





# HCSF Training consists of 4 parts (8 modules):

Part 1	<b>Read Ahead</b> - the intent of the read-ahead is to expose each of you to a wealth of information that will provide a solid knowledge-base and foundation specific to Highway Infrastructure Cyber Security (1 module).	FORMAT: online video, pdf file
2	<b>Quiz</b> - the quiz is to reinforce concepts covered in the Read Ahead and prepare for the workshop. A passing grade of 70% (49 correct out of 70 questions) is required for workshop participation (1 module).	FORMAT: MS Word quiz, pdf file results
3	<b>Workshop</b> - the intent of the in-person workshop is to reinforce concepts addressed within the Read Ahead (5 modules).	FORMAT: in-person, advance pdf file
4	<b>Resource Compendium</b> - is a compilation of references and various resources (1 module).	FORMAT: pdf file



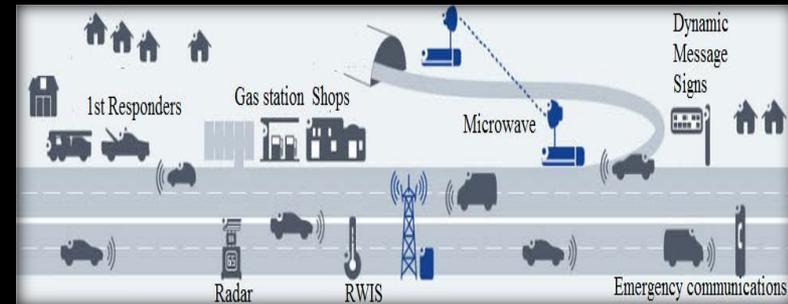
# Our Highway Infrastructure



- The U.S. Highway system includes more than four million miles of interstate highway, strategic highways, arterial roadways, intermodal connectors and their associated infrastructure, such as bridges and tunnels. This network of roadways provides access to various transportation vehicles, including automobiles, school buses, motorcycles, and all types of trucks, trailers, and recreational vehicles.
- The nation's roadway infrastructure is interconnected not just with asphalt and concrete, but by control systems which ensure the infrastructure's safe operation for motorists. These interconnected road networks are controlled by numerous systems composed of traffic signal controllers, ramp meters, dynamic message signs, roadway sensors, road weather information sensors, etc. These devices are frequently connected into a traffic management center where roadway operators monitor both traffic conditions and the status of the control systems to ensure safe and efficient transportation.
- For the last 20 years, the highway industry has embraced Intelligent Transportation Systems (ITS) to improve performance in both operational efficiencies and roadway mobility. ITS leverages advances in communication and computer technologies to maximize safety, mobility, and environmental performance.



- Effective communication with the public is one of the most important elements in effective operation of a modern transportation facility.
- The use of advanced computing, sensing, and communication technologies will continue to support transportation systems to meet the increasing operational challenges on the national ground transportation network.
- Each technological advance brings additional capabilities to meet the objective of transportation agencies, but can also increase the attack surface of these systems.
- The world today is very different than it was when ITS began over 20 years ago; now, it is very important that agency owners include system security and protection in their design and maintenance responsibilities to ensure continuity of service and protection of critical infrastructure support functions.





# Growing Issue of Cyber Security

- The landscape in which transportation systems reside and how it operates is changing as computers and communication systems become essential features to sustain highway and street-level operations in metropolitan areas.
- With this changing environment, the threat environment has also changed, raising to a head the existence of credible cyber security vulnerability in currently deployed transportation equipment.
- The growing issue of cybersecurity and its impact on the highway environment has highlighted safety and operational risks to our roadways' critical infrastructures.
- In order to understand these challenges, a clearer picture of past incidents on Intelligent Transportation System (ITS) deployments, lessons learned from other sectors using industrial control systems (ICS), specific defensive countermeasures, and potential future technology deployments (i.e. connected vehicles) is necessary.
- The biggest challenge to the ITS is a result of increased value of ITS data and connectivity in the connected and networked world that we are now increasingly in.

**A GROWING  
CYBERSECURITY  
THREAT**



Concerns about cybersecurity for the type of control systems used in ITS and traffic management deployments are related to both current technologies as well as legacy systems, coupled with the growing trend to integrate ITS deployments with other networks.

- These concerns will intensify in the future with the addition of connected vehicle applications, and this combination has introduced new threat categories which have not yet been encountered in this domain.
- The potential risks associated with an attack can be further exacerbated if system connectivity extends to the business side of the enterprise.

Another dimension of cybersecurity involves the reliable and trustworthy operation of these transportation management systems.

- As the transportation infrastructure is operated in a more active manner, it becomes important that the ITS components and processes are dependable, resilient, authenticated and used appropriately.





- **Basic Definitions/Concepts:**
  - Cyber Security
  - Hacking / Hacker Classifications
  - Trustworthy
  - Bitcoin
  - Social Engineering



## Cybersecurity

is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.



- It includes **controlling physical access** to the hardware, as well as protecting against harm that may come via **network access, data and code injection**, and due to malpractice by operators, whether **intentional, accidental**, or due to them **being tricked** into deviating from secure procedures.
- The field is of growing importance due to the increasing reliance on computer systems. Computer systems now include a very wide variety of "**smart**" **devices**, including **smartphones, televisions** and tiny devices as part of the **Internet of Things** – and networks include not only the **Internet** and private data networks, but also **Bluetooth, Wi-Fi** and other **wireless networks**.



**HACKING** is any technical effort to manipulate the normal behavior of network connections and connected systems. A *hacker* is any person engaged in hacking. The terms "*hacking*" and "*hackers*" are most commonly associated with malicious programming attacks on the Internet and other networks.



## Origins of Hacking

M.I.T. engineers in the 1950s and 1960s first popularized the term and concept of hacking... the so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities.

Later, outside of M.I.T., others began applying the term to less honorable pursuits.

## Hacking vs. Cracking

Malicious attacks on computer networks are officially known as *cracking*, while *hacking* truly applies only to activities having good intentions. Most non-technical people fail to make this distinction, however. Outside of academia, its extremely common to see the term "hack" misused and be applied to cracks as well.



# Hacker Classifications

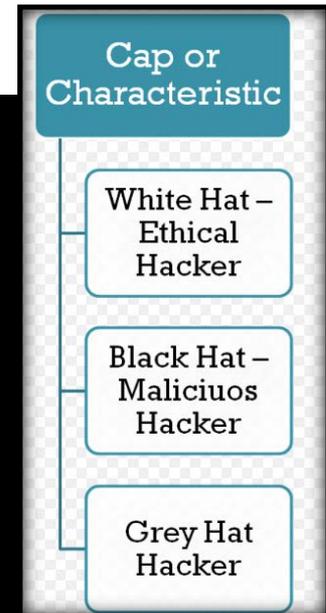
Several subgroups of the computer underground use different terms to demarcate themselves from each other, or try to exclude some specific groups with whom they do not agree.

## White hat

A white hat hacker breaks security for non-malicious reasons, either to test their own security system, perform penetration tests or vulnerability assessments for a client - or while working for a security company which makes security software. The term is generally synonymous with ethical hacker.

## Black hat

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain". Black hat hackers are "the epitome of all that the public fears in a computer criminal".





## Grey hat

A grey hat hacker lies between a black hat and a white hat hacker. A grey hat hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. They may then offer to correct the defect for a fee. Grey hat hackers sometimes find the defect of a system and publish the facts to the world instead of a group of people. Even though grey hat hackers may not necessarily perform hacking for their personal gain, unauthorized access to a system can be considered illegal and unethical.

## Script kiddie

A script kiddie (also known as a *skid* or *skiddie*) is an unskilled hacker who breaks into computer systems by using automated tools written by others (usually by other black hat hackers), hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature), usually with little understanding of the underlying concept.

## Classifications of Hacking

- **White Hat** — an ethical hacker who helps test security systems.
- **Black Hat** — a hacker who breaks into a computer security system for personal gain or malicious intent.
- **Grey Hat** — a mix of the white and black hat, this hacker may break into a computer system, then offer to help the company protect against hackers for a fee.
- **Elite Hacker** — extremely skilled hackers.
- **Script Kiddie** — a non-expert who cracks into a computer system using pre-constructed tools (i.e. another hacker's technique) to do so.
- **Neophyte** — also known as a "n00b" or a "newbie" is someone who is new to hacking and knows very little about it.
- **Hactivist** — a hacker who breaks into websites and reorganizes them with a political, social, or otherwise ideological message.



# Ethical Hacker

Application Pen Tester - A penetration test or "Ethical Hack" evaluates an application's or network's ability to withstand attack. Such an exercise will expose vulnerabilities and the effects of exploitation.



- Vulnerability scanning evaluates a system for potential vulnerabilities or weak configurations, is largely automated and can only ever find a subset of security issues.
- Penetration testing, on the other hand, is a manual process performed by a human.
- A penetration tester will use tools as a part of their work, but they apply their human ingenuity to exploit vulnerabilities and illustrate what an attacker might be capable of when targeting a particular system.



Trustworthiness is the degree of confidence one has that the system performs according to designed behavior as evidenced by characteristics including, but not limited to:

- safety,
- security,
- privacy,
- reliability and
- resilience.



# Bitcoin

Bitcoin is a digital asset and a payment system invented by Satoshi Nakamoto, who published the invention in 2008 and released it as open-source software in 2009.

The system is peer-to-peer; users can transact directly without an intermediary. Transactions are verified by network nodes and recorded in a public distributed ledger called the *block chain*.

The ledger uses bitcoin as its unit of account. The system works without a central repository or single administrator, which has led the U.S. Treasury to categorize bitcoin as a decentralized virtual currency.

Bitcoin is often called the first cryptocurrency, although prior systems existed. Bitcoin is more correctly described as the first decentralized digital currency. It is the largest of its kind in terms of total market value.

**Bitcoin**



**bitcoin**

Logo of the bitcoin reference client

<b>Administration</b>	Decentralized
<b>Date of introduction</b>	3 January 2009; 7 years ago
<b>User(s)</b>	Worldwide
<b>Supply growth</b>	25 bitcoins per block (approximately every ten minutes) until mid 2016, and then afterwards 12.5 bitcoins per block for 4 years until next halving. This halving continues until 2110–40, when 21 million bitcoins will have been issued.
<b>Subunit</b>	
10 <sup>-3</sup>	millibitcoin
10 <sup>-6</sup>	microbitcoin, bit
10 <sup>-8</sup>	satoshi
<b>Symbol</b>	BTC, XBT, ₿
millibitcoin	mBTC
microbitcoin, bit	µBTC
<b>Coins</b>	Unspent outputs of transactions denominated in any multiple of satoshis



# Use of Bitcoin by criminals

Bitcoin as a form of payment for products and services has grown, and merchants have an incentive to accept it because fees are lower than the 2–3% typically imposed by credit card processors.

Unlike credit cards, any fees are paid by the purchaser, not the vendor. The European Banking Authority and other sources have warned that bitcoin users are not protected by refund rights or chargebacks. Despite a large increase in the number of merchants accepting bitcoin, the cryptocurrency does not have much momentum in retail transactions.

The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, and law enforcement. Such criminal activities are primarily centered around black markets and theft, though officials in many countries also recognize that bitcoin as providing legitimate financial services.



**Social Engineering**, refers to psychological manipulation of people into performing actions or divulging confidential information needed to gain system access. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

- All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases.
- These biases, are exploited in various combinations to create attack techniques.
- One example of social engineering would be that the hacker contacts the target on a social networking site and starts a conversation with the target.
- Slowly and gradually, the hacker gains trust of the target and then uses it to get access to sensitive information like password or bank account details.

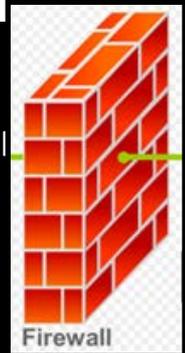


- **Advanced Definitions/Concepts:**
  - Firewall
  - Attack vector
  - Vulnerabilities
  - Exploits
  - Zero Day
  - Malware (Stuxnet)
  - Ransomware
  - DoS attack
  - BlackEnergy
  - Regin (malware)
  - Flame (malware)
  - Pivoting
  - Keyloggers
  - Code Injection
  - Arbitrary Code Execution
  - Metasploit
  - Backdoors
  - Sandbox
  - Man-in-the-Middle
  - Vulnerability Severity



# Firewall

**Firewall** - a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.



Firewalls are often categorized as either *network firewalls* or *host-based firewalls*.

Network firewalls are a software appliance running on general purpose hardware or hardware-based firewall computer appliances that filter traffic between two or more networks. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine.

Firewall appliances may also offer other functionality to the internal network they protect such as acting as a DHCP or VPN server for that network.

The **Dynamic Host Configuration Protocol (DHCP)** is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.



# Attack vector

A **vector**, specifically when talking about malicious code such as viruses or worms, is the *method* that this code uses to propagate itself or infect a computer, thus the term “attack”.

This sense is similar to, and derived from, its meaning **in biology** (a vector is any agent (person, animal, or microorganism) that carries and transmits an infectious pathogen into another living organism.)

## **Attack vectors:**

Malware writers can exploit zero-day vulnerabilities through several different attack vectors. Sometimes, when users visit rogue Web sites, malicious code on the site can exploit vulnerabilities in Web browsers. Web browsers are a particular target for criminals because of their widespread distribution and usage.

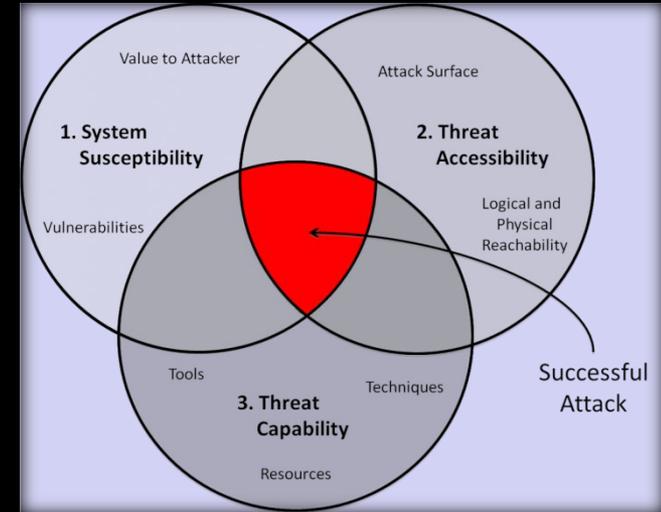


# Vulnerabilities

A vulnerability is a weakness which allows an attacker to reduce a system's information assurance.

Vulnerability - intersection of 3 elements:

1. a system susceptibility or flaw,
2. attacker access to the flaw, and
3. attacker capability to exploit the flaw.



To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

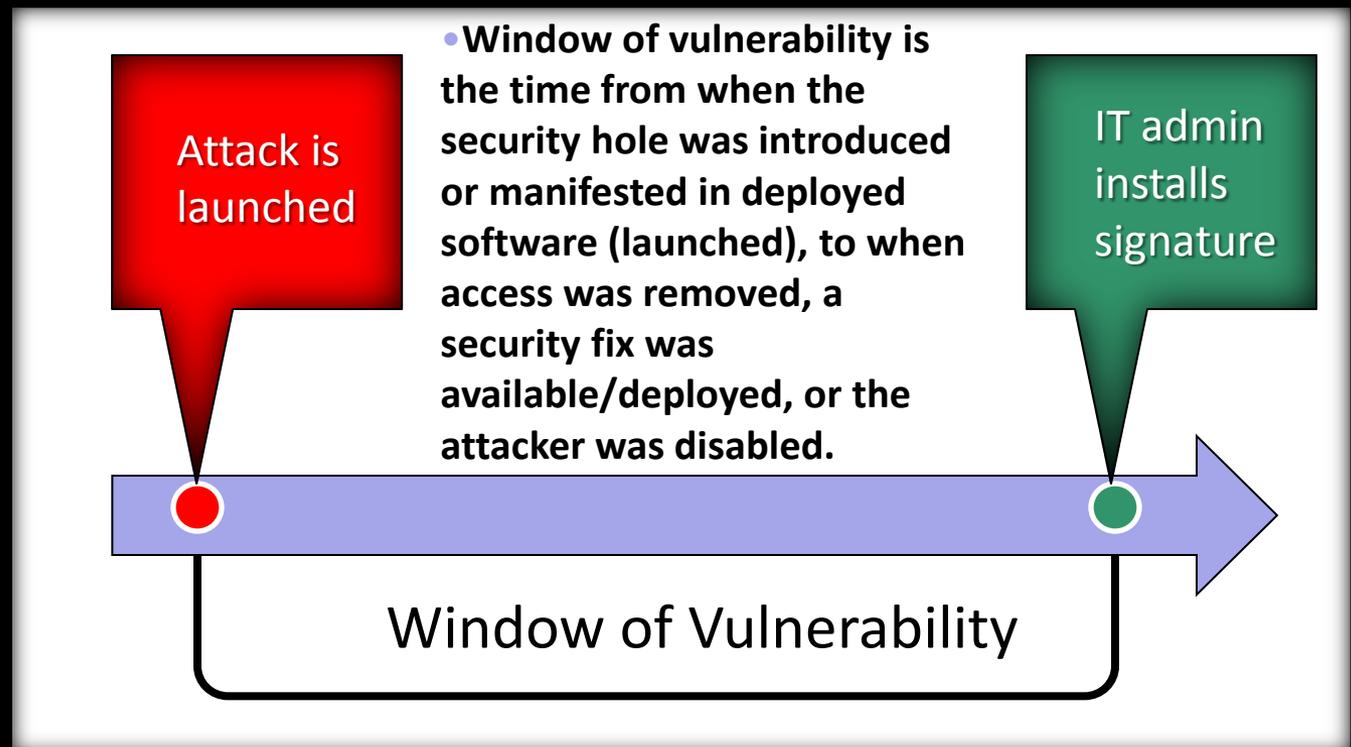
Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating (software) vulnerabilities.



# ...Vulnerabilities

- Then there are vulnerabilities without risk: for example when the affected asset has no value. A vulnerability with one or more known instances of working and fully implemented attacks is classified as an exploitable vulnerability — a vulnerability for which an exploit exists.

- A security risk may be classified as a vulnerability. The use of vulnerability with the same meaning of risk can lead to confusion. The risk is tied to the potential of a significant loss.





# Exploits

- An **exploit** is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized).

```
#!/bin/sh
-rwxr-xr-x 1 root root 14056 Sep 25 01:28 /usr/bin/efstool
$ /usr/bin/efstool `perl -e 'print "A"x3000;`
Segmentation fault
$ gdb -q /usr/bin/efstool
(no debugging symbols found)...(gdb) run `perl -e 'print "A"x3000;`
Starting program: /usr/bin/efstool `perl -e 'print "A"x3000;`
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) print $pc
$1 = 0x41414141
(gdb) x/48x (resp-2800)
0xbfffd60: 0xbfffe93 0xbfffe7d0 0xbfffe848 0x4002463f
0xbfffd70: 0x00000003 0xbfffe93 0xbfffe7d0 0x00000000
0xbfffd80: 0x00000000 0x00000000 0x00000000 0x00000000
0xbfffd90: 0x00000000 0x00000000 0x00000000 0xbfffe93
0xbffddb0: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffddc0: 0x00000000 0xbfffd00 0x00000000 0x00000000
0xbffddd0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffdde0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffddf0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffde00: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffde10: 0x41414141 0x41414141 0x41414141 0x41414141
```

**HACKING**  
THE ART OF EXPLOITATION

- Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service attack.



# ...Exploits

- There are several methods of classifying exploits. The most common is by how the exploit contacts the vulnerable software.
- A *remote exploit* works over a network and exploits the security vulnerability without any prior access to the vulnerable system.
- A *local exploit* requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator. Exploits against client applications also exist, usually consisting of modified servers that send an exploit if accessed with a client application.
- Exploits against client applications may also require some interaction with the user and thus may be used in combination with the social engineering method. Another classification is by the action against the vulnerable system; unauthorized data access, arbitrary code execution, and denial of service are examples. Many exploits are designed to provide superuser-level access to a computer system. However, it is also possible to use several exploits, first to gain low-level access, then to escalate privileges repeatedly until one reaches root. Normally a single exploit can only take advantage of a specific software vulnerability.



# Zero Day exploits

Often, when an exploit is published, the vulnerability is fixed through a patch and the exploit becomes obsolete until newer versions of the software become available. This is the reason why some black hat hackers do not publish their exploits but keep them private to themselves or other hackers.



A **zero-day** (also known as **zero-hour** or **0-day**) vulnerability is known as a "zero-day" because once the flaw becomes known, the software's author has zero days in which to plan and advise any mitigation against its exploitation (for example, by advising workarounds or by issuing patches).

Attacks employing zero-day exploits are often attempted before or on the day that notice of the vulnerability is released to the public; sometimes before the author is aware or has developed and made available corrected code. Zero-day attacks are a severe threat.



**zero day' vulnerability**... essentially, it's an unknown bug in a computer application. Software companies are pretty much constantly working to find and fix problems in their programs, but coding can be a messy business and mistakes often slip through. When a company finds a problem, they release a patch for it -- that's why you're probably pretty used to your operating system or a plug-in asking you to apply updates.

But the companies aren't always the first people to discover a problem. And when one of these bugs is discovered in the digital wild, programmers are expected to fix them as soon as possible -- hence the term "zero day" because that's how much time there is to patch the problem before cybercriminals or other adversaries can potentially exploit it.

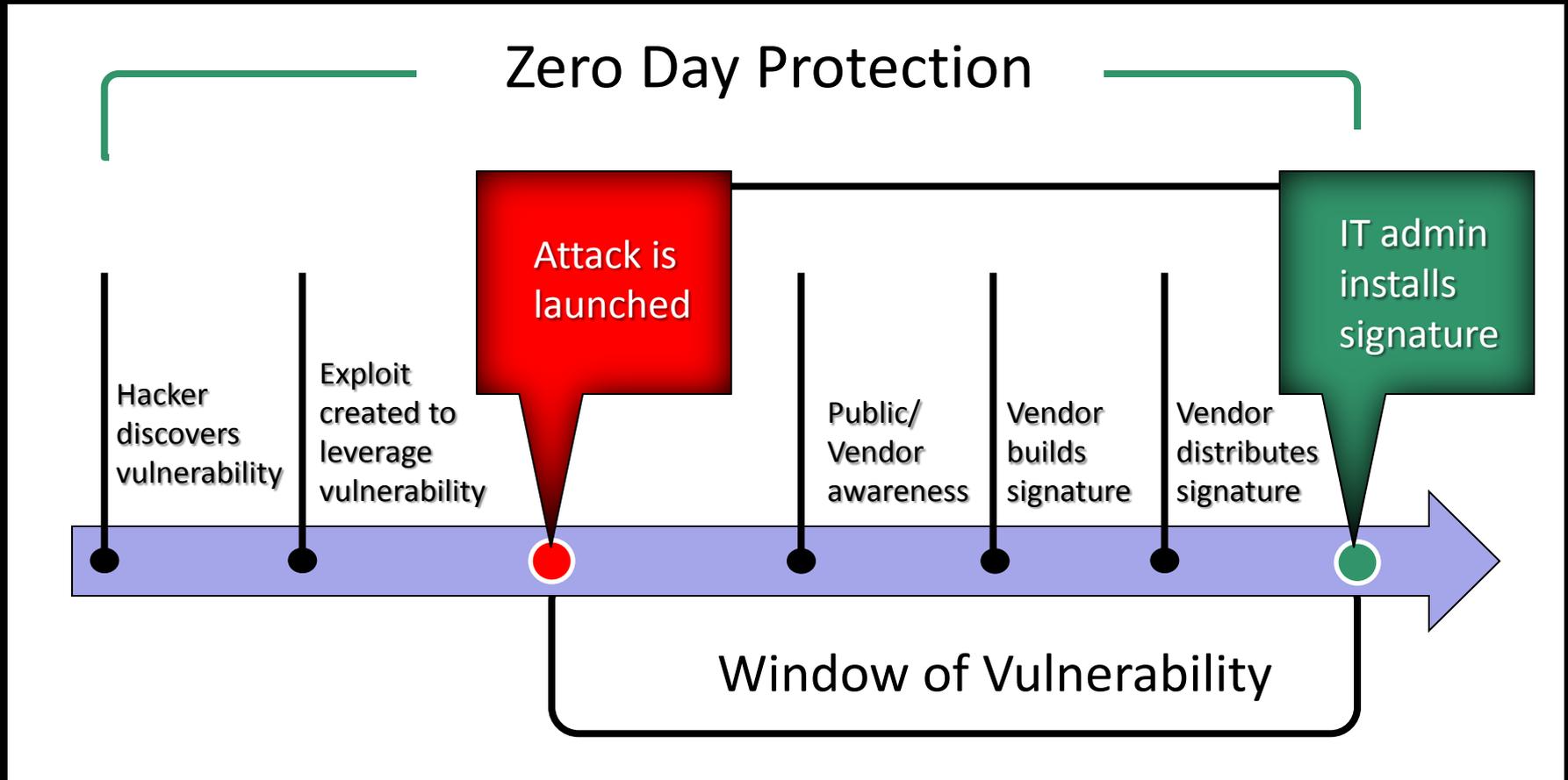
<http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/15/what-is-a-zero-day-vulnerability/>



# Zero Day Protection

Being protected against a new and unknown threat before:

- ✓ the vulnerability is discovered and the
- ✓ exploit is created and launched.





# Malware (malicious software)

Malware or malicious software is used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. Malware is defined by its malicious intent.



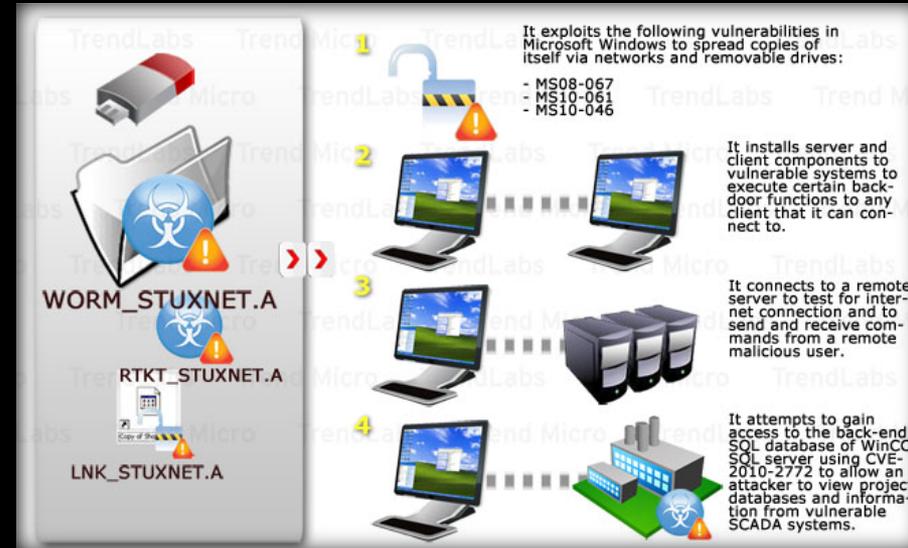
Malware may be stealthy, intended to steal information or spy on computer users for an extended period without their knowledge, or it may be designed to cause harm, often as sabotage (e.g., **Stuxnet**), or to extort payment (**CryptoLocker**).

'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including **computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware**, and other malicious programs. It can take the form of **executable code, scripts, active content**, and other software. Malware is often disguised as, or embedded in, non-malicious files.



# Stuxnet

The malware Stuxnet was designed to sabotage a country's nuclear program by targeting ICS. Stuxnet, the first cyber warfare weapon ever. It wasn't about industrial espionage: it didn't steal, manipulate, or erase information; rather, its goal was to physically destroy.



Additional information can be found at Stuxnet 60 Minutes:  
<https://www.youtube.com/watch?v=zEjUlBmD9kQ>





# Ransomware

- **Ransomware** is a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction.
- Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying.
- Ransomware typically propagates as a trojan, whose payload is disguised as a seemingly legitimate file.
- The use of ransomware scams has grown internationally.
- Wide-ranging attacks involving encryption-based ransomware began to increase through trojans such as CryptoLocker, which had procured an estimated US\$3 million before it was taken down by authorities, and Cryptowall, which was estimated by the US FBI to have accrued over \$18m by June 2015.



## SmartBrief on Cybersecurity

Security and risk management news that matters to the C-Suite

### TOP STORY

#### Many US agencies hit by ransomware cyberattacks, DHS says



Cybercriminals have attempted ransomware attacks on more than two dozen federal government agencies since July, the Department of Homeland Security said. None of the attacks succeeded, DHS said.

[The Hill](#) (3/30)

<http://thehill.com/policy/cybersecurity/274724-dhs-ransomware-attacks-widely-targeting-feds>

03/30/16 04:38 PM EDT

More than two dozen federal agencies have been hit by attempted “ransomware” attacks since last July - the Department of Homeland Security (DHS).

In the potentially damaging cyberattack, hackers remotely lock files in an effort to extort ransom payments. The DHS said 29 agencies have reported 321 incidents of ransomware-related activity since last June. But in no case did the agencies have to pay up, as the ransomware was not able to successfully infect the government's networks.

Ransomware has been thrust into the spotlight by a recent string of successful attacks at hospitals around the country. In February 2015, a California hospital paid a \$17,000 ransom to free its computers from a hacker's virus.

The Justice Department (DOJ) said its Internet Crime Complaint Center (IC3) had received 7,694 overall ransomware complaints since 2005 that have netted cyber crooks more than \$57 million in ransom payments. Much of this is due to a recent ransomware uptick.



# Ransomware

## MANAGING DATA

<http://www.cnbc.com/2016/04/11/the-associated-press-researchers-newer-type-of-ransomware-is-harbinger-of-danger.html>



A Cisco Systems report has revealed that a new type of ransomware comes in the form of an "unusual strain of virus-like hacker software," Tami Abdollah writes. The ransomware attacks computer server vulnerabilities without the need for human interaction. It is the same strain that hit the MedStar Health hospital chain in March. Cisco warned organizations that "the age of self-propagating ransomware, or cryptoworms, is right around the corner."

[CNBC/The Associated Press](#) (4/11)

WASHINGTON (AP) — An unusual strain of virus-like hacker software that exploits computer server vulnerabilities — without requiring human interaction — is a leading example of a new generation of "ransomware," according to a new report by Cisco Systems Inc.

Hackers use such software to target large-scale networks and hold data hostage in exchange for bigger payments. Such a strain, known as samsam, hit the MedStar Health Inc. hospital chain last month.

The ability to demand payment in bitcoin, a difficult-to-trace virtual currency not controlled by any country, was "basically the birth of ransomware" and has helped drive its success since the currency's introduction in 2009.

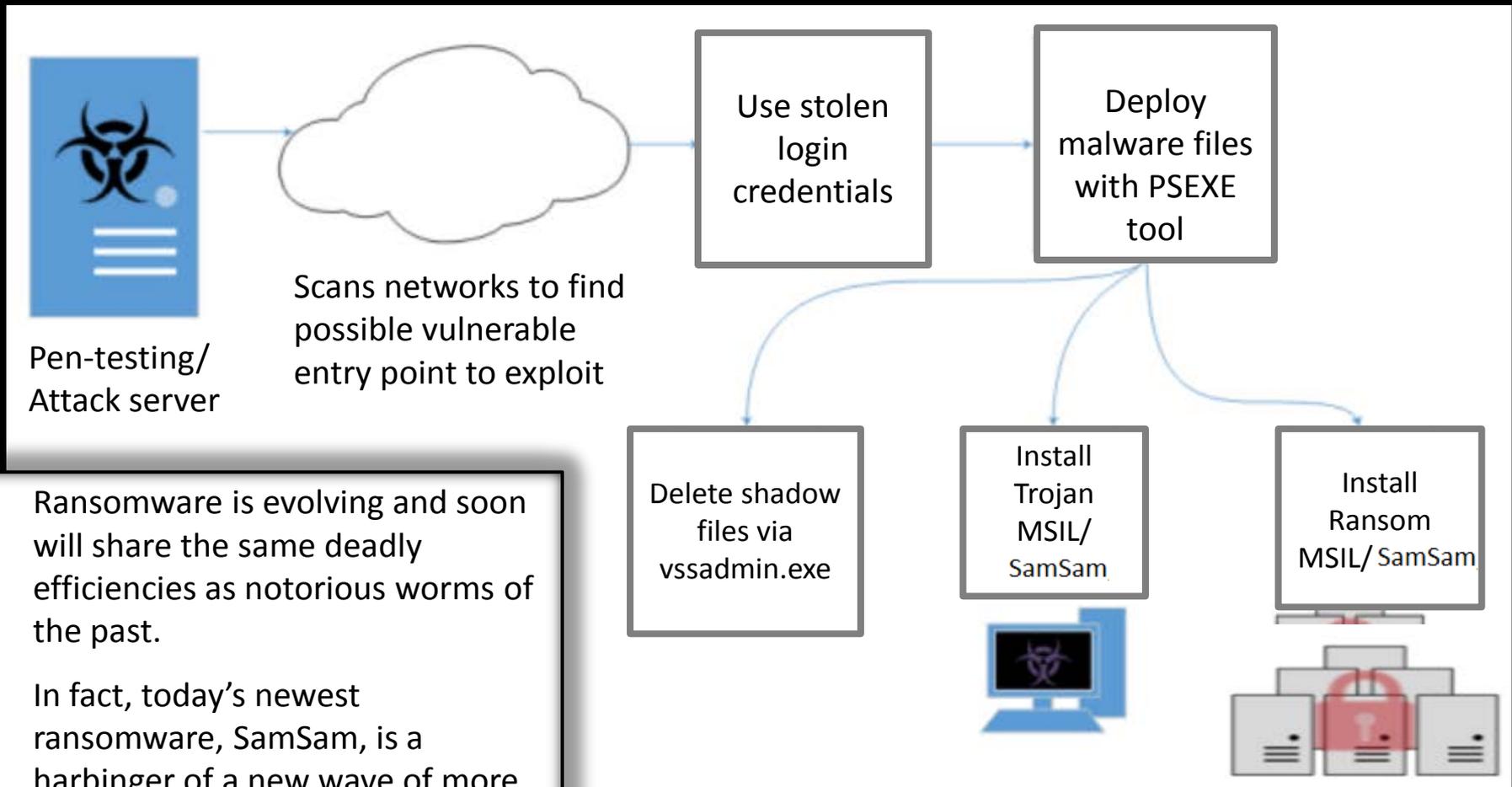
Samsam exploits vulnerabilities giving hackers a way into JBoss application servers that are frequently used by some of the largest corporations. Once inside, the hackers sometimes implant a tool that steals credentials, allowing it to spread through the system, and encrypt scores of digital files along the way.

Most ransomware still requires a human to click a link or open an infected email attachment, but Cisco's report warned that "the age of self-propagating ransomware, or cryptoworms, is right around the corner." Worms are generally virus-like infections that are programmed to spread automatically, without human interaction.

The semi-autonomous nature of this ransomware means that defenses, such as maintaining updated and patched systems and safe backups, are more predictable than teaching users to safely use the Internet.



# SamSam Ransomware



- Ransomware is evolving and soon will share the same deadly efficiencies as notorious worms of the past.
- In fact, today's newest ransomware, SamSam, is a harbinger of a new wave of more malicious, tenacious and costly ransomware.
- SamSam ransomware targets servers instead end-users.

<https://threatpost.com/meet-the-cryptoworm-the-future-of-ransomware/117330/>  
<https://threatpost.com/meet-the-cryptoworm-the-future-of-ransomware/117330/>

<http://www.scmagazine.com/report-warns-of-self-propagating-ransomware/article/489297/>



# DoS attack?

**In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.**



**The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.**

## **What is a Distributed Denial-of-Service (DDoS) attack?**

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.



## BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry

On December 23rd, 2015, around half of the homes in the Ivano-Frankivsk region in Ukraine (population around 1.4 million) were left without electricity for a few hours. According to the Ukrainian news media outlet TSN, the cause of the power outage was a “hacker attack” utilizing a “virus”.

It was discovered that the reported case was not an isolated incident and that other energy companies in Ukraine were targeted by cybercriminals at the same time.

Furthermore, it was found that the attackers have been using a malware family, BlackEnergy. Specifically, the BlackEnergy backdoor has been used to plant a KillDisk component onto the targeted computers that would render them unbootable.

The BlackEnergy operators have used numerous spreading mechanisms to infect their victims, including the infamous PowerPoint 0-day CVE-2014-4114.

While the primary objectives of the 2014 attacks appeared to be espionage, the discovery of BlackEnergy trojan-droppers indicated it capable of infecting SCADA Industrial Control Systems



# Regin (malware)

Regin is a sophisticated malware toolkit revealed in November 2014.

The malware targets specific users of Microsoft Windows-based computers and has been linked to the US intelligence gathering agency NSA and its British counterpart, the GCHQ.

Regin has been compared to Stuxnet and is thought to have been developed by "well-resourced teams of developers," as a targeted multi-purpose data collection tool.

**IT'S MALWARE THAT CAN:**  
capture your screenshots  
record your keystrokes  
silently monitor your web traffic  
steal your passwords  
recover your deleted files



# Regin (malware)

**Regin uses a modular approach allowing it to load features that exactly fit the target, enabling customized spying.**



**The design makes it highly suited for persistent, long-term mass surveillance operations against targets.**

**Regin is stealthy and does not store multiple files on the infected system; instead it uses its own Encrypted Virtual File System (EVFS) entirely contained within what looks like a single file with an innocuous name to the host, within which files are identified only by a numeric code, not a name.**



# Flame (malware)

Flame, also known as Flamer, sKyWIper, and Skywiper, is modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system. The program is being used for targeted cyber espionage.

**What is Flame?**

"One of the most complex threats ever discovered."



Its discovery was announced on 28 May 2012 by MAHER Center of Iranian National, Computer Emergency Response Team (CERT), Kaspersky Lab and CrySyS Lab of the Budapest University of Technology and Economics. The last of these stated in its report that Flame "is certainly the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever found."



# Flame (malware)

Flame can spread to other systems over a local network (LAN) or via USB stick. It can record audio, screenshots, keyboard activity and network traffic.



The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices. This data, along with locally stored documents, is sent on to one of several command and control servers that are scattered around the world. The program then awaits further instructions from these servers.

According to estimates by Kaspersky in May 2012, Flame had initially infected approximately 1,000 machines, with victims including governmental organizations, educational institutions and private individuals. At that time 65% of the infections happened in other countries. Flame has also been reported in Europe and North America. Flame supports a "kill" command which wipes all traces of the malware.



# Flame (malware) – it's Operation

Flame is an uncharacteristically large program for malware at 20 megabytes. It allows other attack modules to be loaded after initial infection. The malware uses five different encryption methods and an SQLite database to store structured information.

The internal code has few similarities with other malware, but exploits two of the same security vulnerabilities used previously by Stuxnet to infect systems.

The malware determines what antivirus software is installed, then customizes its own behavior (for example, by changing the filename extensions it uses) to reduce the probability of detection by that software.

Flame is not designed to deactivate automatically, but supports a "kill" function that makes it eliminate all traces of its files and operation from a system on receipt of a module from its controllers.



# Flame (malware)



List of code names for various families of modules in Flame's source code and their *possible* purpose

Flame, like the previously known cyber weapon Stuxnet, is employed in a targeted manner and can evade current security software through rootkit functionality. Unlike Stuxnet, which was designed to sabotage an industrial process, Flame appears to have been written purely for espionage. It does not appear to target a particular industry, but rather is "a complete attack toolkit designed for general cyber-espionage purposes".

Name	Description
Flame	Modules that perform attack functions
Boost	Information gathering modules
Flask	A type of attack module
Jimmy	A type of attack module
Munch	Installation and propagation modules
Snack	Local propagation modules
Spotter	Scanning modules
Transport	Replication modules
Euphoria	File leaking modules
Headache	Attack parameters or properties

# Code injection

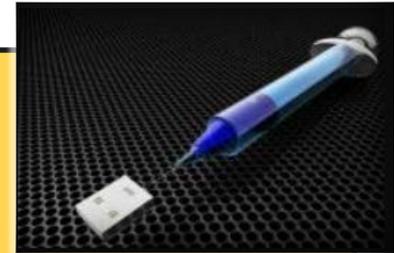
is the exploitation of a computer bug that is caused by processing invalid data. Injection is used by an attacker to introduce (or "inject") code into a vulnerable computer program and change the course of execution. The result of successful code injection is often disastrous (for instance: code injection is used by some computer worms to propagate).

41

- Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, particularly in legacy code. They are often found in SQL, LDAP, Xpath, or NoSQL queries; OS commands; XML parsers, SMTP Headers, program arguments, etc.
- Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover. Certain types of code injection are errors in interpretation, giving special meaning to mere user input.

## **Code injection can be used malevolently for many purposes, including:**

- Arbitrarily modify values in a database through a type of code injection SQL injection. The impact of this can range from website defacement to serious compromise of sensitive data.
- Install malware or execute malevolent code on a server, by injecting server scripting code (such as PHP or ASP).
- Privilege escalation to root permissions by exploiting Shell Injection vulnerabilities.
- Attacking web users with HTML/Script Injection (Cross-site scripting).





# Arbitrary code execution



- Arbitrary code execution is used to describe an attacker's to execute any commands of the attacker's choice on a target machine or in a target process.
- It is commonly used in arbitrary code execution vulnerability to describe a software bug that gives an attacker a way to execute arbitrary code. A program that is designed to exploit such a vulnerability is called an arbitrary code execution exploit.
- Most of these vulnerabilities allow the execution of machine code and most exploits therefore inject and execute shellcode to give an attacker an easy way to manually run arbitrary commands.
- The ability to trigger arbitrary code execution from one machine on another (especially via a wide-area network such as the Internet) is often referred to as remote code execution.
- It is the most powerful effect a bug can have because it allows an attacker to completely take over the vulnerable process. From there the attacker can potentially take complete control over the machine the process is running on.



# Arbitrary code execution

- Arbitrary code execution vulnerabilities are commonly exploited by malware to run on a computer without the owner's consent or by an owner to run homebrew software on a device without the manufacturer's consent.
- Once the invader can execute arbitrary code directly on the OS, there is often an attempt at a privilege escalation exploit in order to gain additional control.
- This may involve the kernel itself or an account such as Administrator, SYSTEM, or root. With or without this enhanced control, exploits have the potential to do severe damage or turn the computer into a zombie - but privilege escalation helps with hiding the attack from the legitimate administrator of the system.

## Threats Against the Host

Threat	Examples
Arbitrary code execution	Buffer overflows in ISAPI DLLs (e.g., MS01-033)
	Directory traversal attacks (MS00-078)
File disclosure	Malformed HTR requests (MS01-031)
	Virtualized UNC share vulnerability (MS00-019)
Denial of service (DoS)	Malformed SMTP requests (MS02-012)
	Malformed WebDAV requests (MS01-016)
	Malformed URLs (MS01-012)
	Brute-force file uploads
Unauthorized access	Resources with insufficiently restrictive ACLs
	Spoofing with stolen login credentials
Exploitation of open ports and protocols	Using NetBIOS and SMB to enumerate hosts
	Connecting remotely to SQL Server



**Metasploit – with many transportation systems running on UNIX (including Linux and Mac OS X) and on Windows, awareness of the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine is highly recommended.**



Metasploit Framework: both a penetration testing system and a development platform for creating security tools and exploits .

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its best-known sub-project is the open source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine.

The Metasploit Project is well known for its anti-forensic and evasion tools, some of which are built into the Metasploit Framework.

Metasploit documentation, videos, and Q & A:

[https://community.rapid7.com/Rapid7\\_Home](https://community.rapid7.com/Rapid7_Home)

Mastering the Framework: <http://www.offensive-security.com/metasploit-unleashed/>

Additional information:

<http://framework.metasploit.com/about/>

<http://www.metasploit.com>



# Metasploit (history)

Metasploit was created by H. D. Moore in 2003 as a portable network tool using Perl. By 2007, the Metasploit Framework had been completely rewritten in Ruby. On October 21, 2009, the Metasploit Project announced that it had been acquired by Rapid7, a security company that provides unified vulnerability management solutions.

Like comparable commercial products such as Immunity's Canvas or Core Security Technologies' Core Impact, Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. Like many information security tools, Metasploit can be used for both legitimate and unauthorized activities. Since the acquisition of the Metasploit Framework, Rapid7 has added two open core proprietary editions called Metasploit Express and Metasploit Pro.

Metasploit's emerging position as the de facto exploit development framework led to the release of software vulnerability advisories often accompanied by a third party Metasploit exploit module that highlights the exploitability, risk and remediation of that particular bug. Metasploit 3.0 began to include fuzzing tools, used to discover software vulnerabilities, rather than just exploits for known bugs. This avenue can be seen with the integration of the lorcon wireless (802.11) toolset into Metasploit 3.0 in November 2006. Metasploit 4.0 was released in August 2011.



## Metasploit Framework

The basic steps for exploiting a system using the Framework include:

- Choosing and configuring an *exploit*;
- An option to check whether the intended target system is susceptible to the chosen exploit;
- Choosing and configuring a *payload* ;
- Choosing the encoding technique so that the intrusion-prevention system (IPS) ignores the encoded payload;

Executing the exploit.

This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework.

It facilitates the tasks of attackers, exploit writers and payload writers.

*Payload*: code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server



# Backdoors

- A **backdoor** is a method, often secret, of bypassing normal authentication in a product, computer system, cryptosystem or algorithm etc.
- Backdoors are often used for securing unauthorized remote access to a computer, or obtaining access to plaintext in cryptographic systems.
- A backdoor may take the form of a hidden part of a program, a separate program (e.g. Back Orifice may subvert the system through a rootkit), or may be a hardware feature. Although normally secretly installed, in some cases backdoors are deliberate and widely known. These kinds of backdoors might have "legitimate" uses such as providing the manufacturer with a way to restore user passwords.
- Default passwords can function as backdoors if they are not changed by the user. Some debugging features can also act as backdoors if they are not removed in the release version.

...the threat of backdoors for transportation infrastructure where multiuser and networked operating systems-based exist; awareness to securing unauthorized remote access, obtaining access to plaintext, and so on, while attempting to remain undetected is real.

## Additional backdoors



- ✓ Object code
- ✓ Asymmetric
- ✓ Compiler



# WHAT IS A SANDBOX?

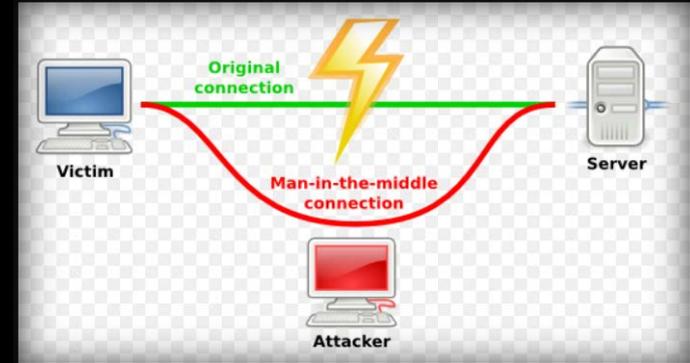
A sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third parties, suppliers, untrusted users and untrusted websites. A sandbox typically provides a tightly controlled set of resources for guest programs to run in. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted.

In the sense of providing a highly controlled environment, sandboxes may be seen as a specific example of virtualization. Sandboxing is frequently used to test unverified programs that may contain a virus or other malicious code, without allowing the software to harm the host device.



# Man-In-the-Middle (MITM) attack

A man-in-the-middle attack is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.



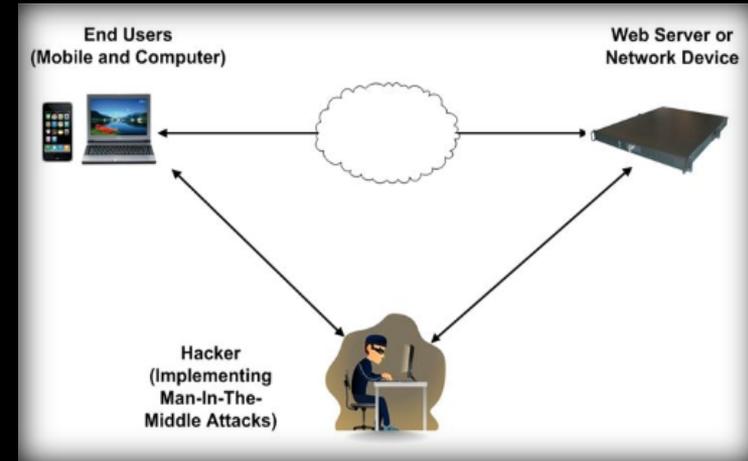
Man-in-the-middle attacks can be thought about through a chess analogy. Cherise, who barely knows how to play chess, claims that she can play two grandmasters simultaneously and either win one game or draw both. She waits for the first grandmaster to make a move and then makes this same move against the second grandmaster. When the second grandmaster responds, Mallory makes the same play against the first. She plays the entire game this way and cannot lose.

A man-in-the-middle attack is a similar strategy and can be used against many cryptographic protocols.



# Man-In-the-Middle (MITM) attack

One example of man-in-the-middle attacks is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.



The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle.

As an attack that aims at circumventing mutual authentication, or lack thereof, a man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to their satisfaction as expected from the legitimate other end.

Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, Transport Layer Security (TLS) can authenticate one or both parties using a mutually trusted certificate authority.



Captured network traffic from what is suspected to be a MITM attack can be analyzed in order to determine if it really was a MITM attack or not. Important evidence to analyze when doing network forensics of a suspected TLS MITM attack include:

- IP address of the server;
- DNS name of the server;
- X.509 certificate of the server:
  - Is the certificate self signed?
  - Is the certificate signed by a trusted CA?
  - Has the certificate been revoked?
  - Has the certificate been changed recently?
  - Do other clients, elsewhere on the Internet, also get the same certificate?

**X.509** is an important standard for a public key infrastructure (PKI) to manage digital certificates and public-key encryption and a key part of the Transport Layer Security protocol used to secure web and email communication.



Sponsored by  
DHS/NCCIC/US-CERT

NIST  
National Institute of  
Standards and Technology

# National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities	Checklists	800-53/800-53A	Product Dictionary	Impact Metrics	Data Feeds	Statistics	FAQs
Home	SCAP	SCAP Validated Tools	SCAP Events	About	Contact	Vendor Comments	Visualizations

# Vulnerability Severity

All vulnerabilities, if exploited successfully, result in an unexpected technical impact to a system or software. Vulnerability severity is generally expressed in terms of its Common Vulnerability Scoring System (CVSS) score.

A great resource on vulnerabilities and their CVSS score is the National Vulnerability Database <http://nvd.nist.gov/>

The CVSS score expresses the probability a vulnerability will be exploited based on the ease of exploitability, access vector, access complexity, and authentication required to exploit it.

Note: the best vulnerabilities from an attacker's perspective:

- Are remotely exploitable
- Can be triggered by an unauthorized user
- Allow Arbitrary Code Execution (ACE) upon exploit.



# Keyloggers

Key loggers are used to monitor keyboard activity. They can be software-based or hardware-based. Usually the information is retrieved across a local network, the internet, or from the physical device connected to the keyboard.

Software-based keyloggers: these are computer programs designed to work on the target computer's software. Keyloggers can be used to monitor network usage without their users' direct knowledge. However, malicious individuals can use keyloggers on public computers to steal passwords or other critical information.

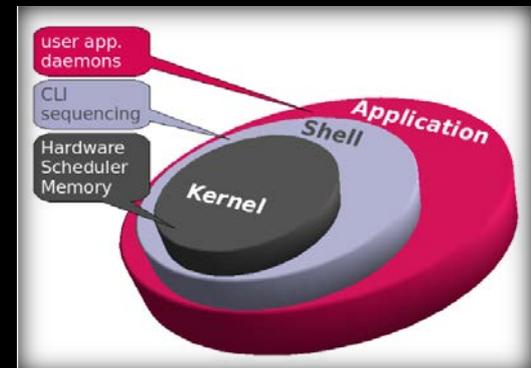
Hypervisor-based: The keyloggers can theoretically reside in a malware hypervisor running underneath the operating system, which thus remains untouched. It effectively becomes a virtual machine.



# Keyloggers

**Kernel-based:** A program on the machine obtains root access to hide itself in the OS and intercepts keystrokes that pass through the kernel. This method is difficult both to write and to combat. Such keyloggers reside at the kernel level, which makes them difficult to detect, especially for user-mode applications that don't have root access. They are frequently implemented as rootkits that subvert the operating system kernel to gain unauthorized access to the hardware. This makes them very powerful. A keylogger using this method can act as a keyboard driver, for example, and thus gain access to any information typed on the keyboard as it goes to the operating system.

The kernel is a computer program that constitutes the central core of a computer's operating system.



## Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

29 April 2016

Alert Number  
162929-001

Please contact the FBI with any questions related to this PIN Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

### Wireless Keystroke Logger Disguised as USB Device Charger Targets Wireless Keyboards

#### Summary

KeySweeper is a covert device that resembles a functional Universal Serial Bus (USB) enabled device charger which conceals hardware capable of harvesting keystrokes from certain wireless keyboards. If placed strategically in an office or other location where individuals might use wireless devices, a malicious cyber actor could potentially harvest personally identifiable information, intellectual property,



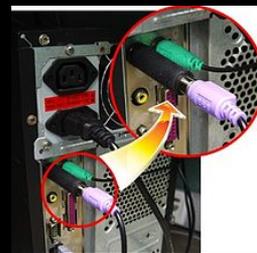
# ...Keyloggers

From a technical perspective there are several categories

- **API-based:** These keyloggers hook keyboard APIs inside a running application. The keylogger registers keystroke events, as if it was a normal piece of the application instead of malware. The keylogger receives an event each time the user presses or releases a key. The keylogger simply records it.
- **Form grabbing based:** Form grabbing-based keyloggers log web form submissions by recording the web browsing on submit events. This happens when the user completes a form and submits it, usually by clicking a button or hitting enter. This type of keylogger records form data before it is passed over the Internet.
- **Memory injection based:** Memory Injection (MitB)-based keyloggers perform their logging function by altering the memory tables associated with the browser and other system functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors to bypass Windows UAC (User Account Control).
- **Packet analyzers:** This involves capturing network traffic associated with HTTP POST events to retrieve unencrypted passwords. This is made more difficult when connecting via HTTPS, which is one of the reasons HTTPS was invented.
- **Remote access software keyloggers:** These are local software keyloggers with an added feature that allows access to locally recorded data from a remote location.



hardware-based keylogger

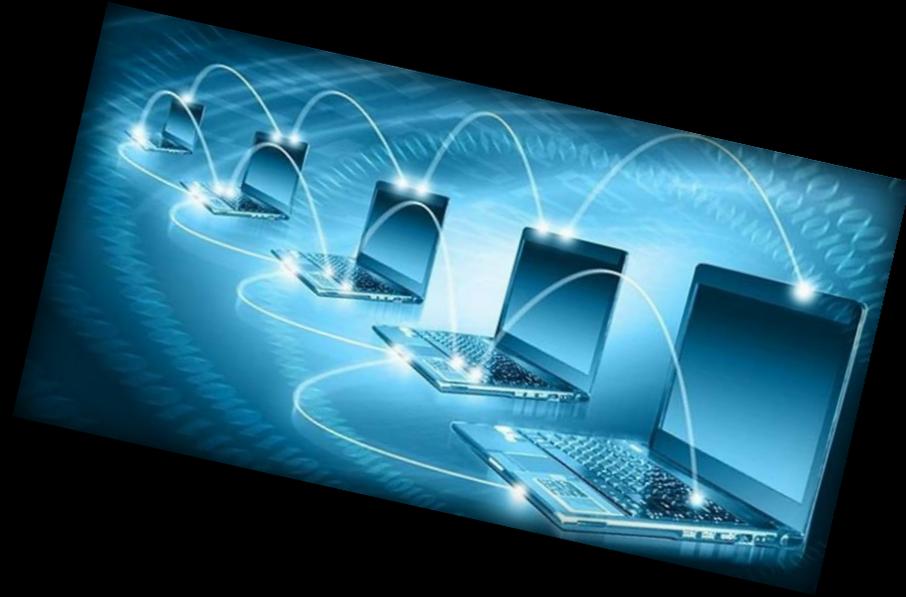


connected hardware-based keylogger



# Pivoting

- Pivoting refers to a method used by penetration testers that uses the compromised system to attack other systems on the same network to avoid restrictions such as firewall configurations, which may prohibit direct access to all machines.
- For example, if an attacker compromises a web server on a corporate network, the attacker can then use the compromised web server to attack other systems on the network. These types of attacks are often called multi-layered attacks.
- Pivoting is also known as *island hopping*.





# ....Pivoting

- Pivoting can further be distinguished into proxy pivoting and VPN pivoting:
- Proxy pivoting generally describes the practice of channeling traffic through a compromised target using a proxy payload on the machine and launching attacks from the computer. This type of pivoting is restricted to certain TCP and UDP ports that are supported by the proxy.
- VPN pivoting enables the attacker to create an encrypted layer to tunnel into the compromised machine to route any network traffic through that target machine, for example, to run a vulnerability scan on the internal network through the compromised machine, effectively giving the attacker full network access as if they were behind the firewall.
- Typically, the proxy or VPN applications enabling pivoting are executed on the target computer as the payload (software) of an exploit.



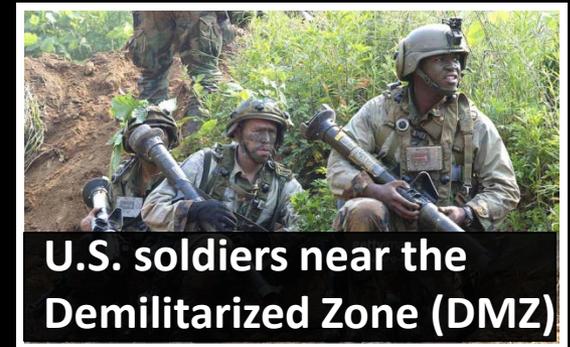
# DMZ (demilitarized zone)

*(sometimes referred to as a perimeter network)*

DMZ is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone", an area in which military operation is not permitted.

Hosts in the DMZ are permitted to have only limited connectivity to specific hosts in the internal network, as the content of DMZ is not as secure as the internal network. Similarly communication between hosts in the DMZ and to the external network is also restricted, to make the DMZ more secure than the Internet, and suitable for housing these special purpose services. This allows hosts in the DMZ to communicate with both the internal and external network, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients, and another firewall would perform some level of control to protect the DMZ from the external network.

DMZ configuration provides security from external attacks, but it typically has no bearing on internal attacks such as sniffing communication via a packet analyzer or spoofing.

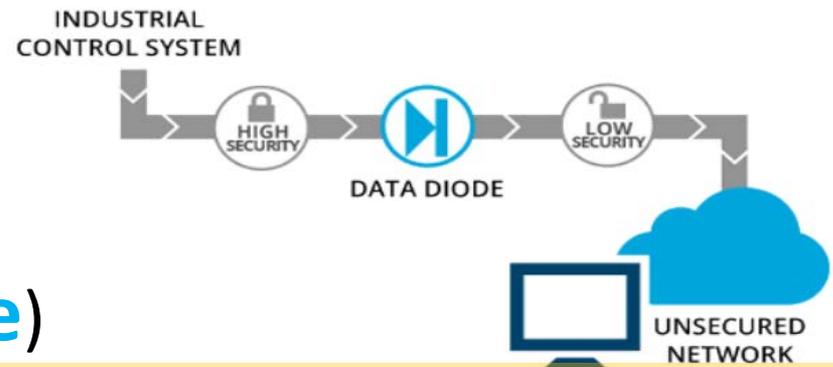


**U.S. soldiers near the Demilitarized Zone (DMZ)**

Hosts most vulnerable to attack are those that provide services to users outside of the local area network. Because of the increased potential of these hosts suffering an attack, they are placed into this specific subnetwork in order to protect the rest of the network if an intruder were to compromise any of them successfully.

# A unidirectional network

(also referred to as a **unidirectional security gateway** or more commonly **Data Diode**)



It is a network appliance or device allowing data to travel only in one direction, used in guaranteeing information security. They are most commonly found at the industrial control level, where they serve as connections between two or more networks of differing security classifications.

## Benefits:

Such functionality can be attractive if sensitive data is stored on a network which requires connectivity with the Internet. Traditionally the data would be vulnerable to intrusions from the Internet, however with a unidirectional network separating a high side with sensitive data, and a low side with Internet connectivity, one can achieve the best of both worlds. This holds true even if both the low and the high network are compromised, as the security guarantees are physical in nature.

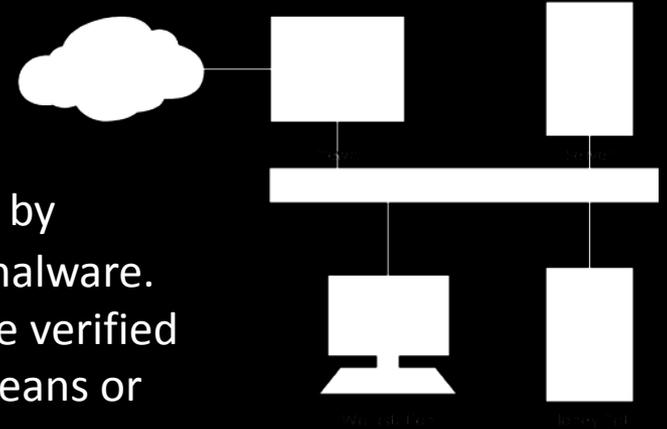
The controlled interface that comprises the send and receive elements of a unidirectional network acts as a one-way "[communications protocol](#) break" between both two-way network domains it connects. This does not preclude unidirectional network use in transferring protocols like [TCP/IP](#), that require communications (including [acknowledgments](#)) between sender and receiver. By employing [TCP/IP client-server](#) proxies prior to, and after one-way transfer, data transported as TCP packet flows can gain the security value of unidirectional transfer.



# Honeypot... the Basic Mousetrap



An application that creates a sandbox-like environment to trap attackers is called a “honeypot.”



**Malware honeypots** are used to detect malware by exploiting the known replication and attack vectors of malware. Replication vectors such as **USB flash drives** can easily be verified for evidence of modifications, either through manual means or utilizing special-purpose honeypots that emulate drives.

**SSH Honey Pot...** **HonSSH is a high-interaction Honey Pot solution. HonSSH will sit between an attacker and a honey pot, creating two separate SSH connections ...**  
**A medium interaction SSH honeypot designed to log brute force attacks and, most importantly, the entire shell interaction performed by the attacker.**

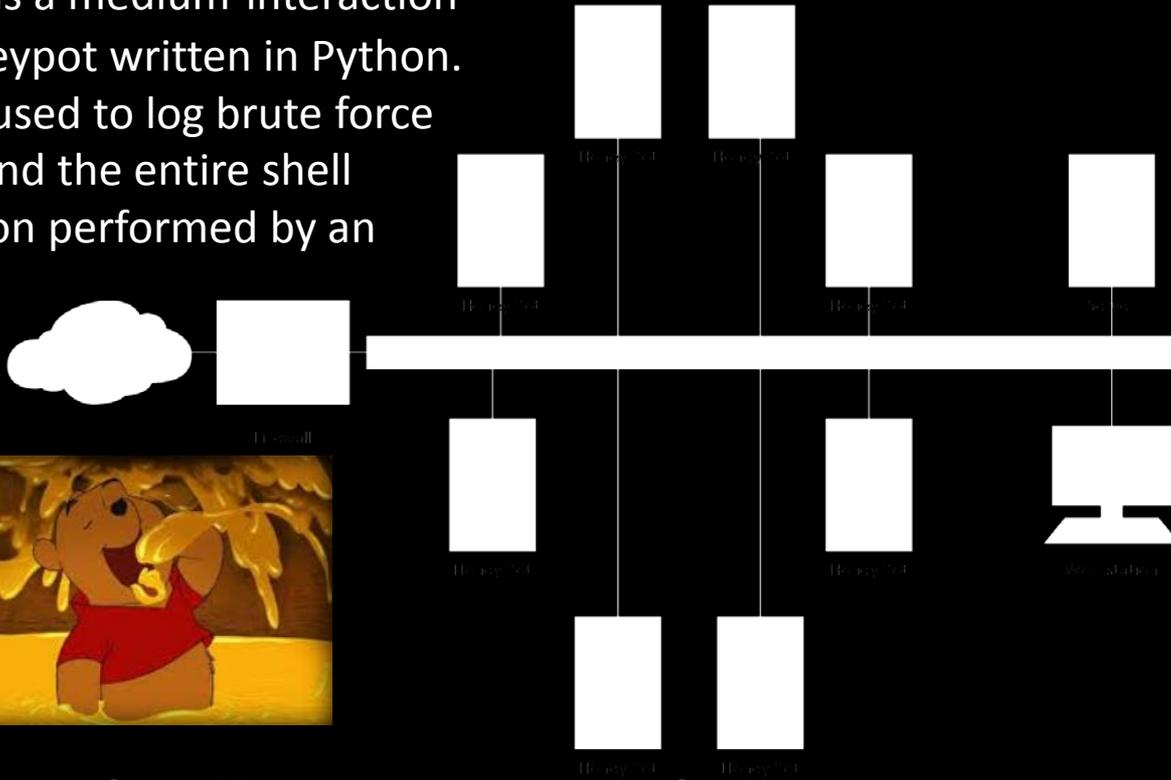
**Database honeypot:** Databases often get attacked by intruders using **SQL Injection**. As such activities are not recognized by basic firewalls, companies often use database firewalls for protection. Some of the available SQL database firewalls provide/support Honeypot architectures so that the intruder runs against a trap database while the web application remains functional.

**Kojoney** is a low level interaction honeypot that emulates an SSH server.



*"For the Win"* an internet cheer used to express a feeling of general enthusiasm or optimism.

**Kippo** is a medium-interaction SSH honeypot written in Python. Kippo is used to log brute force attacks and the entire shell interaction performed by an attacker.



the logging of the SSH honeypot could be fed into a security information and event management (SIEM) solution. This would then act as a sensor either on the internal network or the externally exposed IP addresses to discover attack activity.

## Security Information and Event

**Management (SIEM)** software products and services combine Security Information Management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by network hardware and applications.

**HonSSH** is designed to be used in conjunction with a **high interaction honeypot**. HonSSH sits between the attacker and the honey pot and creates two separate SSH connections.



- ICS/Resilient Control Systems

## Industrial Control Systems (ICS)

is a generic term used to describe any system that gathers information on an industrial process and modifies, regulates, or manages the process to achieve a desired result.

ICS refers to a broad set of control systems, which include:

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control System)
- PCS (Process Control System)
- Any other automated control system.

As technology advances, the terms are getting blurred and the differences in functionality is shrinking.



# Industrial Control Systems

### Power Station



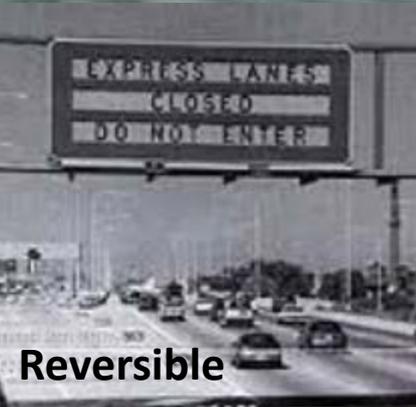
### DMS



### Traffic Signal Controller Cabinet



### CMS



### Reversible Lane Control

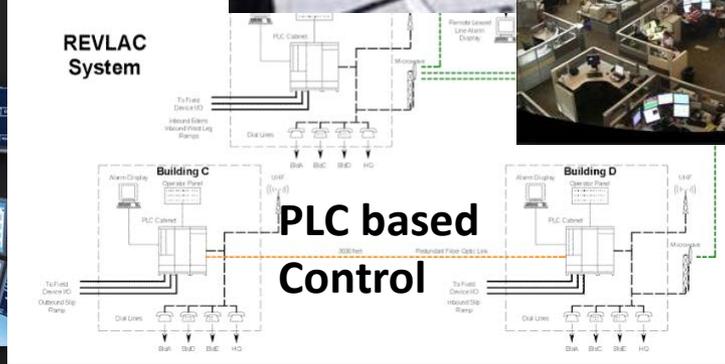
### Traffic Signal System



### SCADA Control Center



### REVLAC System



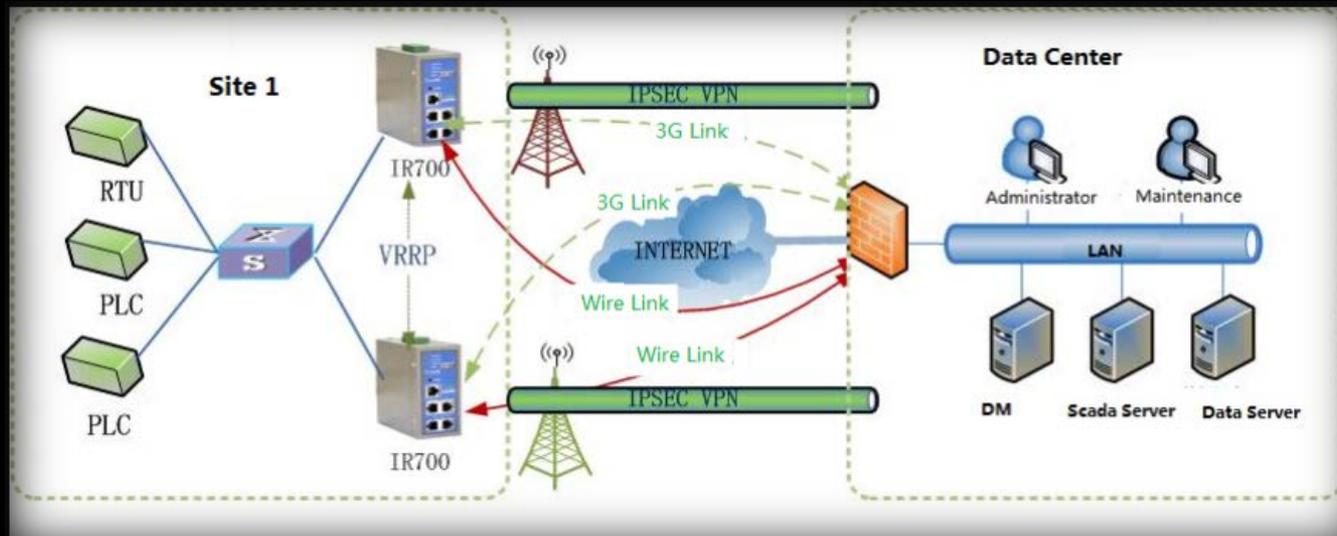
### PLC based Control

### Traffic Management Center





Operators of transportation systems need SCADA systems to manage critical infrastructures such as roadway pumping stations , PLC-based Reversible Lane Control Systems and tunnel ventilation systems (consists of both software and field equipment). Monitoring and controlling these systems is necessary during equipment failures or critical incidents.



Connecting SCADA systems to the Internet puts the infrastructure at risk because it opens up the possibility of intruders finding a way into the network. However, many organizations take that risk to save money, simplify the infrastructure and ease maintenance. It is usually cheaper to transmit data over the Internet instead of investing in dedicated lines or wireless frequency space.



- The benefit of SCADA being 'online' is that the Internet is cheap, robust, standardized and easily accessible, the downside is that without proper protections, the infrastructure is wide open to anyone looking.
- Secure and isolated networks or a virtual private network to restrict communicate with the controllers is recommended. Since SCADA systems will likely be Internet-accessible, focus should then be on putting them behind a secure gateway.

Check out the following sites for an example SCADA advisory

Advisory (ICSA-14-259-01A) Schneider Electric SCADA Expert ClearSCADA Vulnerabilities (Update A)

<https://ics-cert.us-cert.gov/advisories/ICSA-14-259-01A>

<http://www.securityweek.com/vulnerabilities-found-schneider-electric-scada-product-line>



## Embedded Systems

An embedded system is a computer system consisting of hardware and software designed for a specific purpose or dedicated task – they are “embedded” or part of other systems or devices.

## Embedded Systems Components

- **Microprocessor** – Central Processor Unit (CPU).
- **Memory** – Volatile and nonvolatile memory.
- **User interface** – Keyboards, displays, switches.
- **Input/output** – Interface with the physical world.
- **Communication interfaces.**

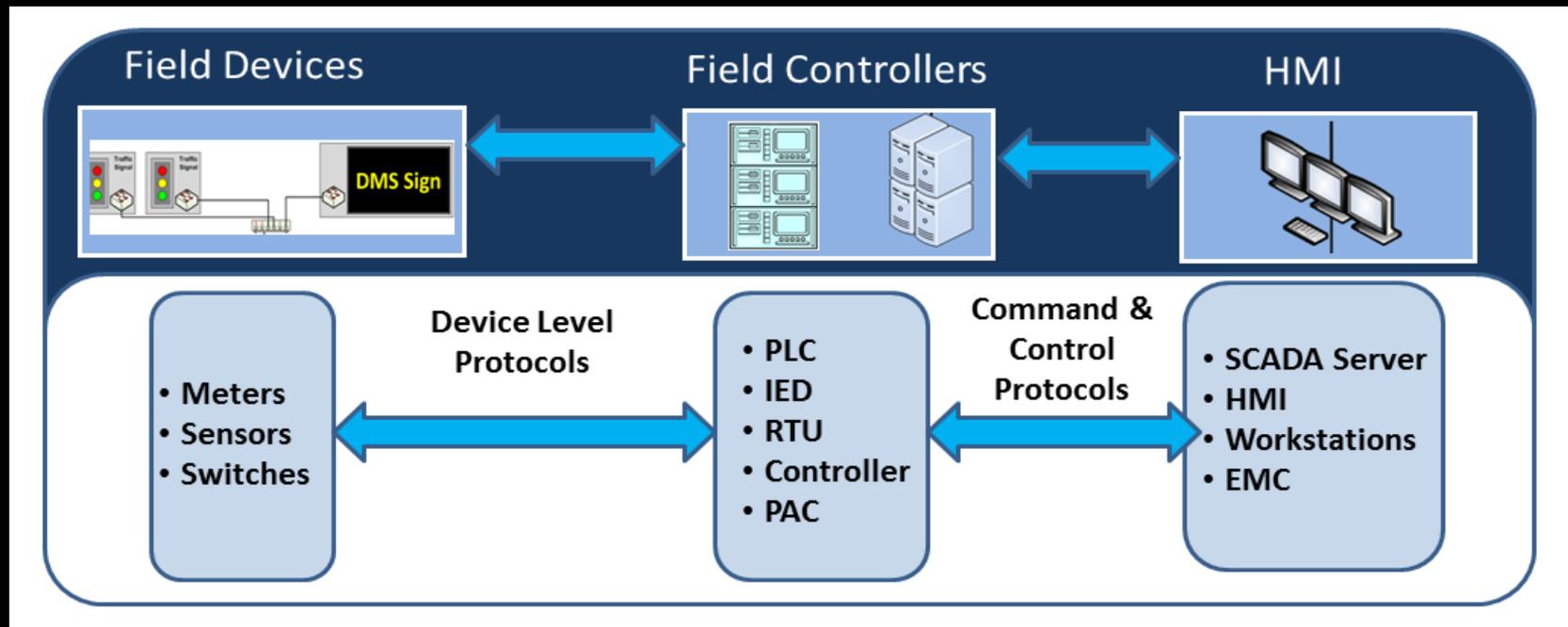
## Embedded Systems used in ICS

- **Field controllers** – Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), DCS controllers, Intelligent Electronic Devices (IEDs), field devices, Foundation Fieldbus, Profibus (Process Field Bus), DeviceNet).
- **Network/Communication equipment** – Routers, switches, modems, radios, terminal servers, and gateways.
- **Miscellaneous** – Firewalls and other security appliances, GPS time synchronization, network printers, hand-held configuration devices, and test equipment.



A **remote terminal unit (RTU)** is a **microprocessor-controlled** electronic device that interfaces objects in the physical world to a **distributed control system** or **SCADA** (supervisory control and data acquisition) system by transmitting **telemetry** data to a master system, and by using messages from the master supervisory system to control connected objects.

**Intelligent Electronic Devices (IED)** are a type of RTU *used* in SCADA systems, to monitor and control processes.



**PAC** or programmable automation controller, combines the industrial PC and programmable logic controller control with the flexibility of monitoring.



- Real-time operating systems (RTOS) – Neutrino & RTOS (QNX), VxWorks (Wind River), Windows CE (Microsoft).
- IEC 61131 program languages:
  - Workbenches – CoDeSys, ISaGRAF
  - Languages:
    - Ladder diagram (LD)
    - Function Block Diagram (FBD)
    - Sequential Text (ST)
    - Instruction List (IL)
- Device Drivers and Device Managers:
  - Ethernet/IP stacks
  - RS@#@/RS485
  - Memory managers
  - User interfaces
  - Services - Web server, ftp server, snmp
  - Debuggers.

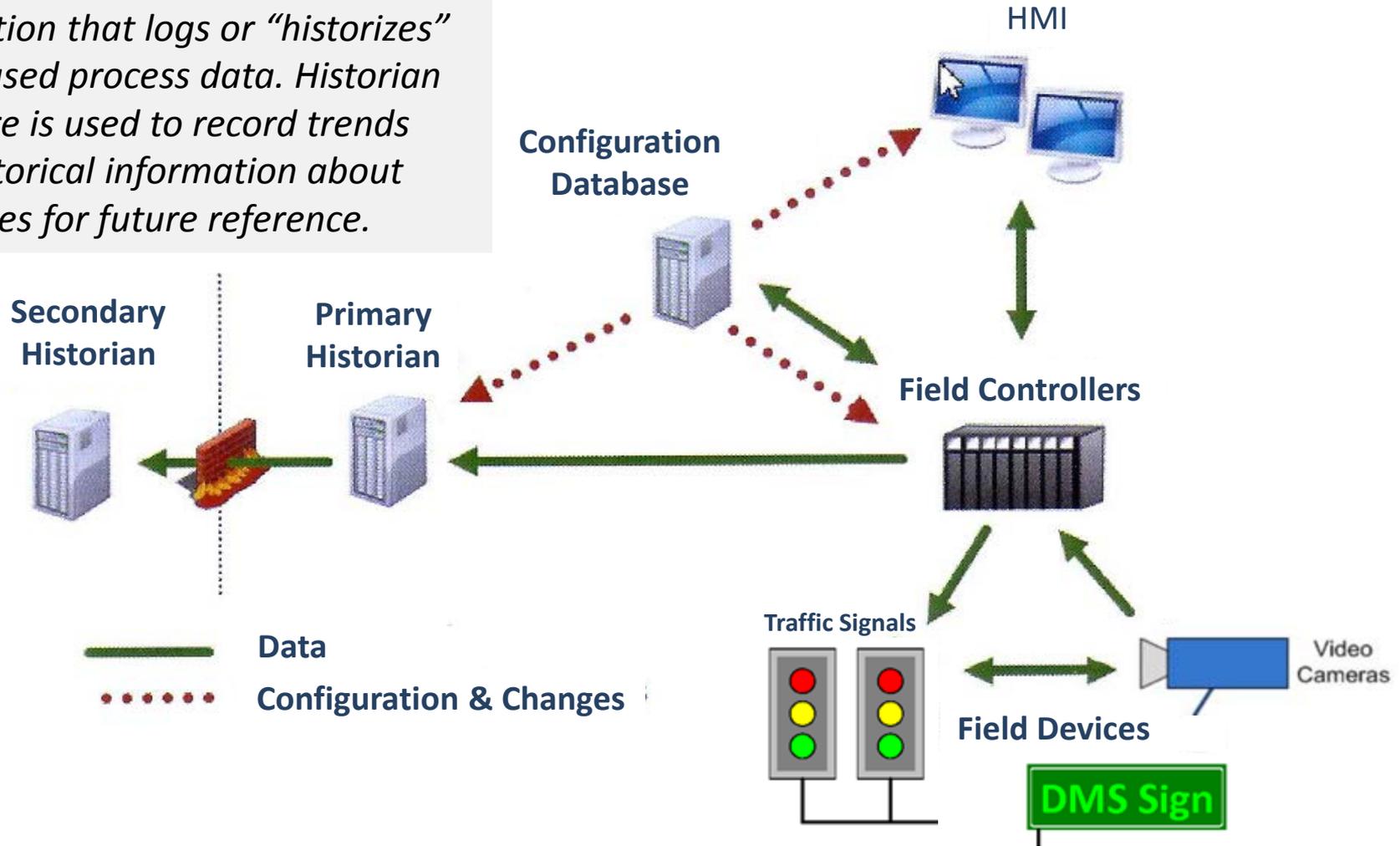




- Power – it can be DC, AC solar or battery backup.
- Processors – various i.e. Intel, PowerPC, ARM (ARM Holdings) MIPS technology.
- Memory – Nonvolatile: flash, EEPROM, EPROM, ROM. Firmware (boot code, real time operating system [RTOS], application programs. Volatile memory: RAM, variables, stacks, and buffers.
- Input/Output – Discrete, analog, fieldbus.
- Communication Ports: Serial – RS232, RS422/485, USB, modems, radio. Network- Ethernet radio, ControlNet, LonWorks.
- User interface: Internal – status lights, small LCD screens, keypads, jumpers, dip switches, switches. External – Browser, applications.

# ICS Data Flows

**Historian** refers to a software application that logs or “historizes” time-based process data. Historian software is used to record trends and historical information about processes for future reference.



**Historian** - captures information about performance monitoring, quality assurance, & tracking with enhanced data capture, data compression, & data presentation capabilities.



In our modern society, computerized or digital control systems have been used to reliably automate many of the industrial operations that we take for granted, from the traffic signal to the automobiles we drive.

However, the complexity of these systems and how the designers integrate them, the roles and responsibilities of the humans that interact with the systems, and the cyber security of these highly networked systems has led to a new paradigm for next generation control systems.

Resilient Control Systems consider all of these elements and how to design in cyber security protections such that the system defends itself from attack by changing its behaviors, and how to better integrate widely distributed computer control systems to prevent cascading failures that result in disruptions to critical industrial control systems (ICS) operations.

In the context of cyber-physical systems, resilient control systems are an aspect that focuses on the unique interdependencies of a control system, as compared to information technology computer systems and networks, due to its importance in operating our critical industrial operations.



Originally intended to provide a more efficient mechanism for controlling industrial operations, the development of digital control systems allowed for flexibility in integrating distributed sensors and operating logic while maintaining a centralized interface for human monitoring and interaction.

This ease of readily adding sensors and logic through software and the dependence of digital control systems upon the communications networks have precipitated the need for cybersecurity due to potential effects on confidentiality, integrity and availability of the information.

To achieve resilience in the next generation of control systems, therefore, addressing the complex control system interdependencies, including the human systems interaction and cyber security, will be a recognized challenge.



Organizational resilience considers the ability of an organization to adapt and survive in the face of threats, including the prevention or mitigation of unsafe, hazardous or compromising conditions that threaten its very existence.

Information technology resilience has been considered from a number of standpoints. Networking resilience has been considered as quality of service (QoS).

Computing has considered such issues as dependability and performance in the face of unanticipated changes. However, based upon the application of control dynamics to industrial processes, functionality and determinism are primary considerations that are not captured by the traditional objectives of information technology.



Considering the paradigm of control systems, one definition has been suggested that "Resilient control systems are those that tolerate fluctuations via their structure, design parameters, control structure and control parameters".

However, this definition is taken from the perspective of control theory application to a control system. The consideration of the malicious actor and cyber security are not directly considered, which might suggest the definition, "an effective reconstitution of control under attack from intelligent adversaries," which is proposed. However, this definition focuses only on resilience in response to a malicious actor.

To consider the cyber-physical aspects of a control system, a definition for resilience considers both benign and malicious human interaction, in addition to the complex interdependencies of the control system application.



Control systems require an interaction with the environment, namely all of the field devices that make up the ICS operation. To be reactive to this environment, control systems require an awareness of its state to make corrective changes to the ICS operational process to maintain normalcy.

With this in mind, in consideration of the discussed cyber-physical aspects of human systems integration and cyber security, as well as other definitions for resilience at a broader critical infrastructure level, the following can be deduced as a definition of a resilient control system:

"A resilient control system is one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature"



## Cyber security

In contrast to the challenges of prediction and integration of the benign human with control systems, the abilities of the malicious actor (or hacker) to undermine desired control system behavior also create a significant challenge to control system resilience.

Application of dynamic probabilistic risk analysis used in human reliability can provide some basis for the benign actor. However, the decidedly malicious intentions of an adversarial individual, organization or nation make the modeling of the human variable in both objectives and motives.

However, in defining a control system response to such intentions, the malicious actor looks forward to some level of recognized behavior to gain an advantage and provide a pathway to undermining the system. Whether performed separately in preparation for a cyber-attack, or on the system itself, these behaviors can provide opportunity for a successful attack without detection.

Therefore, in considering resilient control system architecture, atypical designs that imbed active and passively implemented randomization of attributes, would be suggested to reduce this advantage.



## Complex networks and networked control systems

While much of the current critical infrastructure is controlled by a web of interconnected control systems, either architecture termed as Distributed Control Systems (DCS) or Supervisory Control and Data Acquisition (SCADA), the application of control is moving toward a more decentralized state. In moving to a “smart grid”, the complex interconnected nature of individual facilities creates an opportunity and a challenge to ensuring that the resulting system is more resilient to threats.

The ability to operate these systems to achieve a global optimum for multiple considerations, such as overall efficiency, stability and security, will require mechanisms to holistically design complex networked control systems. Multi-agent methods suggest a mechanism to tie a global objective to distributed assets, allowing for management and coordination of assets for optimal benefit and semi-autonomous, but constrained controllers that can react rapidly to maintain resilience for rapidly changing conditions.



## Standardizing Resilience and Resilient Control System Principles

Standards and policy that define resilience nomenclature and metrics are needed to establish a value proposition for investment, which includes government, academia and industry.

The IEEE Industrial Electronics Society has taken the lead in forming a technical committee toward this end.

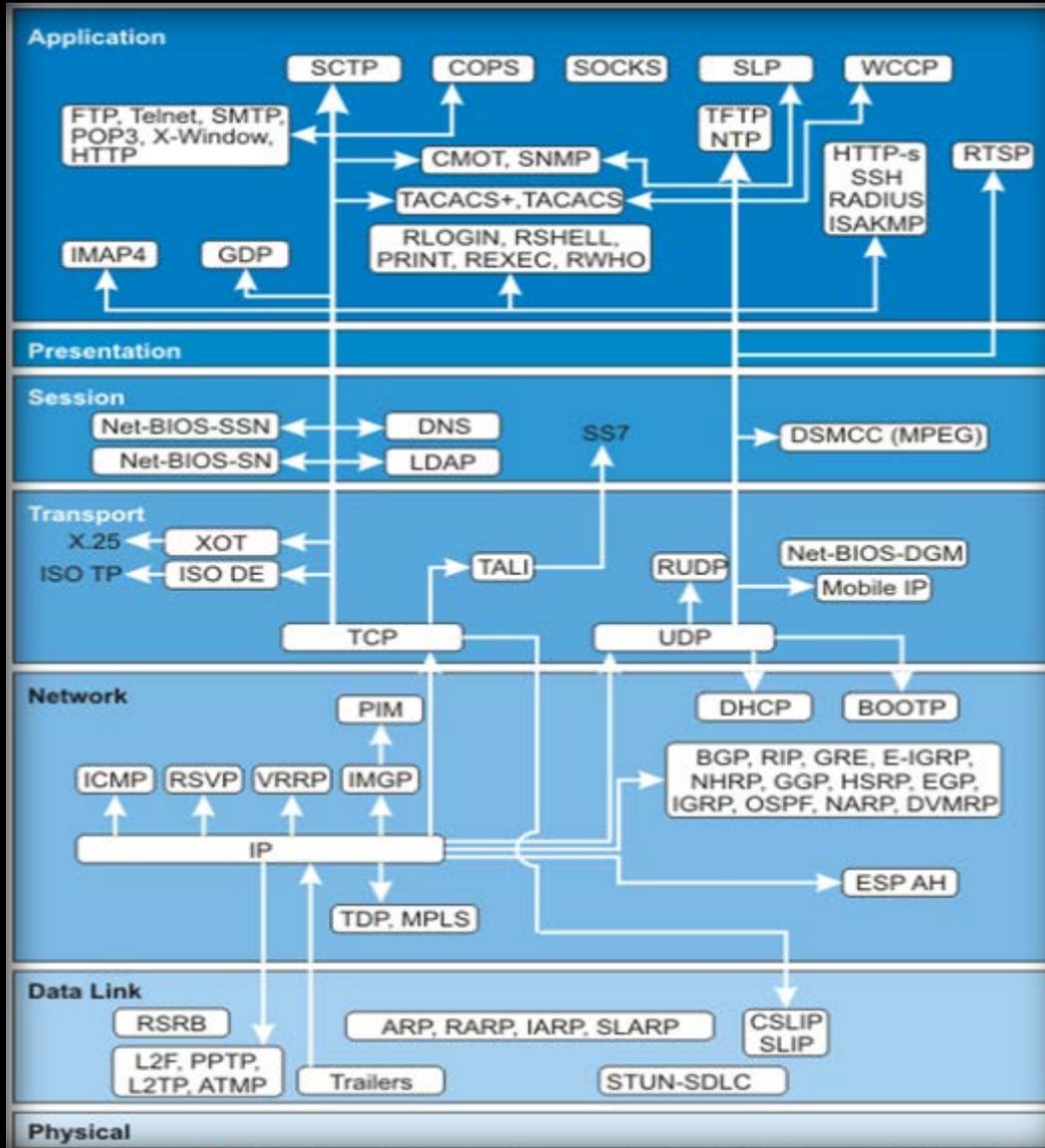
The purpose of this committee will be to establish metrics and standards associated with codifying promising technologies that promote resilience in automation.

This effort is distinct from more supply chain community focus on resilience and security, such as the efforts of ISO and NIST.



# Section 4 Highway Cyber Security Fundamentals

- **Protocols**





There are hundreds of protocols in the ICS domain.

- In order for *computers* to communicate with one another, standard methods of information transfer and processing have been devised. These are referred to as "*protocols*" and some of the more common ones such as TCP, IP, UDP, POP, SMTP, HTTP, and FTP.
- In **computing**, a **protocol** or communication **protocol** is a set of rules in which **computers** communicate with each other. The **protocol** says what part of the conversation comes at which time. It also says how to end the communication.



# Internet Control Message Protocol (ICMP)

- The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite.
- It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
- ICMP can also be used to relay query messages. It is assigned protocol number 1.
- ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and traceroute).

# Network Protocols in various formats.

- Protocol stack: [List of network protocol stacks](#)
- [WIFI/WIMAX Protocols](#)
- [Bluetooth protocol](#)
- [Fiber Channel network protocols](#)
- [Internet Protocol Suite](#) or [TCP/IP model](#) or [TCP/IP stack](#)
- [OSI protocols](#) family of information exchange standards developed jointly by the [ISO](#) and the [ITU-T](#)
- [Routing protocols](#)
- [List of IP protocol numbers](#), protocol numbers used in the Protocol field of the IPv4 header and the Next Header field of IPv6 header

# Network Protocols in various formats.

- [RTPS protocol](#), an interoperability protocol
- [SSH](#) Secure Shell
- [SMB](#) **Server Message Block**, one version of which was also known as **CIFS** (**Common Internet File System**)
- [FTP](#) File Transfer Protocol
- [SMTP](#) **Simple Mail Transfer Protocol**
- [TCP](#) **Transmission Control Protocol**
- [Telnet](#) Telephone Network
- [HTTP](#) **Hyper Text Transfer Protocol**
- [HTTPS](#) **Secure Hyper Text Transfer Protocol**

# Network Protocols in various formats.

- [POP](#) Post Office Protocol
- [HTCPCP](#) Hyper Text Coffee Pot Control Protocol
- [MTP](#) Media Transfer Protocol
- [SFTP](#) Secure File Transfer Protocol
- [SSL](#) Secure Socket Layer
- [TLS](#) Transport Layer Security
- [E6](#) Ethernet globalization protocols
- [NTP](#) Network time protocol
- [PPP](#) Point to Point Protocol
- [NNTP](#) Network News Transfer Protocol
- [QOTD](#) Quote Of The Day
- [IMAP](#) Internet Message Access Protocol
- [Bitcoin Protocol](#) to transfer value on the web

*Secure Sockets Layer (SSL)* is a computer networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.



- The **Transmission Control Protocol (TCP)** is a core protocol of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). **Therefore, the entire suite is commonly referred to as TCP/IP.**
- TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network. TCP is the protocol that major Internet applications such as the World Wide Web, email, remote administration and file transfer rely on.
  - Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability.
- The Transmission Control Protocol provides a communication service at an intermediate level between an application program and the Internet Protocol. It provides host-to-host connectivity at the Transport Layer of the Internet model. An application does not need to know the particular mechanisms for sending data via a link to another host, such as the required packet fragmentation on the transmission medium. At the transport layer, the protocol handles all handshaking and transmission details and presents an abstraction of the network connection to the application.





- At the lower levels of the protocol stack, due to network congestion, traffic load balancing, or other unpredictable network behavior, IP packets may be lost, duplicated, or delivered out of order. TCP detects these problems, requests retransmission of lost data, rearranges out-of-order data, and even helps minimize network congestion to reduce the occurrence of the other problems. If the data still remains undelivered, its source is notified of this failure. Once the TCP receiver has reassembled the sequence of octets originally transmitted, it passes them to the receiving application. Thus, TCP abstracts the application's communication from the underlying networking details. TCP is utilized extensively by many popular applications carried on the Internet.
- TCP is optimized for accurate delivery rather than timely delivery, and therefore, TCP sometimes incurs relatively long delays (on the order of seconds) while waiting for out-of-order messages or retransmissions of lost messages. It is not particularly suitable for real-time applications such as Voice over IP. For such applications, protocols like the Real-time Transport Protocol (RTP) running over the User Datagram Protocol (UDP) are usually recommended instead.
- TCP is a reliable stream delivery service that guarantees that all bytes received will be identical with bytes sent and in the correct order.



# HTTP & HTTPS (Secure)

- The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems.
- HTTP is the foundation of data communication for the World Wide Web.



HTTP functions as a request–response protocol in the client–server computing model. A web browser, for example, may be the *client* and an application running on a computer hosting a web site may be the *server*. The client submits an HTTP *request* message to the server. The server, which provides *resources* such as HTML files and other content, or performs other functions on behalf of the client, returns a *response* message to the client. The response contains completion status information about the request and may also contain requested content in its message body.



# HTTPS (Secure)

HTTPS (also called HTTP over TLS (Transport Layer Security), HTTP over SSL, and HTTP Secure) is a protocol for secure communication over a computer network which is widely used on the Internet.



HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security or its predecessor, Secure Sockets Layer. The main motivation for HTTPS is authentication of the visited website and protection of the privacy and integrity of the exchanged data.

In its popular deployment on the internet, HTTPS provides authentication of the website and associated web server with which one is communicating, which protects against man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication. In practice, this provides a reasonable guarantee that one is communicating with precisely the website that one intended to communicate with (as opposed to an impostor), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.



- HTTPS URLs begin with "https://" and use port 443 by default, whereas HTTP URLs begin with "http://" and use port 80 by default.
- HTTP is not encrypted and is vulnerable to man-in-the-middle and eavesdropping attacks, which can let attackers gain access to website accounts and sensitive information, and modify webpages to inject malware or advertisements. HTTPS is designed to withstand such attacks and is considered secure against them (with the exception of older, deprecated versions of SSL).

## Network layers:

- HTTP operates at the highest layer of the TCP/IP model, the Application layer; as does the TLS security protocol (operating as a lower sublayer of the same layer), which encrypts an HTTP message prior to transmission and decrypts a message upon arrival. Strictly speaking, HTTPS is not a separate protocol, but refers to use of ordinary HTTP over an encrypted SSL/TLS connection.
- Everything in the HTTPS message is encrypted, including the headers, and the request/response load.



# Why was port 80 chosen as the default HTTP port and 443 as the default HTTPS port?

In a Web server or Hypertext Transfer Protocol (HTTP) daemon, port 80 is the port that the server "listens to" or expects to receive from a Web client, assuming that the default was taken when the server was configured or set up. A port can be specified in the range from 0-65536 on the NCSA (National Center for Supercomputing Applications) server. However, the server administrator configures the server so that only one port number can be recognized. By default, the port number for a Web server is 80.

- The Internet Assigned Numbers Authority (IANA) is a department of ICANN, a nonprofit private American corporation that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers. As far as my research indicates that IANA assigned port 80 for HTTP and port 443 as the default port for HTTPS.
- (ICANN (pronounced *EYE-kan*) (The Internet Corporation for Assigned Names and Numbers) is a nonprofit organization that is responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the Internet - thereby ensuring the network's stable and secure operation.  
<https://www.icann.org/>



# Processing Packets

If you think of ports as something real; its just a 16-bit unsigned number (0-65535) that's a label in the header of an IP packet. This helps with application-level multiplexing. When an incoming packet arrives at a network card, the OS gets a notification. It checks what port the incoming packet was directed to, and then forwards the packet to only the right application. If you are running your webserver (Nginx (pronounced "engine x") is a web server) to listen on port 80, only Nginx gets packets sent to port 80.

When a client (IP: 100.200.100.200) makes an HTTP request to server (55.55.55.55), they make that request to destination port 80 on the server (55.55.55.55:80), but the source port is randomly chosen by the OS for the web browser (something like 45490). The HTTP response from the web server then comes from (55.55.55.55:80), but sent to the destination (your IP) (100.200.100.200:45490). Your computer's OS knows that incoming packets on port 45490 (from 55.55.55.55:80) need to be given to the web browser that made the request. As each unique connection to a web site from the client gets a unique random port, so you can have multiple web browsers connecting to the same web site and when a page is reloaded in one browser the other windows aren't affected.

Each IP packet has both the source and destination IP addresses and port available to it in the header. The OS and application (web browser or web server) can use both to figure out the appropriate action on how to process the packet.



The **User Datagram Protocol (UDP)** is one of the core members of the [Internet protocol suite](#)

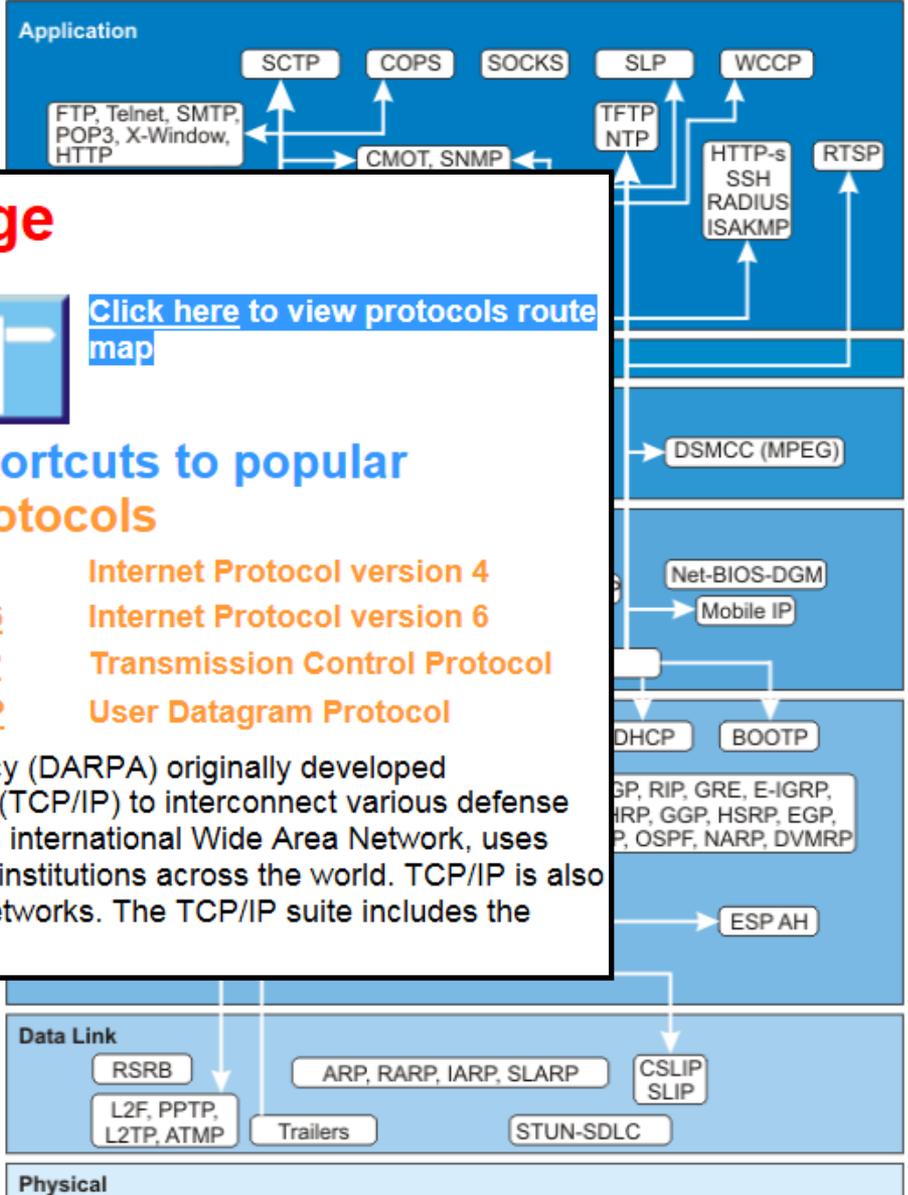
- UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network protocol. There is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.
- With UDP, computer applications can send messages, in this case referred to as *datagrams*, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. UDP is suitable for purposes where error checking and correction is either not necessary or is performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system. If error correction facilities are needed at the network interface level, an application may use the Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP) which are designed for this purpose.

Protocol	Family	Family	Protocol
(ISO8073)	<a href="#">ISO</a>	<a href="#">AppleTalk</a>	AppleArp, AppleTalk, EtherTalk, AARP, ADSP, AEP, AFP, ASP, ATP, DDP, NBP, PAP, RTMP, ZIP
A1	<a href="#">CDMA2000</a>	<a href="#">ATM</a>	ATM Cell (AAL0-AAL5), ATM Cell NNI, ATM Cell UNI, ATM SAR, IP Over ATM, AAL2
A10	<a href="#">CDMA2000</a>	<a href="#">ATM Signaling &amp; Routing</a>	ITU Q2931, ITU Q2971, B-ICI, B-ISUP, IISP, PNNI Routing, PNNI Signaling, Q.2140, Q.SAAL, SPANS, UNI 3.x, UNI 4.0, ViVID MPOA, SPANS
A11	<a href="#">CDMA2000</a>	<a href="#">Audio/Visual Over ATM</a>	ATM Circuit Emulation, DSMCC, DVB, MPEG-2
A12	<a href="#">CDMA2000</a>	<a href="#">Banyan</a>	Banyan, IPC, NetRPC, RTP, SPP, StreetTalk, VARP, VIP
A13	<a href="#">CDMA2000</a>	<a href="#">Bridge/Router</a>	BPDU, CDP, Cisco ISL, Cisco HDLC (cHDLC), Cisco SRB, DISL, DRiP, MAPOS, NSP, Proteon, RND, SSP, VTP, Wellfleet
A14	<a href="#">CDMA2000</a>	<a href="#">CDMA2000</a>	A1, A3, A7, A8, A9, A10, A11, A12, A13, A14, A15
A15	<a href="#">CDMA2000</a>	<a href="#">CDPD</a>	MDLP, MNRP, SNDCP

# Protocols

The TCP/IP suite is illustrated here in relation to the OSI model: Click the protocols on the map to see more details

Application Layer	
COPS	Common Open Policy Service
FANP	Flow Attribute Notification Protocol
Finger	User Information Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTP/2	Hypertext Transfer Protocol Version 2



## TCP / IP Reference Page

Protocols according to layers [Data Link Layer](#) [Network Layer](#) [Transport Layer](#) [Session Layer](#) [Application Layer](#) [Routing](#) [Tunneling](#) [Security](#)



[Click here to view protocols route map](#)

### Shortcuts to popular Protocols

- [IP](#) Internet Protocol version 4
- [IPv6](#) Internet Protocol version 6
- [TCP](#) Transmission Control Protocol
- [UDP](#) User Datagram Protocol

The Defense Advance Research Projects Agency (DARPA) originally developed Transmission Control Protocol/Internet Protocol (TCP/IP) to interconnect various defense department computer networks. The Internet, an international Wide Area Network, uses TCP/IP to connect government and educational institutions across the world. TCP/IP is also in widespread use on commercial and private networks. The TCP/IP suite includes the following protocols

Data Link Layer	
ARP/RARP	Ac...
DCAP	Da...
Network Layer	
DHCP	Dy...
DVMRP	Di...
ICMP/ICMPv6	Int...
IGMP	Int...
IP	Int...
IPv6	Int...
MARS	Mu...
PIM	Pr...
RIP2	Ro...
RIPng for IPv6	Ro...
RSVP	Re...
VRRP	Vir...
Transport Layer	
ISTP	Mc...
Mobile IP	Mc...
RUDP	Reliable UD...
TALI	Transpor...
TCP	Transmissi...
UDP	User Datag...
Van Jacobson	compress...
XOT	X.25 over T...

NHRP	Next Hop Resolution Protocol
OSPF	Open Shortest Path First
TRIP	Telephony Routing over IP
Tunneling	
ATMP	Ascend Tunnel Management Protocol
L2F	The Layer 2 Forwarding Protocol
L2TP	Layer 2 Tunneling Protocol
PPTP	Point to Point Tunneling Protocol
Security	
AH	Authentication Header
ESP	Encapsulating Security Payload
TLS	Transport Layer Security Protocol

# "Protocol Analyzer"

- is a tool (hardware or software) used to capture and analyze signals and data traffic over a communication channel.
- Such a channel varies from a local computer bus to a satellite link, that provides a means of communication using a standard communication protocol (networked or point-to-point).
- Each type of communication protocol has a different tool to collect and analyze signals and data.

Specific types of protocol analyzers include:

- **telecom network protocol analyzer**
- network **packet analyzer**
- **bus analyzer**
- IP **load tester**



## Open Systems Interconnection (OSI)

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols	DOD4 Model
<b>Application (7)</b> Serves as the window for users and application processes to access the network services.	<b>End User layer</b> Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	<b>User Applications</b> SMTP	Process
<b>Presentation (6)</b> Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	<b>Syntax layer</b> encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • <b>Character Set Translation</b>	JPEG/ASCII EBDIC/TIFF/GIF PICT	
<b>Session (5)</b> Allows session establishment between processes running on different stations.	<b>Synch &amp; send to ports</b> (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	<b>Logical Ports</b> RPC/SQL/NFS NetBIOS names	
<b>Transport (4)</b> Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	<b>TCP</b> Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	<b>PACKET FILTERING</b>  TCP/SPX/UDP  <b>Routers</b>  IP/IPX/ICMP	Host to Host
<b>Network (3)</b> Controls the operations of the subnet, deciding which physical path the data takes.	<b>Packets</b> ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Can be used on all layers
<b>Data Link (2)</b> Provides error-free transfer of data frames from one node to another over the Physical layer.	<b>Frames</b> ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	<b>Switch Bridge WAP</b> PPP/SLIP	Network
<b>Physical (1)</b> Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	<b>Physical structure</b> Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	<b>Hub</b> Land Based Layers	



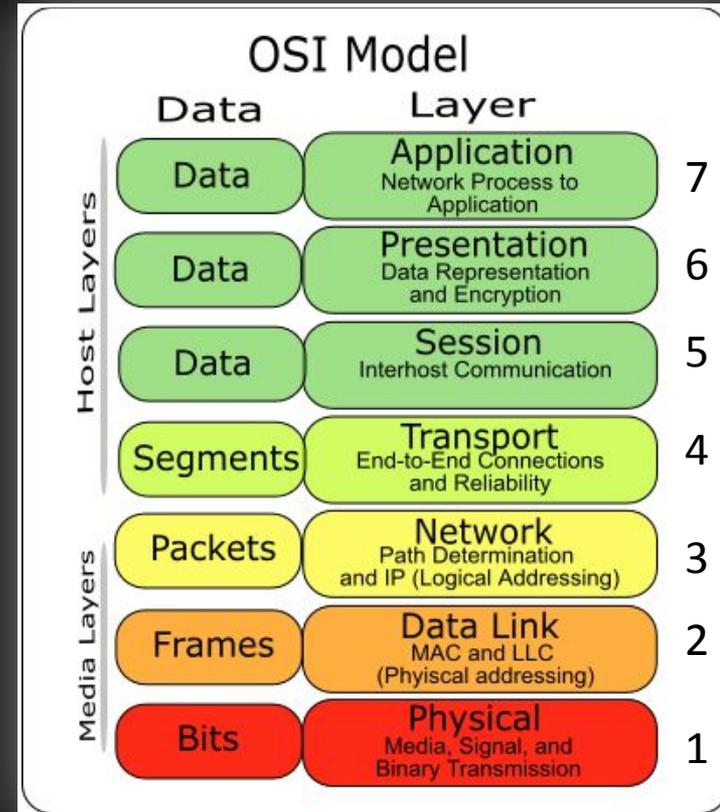
# Why Understanding the OSI Reference Model is Important... it's time well spent.

- A lot of networking books and other resources gloss over the OSI Reference Model, including only passing mention of it, or relegating it to an appendix.
- The usual stated reason for this is that the OSI model is “too theoretical” and “doesn't apply to modern networking protocols. We believe that this is a misguided notion. While it is certainly true the OSI model is primarily theoretical, and that networking protocols aren't always designed to fit strictly within the confines of its layers, it's *not* true that the OSI model has little applicability to the “real world”. In fact, it is difficult to read about networking technology today without seeing references to the OSI model and its layers, because the model's structure helps to frame discussions of protocols and contrast various technologies. As just a few examples: the OSI Reference Model provides the basis for understanding how different technologies have some important similarities; it explains how a PC can communicate using any of several different sets of protocols, even simultaneously; it is an important part of understanding the differences between interconnection devices; and it also explains how many WAN technologies interoperate.
- Far from being obsolete, the OSI model layers are now showing up more than ever in discussions of technology. In fact, some protocols are even *named* specifically in terms of their place in the OSI Reference Model! For an example, consider the Layer Two Tunneling Protocol. Also, switches are now commonly categorized as being layer 2, layer 3 or even higher-layer switches.
- In theoretical discussions, the OSI Reference Model helps you understand how networks and network protocols function. In the “real world”, it also helps you figure out which protocols and devices can interact with each other. So, we encourage you to read on.



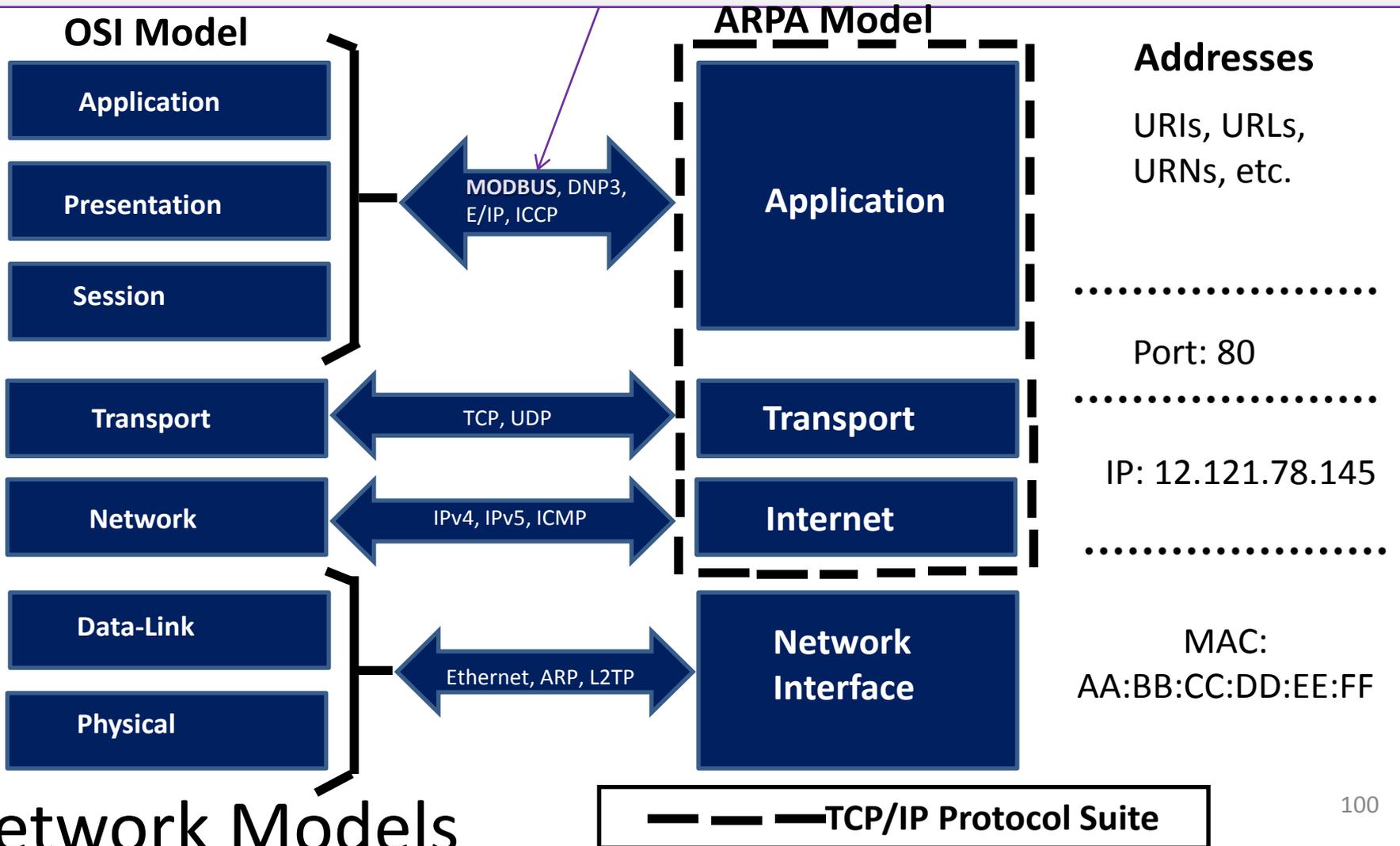
## Open Systems Interconnection (OSI)

Model conceptually divides computer network architecture into seven layers in a logical progression. The lower layers deal with electrical signals, chunks of binary data, and routing of these data across networks. Higher levels cover network requests and responses, representation of data, and network protocols as seen from a user's point of view.



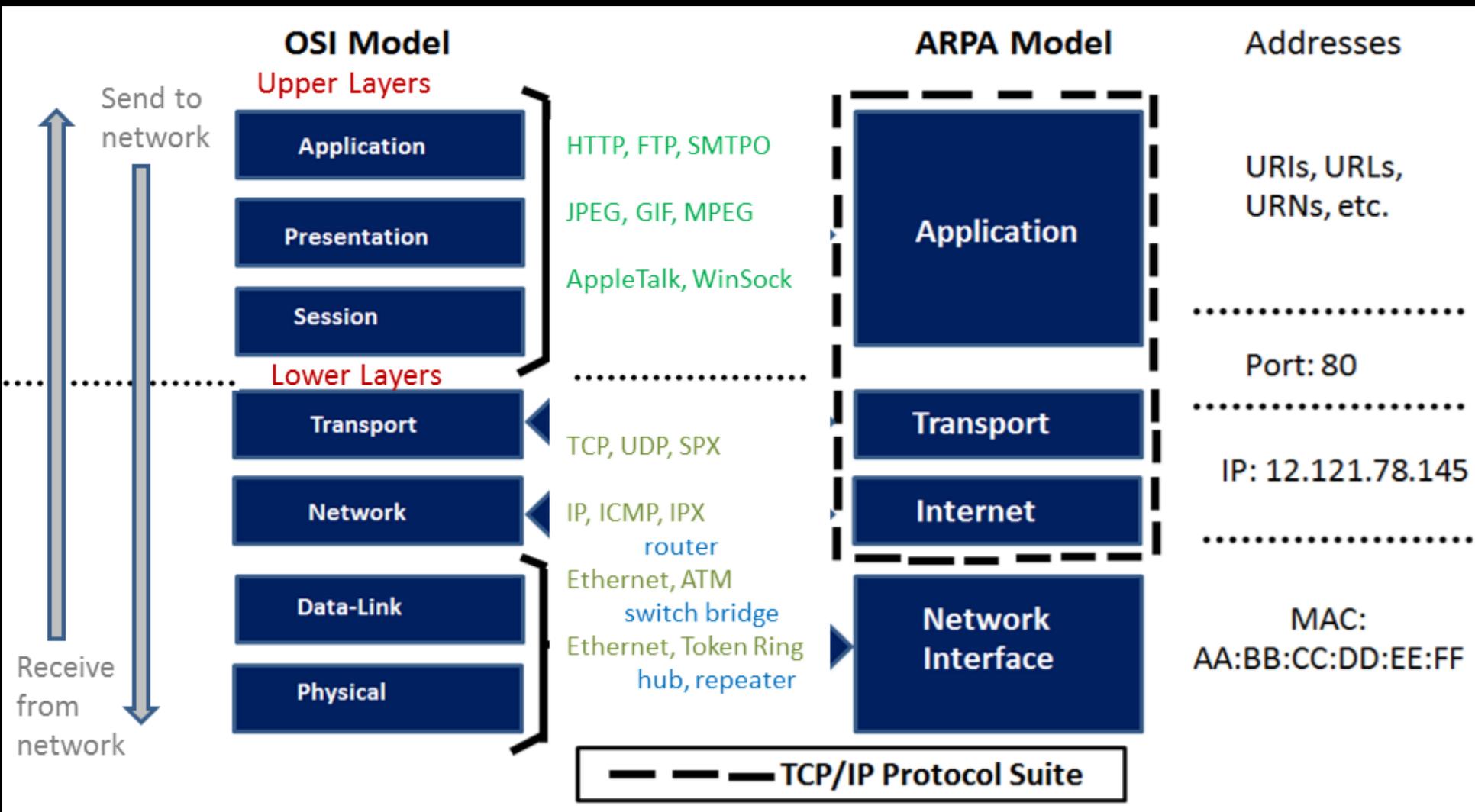
- **Advanced Research Projects Agency (ARPA) Network** was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet. ARPANET was initially funded by the US DoD.

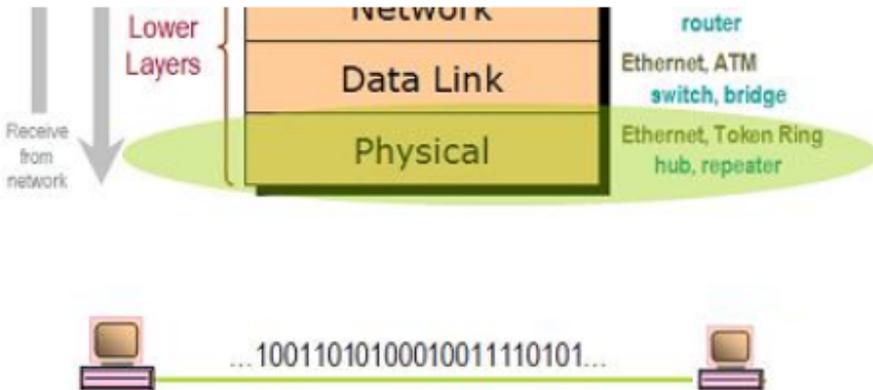
The **ModBus** protocol was initially created for use over serial connections and was adapted for use over TCP/IP. It is one of the oldest and more popular ICS protocol in use today. Modbus is used for both command and control and device level communications. A client issues a single packet request to server which acts on the request and returns a single-packet response that indicates success or failure.





# OSI & ARPA Models



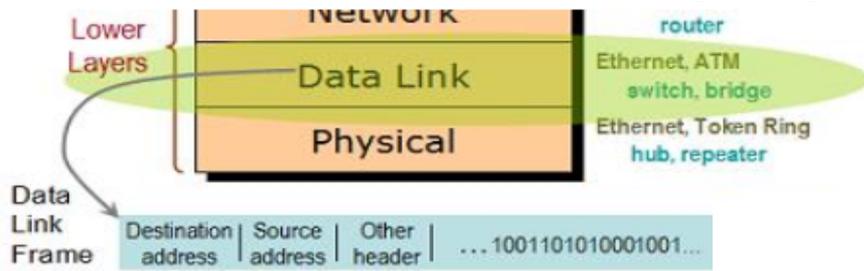


## 1. Physical Layer

At Layer 1, the Physical layer of the OSI model is responsible for ultimate transmission of digital data [bits](#) from the Physical layer of the sending (source) device over network communications

media to the Physical layer of the receiving (destination) device. Examples of Layer 1 technologies include [Ethernet cables](#) and [Token Ring networks](#). Additionally, [hubs](#) and other [repeaters](#) are standard network devices that function at the Physical layer, as are cable connectors.

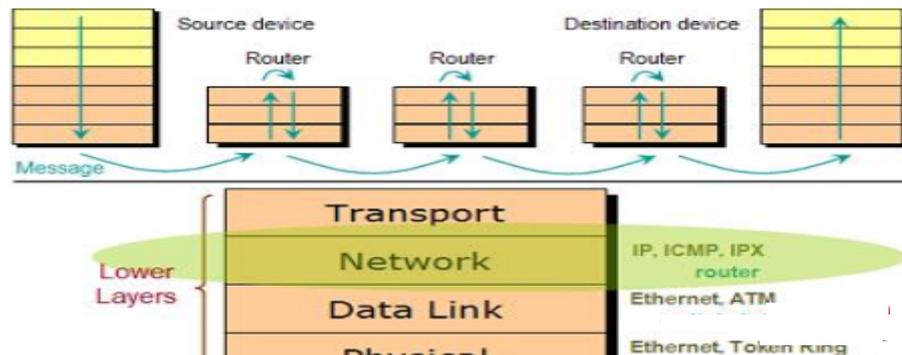
At the Physical layer, data are transmitted using the type of signaling supported by the physical medium: electric voltages, radio frequencies, or pulses of infrared or ordinary light.



## 2. Data Link Layer

When obtaining data from the Physical layer, the Data Link layer checks for physical transmission errors and packages bits into data *frames*.

The Data Link layer also manages physical addressing schemes such as [MAC](#) addresses for Ethernet networks, controlling access of any various network devices to the physical medium. Because the Data Link layer is the single most complex layer in the OSI model, it is often divided into two parts, the *Media Access Control* sublayer and the *Logical Link Control* sublayer.

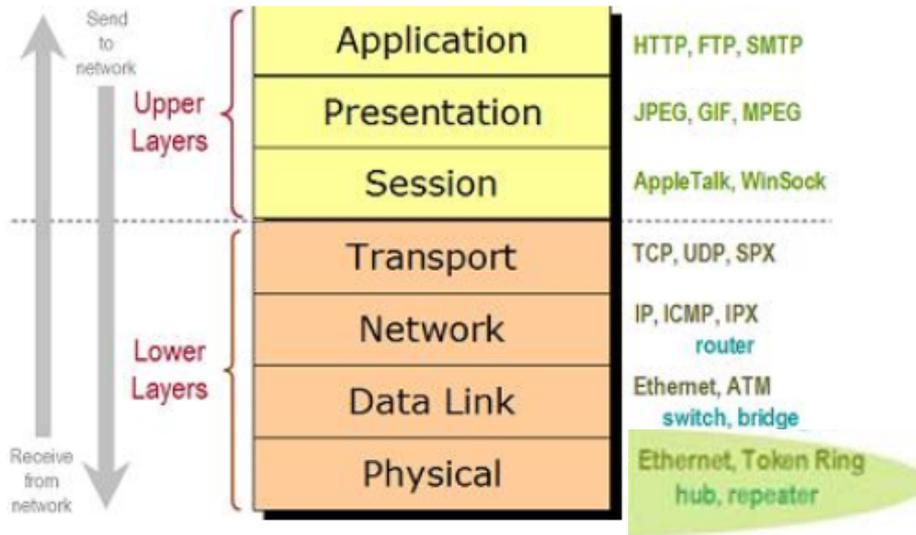


## 3. Network Layer

The Network layer adds the concept of routing above the Data Link layer. When data arrives at the Network layer, the source and destination addresses contained inside each frame are examined to determine if the data has reached its final destination. If the data has reached

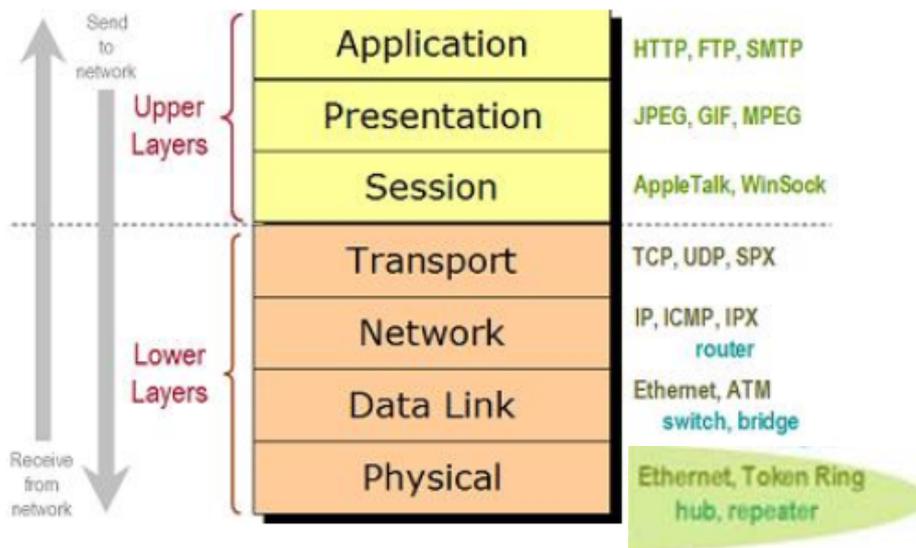
the final destination, this Layer 3 formats the data into packets delivered up to the Transport layer. Otherwise, the Network layer updates the destination address and pushes the frame back down to the lower layers.

To support routing, the Network layer maintains logical addresses such as [IP addresses](#) for devices on the network. The Network layer also manages the mapping between these logical addresses and physical addresses. In IP networking, this mapping is accomplished through the [Address Resolution Protocol \(ARP\)](#).



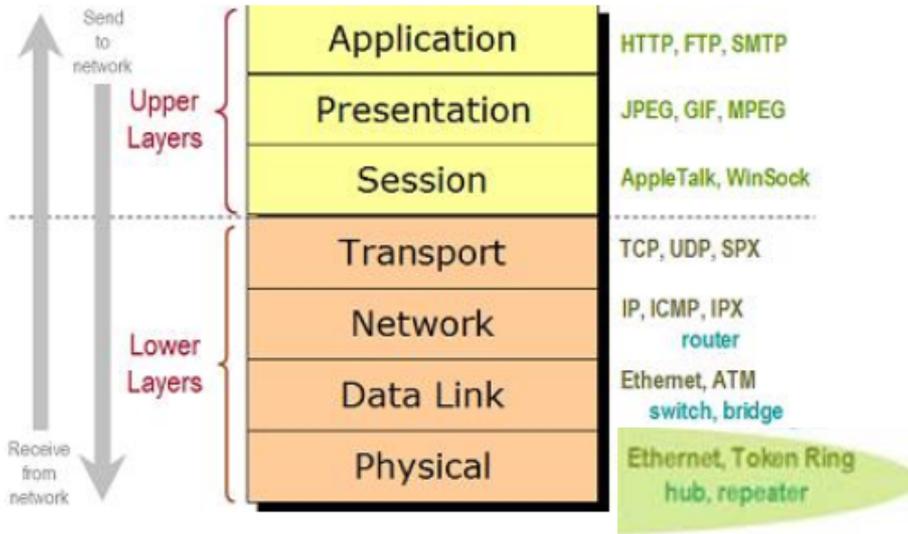
## 4. Transport Layer

The Transport Layer delivers data across network connections. [TCP](#) is the most common example of a Transport Layer 4 [network protocol](#). Different transport protocols may support a range of optional capabilities including error recovery, flow control, and support for re-transmission.



## 5. Session Layer

The Session Layer manages the sequence and flow of events that initiate and tear down network connections. At Layer 5, it is built to support multiple types of connections that can be created dynamically and run over individual networks.



## 6. Presentation Layer

The Presentation layer is the simplest in function of any piece of the OSI model. At Layer 6, it handles syntax processing of message data such as format conversions and encryption / decryption needed to support the Application layer above it.

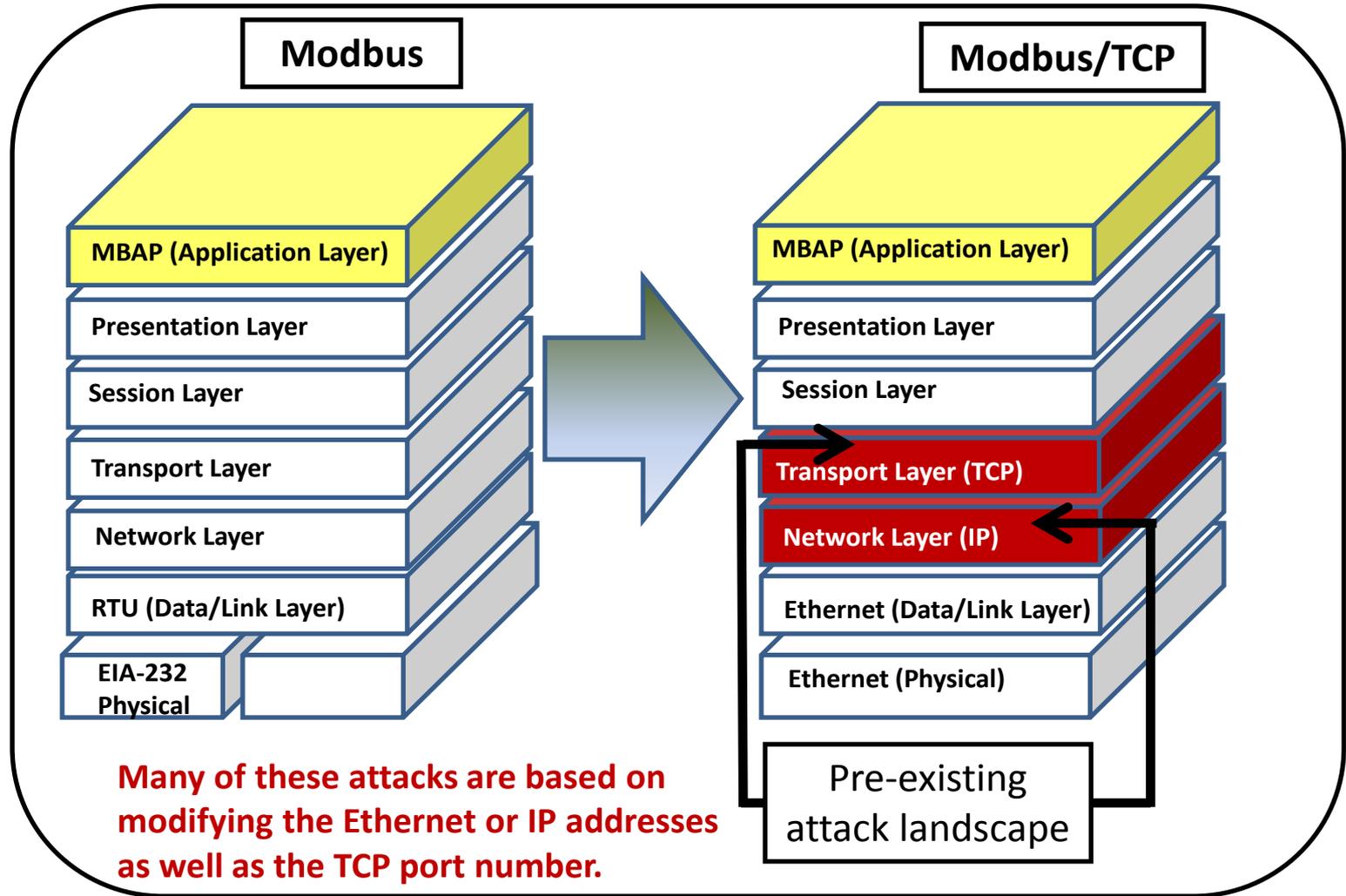
## 7. Application Layer

The Application layer supplies network services to end-user applications. Network services are typically protocols that work with user's data. For

example, in a Web browser application, the Application layer protocol [HTTP](#) packages the data needed to send and receive Web page content. This Layer 7 provides data to (and obtains data from) the Presentation layer.



# Protocol Vulnerabilities:

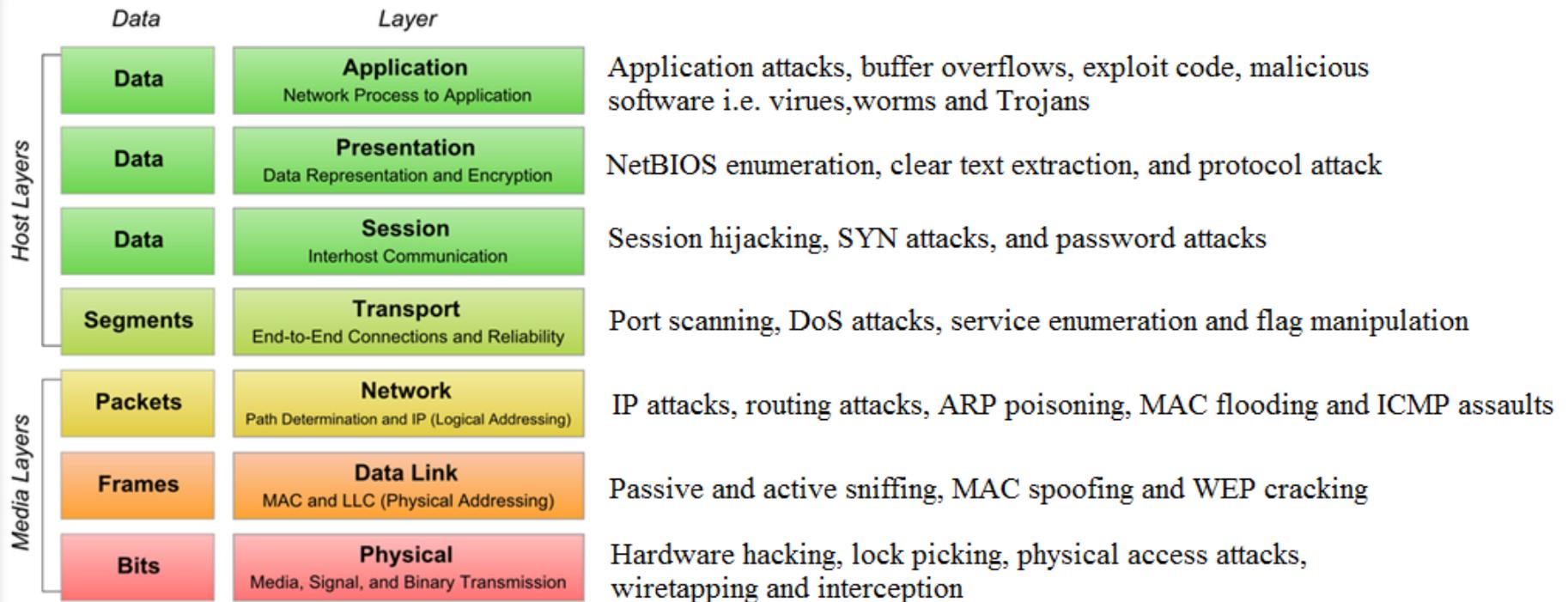


**TCP:**  
Transmission  
Control  
Protocol

<http://packetlife.net/library/cheat-sheets/>



# Common Attacks





- Network Packets
- Network Components
- Kernel
- Shell
- PCAPS
- Packet Traversal
- ARP
- MAC
- EUI



# Network Packets

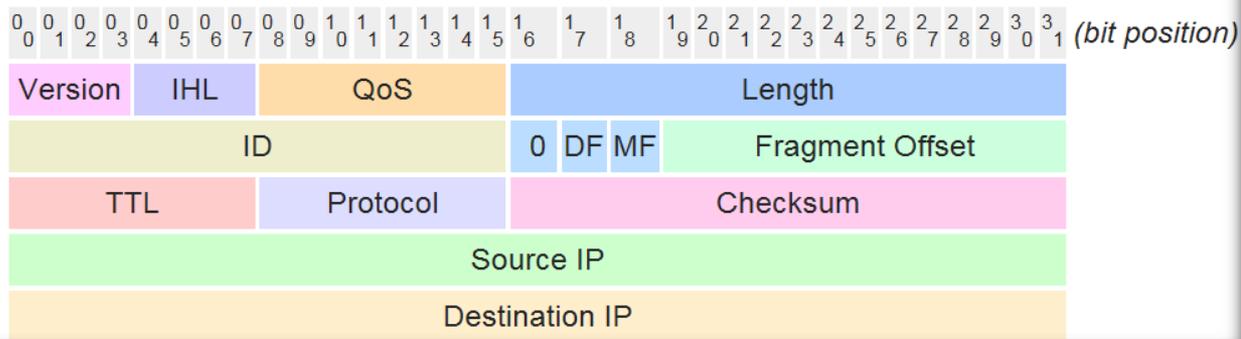
A **network Packet** is a formatted unit of data carried by a packet-switched network. Computer communications links that do not support packets, such as traditional point-to-point telecommunications links, simply transmit data as a bit stream. When data is formatted into packets, the bandwidth of the communication medium can be better shared among users than if the network were circuit switched.

A packet consists of control information and user data, which is also known as the payload. Control information provides data for delivering the payload, for example: source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers.

In the seven-layer OSI model of computer networking, *packet* strictly refers to a data unit at layer 3, the Network Layer. The correct term for a data unit at Layer 2, the Data Link Layer, is a *frame*, and at Layer 4, the Transport Layer, the correct term is a *segment* or *datagram*.

## Example: IP packets

IP packets are composed of a header and payload. The IPv4 packet header consists of:



For the case of TCP/IP communication over Ethernet, a TCP segment is carried in one or more IP packets, which are each carried in one or more Ethernet frames.



PCAPS - the Packet Capture library provides a high level interface to packet capture systems. All packets on the network, even those destined for other hosts, are accessible through this mechanism.

In the field of computer network administration, pcap (packet capture) consists of an application programming interface (API) for capturing network traffic. Unix-like systems implement pcap in the libpcap library; Windows uses a port of libpcap known as WinPcap.

Monitoring software may use libpcap and/or WinPcap to capture packets travelling over a network and, in newer versions, to transmit packets on a network at the link layer, as well as to get a list of network interfaces for possible use with libpcap or WinPcap.



- The pcap API is written in C, so other languages such as Java, .NET languages, and scripting languages generally use a wrapper; no such wrappers are provided by libpcap or WinPcap itself.
- C++ programs may link directly to the C API or use an object-oriented wrapper.
- Programs that use libpcap/WinPcap (short list):
  - ngrep, aka "network grep", isolate strings in packets, show packet data in human-friendly output.
  - Wireshark a graphical packet-capture and protocol-analysis tool.
  - Snort, a network-intrusion-detection system.
  - Nmap, a port-scanning and fingerprinting network utility.



The first 6 characters of the MAC address are the OUI (Organizationally Unique Identifier) of the network card (hex – base 16).

List of vendors and associated OUIs can be found at:  
<http://standards-oui.ieee.org/oui/oui.txt>

OUI/MA-L company_id		Organization Organization Address
E0-43-DB E043DB	(hex) (base 16)	Shenzhen ViewAt Technology Co.,Ltd. Shenzhen ViewAt Technology Co.,Ltd. 9A, Microprofit, 6th Geexin South Road shenzhen guangdong 518057 CN
24-05-F5 2405F5	(hex) (base 16)	Integrated Device Technology (Malaysia) Integrated Device Technology (Malaysia) Phase 3, Bayan Lepas FIZ Bayan Lepas Penang 11900 MY
2C-30-33 2C3033	(hex) (base 16)	NETGEAR NETGEAR 350 East Plumeria Drive San Jose null 95134 US
84-7E-40 847E40	(hex) (base 16)	Texas Instruments Texas Instruments 12500 TI Boulevard, MS 8723 Dallas TX 75243 US
78-C5-E5 78C5E5	(hex) (base 16)	Texas Instruments Texas Instruments 12500 TI Boulevard, MS 8723 Dallas TX 75243 US

Network Interface Card (NIC) – OSI Layer 1 & 2 device

- OSI Unique Layer 2 address (MAC); Promiscuous-passes all traffic to the kernel

Switched (Switch) – typically OSI Layer 2

- Packets delivered to the intended port; Reduced or no collision domain

Non-Switched (Hub) – OSI layer 1

- Packets are delivered to every port; Shared collision domain

Router – typically OSI Layer 3

- Directs traffic by comparing the destination address to entries and passes it to the next hop.



Nmap which stands for “Network Mapper” <https://nmap.org/>

Nmap is a free and open source ([license](#)) utility for network discovery and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

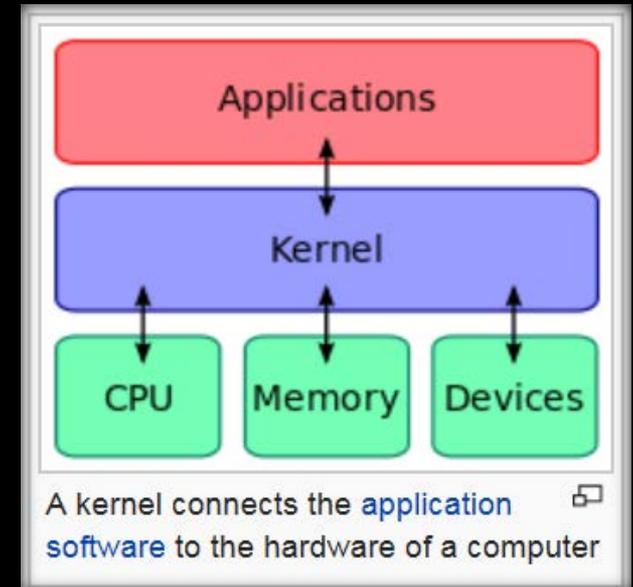
(Nmap is free open source utility [www.insecure.org](http://www.insecure.org)) network discovery tool that can be used for identifying the systems currently connected to your network... network mapping and security auditing. Identifies ports open on a host

It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer ([Zenmap](#)), a flexible data transfer, redirection, and debugging tool ([Ncat](#)), a utility for comparing scan results ([Ndiff](#)), and a packet generation and response analysis tool ([Nping](#)).



# Kernel (Operating System)

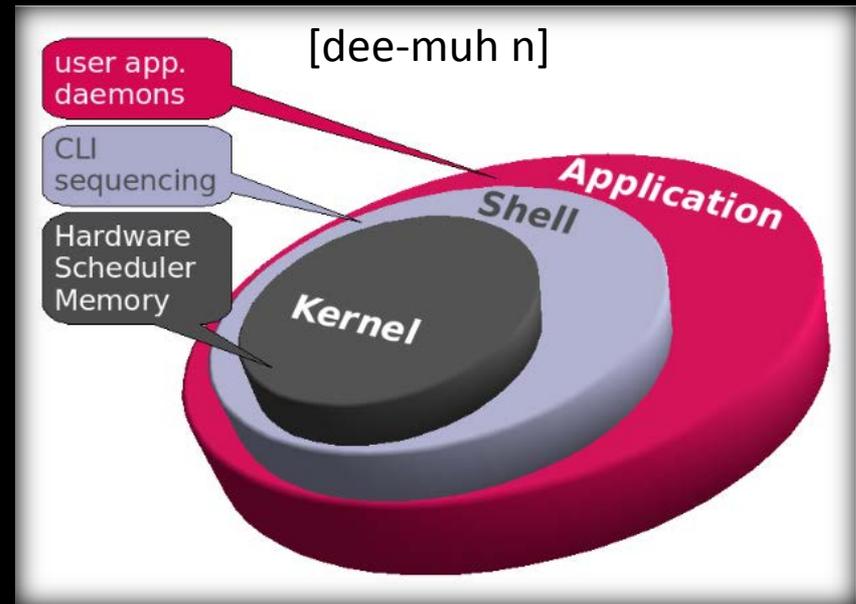
- The kernel is a computer program that constitutes the central core of a computer's operating system. It has complete control over everything that occurs in the system. As such, it is the first program loaded on startup, and then manages the remainder of the startup, as well as input/output requests from software, translating them into data processing instructions for the central processing unit. It is also responsible for managing memory, and for managing and communicating with computing peripherals.
- A kernel connects the application software to the hardware of a computer
- The critical code of the kernel is usually loaded into a *protected area* of memory, which prevents it from being overwritten by other, less frequently used parts of the operating system or by applications. This separation prevents user data and kernel data from interfering with each other and thereby diminishing performance or causing the system to become unstable (and possibly crashing).





# Kernel/Shell/Applications

Shell is a user interface for access to an operating system's services. In general, operating system shells use either a command-line interface (CLI) or graphical user interface (GUI), depending on a computer's role and particular operation.



a **daemon** is a computer program that runs as a background process, rather than being under the direct control of an interactive user. Traditionally, the process names of a daemon end with the letter *d*, for clarification that the process is, in fact, a daemon, and for differentiation between a daemon and a normal computer program. For example, syslogd is the daemon that implements the system logging facility, and sshd is a daemon that services incoming SSH connections.

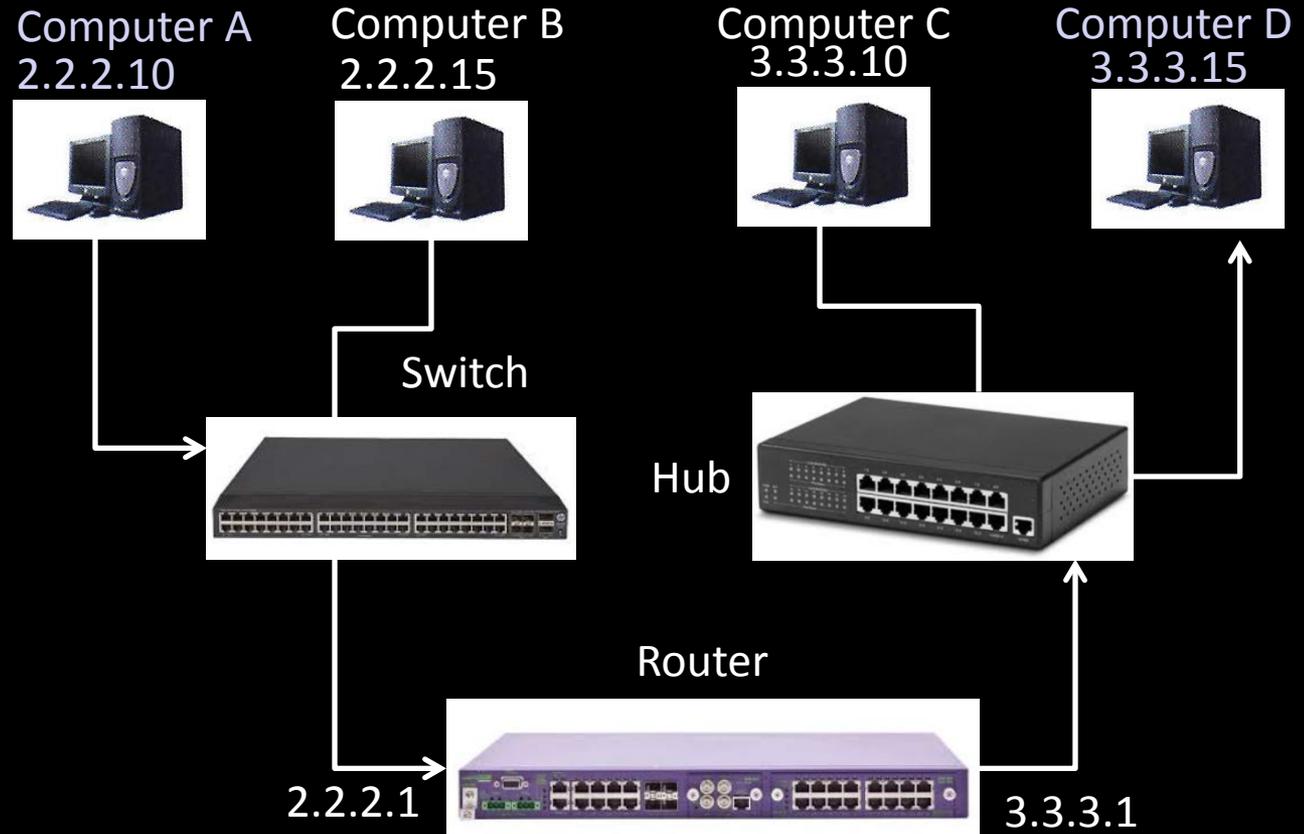
Systems often start daemons at boot time and serve the function of responding to network requests, hardware activity, or other programs by performing some task. Daemons can also configure hardware (like udevd on some Linux systems), run scheduled tasks (like cron), and perform a variety of other tasks.



# Basic Packet Traversal

**Basic Packet Traversal** - ways a packet can traverse several networks to reach a specified destination.

**Hops** – the various routes traversed by a packet to reach the designated destination



## Network Address Translation (NAT)

- Public address assigned to computer or group of computers inside a private network
- Limits number of IP address; it's economical and increases security



## *Address Resolution Protocol (ARP)*

### What is ARP?

- used to find the media access control (MAC) address of a network neighbor for a given Ipv4 address.
- a tool to view ARP table
- Used to forward IP datagrams to local routers

### Why look at the ARP table?

- List all the hosts with which the host has recently communicated.

```
C:\>arp -a

Interface: 192.168.90.128 --- 0x10003
  Internet Address      Physical Address      Type
  192.168.90.1         00-50-56-c0-00-08    dynamic
  192.168.90.2         00-50-56-fd-08-00    dynamic
  192.168.90.254      00-50-56-ff-22-17    dynamic
```

- Note: the IP address & MAC address for each host is displayed.

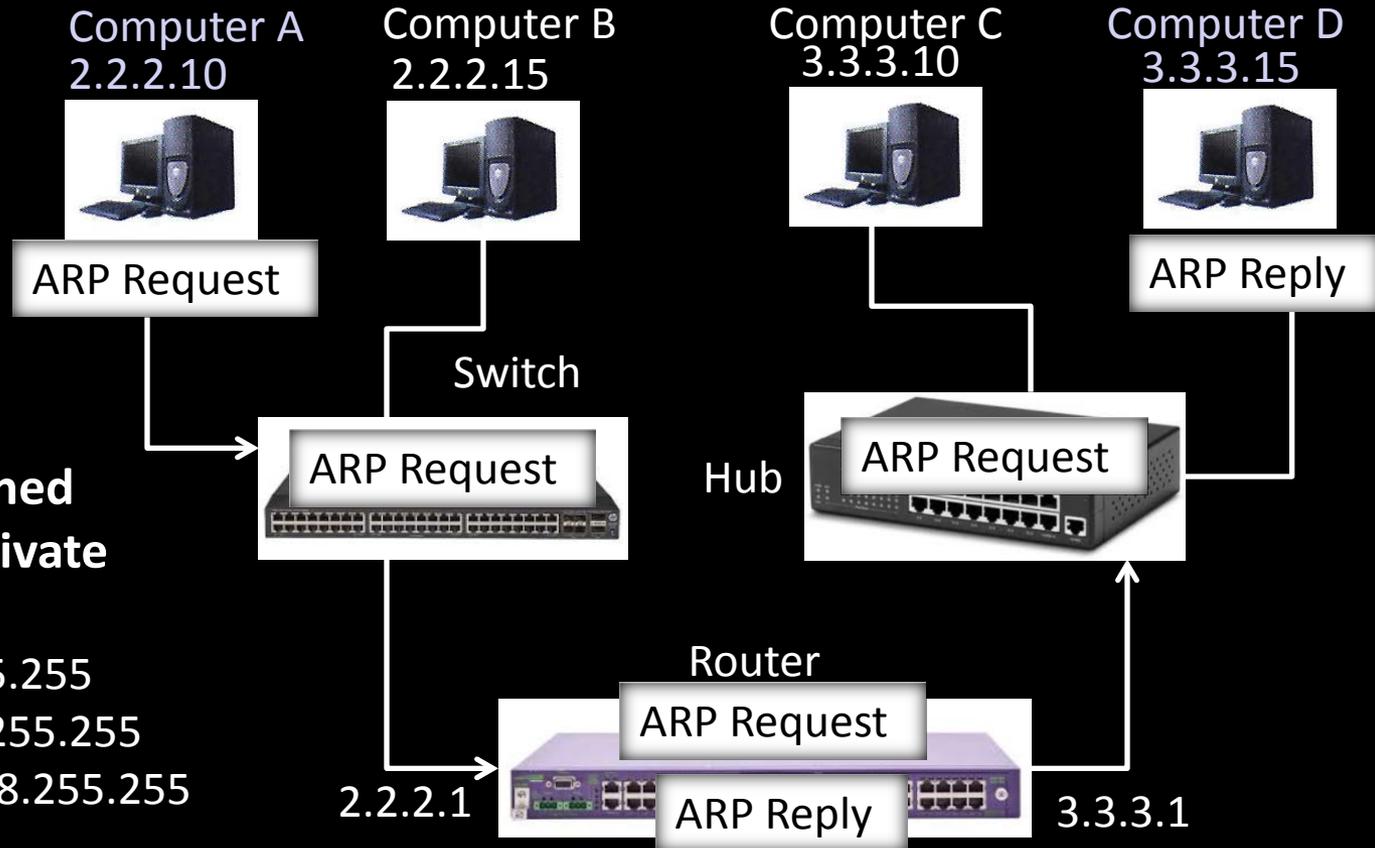


# Address Resolution Protocol (ARP)

**ARP** – protocol for determining a network host's hardware address (MAC) when only its IP address is known

**(IANA) Internet Assigned Numbers Authority private addresses:**

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255



## Request For Comments (RFC)

The Internet is governed by a set of documents referred to as RFC – a publication of Internet Engineering Task Force (IETF) and the Internet Society, the principal technical development and standards-setting bodies for the Internet.

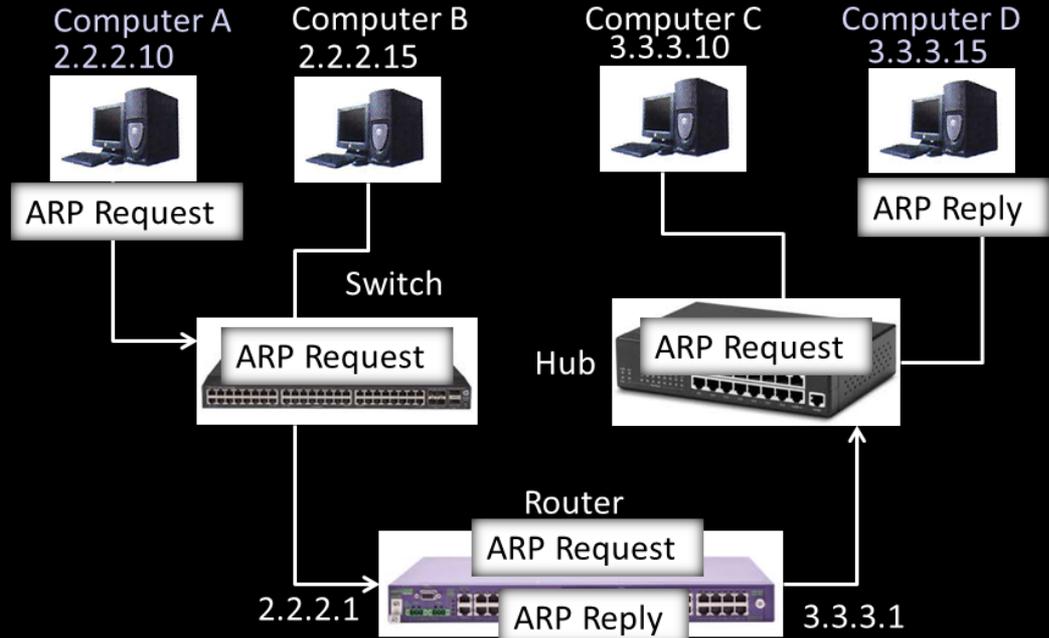
Check out: <https://www.ietf.org/rfc.html>



# ARP Packet contents

The MAC address in **red** is the address that was “requested” by the requestor in order to send the data destined for the target IP in the original ARP request.

- **Computer A – ARP Request**



Sender IP: 2.2.2.10  
 Sender MAC: AA:BB:CC:DD:EE:10  
 Target IP: 2.2.2.1  
 Target MAC: 00:00:00:00:00:00 (broadcast)

ARP Request

- **Router – ARP Reply**

Sender IP: 2.2.2.1  
 Sender MAC: **AA:BB:CC:DD:EE:01**  
 Target IP: 2.2.2.10  
 Target MAC: AA:BB:CC:DD:EE:10

ARP Reply



# ARP spoofing

In computer networking, ARP spoofing, ARP cache poisoning, or ARP poison routing, is a technique by which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks.

The attack can only be used on networks that use the Address Resolution Protocol, and is limited to local network segments.



The Address Resolution Protocol is a widely used communications protocol for resolving Internet layer addresses into link layer addresses.

When an Internet Protocol (IP) datagram is sent from one host to another in a local area network, the destination IP address must be resolved to a MAC address for transmission via the data link layer. When another host's IP address is known, and its MAC address is needed, a broadcast packet is sent out on the local network. This packet is known as an *ARP request*. The destination machine with the IP in the ARP request then responds with an *ARP reply*, which contains the MAC address for that IP.

ARP is a stateless protocol. Network hosts will automatically cache any ARP replies they receive, regardless of whether Network hosts requested them. Even ARP entries which have not yet expired will be overwritten when a new ARP reply packet is received. There is no method in the ARP protocol by which a host can authenticate the peer from which the packet originated. This behavior is the vulnerability which allows ARP spoofing to occur.



# Anatomy of an ARP spoofing attack<sup>122</sup>

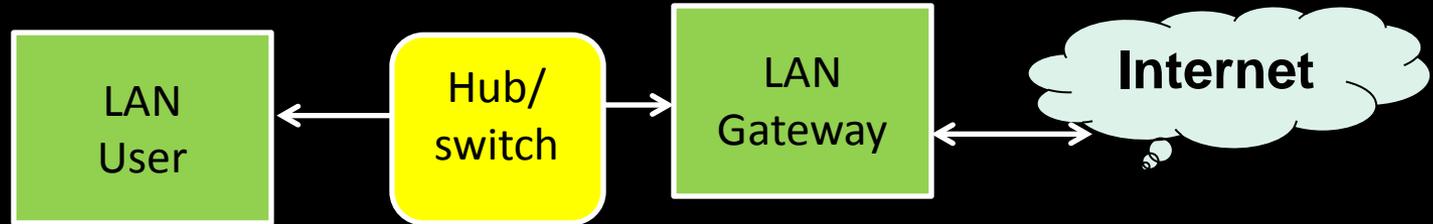
The basic principle behind ARP spoofing is to exploit the above-mentioned vulnerabilities in the ARP protocol by sending spoofed ARP messages onto the LAN. ARP spoofing attacks can be run from a compromised host on the LAN, or from an attacker's machine that is connected directly to the target LAN.

Generally, the goal of the attack is to associate the attacker's host MAC address with the IP address of a target host, so that any traffic meant for the target host will be sent to the attacker's host. The attacker may choose to inspect the packets (spying), while forwarding the traffic to the actual default gateway to avoid discovery, modify the data before forwarding it (man-in-the-middle attack), or launch a denial-of-service (DoS) attack by causing some or all of the packets on the network to be dropped.

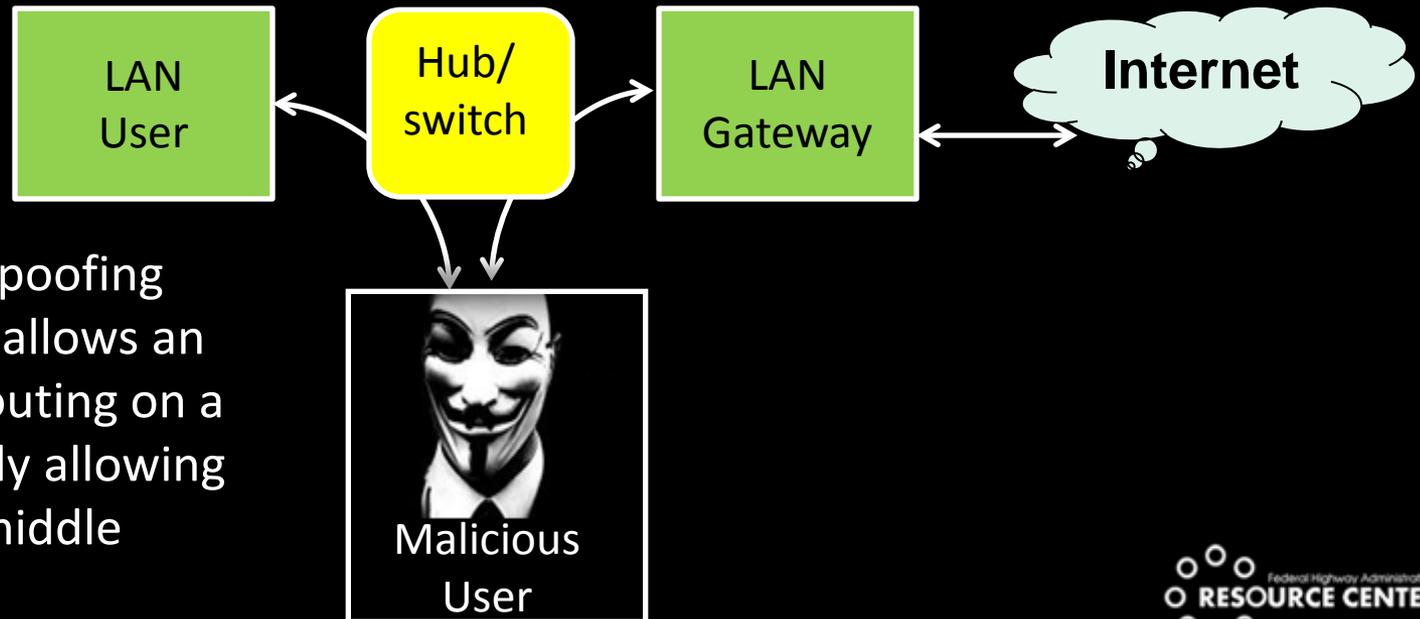


# ARP Spoofing

## Routing under normal operations



## Routing subject to ARP cache poisoning



A successful ARP spoofing (poisoning) attack allows an attacker to alter routing on a network, effectively allowing for a man-in-the-middle attack.



Some of the tools that can be used to carry out ARP spoofing attacks:

- Arpspoof (part of the DSniff suite of tools)
- Arpoison
- Subterfuge
- Ettercap
- Seringe
- ARP-FILLUP -V0.1
- arp-sk -v0.0.15
- ARPOc -v1.13
- arpalert -v0.3.2
- arping -v2.04
- arpmitm -v0.2
- arpoison -v0.5
- ArpSpyX -v1.1
- ArpToXin -v 1.0
- Cain And Abel -v 4.3
- cSploit -v 1.6.2
- SwitchSniffer
- APE - ARP Poisoning Engine
- Simsang
- zANTI -v2



- **anti-arp spoof**
- **Antidote:** Linux daemon, monitors mappings, unusually large number of ARP packets.
- **Arp\_Antidote:** Linux Kernel Patch for 2.4.18 - 2.4.20, watches mappings, can define action to take when.
- **Arpalert:** Predefined list of allowed MAC addresses, alert if MAC that is not in list.
- **ArpON:** Portable handler daemon for securing ARP against spoofing, cache poisoning or poison routing attacks in static, dynamic and hybrid networks.
- **Arpwatch**
- **Arpwatch/ArpwatchNG/Winarpwatch:** Keep mappings of IP-MAC pairs, report changes via Syslog, Email.
- **DefendARP:** A host-based ARP table monitoring and defense tool designed for use when connecting to public wifi. DefendARP detects ARP poisoning attacks, corrects the poisoned entry, and identifies the MAC and IP address of the attacker.
- **Prelude IDS:** ArpSpooF plugin, basic checks on addresses.
- **Snort:** Snort preprocessor Arpspoof, performs basic checks on addresses
- **XArp:** Advanced ARP spoofing detection, active probing and passive checks. Two user interfaces: normal view with predefined security levels, pro view with per-interface configuration of detection modules and active validation. Windows and Linux, GUI-based.



ARP-scan is a commandline utility for linux used to scan the network to identify IP & MAC addresses.

```
root@kali:~/Desktop# arp-scan -g 192.168.10.0/24
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.2 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.10.2    00:50:56:a0:48:fb    VMware, Inc.
192.168.10.10  00:10:18:4e:2a:b0    BROADCOM CORPORATION
192.168.10.11  00:50:56:a0:2d:26    VMware, Inc.
192.168.10.12  00:50:56:a0:56:1b    VMware, Inc.
192.168.10.21  00:50:56:a0:2f:e4    VMware, Inc.
192.168.10.22  00:50:56:a0:1b:d2    VMware, Inc.
192.168.10.32  00:50:56:a0:1c:b6    VMware, Inc.
192.168.10.40  00:a0:1d:30:b2:1c    SIXNET
192.168.10.41  00:50:56:a0:22:b3    VMware, Inc.
192.168.10.42  00:50:56:a0:1d:a2    VMware, Inc.
192.168.10.50  00:50:56:a0:39:b3    VMware, Inc.
192.168.10.55  00:50:56:a0:4c:6d    VMware, Inc.
192.168.10.66  00:50:56:a0:5f:f9    VMware, Inc.
192.168.10.97  00:50:56:a0:2d:b3    VMware, Inc.
192.168.10.99  54:42:49:7b:2c:10    Sony Corporation
192.168.10.254 00:19:e2:ab:32:8c    Juniper Networks

102 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.2: 256 hosts scanned in 1.856 seconds (137.93 hosts/sec). 18 responded
root@kali:~/Desktop#
```



# MAC address

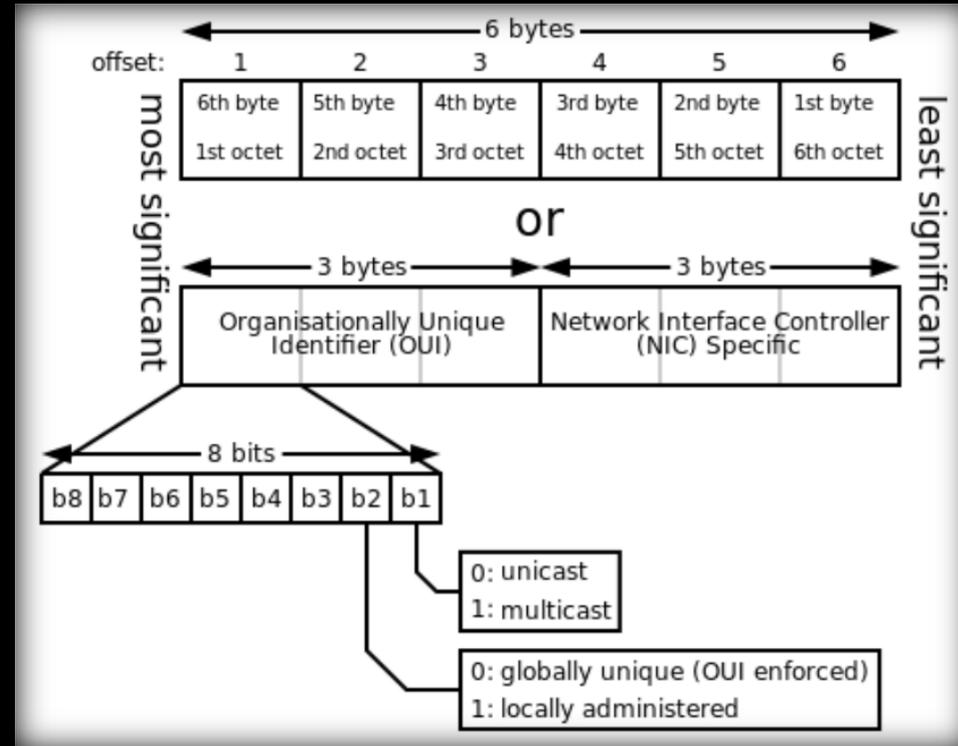
Media Access Control address (MAC address), also called physical address, is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and WiFi. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.

MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the Burned-In Address (BIA). It may also be known as an Ethernet Hardware Address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.

A network node may have multiple NICs and each NIC must have a unique MAC address.

MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-64.

The IEEE claims trademarks on the names EUI-48 and EUI-64, in which EUI is an abbreviation for *Extended Unique Identifier*.





## The following technologies use the MAC-48 identifier format:

- **Ethernet**
- **802.11 wireless networks**
- **Bluetooth**
- **IEEE 802.5 token ring**
- **most other IEEE 802 networks**
- **Fiber Distributed Data Interface (FDDI)**
- **Asynchronous Transfer Mode (ATM)**, switched virtual connections only, as part of an NSAP address
- **Fiber Channel and Serial Attached SCSI** (as part of a World Wide Name)
- The **ITU-T G.hn standard**, which provides a way to create a high-speed (up to 1 gigabit/s) local area network using existing home wiring (power lines, phone lines and coaxial cables). The **G.hn Application Protocol Convergence (APC)** layer accepts Ethernet frames that use the MAC-48 format and encapsulates them into **G.hn Medium Access Control Service Data Units (MSDUs)**.



- Every device that connects to an IEEE 802 network (such as Ethernet and WiFi) has a MAC-48 address. Common consumer devices to use MAC-48 include every PC, smartphone or tablet computer.
- The distinction between EUI-48 and MAC-48 identifiers is purely nominal: MAC-48 is used for network hardware; EUI-48 is used to identify other devices and software. *(Thus, by definition, an EUI-48 is not in fact a "MAC address", although it is syntactically indistinguishable from one and assigned from the same numbering space.)*
- The IEEE now considers the label MAC-48 to be an obsolete term, previously used to refer to a specific type of EUI-48 identifier used to address hardware interfaces within existing 802-based networking applications, and thus not to be used in the future. Instead, the proprietary term EUI-48 should be used for this purpose.



EUI-64 identifiers are used in:

- [FireWire](#)
- [IPv6](#) (Modified EUI-64 as the least-significant 64 bits of a unicast network address or link-local address when stateless autoconfiguration is used)
- [ZigBee](#) / [802.15.4](#) / [6LoWPAN](#) wireless personal-area networks

The IEEE has built in several special address types to allow more than one network interface card to be addressed at one time:

- Packets sent to the *broadcast address*, all one bits, are received by all stations on a local area network. In hexadecimal the broadcast address would be FF:FF:FF:FF:FF:FF. A broadcast frame is flooded and is forwarded to and accepted by all other nodes.
- Packets sent to a *multicast address* are received by all stations on a LAN that have been configured to receive packets sent to that address.
- Functional addresses identify one or more Token Ring NICs that provide a particular service, defined in [IEEE 802.5](#).



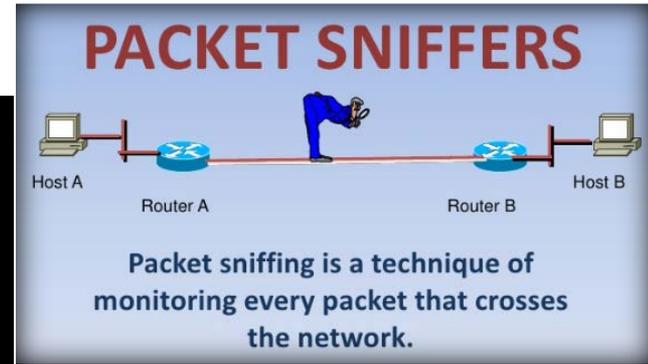
- Sniffers
- Discovery
- IPv4
- Routing Tables
- RFC



# Packet Sniffer

A **Packet Sniffer** (also known as a **network analyzer**, **protocol analyzer** or **packet analyzer** —or, for particular types of networks, an **Ethernet sniffer** or **wireless sniffer**) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.

A Request for Comments (RFC) is a type of publication from the Internet Engineering Task Force (IETF) and the Internet Society (ISOC), the principal technical development and standards-setting bodies for the Internet.



Wireshark --- THE Standard for performing network analysis

- GUI network protocol analyzer and packet sniffer
- Uses libpcap standard library for opening and capturing network traffic

[http://packetlife.net/media/library/13/Wireshark\\_Display\\_Filters.pdf](http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf)



# Packet Sniffers

- Analyze network problems
- Detect network intrusion attempts
- Detect network misuse by internal and external users
- Gain information for effecting a network intrusion
- Isolate exploited systems
- Monitor WAN bandwidth utilization
- Monitor data-in-motion
- Monitor WAN and endpoint security status
- Gather and report network statistics
- Filter suspect content from network traffic
- Documenting regulatory compliance through logging all perimeter and endpoint traffic
- Monitor network usage (including internal and external users and systems)
- Serve as primary data source for day-to-day network monitoring and management
- Spy on other network users and collect sensitive information such as login details or users cookies (depending on any content encryption methods that may be in use)
- Reverse engineer proprietary protocols used over the network
- Debug client/server communications
- Debug network protocol implementations
- Verify adds, moves and changes
- Verify internal control system effectiveness (firewalls, access control, Web filter, spam filter, proxy)





# Passive Network Discovery

## What is Passive Network Discovery?

- Use information stored locally on a compromised host to identify new host and network targets.
- Attempt to identify new targets without sending any network packets.

## Why perform Passive Network Discovery?

- It's more difficult to detect than active discovery.
  - May provide valuable information that active discovery cannot.
- ✓ There are many tools and system commands to aid in the network discovery process.
  - ✓ Much can be learned from computer configuration files such as services being used, hosts that may be accessed on a frequent basis, hosts designated as domain name servers, etc.
  - ✓ History files provide information as to what the host is being used, commands issued, processes running, etc.
  - ✓ Caches provide information that various system processes store as information is received and processed. Commands to retrieve cached data and researching files that are cached provide important information on users, networks accessed, etc.

Tools
Tcpdump, Wireshark
Ipconfig (windows)
Ifconfig (linux)
Netstat
Arp
Net
Route
Iptables
EtherApe (GUI)

Configuration Files
Custom Scripts (cron, start-up)
Apache (mysql, etc.)
Resolv.conf, hosts

History Files
.bash_history
RDP
Log Files

Caches
Arp
Nbtstat
DNS
Browser



## Ipconfig

- The windows ipconfig command displays the IP address, subnet mask, and default gateway for all adapters.
- The /all parameter displays the full TCP/IP configuration.

```
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : idaho-b2a8de164
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : localdomain

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : localdomain
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
    Physical Address. . . . . : 00-0C-29-1E-24-96
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.90.128
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.90.2
    DHCP Server . . . . . : 192.168.90.254
    DNS Servers . . . . . : 192.168.90.2
```

## Ifconfig

- *Interface Configuration* is a system administration utility in Unix-like operating systems to configure, control, and query TCP/IP network interface parameters.

```
root@kali:~/Desktop# /sbin/ifconfig -a
eth0  Link encap:Ethernet HWaddr 00:0c:29:e3:10:e6
       inet addr:172.16.255.141 Bcast:172.16.255.255 Mask:255.255.255.0
       inet6 addr: fe80::20c:29ff:fee3:10e6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:26416 errors:0 dropped:0 overruns:0 frame:0
       TX packets:15037 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:29605461 (28.2 MiB) TX bytes:1560405 (1.4 MiB)
       Interrupt:19 Base address:0x2000

lo    Link encap:Local Loopback
       inet addr:127.0.0.1 Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING MTU:65536 Metric:1
       RX packets:1525 errors:0 dropped:0 overruns:0 frame:0
       TX packets:1525 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:0
       RX bytes:257391 (251.3 KiB) TX bytes:257391 (251.3 KiB)
```

- The most useful information displayed by ifconfig includes:

- ✓ *HWaddr* – Interface MAC address
- ✓ *inet addr* – Interface IP address
- ✓ *Bcast* – Network broadcast address
- ✓ *Mask* – Network mask (akanetmask)
- ✓ *inet6 addr* – Ipv6



# Payload

**Vulnerability**

- Vulnerability is a software flaw that may be susceptible to exploitation.

**Exploit**

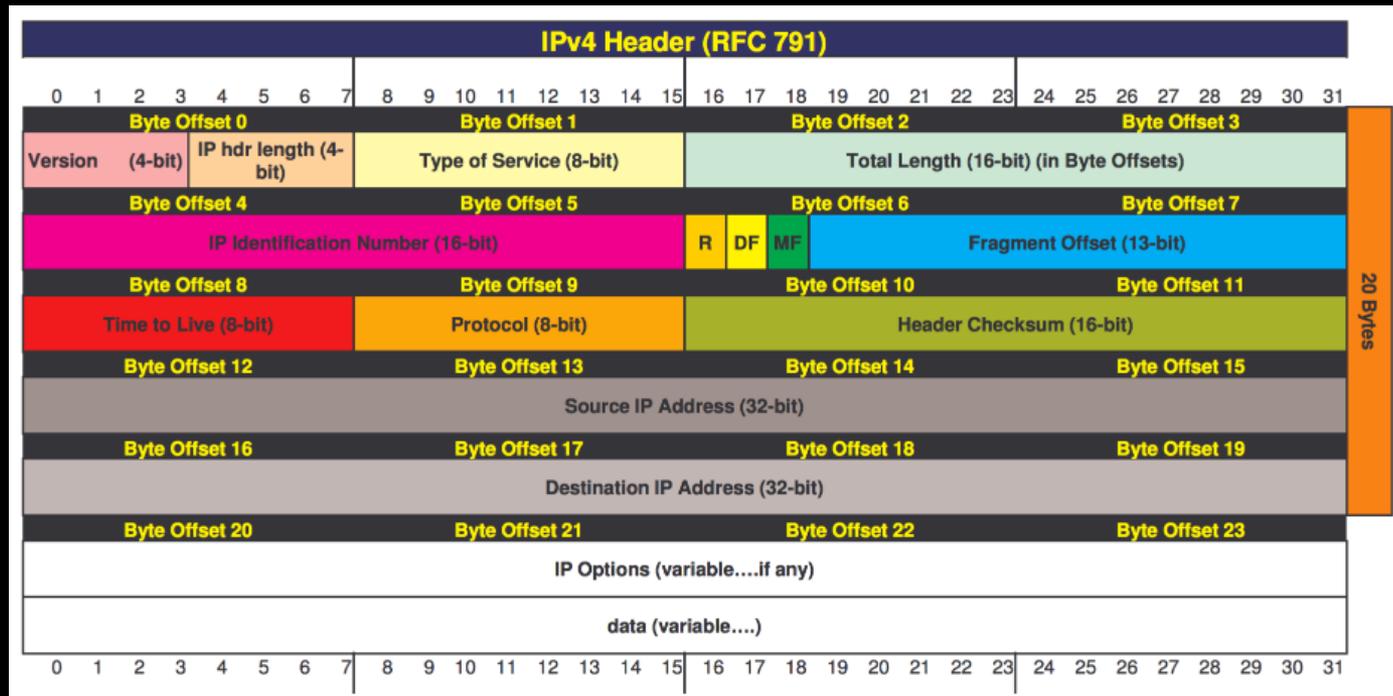
- Exploit is an instance of an attacker taking advantage of a vulnerability.

**Payload**

- Payload is the module the chosen exploit will run when a machine is compromised.



Internet Protocol version 4 (IPv4) is the 4<sup>th</sup> version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet, and was the first version deployed for production in the ARPANET in 1983. It still routes most Internet traffic today, despite the ongoing deployment of a successor protocol, IPv6.



IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).



Routing Table is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it. The construction of routing tables is the primary goal of routing protocols.

Static routes are entries made in a routing table by non-automatic means and which are fixed rather than being the result of some network topology "discovery" procedure.

A routing table uses the same idea that one does when using a map in package delivery. Whenever a node needs to send data to another node on a network, it must first know *where* to send it. If the node cannot directly connect to the destination node, it has to send it via other nodes along a proper route to the destination node. Most nodes do not try to figure out which route(s) might work; instead, a node will send an IP packet to a gateway in the LAN, which then decides how to route the "package" of data to the correct destination. Each gateway will need to keep track of which way to deliver various packages of data, and for this it uses a Routing Table.



# ...Routing Table

- A routing table is a database which keeps track of paths, like a map, and allows the gateway to provide this information to the node requesting the information.
- With hop-by-hop routing, each routing table lists, for all reachable destinations, the address of the next device along the path to that destination: the next hop. Assuming that the routing tables are consistent, the simple algorithm of relaying packets to their destination's next hop thus suffices to deliver data anywhere in a network. Hop-by-hop is the fundamental characteristic of the IP Internetwork Layer and the OSI Network Layer.
- The primary function of a router is to forward a packet toward its destination network, which is the destination IP address of the packet. To do this, a router needs to search the routing information stored in its routing table.



- A routing table is a data file in RAM that is used to store route information about directly connected and remote networks. The routing table contains network/next hop associations. These associations tell a router that a particular destination can be optimally reached by sending the packet to a specific router that represents the "next hop" on the way to the final destination. The next hop association can also be the outgoing or exit interface to the final destination.
- The network/exit-interface association can also represent the destination network address of the IP packet. This association occurs on the router's directly connected networks.

## Why look at routing tables?

- Identify router/gateway IP addresses
- Identify new network and host targets
- Gateway hosts, great target for Man-in-the-Middle (MitM) attack.

How can you tell if the host is acting as a gateway?

- Not Forwarding = 0, Forwarding = 1
- Identify new network and host targets



# Request for Comments (RFC)

Request for Comments (RFC) is a type of publication from the Internet Engineering Task Force (IETF) and the Internet Society, the principal technical development and standards-setting bodies for the Internet.

An RFC is authored by engineers and computer scientists in the form of a memorandum describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems.



There are over 7400 RFCs published by the IETF and the Internet Society.  
i.e. RFC 793 – Transmission Control Protocol.

<https://www.ietf.org/rfc.html>

## RFC references

- RFC 4423 - Host Identity Protocol (HIP) Architecture (early "informational" snapshot)
- RFC 5201 - Host Identity Protocol base (Obsoleted by RFC 7401)
- RFC 5202 - Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP) (Obsoleted by RFC 7402)
- RFC 5203 - Host Identity Protocol (HIP) Registration Extension
- RFC 5204 - Host Identity Protocol (HIP) Rendezvous Extension
- RFC 5205 - Host Identity Protocol (HIP) Domain Name System (DNS) Extension
- RFC 5206 - End-Host Mobility and Multihoming with the Host Identity Protocol
- RFC 5207 - NAT and Firewall Traversal Issues of Host Identity Protocol (HIP) Communication
- RFC 6092 - Basic Requirements for IPv6 Customer Edge Routers
- RFC 7401 - Host identity protocol version 2 (HIPv2)
- RFC 7402 - Using the Encapsulating Security Payload (ESP) transport format with the Host Identity Protocol (HIP)



- Passwords/Hash:
  - Rootkit
  - HASH
  - Pass the HASH
  - Salt



# Rootkit

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software.



The term *rootkit* is a concatenation of "root" (the traditional name of the privileged account on Unix-like operating systems) and the word "kit" (which refers to the software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.



# Rootkit Installation & Detection



Rootkit installation can be automated, or an attacker can install it once they've obtained root or Administrator access. Obtaining this access is a result of direct attack on a system (i.e.), exploiting a known vulnerability (such as privilege escalation) or a password (obtained by cracking or social engineering). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root or Administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it. Detection methods include using an alternative and trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis. Removal can be complicated or practically impossible, especially in cases where the rootkit resides in the kernel; reinstallation of the operating system may be the only available solution to the problem. When dealing with firmware rootkits, removal may require hardware replacement, or specialized equipment.



A **root name server** is a name server for the root zone of the Domain Name System (DNS) of the Internet. It directly answers requests for records in the root zone and answers other requests by returning a list of the authoritative name servers for the appropriate Top-Level Domain (TLD).

The root name servers are a critical part of the Internet infrastructure because they are the first step in translating (resolving) human readable host names into IP addresses that are used in communication between Internet hosts.

A combination of limits in the DNS and certain protocols, namely the practical size of unfragmented User Datagram Protocol (UDP) packets, resulted in a decision to limit the number of root servers to thirteen server addresses.



# HASH

- A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. Hash functions accelerate table or database lookup by detecting duplicated records in a large file.
- An example is useful in cryptography. A cryptographic hash function allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown, it is deliberately difficult to reconstruct it (or equivalent alternatives) by knowing the stored hash value. This is used for assuring integrity of transmitted data, and is the building block for HMACs, which provide message authentication.

Some standard applications that employ hash functions include authentication, message integrity (using an HMAC (Hashed MAC)), message fingerprinting, data corruption detection, and digital signature efficiency.



# Pass the HASH (PTH)

- PASS THE HASH (PTH) - a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NT LAN Manager (NTLM) and/or LanMan hash.
- LAN Manager hash is a compromised password hashing function that was the primary hash that Microsoft LAN Manager and Microsoft Windows versions prior to Windows NT used to store user passwords, hash of a user's password, instead of requiring the associated plaintext password (Privilege Escalation).



# Salt



- **Salt** is random data that is used as an additional input to a one-way function that hashes a password or passphrase.
- The primary function of salts is to defend against dictionary attacks versus a list of password hashes and against pre-computed rainbow table attacks.
- A new salt is randomly generated for each password. In a typical setting, the salt and the password are concatenated and processed with a cryptographic hash function, and the resulting output (but not the original password) is stored with the salt in a database.
- Hashing allows for later authentication while protecting the plaintext password in the event that the authentication data store is compromised.
- Cryptographic salts are broadly used in many modern computer systems, from UNIX system credentials to Internet security.



- **Defense in Depth:**

- Nmap
- IDS / IPS / HIDS
- Metasploit
- tcpdump
- Snort
- Wireshark
- Cryptography / Encryption
- Keys



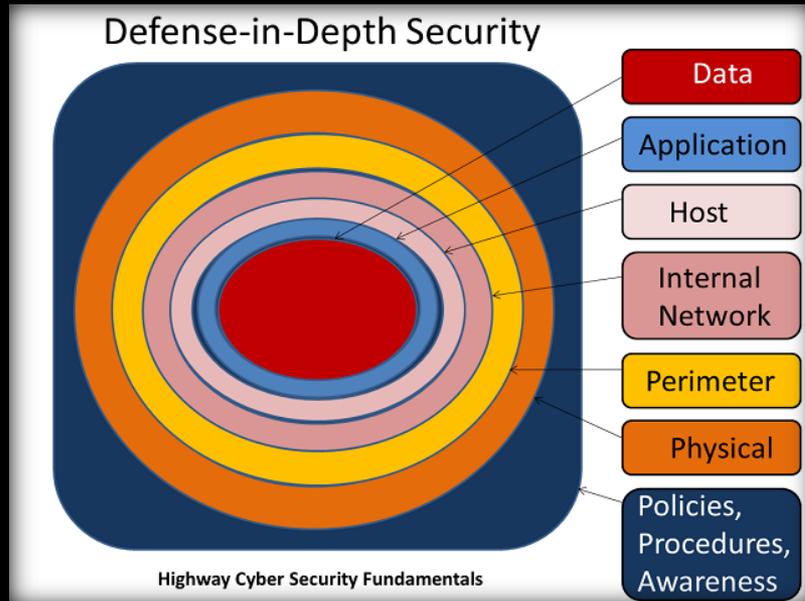
**Defense in Depth** is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of *personnel, procedural, technical* and *physical* for the duration of the system's life cycle.

The idea behind the defense in depth approach is to defend a system against any particular attack using several independent methods. It is a layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security.

Defense in depth is originally a military strategy that seeks to delay rather than prevent the advance of an attacker by yielding space to buy time. The placement of protection mechanisms, procedures and policies is intended to increase the dependability of an ICS, where multiple layers of defense prevent espionage and direct attacks against critical systems. In terms of computer network defense, defense in depth measures should not only prevent security breaches but also buy an organization time to detect and respond to an attack and so reduce and mitigate the consequences breach.



Using more than one of the following layers constitutes defense in depth:



- Anti virus software
- Authentication and password security
- Biometrics
- Demilitarized zones (DMZ)
- Data-centric security
- Encryption
- Firewalls (hardware or software)
- Hashing passwords
- Intrusion detection systems (IDS)
- Logging and auditing
- Multi-factor authentication
- Vulnerability scanners
- Physical security (e.g. deadbolt locks)
- Timed access control
- Intrusion Protection System (IPS)
- Internet Security Awareness Training
- Virtual private network (VPN)
- Sandboxing



- An **intrusion detection system (IDS)** is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.
- IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. **There are network based (NIDS) and host based (HIDS) intrusion detection systems.** NIDS is a network security system focusing on the attacks that come from the inside of the network (authorized users). Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system.
- **Intrusion Detection and Prevention Systems (IDPS)** are primarily focused on identifying possible incidents, logging information about them, and reporting attempts.



- In addition, organizations use IDPS's for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies.
- IDPS's have become a necessary addition to the security infrastructure of nearly every organization. IDPS's typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPS's can also respond to a detected threat by attempting to prevent it from succeeding.
- They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

## Additional Tactics & Techniques:

<http://www.securityfocus.com/infocus/1577>

<http://www.securityfocus.com/infocus/1852>

<http://www.oracle.com/technetwork/systems/articles/snort-base-jsp-138895.html>

<http://www.oracle.com/technetwork/systems/articles/intrusion-detection-jsp-140939.html>



- **Alarm filtering:** The process of categorizing attack alerts produced from an IDS in order to distinguish false positives from actual attacks.
- **Attacker or Intruder:** An entity which tries to find a way to gain unauthorized access to information, inflict harm or engage in other malicious activities.
- **Burglar Alarm:** A signal suggesting that a system has been or is being attacked.
- **Clandestine user:** A person who acts as a supervisor and tries to use his privileges so as to avoid being captured.
- **Confidence value:** A value an organization places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack.
- **Detection Rate:** The detection rate is defined as the number of intrusion instances detected by the system (True Positive) divided by the total number of intrusion instances present in the test set.
- **False Alarm Rate:** defined as the number of 'normal' patterns classified as attacks (False Positive) divided by the total number of 'normal' patterns.



- **False Negative:** When no alarm is raised when an attack has taken place.
- **False Positive:** An event signaling an IDS to produce an alarm when no attack has taken place.
- **Masquerader:** A person who attempts to gain unauthorized access to a system by pretending to be an authorized user. They are generally outside users.
- **Misfeasor:** They are commonly internal users and can be of two types:
  - An authorized user with limited permissions.
  - A user with full permissions and who misuses their powers.
- **Noise:** Data or interference that can trigger a false positive or obscure a true positive.
- **Site policy:** Guidelines within an organization that control the rules and configurations of an IDS.
- **Site policy awareness:** An IDS's ability to dynamically change its rules and configurations in response to changing environmental activity.
- **True Negative:** An event when no attack has taken place and no detection is made.
- **True Positive:** A legitimate attack which triggers an IDS to produce an alarm.

Intrusion detection systems are of two main types, network based (NIDS) and host based (HIDS) intrusion detection systems.



- Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks.
- Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulation network intrusion detection systems.
- NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the designing of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS. On-line NIDS deals with the network in real time. It analyses the Ethernet packets and applies some rules, to decide if it is an attack or not. Off-line NIDS deals with stored data and passes it through some processes to decide if it is an attack or not.



Host-based Intrusion Detection System (HIDS) refers to intrusion detection that takes place on a single host system. Currently, HIDS involves installing an agent on the local host that monitors and reports on the system configuration and application activity. Some common abilities of HIDS systems include log analysis, event correlation, integrity checking, policy enforcement, rootkit detection, and alerting. They often also have the ability to baseline a host system to detect variations in system configuration. In specific vendor implementations these HIDS agents also allow connectivity to other security systems.

## HIDS Intrusion Prevention

Most HIDS packages now have the ability to actively prevent malicious or anomalous activity on the host system. Due to the potential impact this can have on the end user, HIDS is frequently deployed in "monitor only" mode initially. This enables the administrator to create a baseline of the system configuration and activity. Active blocking of applications, system changes, and network activity is limited to only the most egregious activities. Administrators can then tune the system policy based on what is considered "normal activity".

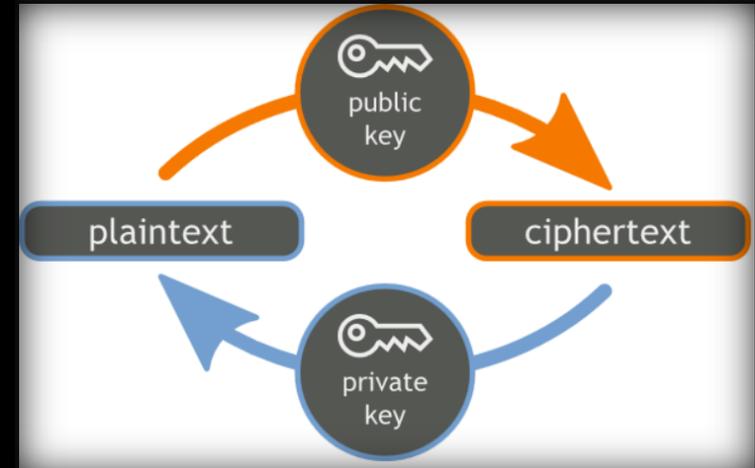


- Host Intrusion Detection Systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected.
- It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.
- Intrusion detection systems can also be system-specific using custom tools and honeypots.



# Keys

In cryptography, a **Key** is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes.



- 128-bit keys are commonly used and considered very strong.
- The keys used in public key cryptography have some mathematical structure.
  - For example, public keys used in the RSA system are the product of two prime numbers.
  - Thus public key systems require longer key lengths than symmetric systems for an equivalent level of security.
- 3072 bits is the suggested key length for systems which aim to security equivalent to a 128 bit symmetric cipher.



Transportation owners/operators should be aware of Cryptography, Deterministic Builds, protecting keys ((Key Agreement Schemes, Password-based Key Derivation Functions (PBKDF2), algorithms for performing encryption or decryption)) and various testing & scanning procedures against various threats such as Man-in-the-Middle (MitM), etc.

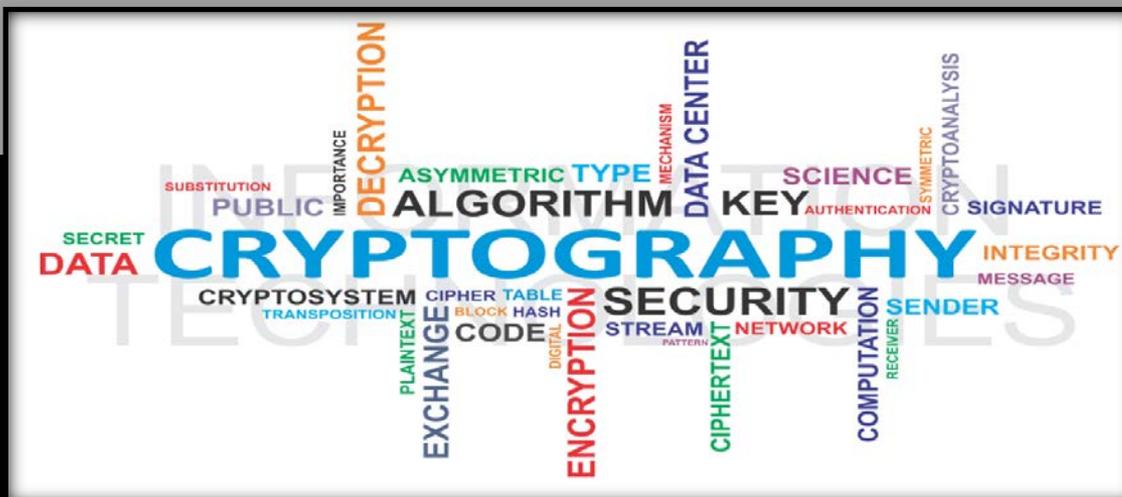
**“Deterministic builds”** ... fingerprint of the app ... to protect against targeted attacks.

Current popular software development practices simply cannot survive targeted attacks of the scale and scope that we are seeing today.

<https://blog.torproject.org/category/tags/deterministic-builds>

This will eventually allow us to create a number of auxiliary authentication mechanisms for our packages, beyond just trusting a single offline build machine and a single cryptographic key's integrity.

Interesting examples include providing multiple independent cryptographic signatures for packages, listing the package hashes in the Tor consensus, and encoding the package hashes in the Bitcoin blockchain.



**Perfect Forward Secrecy** - in cryptography, PFS is a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future.

The key used to protect transmission of data must not be used to derive any additional keys, and if the key used to protect transmission of data is derived from some other keying material, then that material must not be used to derive any more keys. In this way, compromise of a single key permits access only to data protected by that single key.



The NIST AES Standardization Process - correctly implementing the AES algorithm, using the tests found in The Advanced Encryption Standard Algorithm Validation Suite (AESAVS). This testing is performed by NVLAP accredited Cryptographic And Security Testing (CST) Laboratories.

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography is the same level of security provided by keys of smaller size. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks.



# Encryption

In cryptography, encryption is the process of encoding messages or information in such a way that only authorized parties can read it.

Encryption does not of itself prevent interception, but denies the message content to the interceptor.



In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted.

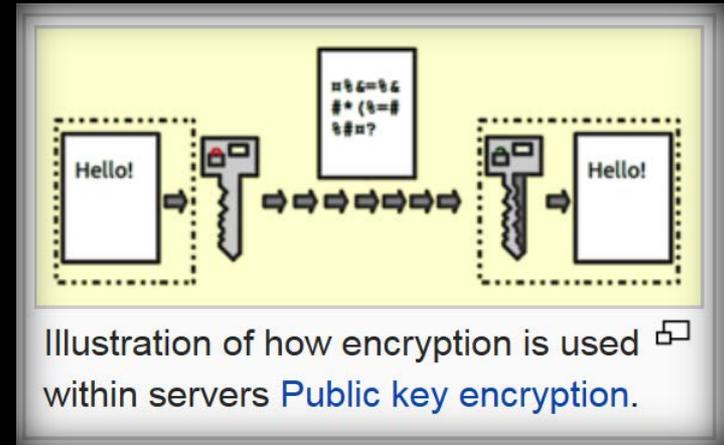
For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required.

An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.



# Public key encryption

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read.



- Encryption has long been used by military and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems.
- Encryption can be used to protect data "at rest", such as information stored on computers and storage devices.
- Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet), mobile telephones, Bluetooth devices. There have been numerous reports of data in transit being intercepted in recent years.
- Data should also be encrypted when transmitted across networks in order to protect against eavesdropping of network traffic by unauthorized users.



The NSA ANT catalog is a classified document listing technology available to the United States National Security Agency (NSA) Tailored Access Operations (TAO) by the Advanced Network Technology (ANT) Division to aid in cyber surveillance. Most devices are described as already operational and available to US nationals and members of the Five Eyes alliance.

[nsaplayset.org](https://nsaplayset.org)

[github.com](https://github.com)

Exploits described in the document are mostly targeted at devices manufactured by US companies, including Apple, Cisco, Dell, Juniper Networks, Maxtor, Seagate, and Western Digital, although there is nothing in the document that suggests that the companies were complicit.



**Elliptic curve cryptography (ECC)** is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. They are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization.

**NSA quantum encryption** – the distribution of secret keys through quantum means has certainly become the most mature application of quantum information science. Based on the seemingly fantastical but very real properties of quantum mechanics — the physics of very small things — a quantum computer would have the power to instantly perform mathematical calculations that would take years with classical machines, and that could threaten today’s crypto. The NSA has funded quantum computer projects for more than a decade, and recently, leaked documents revealed that the agency is “pursuing more than just basic, unclassified research,” secretly working on a quantum computer that could be a first step towards machines that could “attack high-grade public key encryption systems.”



**Vulnerability scanning** evaluates a system for potential vulnerabilities or weak configurations, is largely automated and can only ever find a subset of security issues.

**Penetration testing**, on the other hand, is a manual process performed by a human. A penetration tester will use tools as a part of their work, but they apply their human ingenuity to exploit vulnerabilities and illustrate what an attacker might be capable of when targeting a particular system.



Use tcpdump to capture in a pcap file (Wireshark dump)

*tcpdump* is a command line network sniffer (a powerful command-line packet analyzer), used to capture network packets. When you have only command line terminal access of your system, this tool is very helpful to sniff network packets. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

Tcpdump works on most Unix-like operating systems: Linux, Solaris, BSD, OS X, HP-UX, Android and AIX among others. In those systems, tcpdump uses the libpcap library to capture packets. The port of tcpdump for Windows is called WinDump; it uses WinPcap, the Windows port of libpcap.

*tcpdump man page*: When you create a pcap file using *tcpdump* it will truncate your capture file to shorten it and you may not be able to understand that.



## Cyberattackers are getting quieter once they're inside the network

02/05/2016

By Wade Williamson

SECURITY FEATURES

### Which threat trends are on the rise?

Our research indicates that cyber attackers are getting quieter once they are inside the network. They know they are being watched and as such, they are choosing attack methods that will help them to hide longer in the network so they can spy and steal more data over a longer period of time.

For example, we noticed a big jump in a fairly new and stealthy approach to command-and-control called **hidden tunnels**. This technique allows an attacker to pass hidden messages by embedding data within seemingly normal HTTP and HTTPS packets. This allows the attacker's hidden messages to bypass traditional security controls such as firewalls and intrusion prevention systems.

### What happens to the network post-intrusion? What is the most commonly observed post-intrusion behavior?

Once inside the network, cyber attackers begin to perform internal reconnaissance, which is then followed by lateral movement. In more plain terms, once an attacker gets inside a network, they need to look around to find where to go next, and then start to move deeper within the network. Attackers appear to be getting quieter when performing these steps.



<http://www.itproportal.com/2016/05/02/cyberattackers-are-getting-quieter-once-theyre-inside-the-network/>



## Cyberattackers are getting quieter once they're inside the network

02/05/2016

By Wade Williamson  
SECURITY FEATURES

Because brute force techniques are so noisy, more experienced and skilled attackers tend to try other access techniques first – preferably automated techniques that are difficult to distinguish from normal network traffic and where failures are unlikely to be alerted upon.



### **In which ways can an attacker do damage once inside the network?**

Once an attacker has a toehold within the network with remote access and control of a compromised host, an obvious objective is to start collecting user and administrative credentials

The attacker can repeat this process to move deeper and deeper into the network, and ultimately gain access to critical data or assets. Once these assets are found, cyber attackers can either steal the data (exfiltration), or in some cases the attacker will simply encrypt or destroy the data.

<http://www.itproportal.com/2016/05/02/cyberattackers-are-getting-quieter-once-theyre-inside-the-network/>



# Snort: <https://www.snort.org/> is an open-source network intrusion detection and prevention system

It is *widely used and has become the standard for (IDP/IPS) Intrusion Detection Perimeter/Intrusion Prevention Systems.* Snort's open source network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks.



Snort performs protocol analysis, content searching and matching. These basic services have many purposes including application-aware triggered quality of service, to de-prioritize bulk traffic when latency-sensitive applications are in use.

The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. The program will then perform a specific action based on what has been identified.



# Wireshark (the standard for performing network protocol analysis).

It is the world's foremost network protocol analyzer.

It lets you see what's happening on your network at a microscopic level.  
It is the de facto standard across many industries.

Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text



In cryptography, an initialization vector(IV) or starting variable (SV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom.

Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.

For block ciphers, the use of an IV is described by so-called modes of operation.

Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereof.



Some cryptographic primitives require the IV only to be non-repeating, and the required randomness is derived internally. In this case, the IV is commonly called a nonce (*number used once*), and the primitives are described as *stateful* as opposed to *randomized*.

This is because the IV need not be explicitly forwarded to a recipient but may be derived from a common state updated at both sender and receiver side. (In practice, a short nonce is still transmitted along with the message to consider message loss.)

An example of stateful encryption schemes is the counter mode of operation, which uses a sequence number as a nonce.



The size of the IV is dependent on the cryptographic primitive used; for block ciphers, it is generally the cipher's block size. Ideally, for encryption schemes, the unpredictable part of the IV has the same size as the key to compensate time/memory/data tradeoff attacks.

When the IV is chosen at random, the probability of collisions due to the birthday problem must be taken into account. Traditional stream ciphers such as RC4 do not support an explicit IV as input, and a custom solution for incorporating an IV into the cipher's key or internal state is needed.

Some designs realized in practice are known to be insecure; the WEP protocol is a notable example, and is prone to related-IV attacks.



- EKMS
- Keyed hash algorithm
- Key authentication
- Key derivation function
- Key distribution center
- Key escrow
- Key exchange
- Key generation
- Key management
- Key schedule
- Key server
- Key signature (cryptography)
- Key signing party
- Key stretching
- Key-agreement protocol
- Password psychology
- Public key fingerprint
- Random number generator
- Self-certifying key
- Session key
- Tripcode
- Machine-readable paper key
- Weak key



# Egress filtering

- Egress filtering is the practice of monitoring and potentially restricting the flow of information outbound from one network to another. Typically it is information from a private TCP/IP computer network to the Internet that is controlled.
- TCP/IP packets that are being sent out of the internal network are examined via a router, firewall, or similar edge device. Packets that do not meet security policies are not allowed to leave - they are denied "egress".
- Egress filtering helps ensure that unauthorized or malicious traffic never leaves the internal network.
- In a corporate network, typical recommendations are that all traffic except that emerging from a select set of servers would be denied egress. Restrictions can further be made such that only select protocols such as HTTP, email, and DNS are allowed. User workstations would then need to be configured either manually or via proxy auto-config to use one of the allowed servers as a proxy.
- Egress filtering may require policy changes and administrative work whenever a new application requires external network access. For this reason egress filtering is an uncommon feature on consumer and very small business networks.

