

# Advanced security methodologies - Computer and network attacks

Pascal Steichen

M2SSIC-Metz

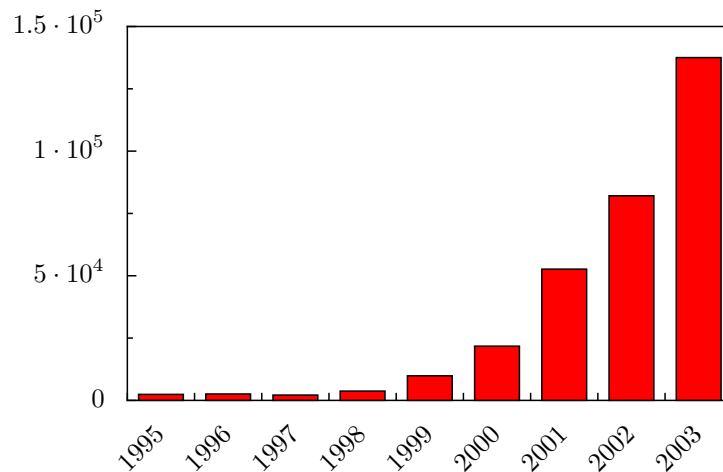
# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	History . . . . .	5
1.2	Definition . . . . .	9
1.3	Motivation . . . . .	9
<b>2</b>	<b>Methodology</b>	<b>10</b>
<b>3</b>	<b>Taxonomy</b>	<b>12</b>
3.1	Process based taxonomy . . . . .	13
3.2	Bishop’s Vulnerability Taxonomy . . . . .	13
3.3	Howard’s Taxonomy . . . . .	14
3.4	Lough’s Taxonomy . . . . .	15
3.5	Hansman’s taxonomy . . . . .	16
<b>4</b>	<b>Attack pattern</b>	<b>20</b>
<b>5</b>	<b>Featured attacks</b>	<b>21</b>
<b>6</b>	<b>Bibliographic references</b>	<b>23</b>

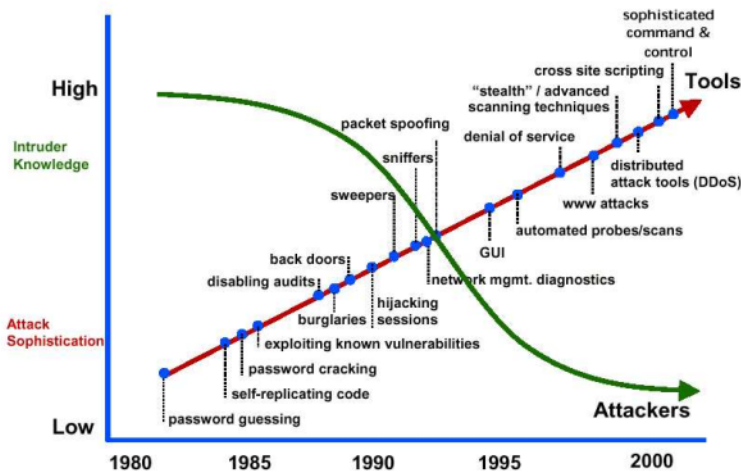
# 1 Introduction

Since the invention of computers and networks, people have found various ways to attack them. Attacks over the years have ranged from using a sledge hammer on a computer, to advanced distributed denial of service attacks. This lecture focuses on computer and network attacks and analysing different taxonomies. This is to help combat new attacks, improve computer and network security and to provide consistency in language when describing attacks.

Since 1999 there has been a marked increase in the number of incidents reported as statistics from the Computer Emergency Response Team Coordination Center (CERT/CC) show.



Not only has there been a marked increase in the number of attacks, the sophistication of the attacks has also increased. With the increased sophistication, many attacks are now relatively “user-friendly” and in-depth technical knowledge is no longer required to launch an attack. This has led to the rise of various groups of attackers, such as “script-kiddies”, who while ignorant of how their attack works, can cause great damage.

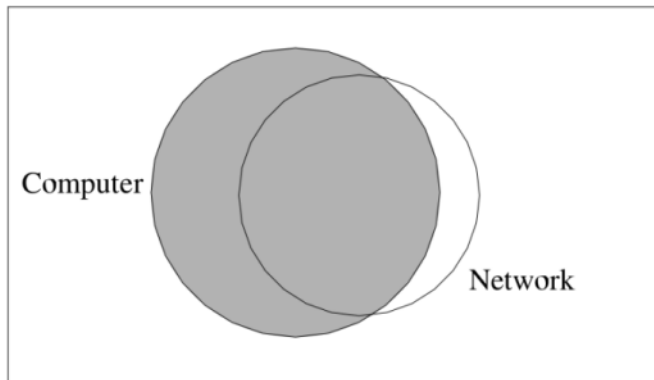


Before examining the types of attacks that can be launched against a computer or network, it is necessary to explain what network and computer attacks are. Network attacks are almost a subset of computer attacks, but some network attacks are outside the computer attack domain.

Computer attacks are attacks aimed at attacking a computer system in some way. This attack may involve destroying or accessing data, subverting the computer or degrading its performance. Traditionally attacks on computers have included methods such as viruses, worms, buffer-overflow exploits and denial of service attacks.

Network attacks are mostly attacks on computers that use a network in some way. A network could be used to send the attack (such as a worm), or it could be the means of attack (such as Distributed Denial of Service attack). An attack on a computer that requires a network, is a network attack. In general, network attacks are a subset of computer attacks.

However, there are several types of network attacks that do not attack computers, but rather the network they are attached to. Flooding a network with packets does not attack an individual computer, but clogs up the network. Although a computer may be used to initiate the attack, both the target and the means of attacking the target are network related.



## 1.1 History

Computer and network attacks have evolved greatly over the last few decades. Since computers and networks were invented, there has always been the opportunity to attack them. However, over the last 25 years attacks have split into distinct categories. New attacks, such as worms and viruses have been developed and attacks have become increasingly complicated.

**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.

**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.
- 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.
- 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.
- 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.

- 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.
- 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.
- 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 European Union's global cyber-crime Treaty.

**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.

**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.

**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.

**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.

**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.

**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.

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.

## 1.2 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.

## 1.3 Motivation

There are several motivations for examining computer and network attacks, and proposing a taxonomy for them. As mentioned previously, over the past

few years, attacks have increased and become more sophisticated and so pose a significant threat to computer and network users. It is important that attacks are examined closely to help combat them. Also, if a taxonomy is to be proposed, there must be an understanding of the attacks that will be classified.

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.

A taxonomy will also allow for the applying of previous knowledge to new attacks. If a new attack is identified, and classified appropriately, it should be possible to look at other attacks in the same category to get ideas on how to deal with the new attack.

There are several bodies that will benefit from a taxonomy. Information bodies, Computer Emergency Response Teams (CERTs) and advisory bodies will be able to communicate between themselves more efficiently using a common classification. When a new attack is discovered, if all interested bodies have a common classification, much confusion is avoided.

## 2 Methodology

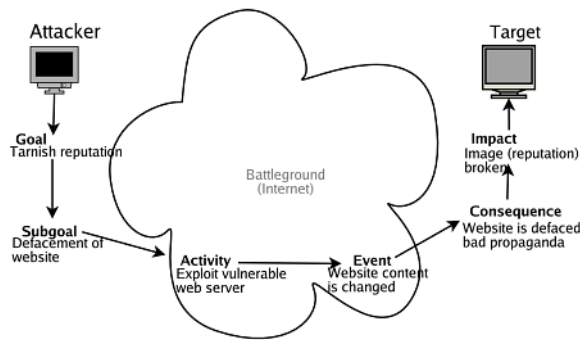
There are several distinct stages that make up an attack on a computer or network, from the initial motivation of the attacker, to the final execution of the attack. In general there are four main stages:

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

It is important to briefly explain the attack method. An attacker may have many different reasons for launching an attack. Some attackers may simply want to test their skills, others may want to prove a point. Motivation will have some impact on what attacks are chosen and how they are executed.

Before launching the attack, the attacker must select a target and gather information. These two activities take place either concurrently or consecutively, depending on what the attacker wishes to achieve. Information gathering involves extracting useful information from the target network or host, while target selection is the choosing of a promising target. During these stages, the attacker will usually use tools such as packet sniffers and port scanners to gather information on potential targets.

Once the attacker has a target and some information on the potential weaknesses of the target, they can select an attack that is appropriate. The final stage is the execution of the attack, in which the attacker proceeds to launch the attack against the target.



**Goals** The prime goal, which motivates the act. Can vary considerably, e.g. stealing money/data, breaking reputation, etc. The goals are mostly the same as in the physical world.

**Sub-goals** Needed to reach the above prime goal. The sub-goals are reaching from getting elevated privileges on a target machine, to controlling whole networks. These are the more technical (electronic world specific) goals to reach the above prime goal.

**Activities** The actions needed to reach one or more of the sub-goals, like getting login credentials, flooding a network, etc. This can be seen as the actual "crack".

**Events** The results of the above activities: suspended service, halted program, granted access, etc. - are called events.

**Consequences** These are the direct business results of the events, a computer being unavailable for business transactions, or balance sheets showing biased figures.

**Impacts** The impact is the business effect, the very prime damage which was intended. Examples are lost of revenue, tarnished reputation.

### 3 Taxonomy

To develop a taxonomy for computer and network attacks is not a straight nor easy task. Attacks can be classified by many different ways, mostly depending on the environment one stays in.

Scientifically speaking a taxonomy is an approximation of reality that is used to gain greater understanding of a field of study. As such a taxonomy should have classification categories with the following characteristics:

1. accepted

The taxonomy should be structured so that it can be become generally approved.

2. comprehensible

A comprehensible taxonomy will be able to be understood by those who are in the security field, as well as those who only have an interest in it.

3. completeness/exhaustive

For a taxonomy to be complete/exhaustive, it should account for all possible attacks and provide categories for them. While it is hard to prove a taxonomy is complete or exhaustive, they can be justified through the successful categorisation of actual attacks.

4. determinism

The procedure of classifying must be clearly defined.

5. mutually exclusive

A mutually exclusive taxonomy will categorise each attack into, at most, one category.

6. repeatable

Classifications should be repeatable.

7. terminology complying with established security terminology

Existing terminology should be used in the taxonomy so as to avoid confusion and to build on previous knowledge.

8. terms well defined

There should be no confusion as to what a term means.

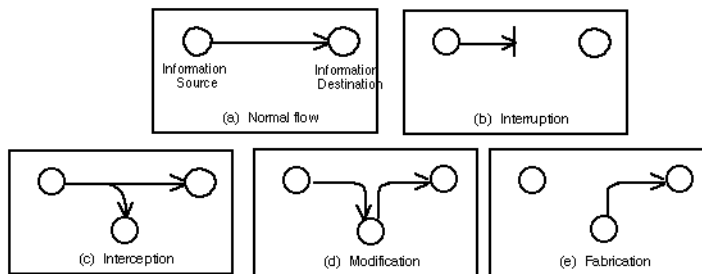
9. unambiguous

Each category of the taxonomy must be clearly defined so that there is no ambiguity as to where an attack should be classified.

10. useful

A useful taxonomy will be able to be used in the security industry. For example, the taxonomy should be able to be used by incident response teams.

### 3.1 Process based taxonomy



1. Interruption

An asset of the system is destroyed or becomes unavailable or unusable.

2. Interception

An unauthorized party gains access to an asset.

3. Modification

An unauthorized party not only gains access to, but tampers with an asset.

4. Fabrication

An unauthorized party inserts counterfeit objects into the system.

### 3.2 Bishop's Vulnerability Taxonomy

Matt Bishop has made several important contributions to the field of security taxonomies. Bishop presents a taxonomy of Unix vulnerabilities in which the underlying flaws of vulnerabilities are used to create a classification scheme. Six "axes" are used to classify vulnerabilities:

- 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.

Bishop's approach is interesting, as instead of a flat or tree-like taxonomy, he uses axes. In the proposed taxonomy a similar structure is used. Bishop also preformed a critical analysis of other vulnerability taxonomies. Previous taxonomies such as PA, RISOS and Aslam's taxonomy have been assessed and compared, and he also examines the issues surrounding taxonomies and especially what makes a good taxonomy. Bishop suggests that one of the main benefits of a taxonomy is that it should help to work out where to invest resources.

### 3.3 Howard's Taxonomy

John Howard presents a taxonomy of computer and network attacks. The approach taken is broad and process-based, taking into account factors such as attacker motivation and objectives.

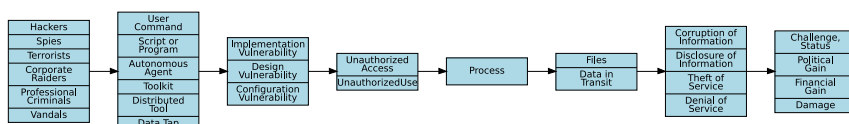
The figure below shows Howard's taxonomy. The taxonomy consists of five stages: attackers, tools, access, results and objectives. The attackers consist of a range of types of people who may launch an attack. These range from hackers to terrorists. Tools are the means that the attackers use to gain access. Access is gained through either an implementation, design or configuration vulnerability. Once access is gained, the results may be achieved such as corruption or disclosure of information. From this process the attacker achieves their objectives which may vary from inflicting damage, to gaining status.

Howard attempts to focus attention on a process driven taxonomy, rather than a classification scheme such as in the animal kingdom. This means the whole attack process is considered, which is certainly valuable. However, as Lough points out, Howard fails to meet one of his taxonomy requirements: mutual exclusion. Some of the categories may overlap. For example the attacker's category contains classes that may not be mutually exclusive. As Lough points out:

“Depending on one’s point of view, a terrorist’s actions could be indistinguishable from those of a vandal. A spy could be a professional criminal.”

Howard’s approach is still useful in gaining insight to the process of attacks. However, for information bodies such as CERT, such a taxonomy may not be practical. Information bodies are more concerned with the attack itself, than with the motivations and objectives behind it.

Howard extends his work further by refining some of the stages. However, the problems mentioned above still exist with the refined taxonomy.



### 3.4 Lough’s Taxonomy

In 2001, Daniel Lough proposed another taxonomy named VERDICT. VERDICT stands for Validation Exposure Randomness Deallocation Improper Conditions Taxonomy and is based on characteristics of attacks. Instead of a tree-like taxonomy, Lough proposed using four characteristics of attacks:

- 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.

Lough proposes that any attack can be classified using these four characteristics. By basing the taxonomy on characteristics, the taxonomy can easily and tidily classify blended attacks. Lough’s approach is similar to Bishop’s axes.

Lough’s taxonomy is interesting however, there are a few shortcomings to Lough’s taxonomy. While it is useful for applying to a new technology

(Lough applies it to 802.11 and finds numerous vulnerabilities) to discover new vulnerabilities and to classify existing ones, it may be helpful to have a more specific taxonomy.

In terms of an information body, Lough's taxonomy may not be useful for the day to day task of identifying and classifying new attacks, and issuing advisories. Lough's taxonomy is general, and does not speak about attacks in terms of worms, viruses, and trojans, which is how attacks are usually described.

In the end, the goals of the taxonomy determine its usefulness. Lough's taxonomy, succeeds in providing a taxonomy that is useful for analysis and for the prediction of new attacks, but not for daily use and classification of attacks.

### 3.5 Hansman's taxonomy

Hansman's taxonomy works by using the concept of dimensions. Dimensions are a way of allowing for a classification of an attack to take a more holistic view of the attack. The taxonomy proposes four dimensions for attack classification. Before examining how the taxonomy works, the dimensions used are briefly explained.

The **first, or base, dimension** is used to categorise the attack into an attack class that is based on the attack vector, or if there is no attack vector, the attack is classified into the closest category.

The attack target is covered in the **second dimension**. The target can be classified down to very specific targets, such as sendmail 8.12.10 or can cover a class of targets, such as Unix based systems.

The **third dimension** covers the vulnerabilities and exploits, if they exist, that the attack uses. The vulnerabilities and exploits do not have a structured classification due to the possible infinite number of vulnerabilities and exploits. Instead the list defined by the Common Vulnerabilities Exposures project is used as a starting point.

The **fourth dimension** takes into account the possibility for an attack to have a payload or effect beyond itself. In many cases an attack will be clearly a certain kind of attack, but yet it will have a payload or cause an effect that is different. For example, a virus that installs a trojan horse, is still clearly a virus, but has a trojan as a payload.

In each dimension, the classifier must classify attacks as specifically as possible. This means attacks should be classified down to the smallest sub-class in each dimension that makes sense.

The taxonomy allows for the possibility of further dimensions which, although not necessary, may enhance the knowledge of the attack. Some further dimensions are discussed below.

Some of Howard's ideas have been applied in the Hansman's taxonomy, notably in the third and fourth dimensions.

An attack must have at least the first dimension, but depending on the attack, or how specific the classifier wishes to be, all, some or none of the other dimensions may be used.

### **The First Dimension**

- Virus  
Self-replicating program that propagates through some form of infected files.
- Worms  
Self-replicating program that propagates without using infected files. Usually worms propagate through network services on computers or through email.
- Trojans  
A program made to appear benign that serves some malicious purpose.
- Buffer Overflows  
A process that gains control or crashes another process by overflowing the other process' buffer.
- Denial of Service Attacks  
An attack which prevents legitimate users from accessing or using a host or network.
- Network Attacks  
Attacks focused on attacking a network or the users on the network by manipulating network protocols, ranging from the data-link layer to the application layer.
- Physical Attacks  
Attacks based on damaging physical components of a network or computer.
- Password Attacks  
Attacks aimed at gaining a password.

- Information Gathering Attacks

Attacks in which no physical or digital damage is done and no subversion occurs, but in which important information is gained by the attacker, possibly to be used in a further attack.

**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:	Resource hogs Crashers
	Network-based:	TCP flooding UDP flooding ICMP flooding
Network attacks:	Distributed Spoofing Session hijacking	
	Wireless attacks:	WEP cracking
	Web application attacks	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:	Packet sniffing
	Mapping	
	Security scanning	

## 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

can be put into three main sub-classes: computer, network equipment and peripheral devices. Computer targets are computer components, such as CPUs and hard-disks. Network equipment targets are network hardware such as hubs, or network cable. Finally, peripheral devices are devices that are not essential to a computer, for example monitors.

- Software targets

have two main classes: operating system and application targets. Operating system targets are targets within the operating system itself, while application targets are targets that are running on top of the operating system.

- Network targets

are when the network itself or its protocols are targeted. For example, a ping flood attacks a network rather than hardware or software.

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	
				...	...	
				MacOS family	MacOS X:	10.1 10.2
		...	...			
Application:		Server:	Database	...		
			Email	...		
			Web:	IIS:	4.0 5.0	
			User:	Word processor	MS Word:	2000 2003
			Email client:	...		
	Network:	Protocols:	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

The third dimension deals with attacks having payloads or effects beyond themselves. For example, a worm may have a trojan payload, or it may simply destroy some files. The payload may be another attack itself and so the first dimension can be used to classify the payload if this is the case. The fourth dimension consists of five categories:

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

## Other Dimensions

Besides the four dimensions described above, a number of further dimensions could be added to enhance the taxonomy. Several are discussed below and

although they are more abstract and are not as essential as the previous dimensions, they are still useful in classifying attacks, especially in regards to how to react to a new attack that falls into a certain category. For example, the following are dimensions that would be useful for an organisation dealing with attacks:

- **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 Wuarhive FTPD	Trojan	Unix family		Subversion

## 4 Attack pattern

Attack patterns are a powerful mechanism to capture and communicate the attacker's perspective. They are descriptions of common methods for

exploiting software. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples.

To assist in enhancing security throughout the software development life-cycle, and to support the needs of developers, testers and educators, the Common Attack Pattern Enumeration and Classification (CAPEC) is sponsored by the Department of Homeland Security as part of the Software Assurance strategic initiative of the National Cyber Security Division. The objective of this effort is to provide a publicly available catalogue of attack patterns along with a comprehensive schema and classification taxonomy. This site now contains the initial set of content and will continue to evolve with public participation and contributions to form a standard mechanism for identifying, collecting, refining, and sharing attack patterns among the software community.

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

## 5 Featured attacks

- Man-in-the-middle attack

A man-in-the-middle attack (or eavesdropping) attack is performed when an attacker intercepts a communication between two or more parties, masquerades as one of them modifying or not the transmission data.

- Session hijacking/killing

The TCP/IP protocol has a weakness which makes it possible to an attacker to take over, "hijack", an already established session. By sending a forged *TCP reset* packet the session could for instance be prematurely be killed.

- Spoofing

Spoofing is a method to get someone's "identity" (like its IP address, DNS name, ARP address, etc.) on a network.

- Race condition

The race condition attack is a complex one. The execution of an application is, from the computer (OS, hardware) point of view, done in discrete steps. If these steps are not atomic operations, then an attacker has a brief window of time where he could slip in some code to be executed instead of the original one.

- Replay attack

A replay attack, can be performed if the attacker has the opportunities to record an entire transaction between, say a client and a server. The attacker can then "replay" part of the conversation for his malicious intends.

- Sniffer attack

A "sniffer" is a program that silently records all network traffic on a LAN, this method is often used to get user-names and/or passwords transmitted in the clear of the network.

- Buffer overflow

This one of the most common attacks, cause a lot of programming languages are vulnerable to buffer overflows. These occur when a too large value is attributed to a fixed sized buffer, without adequate bounds checking being done.

- Back door

Back doors in the sense of application development are when a rogue programmer somehow manages to write special code in the application, during its creation process, for instance allowing to bypass access control later on via a "magic" account.

- Parsing error

Programmes that doesn't properly check input from users, for example, are vulnerable to parsing error attacks, that try to pass security compromising content.

- Denial-of-service attack

Systems (applications, hosts or even networks) can be rendered unusable by cascading service requests, or high-frequency input flows. Thus legitimate users are denied of the service. These attacks can be very large-scale and coming from different sources, in this case we talk about a distributed denial-of-service attack.

- Defaults account attack

Many applications, especially operating systems, have default accounts with insecure, or no passwords. This is of course a potential risk, where attackers can easily get a **legitimate** access to systems.

- Password cracking

Standard *cracking* programs give attackers the possibility to guess passwords, so called weak passwords can this way be obtained in a few seconds.

## 6 Bibliographic references

- [A Short History of Computer Viruses and Attacks](#)
- [NSA eavesdropping paper](#)
- [A Taxonomy of Computer and Network Attacks \(Dr. John D. Howard\)](#)
- [Taxonomy of the Computer Security Incident related terminology \(Jimmy Arvidsson\)](#)
- [A taxonomy of network and computer attacks \(Simon Hansman, Ray Hunt\) <http://ce.sharif.edu/courses/83-84/1/ce534/resources/root/Papers/attacks>](#)
- [Common Attack Pattern Enumeration and Classification - A Community Knowledge Resource for Building Secure Software](#)
- [Build Security In - Attack patterns](#)