

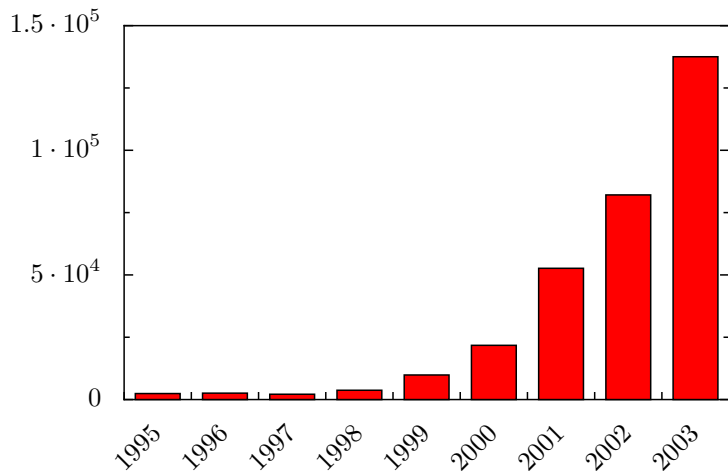
Advanced security methodologies - Computer and network attacks

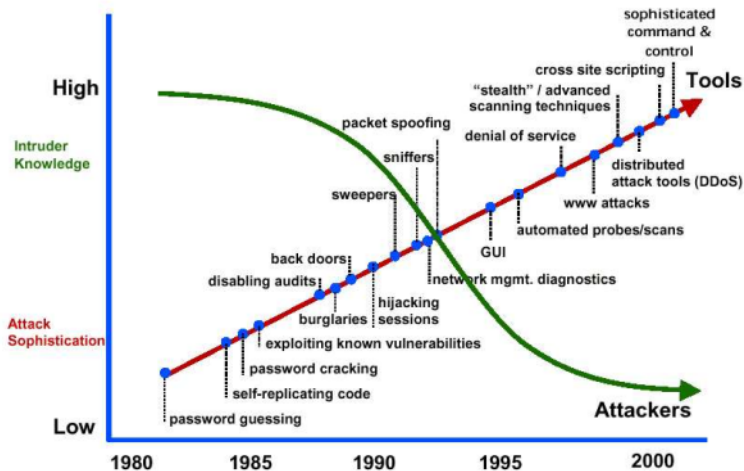
Pascal Steichen

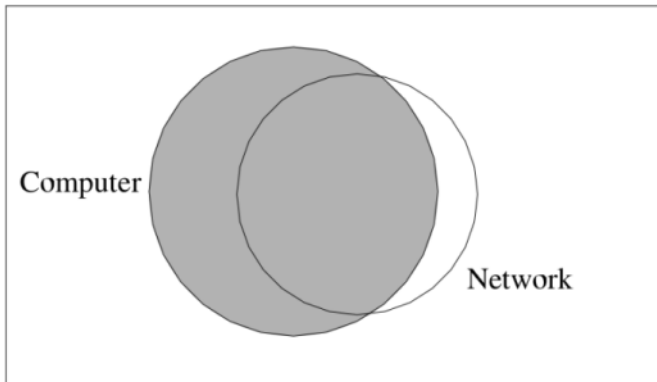
M2SSIC-Metz

- 1 Introduction
 - History
 - Definition
 - Motivation
- 2 Methodology
- 3 Taxonomy
 - Process based taxonomy
 - Bishop's Vulnerability Taxonomy
 - Howard's Taxonomy
 - Lough's Taxonomy
 - Hansman's taxonomy
- 4 Attack pattern
- 5 Featured attacks

Introduction







History

1945: Rear Admiral Grace Murray Hopper discovers a moth trapped between relays in a Navy computer. She calls it a "bug," a term used since the late 19th century to refer to problems with electrical devices.

History

- 1945: Rear Admiral Grace Murray Hopper discovers a moth trapped between relays in a Navy computer. She calls it a "bug," a term used since the late 19th century to refer to problems with electrical devices.
- 1949: Hungarian scientist John von Neumann (1903-1957) devises the theory of self-replicating programs, providing the theoretical foundation for computers that hold information in their "memory".

History

- 1945: Rear Admiral Grace Murray Hopper discovers a moth trapped between relays in a Navy computer. She calls it a "bug," a term used since the late 19th century to refer to problems with electrical devices.
- 1949: Hungarian scientist John von Neumann (1903-1957) devises the theory of self-replicating programs, providing the theoretical foundation for computers that hold information in their "memory".
- 1960: AT&T introduces its Dataphone, the first commercial modem.

History

- 1945: Rear Admiral Grace Murray Hopper discovers a moth trapped between relays in a Navy computer. She calls it a "bug," a term used since the late 19th century to refer to problems with electrical devices.
- 1949: Hungarian scientist John von Neumann (1903-1957) devises the theory of self-replicating programs, providing the theoretical foundation for computers that hold information in their "memory".
- 1960: AT&T introduces its Dataphone, the first commercial modem.
- 1963: Programmers develop the American Standard Code for Information Interchange (ASCII), a simple computer language that allows machines produced by different manufacturers to exchange data.

History

1964: AT&T begins monitoring telephone calls to try to discover the identities of "phone freaks," or "phreakers," who use "blue boxes" as tone generators to make free phone calls. The team's surveillance chief tells Newsweek magazine in 1975 that the company monitored 33 million toll calls to find phreakers. AT&T scores 200 convictions by the time the investigation ends in 1970.

History

- 1964: AT&T begins monitoring telephone calls to try to discover the identities of "phone freaks," or "phreakers," who use "blue boxes" as tone generators to make free phone calls. The team's surveillance chief tells Newsweek magazine in 1975 that the company monitored 33 million toll calls to find phreakers. AT&T scores 200 convictions by the time the investigation ends in 1970.
- 1969: Programmers at AT&T's Bell Laboratories develop the UNIX operating system, the first multi-tasking operating system.

History

- 1964:** AT&T begins monitoring telephone calls to try to discover the identities of "phone freaks," or "phreakers," who use "blue boxes" as tone generators to make free phone calls. The team's surveillance chief tells Newsweek magazine in 1975 that the company monitored 33 million toll calls to find phreakers. AT&T scores 200 convictions by the time the investigation ends in 1970.
- 1969:** Programmers at AT&T's Bell Laboratories develop the UNIX operating system, the first multi-tasking operating system.
- 1969:** The Advanced Research Projects Agency launches ARPANET, an early network used by government research groups and universities, and the forerunner of the Internet.

History

1972: John Draper, soon to be known as "Captain Crunch," discovers that the plastic whistle in a box of breakfast cereal reproduces a 2600-hertz tone. With a blue box, the whistle unlocks AT&T's phone network, allowing free calls and manipulation of the network. Among other phreakers of the 1970s is famous future hacker Kevin Mitnick.

History

- 1972: John Draper, soon to be known as "Captain Crunch," discovers that the plastic whistle in a box of breakfast cereal reproduces a 2600-hertz tone. With a blue box, the whistle unlocks AT&T's phone network, allowing free calls and manipulation of the network. Among other phreakers of the 1970s is famous future hacker Kevin Mitnick.
- 1972: Future Apple Computer co-founder Steve Wozniak builds his own "blue box." Wozniak sells the device to fellow University of California-Berkeley students.

History

- 1972: John Draper, soon to be known as "Captain Crunch," discovers that the plastic whistle in a box of breakfast cereal reproduces a 2600-hertz tone. With a blue box, the whistle unlocks AT&T's phone network, allowing free calls and manipulation of the network. Among other phreakers of the 1970s is famous future hacker Kevin Mitnick.
- 1972: Future Apple Computer co-founder Steve Wozniak builds his own "blue box." Wozniak sells the device to fellow University of California-Berkeley students.
- 1974: Telenet, a commercial version of ARPANET, debuts.

History

1979: Engineers at Xerox Palo Alto Research Center discover the computer "worm," a short program that scours a network for idle processors. Designed to provide more efficient computer use, the worm is the ancestor of modern worms – destructive computer viruses that alter or erase data on computers, often leaving files irretrievably corrupted.

History

- 1979: Engineers at Xerox Palo Alto Research Center discover the computer "worm," a short program that scours a network for idle processors. Designed to provide more efficient computer use, the worm is the ancestor of modern worms – destructive computer viruses that alter or erase data on computers, often leaving files irretrievably corrupted.
- 1983: The FBI busts the "414s," a group of young hackers who break into several U.S. Government networks, in some cases using only an Apple II+ computer and a modem.

History

- 1979:** Engineers at Xerox Palo Alto Research Center discover the computer "worm," a short program that scours a network for idle processors. Designed to provide more efficient computer use, the worm is the ancestor of modern worms – destructive computer viruses that alter or erase data on computers, often leaving files irretrievably corrupted.
- 1983:** The FBI busts the "414s," a group of young hackers who break into several U.S. Government networks, in some cases using only an Apple II+ computer and a modem.
- 1983:** University of Southern California doctoral candidate Fred Cohen coins the term "computer virus" to describe a computer program that can "affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself." Anti-virus makers later capitalize on Cohen's research on virus defence techniques.

History

1984: In his novel, "Neuromancer," author William Gibson popularizes the term "cyberspace," a word he used to describe the network of computers through which characters in his futuristic novels travel.

History

- 1984: In his novel, "Neuromancer," author William Gibson popularizes the term "cyberspace," a word he used to describe the network of computers through which characters in his futuristic novels travel.
- 1986: One of the first PC viruses ever created, "The Brain," is released by programmers in Pakistan.

History

- 1984: In his novel, "Neuromancer," author William Gibson popularizes the term "cyberspace," a word he used to describe the network of computers through which characters in his futuristic novels travel.
- 1986: One of the first PC viruses ever created, "The Brain," is released by programmers in Pakistan.
- 1988: Twenty-three-year-old programmer Robert Morris unleashes a worm that invades ARPANET computers. The small program disables roughly 6,000 computers on the network by flooding their memory banks with copies of itself. Morris confesses to creating the worm out of boredom. He is fined \$10,000 and sentenced to three years' probation.

History

1991: Programmer Philip Zimmerman releases "Pretty Good Privacy" (PGP), a free, powerful data-encryption tool. The U.S. Government begins a three-year criminal investigation on Zimmerman, alleging he broke U.S. encryption laws after his program spread rapidly around the globe. The government later drops the charges.

History

- 1991: Programmer Philip Zimmerman releases "Pretty Good Privacy" (PGP), a free, powerful data-encryption tool. The U.S. Government begins a three-year criminal investigation on Zimmerman, alleging he broke U.S. encryption laws after his program spread rapidly around the globe. The government later drops the charges.
- 1991: Symantec releases the Norton Anti-Virus software.

History

- 1991: Programmer Philip Zimmerman releases "Pretty Good Privacy" (PGP), a free, powerful data-encryption tool. The U.S. Government begins a three-year criminal investigation on Zimmerman, alleging he broke U.S. encryption laws after his program spread rapidly around the globe. The government later drops the charges.
- 1991: Symantec releases the Norton Anti-Virus software.
- 1994: Inexperienced e-mail users dutifully forward an e-mail warning people not to open any message with the phrase "Good Times" in the subject line. The missive, which warns of a virus with the power to erase a recipient's hard drive, demonstrates the self-replicating power of e-mail virus hoaxes that continue to circulate in different forms today.

History

1995: Microsoft Corp. releases Windows 95. Anti-virus companies worry that the operating system will be resistant to viruses. Later in the year, however, evolved "macro" viruses appear that are able to corrupt the new Windows operating system.

History

- 1995:** Microsoft Corp. releases Windows 95. Anti-virus companies worry that the operating system will be resistant to viruses. Later in the year, however, evolved "macro" viruses appear that are able to corrupt the new Windows operating system.
- 1998:** Intruders infiltrate and take control of more than 500 military, government and private sector computer systems. The incidents – dubbed "Solar Sunrise" after the well-known vulnerabilities in computers run on the Sun Solaris operating system – were thought to have originated from operatives in Iraq. Investigators later learn that two California teenagers were behind the attacks. The experience gives the Defence Department its first taste of what hostile adversaries with greater skills and resources would be able to do to the nation's command and control centre, particularly if used in tandem with physical attacks.

History

1999: The infamous "Melissa" virus infects thousands of computers with alarming speed, causing an estimated \$80 million in damage and prompting record sales of anti-virus products. The virus starts a program that sends copies of itself to the first 50 names listed in the recipient's Outlook e-mail address book. It also infects Microsoft Word documents on the user's hard drive, and mails them out through Outlook to the same 50 recipients.

History

1999: The infamous "Melissa" virus infects thousands of computers with alarming speed, causing an estimated \$80 million in damage and prompting record sales of anti-virus products. The virus starts a program that sends copies of itself to the first 50 names listed in the recipient's Outlook e-mail address book. It also infects Microsoft Word documents on the user's hard drive, and mails them out through Outlook to the same 50 recipients.

May 2000: The "I Love You" virus infects millions of computers virtually overnight, using a method similar to the Melissa virus. The virus also sends passwords and user-names stored on infected computers back to the virus's author. Authorities trace the virus to a young Filipino computer student, but he goes free because the Philippines has no laws against hacking and spreading computer viruses. This spurs the creation of the

History

2000: Yahoo, eBay, Amazon, Datek and dozens of other high-profile Web sites are knocked off-line for up to several hours following a series of so-called "distributed denial-of-service attacks." Investigators later discover that the DDOS attacks – in which a target system is disabled by a flood of traffic from hundreds of computers simultaneously – were orchestrated when the hackers co-opted powerful computers at the University of California-Santa Barbara.

History

2001: The "Anna Kournikova" virus, promising digital pictures of the young tennis star, mails itself to every person listed in the victim's Microsoft Outlook address book. This relatively benign virus frightens computer security analysts, who believe it was written using a software "tool-kit" that allows even the most inexperienced programmer to create a computer virus.

History

July 2001: The Code Red worm infects tens of thousands of systems running Microsoft Windows NT and Windows 2000 server software, causing an estimated \$2 billion in damages. The worm is programmed to use the power of all infected machines against the White House Web site at a predetermined date. In an ad-hoc partnership with virus hunters and technology companies, the White House deciphers the virus's code and blocks traffic as the worm begins its attack. It is known to be the first blended attack. Blended attacks contain two or more attacks merged together to produce a more potent attack.

History

2001: Debuting just days after the Sept. 11 attacks, the "Nimda" virus infects hundreds of thousands of computers around the world. The virus is considered one of the most sophisticated, with up to five methods of infecting systems and replicating itself.

History

- 2001: Debuting just days after the Sept. 11 attacks, the "Nimda" virus infects hundreds of thousands of computers around the world. The virus is considered one of the most sophisticated, with up to five methods of infecting systems and replicating itself.
- 2001: President Bush appoints Richard Clarke to serve as America's first cyber-security "czar."

History

- 2001: Debuting just days after the Sept. 11 attacks, the "Nimda" virus infects hundreds of thousands of computers around the world. The virus is considered one of the most sophisticated, with up to five methods of infecting systems and replicating itself.
- 2001: President Bush appoints Richard Clarke to serve as America's first cyber-security "czar."
- 2002: Melissa virus author David L. Smith, 33, is sentenced to 20 months in federal prison.

History

2002: The "Klez" worm – a bug that sends copies of itself to all of the e-mail addresses in the victim's Microsoft Outlook directory – begins its march across the Web. The worm overwrites files and creates hidden copies of the originals. The worm also attempts to disable some common anti-virus products and has a payload that fills files with all zeroes. Variants of the Klez worm remain the most active on the Internet.

History

2002: A denial-of-service attack hits all 13 of the "root" servers that provide the primary roadmap for almost all Internet communications. Internet users experience no slowdowns or outages because of safeguards built into the Internet's architecture. But the attack – called the largest ever – raises questions about the security of the core Internet infrastructure.

History

2002: A denial-of-service attack hits all 13 of the "root" servers that provide the primary roadmap for almost all Internet communications. Internet users experience no slowdowns or outages because of safeguards built into the Internet's architecture. But the attack – called the largest ever – raises questions about the security of the core Internet infrastructure.

Jan. 2003: The "Slammer" worm infects hundreds of thousands of computers in less than three hours. The fastest-spreading worm ever wreaks havoc on businesses worldwide, knocking cash machines off-line and delaying airline flights.

Present

Information warfare is a new and developing area of research. No common consensus has yet been reached on what information warfare is precisely. It is apparent that information warfare is an evolution in the way war is waged. Information warfare is essentially a country using relevant information to attack another country or defend itself. Instead of just waging war with bullets, information is used as a weapon. The attacks used in information warfare are varied. Traditional computer and network attacks are used, as well as less traditional attacks such as Electromagnetic Pulse (EMP) weapons.

Definition

In general terms an attack is a "maliciously" intended act against a system.

"maliciously" intended This tells us something about the goals. They are generally hostile and as such sets the non-malicious acts (or threats) beside. They should however not be neglected in a complete security approach.

Definition

In general terms an attack is a "maliciously" intended act against a system.

"maliciously" intended This tells us something about the goals. They are generally hostile and as such sets the non-malicious acts (or threats) beside. They should however not be neglected in a complete security approach.

act This highlights the difference between an attack and an incident. The attack being the single step of an intrusion process, whereas the incident is defined as a group of attacks visible from the higher levels.

Definition

In general terms an attack is a "maliciously" intended act against a system.

"maliciously" intended This tells us something about the goals. They are generally hostile and as such sets the non-malicious acts (or threats) beside. They should however not be neglected in a complete security approach.

act This highlights the difference between an attack and an incident. The attack being the single step of an intrusion process, whereas the incident is defined as a group of attacks visible from the higher levels.

system Target systems can be anything: software, protocols, algorithms, data structures, physical components, etc. even non-electronic systems. Another aspect is the scope of the system, it can be specifically or randomly chosen.

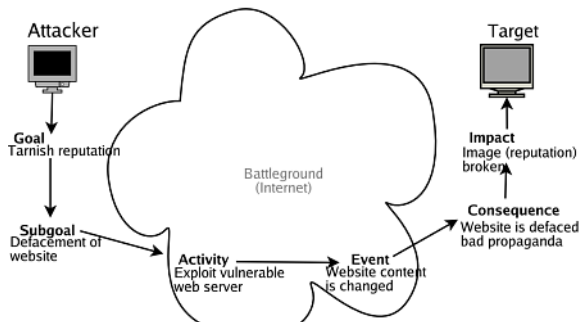
Motivation

A taxonomy of computer and network attacks is useful for a number of reasons. While computer and network attacks have become a common occurrence, the language used to describe them is often inconsistent. For example, one information body may label an attack a worm, while another may consider it a virus. Therefore, there needs to be a common language and classification for discussing attacks. A consistent taxonomy should be able to provide this.

Methodology

There are several distinct stages that make up an attack on a computer or network, from the initial motivation of the attacker, to the final execution of the attack. In general there are four main stages:

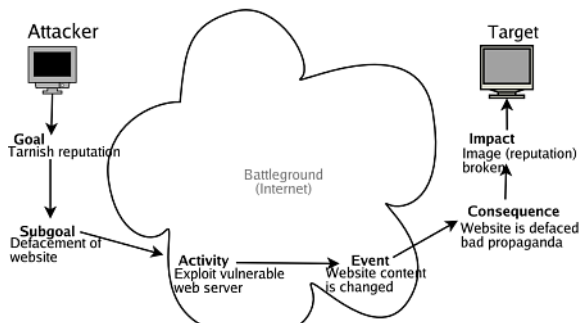
1 Attacker Motivation and Objectives



Methodology

There are several distinct stages that make up an attack on a computer or network, from the initial motivation of the attacker, to the final execution of the attack. In general there are four main stages:

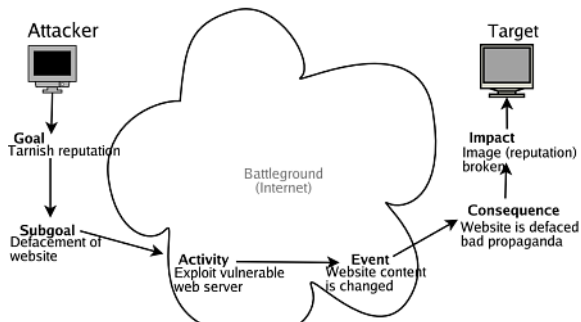
- 1 Attacker Motivation and Objectives
- 2 Information Gathering/Target Selection



Methodology

There are several distinct stages that make up an attack on a computer or network, from the initial motivation of the attacker, to the final execution of the attack. In general there are four main stages:

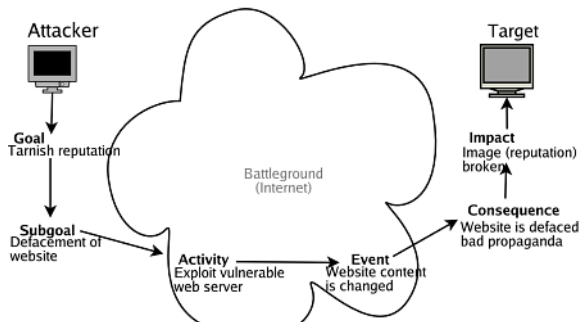
- 1 Attacker Motivation and Objectives
- 2 Information Gathering/Target Selection
- 3 Attack Selection



Methodology

There are several distinct stages that make up an attack on a computer or network, from the initial motivation of the attacker, to the final execution of the attack. In general there are four main stages:

- 1 Attacker Motivation and Objectives
- 2 Information Gathering/Target Selection
- 3 Attack Selection
- 4 Attack Execution



Taxonomy

① accepted

Taxonomy

- 1 accepted
- 2 comprehensible

Taxonomy

- ① accepted
- ② comprehensible
- ③ completeness/exhaustive

Taxonomy

- ① accepted
- ② comprehensible
- ③ completeness/exhaustive
- ④ determinism

Taxonomy

- 1 accepted
- 2 comprehensible
- 3 completeness/exhaustive
- 4 determinism
- 5 mutually exclusive

Taxonomy

- 1 accepted
- 2 comprehensible
- 3 completeness/exhaustive
- 4 determinism
- 5 mutually exclusive
- 6 repeatable

Taxonomy

- 1 accepted
- 2 comprehensible
- 3 completeness/exhaustive
- 4 determinism
- 5 mutually exclusive
- 6 repeatable
- 7 terminology complying with established security terminology

Taxonomy

- 1 accepted
- 2 comprehensible
- 3 completeness/exhaustive
- 4 determinism
- 5 mutually exclusive
- 6 repeatable
- 7 terminology complying with established security terminology
- 8 terms well defined

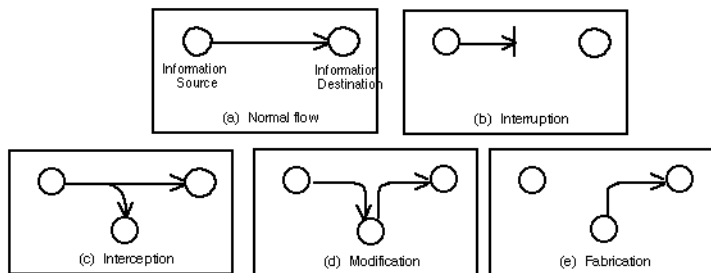
Taxonomy

- 1 accepted
- 2 comprehensible
- 3 completeness/exhaustive
- 4 determinism
- 5 mutually exclusive
- 6 repeatable
- 7 terminology complying with established security terminology
- 8 terms well defined
- 9 unambiguous

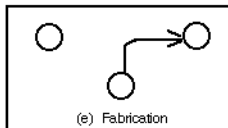
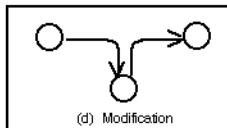
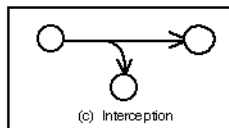
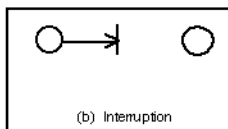
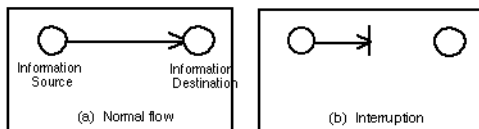
Taxonomy

- 1 accepted
- 2 comprehensible
- 3 completeness/exhaustive
- 4 determinism
- 5 mutually exclusive
- 6 repeatable
- 7 terminology complying with established security terminology
- 8 terms well defined
- 9 unambiguous
- 10 useful

Process based taxonomy

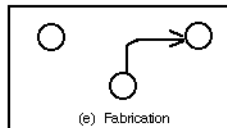
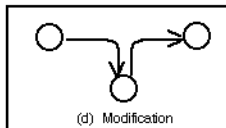
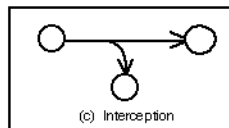
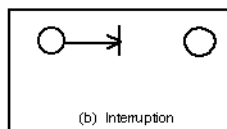
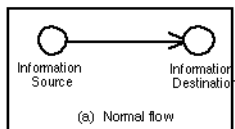
**1** Interruption

Process based taxonomy



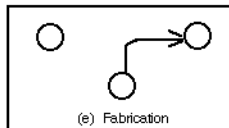
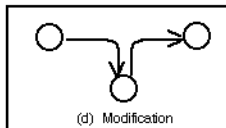
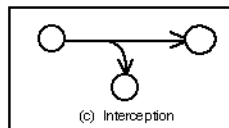
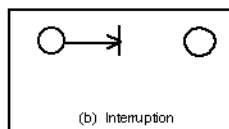
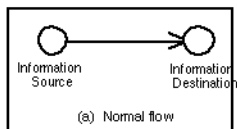
- 1 Interruption
- 2 Interception

Process based taxonomy



- 1 Interruption
- 2 Interception
- 3 Modification

Process based taxonomy



- 1 Interruption
- 2 Interception
- 3 Modification
- 4 Fabrication

Bishop's Vulnerability Taxonomy

- Nature: The nature of the flaw (vulnerability).

Bishop's Vulnerability Taxonomy

- Nature: The nature of the flaw (vulnerability).
- Time of introduction: When the vulnerability was introduced.

Bishop's Vulnerability Taxonomy

- Nature: The nature of the flaw (vulnerability).
- Time of introduction: When the vulnerability was introduced.
- Exploitation Domain: What is gained through the exploitation.

Bishop's Vulnerability Taxonomy

- Nature: The nature of the flaw (vulnerability).
- Time of introduction: When the vulnerability was introduced.
- Exploitation Domain: What is gained through the exploitation.
- Effect Domain: What can be affected by the vulnerability.

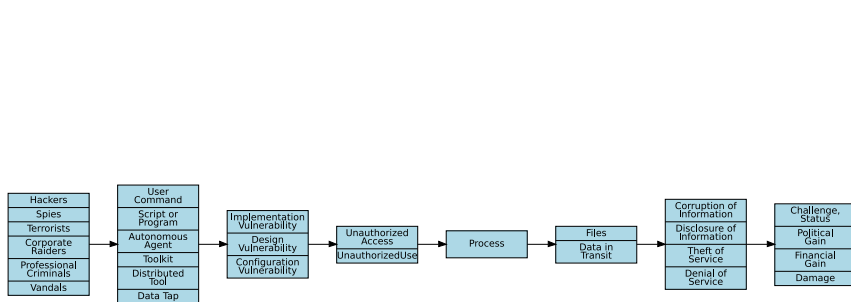
Bishop's Vulnerability Taxonomy

- Nature: The nature of the flaw (vulnerability).
- Time of introduction: When the vulnerability was introduced.
- Exploitation Domain: What is gained through the exploitation.
- Effect Domain: What can be affected by the vulnerability.
- Minimum Number: The minimum number of components necessary to exploit the vulnerability.

Bishop's Vulnerability Taxonomy

- Nature: The nature of the flaw (vulnerability).
- Time of introduction: When the vulnerability was introduced.
- Exploitation Domain: What is gained through the exploitation.
- Effect Domain: What can be affected by the vulnerability.
- Minimum Number: The minimum number of components necessary to exploit the vulnerability.
- Source: The source of identification of the vulnerability.

Howard's Taxonomy



Lough's Taxonomy

- Improper Validation: Insufficient or incorrect validation results in unauthorised access to information or a system.

Lough's Taxonomy

- Improper Validation: Insufficient or incorrect validation results in unauthorised access to information or a system.
- Improper Exposure: A system or information is improperly exposed to attack.

Lough's Taxonomy

- Improper Validation: Insufficient or incorrect validation results in unauthorised access to information or a system.
- Improper Exposure: A system or information is improperly exposed to attack.
- Improper Randomness: Insufficient randomness results in exposure to attack.

Lough's Taxonomy

- **Improper Validation:** Insufficient or incorrect validation results in unauthorised access to information or a system.
- **Improper Exposure:** A system or information is improperly exposed to attack.
- **Improper Randomness:** Insufficient randomness results in exposure to attack.
- **Improper Deallocation:** Information is not properly deleted after use and thus can be vulnerable to attack.

Hansman's taxonomy

The First Dimension

- Virus

Hansman's taxonomy

The First Dimension

- Virus
- Worms

Hansman's taxonomy

The First Dimension

- Virus
- Worms
- Trojans

Hansman's taxonomy

The First Dimension

- Virus
- Worms
- Trojans
- Buffer Overflows

Hansman's taxonomy

The First Dimension

- Virus
- Worms
- Trojans
- Buffer Overflows
- Denial of Service Attacks

Hansman's taxonomy

The First Dimension

- Virus
- Worms
- Trojans
- Buffer Overflows
- Denial of Service Attacks
- Network Attacks

Hansman's taxonomy

The First Dimension

- Virus
- Worms
- Trojans
- Buffer Overflows
- Denial of Service Attacks
- Network Attacks
- Physical Attacks

Hansman's taxonomy

The First Dimension

- Virus
- Worms
- Trojans
- Buffer Overflows
- Denial of Service Attacks
- Network Attacks
- Physical Attacks
- Password Attacks

Hansman's taxonomy

The First Dimension

- Virus
- Worms
- Trojans
- Buffer Overflows
- Denial of Service Attacks
- Network Attacks
- Physical Attacks
- Password Attacks
- Information Gathering Attacks

Table 1 The first dimension's categories

Level 1	Level 2	Level 3
Viruses:	File infectors System/boot record infectors Macro	
Worms:	Mass mailing Network aware	
Buffer overflows:	Stack Heap	
Denial of service attacks:	Host-based: Network-based:	Resource hogs Crashers TCP flooding UDP flooding ICMP flooding
Network attacks:	Distributed Spoofing Session hijacking Wireless attacks: Web application attacks	WEP cracking Cross site scripting Parameter tampering Cookie poisoning Database attacks Hidden field manipulation
Physical attacks:	Basic Energy weapon:	HERF LERF EMP
Password attacks:	Van Eck Guessing:	Brute force Dictionary attack
Information gathering attacks:	Exploiting implementation Sniffing: Mapping Security scanning	Packet sniffing

The Second Dimension

The second dimension covers the target(s) of the attack. As an attack may have multiple targets, there may be multiple entries in this dimension.

- Hardware targets

The Second Dimension

The second dimension covers the target(s) of the attack. As an attack may have multiple targets, there may be multiple entries in this dimension.

- Hardware targets
- Software targets

The Second Dimension

The second dimension covers the target(s) of the attack. As an attack may have multiple targets, there may be multiple entries in this dimension.

- Hardware targets
- Software targets
- Network targets

Table 2 The second dimension's categories

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	
Hardware:	Computer:	Hard-disks	...			
		Network equipment:	Routers			
			Switches			
			Hubs			
			Cabling			
	Peripheral devices:	Monitor				
			Keyboard			
	Software:	Operating system:	Windows family:	Windows XP		
				Windows 2003 Server		
				...		
Unix family			Linux:	RedHat Linux 6.0		
				RedHat Linux 7.0		
			FreeBSD:	4.8		
				5.1		
				...		
Application:		Server:	Database			
			Email			
	Web:		IIS:	4.0		
				5.0		
				...		
Network:	User:	Word processor	MS Word:	2000		
				2003		
				...		
	Protocols:	Email client:				
		Transport-layer:	IP			
			Network-layer:	TCP		
				...		

The Third Dimension

The third dimension covers the vulnerabilities and exploits that the attack uses. An attack may exploit multiple vulnerabilities, so there may be more than one entry in the third dimension. Entries in the third dimension are usually a Common Vulnerabilities and Exposures (CVE) entry, but in the case that a CVE entry does not exist, the vulnerability is classified generally as described later on in this section.

The Fourth Dimension

- 1 First Dimension Attack Payload

The Fourth Dimension

- 1 First Dimension Attack Payload
- 2 Corruption of Information

The Fourth Dimension

- 1 First Dimension Attack Payload
- 2 Corruption of Information
- 3 Disclosure of Information

The Fourth Dimension

- 1 First Dimension Attack Payload
- 2 Corruption of Information
- 3 Disclosure of Information
- 4 Theft of Service

The Fourth Dimension

- 1 First Dimension Attack Payload
- 2 Corruption of Information
- 3 Disclosure of Information
- 4 Theft of Service
- 5 Subversion

Other Dimensions

- **Damage:** A damage dimension would attempt to measure the amount of damage that the attack does. Attacks have different degrees of damage. An attack such as the recent SoBig virus cause more damage than a simple virus such as the Infector virus

Other Dimensions

- **Damage:** A damage dimension would attempt to measure the amount of damage that the attack does. Attacks have different degrees of damage. An attack such as the recent SoBig virus cause more damage than a simple virus such as the Infector virus
- **Cost:** Cleaning up after an attack costs money. In some cases billions of dollars are spent on attack recovery.

Other Dimensions

- **Damage:** A damage dimension would attempt to measure the amount of damage that the attack does. Attacks have different degrees of damage. An attack such as the recent SoBig virus cause more damage than a simple virus such as the Infector virus
- **Cost:** Cleaning up after an attack costs money. In some cases billions of dollars are spent on attack recovery.
- **Propagation:** This category applies more to replicating attacks. The propagation of an attack is the speed at which it reproduces or spreads. For attacks such as worms and viruses, a dimension covering this aspect would be useful.

Other Dimensions

- **Damage:** A damage dimension would attempt to measure the amount of damage that the attack does. Attacks have different degrees of damage. An attack such as the recent SoBig virus cause more damage than a simple virus such as the Infector virus
- **Cost:** Cleaning up after an attack costs money. In some cases billions of dollars are spent on attack recovery.
- **Propagation:** This category applies more to replicating attacks. The propagation of an attack is the speed at which it reproduces or spreads. For attacks such as worms and viruses, a dimension covering this aspect would be useful.
- **Defence:** The methods in how an attack has been defended against could be made into a further defence dimension.

Table 3 Classification results

Attack	1st Dimension	2nd Dimension	3rd Dimension	4th Dimension
Blaster	Network-aware worm	MS Windows NT 4.0, 2000, XP, Server 2003	CAN-2003-0352	TCP packet flooding DoS
Chernobyl	File infector virus	MS Windows 95 & 98		Corruption of information
Code Red	Network-aware worm	IIS 4, 5 & 6.0 beta	CVE-2001-0500	Stack buffer overflow & TCP packet flooding DoS
Use of John the Ripper	Guessing password attack	Unix family, Windows NT, 2000 & XP	Configuration	Disclosure of information
Infector	File infector virus	DOS family		Host-based crasher DoS
Land	Crasher DoS	Windows 95 and NT 4.0, Windows for Workgroups, 3.11, ...	CVE-1999-016	
Melissa	Mass-mailing worm	MS Word 97 & 2000	Configuration	Macro virus & TCP packet flooding DoS
Michelangelo	System boot record infector virus	DOS family		Corruption of information
Nimda	Mass-mailing worm	MS IE 5.5 SP1 & earlier except 5.01 SP2	CVE-2001-0333 & CVE-2001-0154	File infector virus, Trojan and DoS
PKZIP 3 Trojan	Trojan	DOS family		Corruption of information
Ramen	Network-aware worm	RedHat Linux 6.2 & 7.0	CVE-2000-0573, CVE-2000-0666 & CVE-2000-0917	Host-based DOS, UDP and TCP packet flooding DoS & subversion
Slammer	Network-aware worm	MS SQL Server 2000	CAN-2002-0649	Stack buffer overflow & UDP packet flooding DoS
Sobig.F	Mass-mailing worm	Email client	Configuration	Trojan
Trojaned Wuarchive FTPD	Trojan	Unix family		Subversion

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality
- Spoofing

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality
- Spoofing
- Probabilistic Techniques

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality
- Spoofing
- Probabilistic Techniques
- Exploitation of Authentication

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality
- Spoofing
- Probabilistic Techniques
- Exploitation of Authentication
- Resource Depletion

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality
- Spoofing
- Probabilistic Techniques
- Exploitation of Authentication
- Resource Depletion
- Exploitation of Privilege/Trust

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality
- Spoofing
- Probabilistic Techniques
- Exploitation of Authentication
- Resource Depletion
- Exploitation of Privilege/Trust
- Injection (Injecting Control Plane content through the Data Plane)

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality
- Spoofing
- Probabilistic Techniques
- Exploitation of Authentication
- Resource Depletion
- Exploitation of Privilege/Trust
- Injection (Injecting Control Plane content through the Data Plane)
- Data Structure Attacks

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality
- Spoofing
- Probabilistic Techniques
- Exploitation of Authentication
- Resource Depletion
- Exploitation of Privilege/Trust
- Injection (Injecting Control Plane content through the Data Plane)
- Data Structure Attacks
- Resource Manipulation

Attack pattern

Common Attack Pattern Enumeration and Classification (CAPEC):

- Abuse of Functionality
- Spoofing
- Probabilistic Techniques
- Exploitation of Authentication
- Resource Depletion
- Exploitation of Privilege/Trust
- Injection (Injecting Control Plane content through the Data Plane)
- Data Structure Attacks
- Resource Manipulation
- Time and State Attacks

Featured attacks

- Man-in-the-middle attack

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing
- Race condition

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing
- Race condition
- Replay attack

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing
- Race condition
- Replay attack
- Sniffer attack

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing
- Race condition
- Replay attack
- Sniffer attack
- Buffer overflow

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing
- Race condition
- Replay attack
- Sniffer attack
- Buffer overflow
- Back door

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing
- Race condition
- Replay attack
- Sniffer attack
- Buffer overflow
- Back door
- Parsing error

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing
- Race condition
- Replay attack
- Sniffer attack
- Buffer overflow
- Back door
- Parsing error
- Denial-of-service attack

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing
- Race condition
- Replay attack
- Sniffer attack
- Buffer overflow
- Back door
- Parsing error
- Denial-of-service attack
- Defaults account attack

Featured attacks

- Man-in-the-middle attack
 - Session hijacking/killing
 - Spoofing
- Race condition
- Replay attack
- Sniffer attack
- Buffer overflow
- Back door
- Parsing error
- Denial-of-service attack
- Defaults account attack
- Password cracking