threats

The quality of data coming from the sensor logs depends on several factors including:

- **Collection**, the collection techniques specify how the data is to be analyzed.
- **Consolidation**, it is important to find good techniques to filter out relevant data and consolidate sensor data.
- **Correlation**, a good data mining scheme must be used for appropriate queries.

1.4 Security Threats

1.4.4 Awareness

Security threat awareness is meant to bring sidespread and massive attention of the population to the security threat.

*"First 5 days after the weekend are always the **hardest**"*