**CYBER SECURITY**

**(UNIT 2)**

**Introduction to Application Security**

Application Security is the protection of an application against security threats. This is a difficult task, as the application designer or corporate security manager must incorporate defences against every imaginable attack, whereas an attacker only has to find one vulnerability or point of attack to succeed. Past techniques of protecting applications have certainly been limited, but new technology has been developed to solve this challenging problem. Application Security is comprised of Network Security, Data Security and Software Protection:

•Network Security addresses external attacks generally against resources inside the firewall providing a service across a network. Network security has traditionally been addressed using firewalls, intrusion detection systems and virus scanners

• Data Security is the protection of data used locally by an application or transmitted between users and servers. Cryptography is the main solution here as it is highly effective at protecting data during transmission and storage by ensuring its integrity and confidentiality

• Software Protection is the protection of the software, or services rendered by the software, from attacks, thereby preventing theft of intellectual property and licensed content and ensuring that the software continues to function as intended. Typically these attacks include reverse engineering, tampering, copying, and automated forms of these attacks that can be launched across the network or on a desktop by relatively unsophisticated attackers

**Data Security Considerations-Backup**

In  [information technology](https://en.wikipedia.org/wiki/Information_technology%22%20%5Co%20%22Information%20technology), a **backup**, or the process of backing up, refers to the copying and [archiving](https://en.wikipedia.org/wiki/Archiving) of computer [data](https://en.wikipedia.org/wiki/Data) so it may be used to *restore* the original after a [data loss](https://en.wikipedia.org/wiki/Data_loss) event.

Backups have two distinct purposes. The primary purpose is to recover data after its loss, be it by [data deletion](https://en.wikipedia.org/wiki/File_deletion) or [corruption](https://en.wikipedia.org/wiki/Data_corruption). Data loss can be a common experience of computer users; a 2008 survey found that 66% of respondents had lost files on their home PC. The secondary purpose of backups is to recover data from an earlier time, according to a user-defined [data retention](https://en.wikipedia.org/wiki/Data_retention) policy, typically configured within a [backup application](https://en.wikipedia.org/wiki/Backup_software) for how long copies of data are required. Though backups represent a simple form of [disaster recovery](https://en.wikipedia.org/wiki/Disaster_recovery), and should be part of any [disaster recovery plan](https://en.wikipedia.org/wiki/Disaster_recovery_plan) backups by themselves should not be considered a complete disaster recovery plan. One reason for this is that not all backup systems are able to reconstitute a computer system or other complex configuration such as a [computer cluster](https://en.wikipedia.org/wiki/Computer_cluster), [active directory](https://en.wikipedia.org/wiki/Active_directory) server, or [database server](https://en.wikipedia.org/wiki/Database_server) by simply restoring data from a backup.

Since a backup system contains at least one copy of all data considered worth saving, the [data storage](https://en.wikipedia.org/wiki/Computer_data_storage) requirements can be significant. Organizing this storage space and managing the backup process can be a complicated undertaking. A data repository model may be used to provide structure to the storage. Nowadays, there are many different types of [data storage devices](https://en.wikipedia.org/wiki/Data_storage_device) that are useful for making backups. There are also many different ways in which these devices can be arranged to provide geographic redundancy, [data security](https://en.wikipedia.org/wiki/Data_security), and portability.

Before data are sent to their storage locations, they are selected, extracted, and manipulated. Many different techniques have been developed to optimize the backup procedure. These include optimizations for dealing with open files and live data sources as well as compression, encryption, and [de-duplication](https://en.wikipedia.org/wiki/Data_deduplication), among others. Every backup scheme should include [dry runs](https://en.wikipedia.org/wiki/Dry_run_%28testing%29) that validate the reliability of the data being backed up. It is important to recognize the limitations and human factors involved in any backup scheme.

**Data Repository Models**

Any backup strategy starts with a concept of a data repository. The backup data needs to be stored, and probably should be organized to a degree. The organisation could be as simple as a sheet of paper with a list of all backup media (CDs etc.) and the dates they were produced. A more sophisticated setup could include a computerized index, catalog, or relational database. Different approaches have different advantages:

**Full Backups:**

A [full backup](http://en.wikipedia.org/wiki/Full_backup) is exactly what the name implies. It is a full copy of your entire data set. Although full backups arguably provide the best protection, most organizations only use them on a periodic basis because they are time consuming, and often require a large number of tapes or disk.



**Incremental Backup:**

Because full backups are so time consuming, [incremental backups](http://searchstoragechannel.techtarget.com/tip/Using-an-incremental-backup-strategy-to-save-your-customers-money) were introduced as a way of decreasing the amount of time that it takes to do a backup. Incremental backups only backup the data that has changed since the previous backup. For example, suppose that you created a full backup on Monday, and used incremental backups for the rest of the week. Tuesday's backup would only contain the data that has changed since Monday. Wednesday's backup would only contain the data that has changed since Tuesday.

The primary disadvantage to incremental backups is that they can be time-consuming to [restore](http://searchstorage.techtarget.com/definition/restore). Going back to my previous example, suppose that you wanted to restore the backup from Wednesday. To do so, you would have to first restore Monday's full backup. After that, you would have to restore Tuesday's tape, followed by Wednesday's. If any of the tapes happen to be missing or damaged, then you will not be able to perform the full restoration.



**Differential Backups:**

A [differential backup](http://www.acronis.com/resource/solutions/backup/2005/incremental-backups.html) is similar to an incremental backup in that it starts with a full backup, and subsequent backups only contain data that has changed. The difference is that while an incremental backup only includes the data that has changed since the previous backup, a differential backup contains all of the data that has changed since the last full backup.

Suppose for example that you wanted to create a full backup on Monday and differential backups for the rest of the week. Tuesday's backup would contain all of the data that has changed since Monday. It would therefore be identical to an incremental backup at this point. On Wednesday, however, the differential backup would backup any data that had changed since Monday.

The advantage that differential backups have over incremental is shorter restore times. Restoring a differential backup never requires more than two tape sets. Incremental backups on the other hand, may require a great number of tape sets. Of course the tradeoff is that as time progresses, a differential backup tape can grow to contain much more data than an incremental backup tape.



# Archieval Storage and Disposal of Data

The following regulations apply to any research approved by the IRB through expedited or full review.  Furthermore, research automatically exempt from review or which received an IRB approved exemption, while not constrained by the following storage and disposal regulations are encouraged to adhere to relevant regulations that protect the confidentiality of research subjects.

Investigators should be cognizant of the fact that any guarantees made to research subjects during the consent process (e.g., limited access to the data, anonymity, confidentiality etc.) remain in force after the study concludes and throughout the data storage process.  It is the investigator’s responsibility to ensure secure storage of the data that maintains these guarantees and to demonstrate to the satisfaction of the IRB that these guarantees are being met throughout the conduct of the study and the data storage period.

**A) STORAGE OF NON-SENSITIVE DATA**

Data is non-sensitive when it has been obtained anonymously from subjects such that no identifiers can link any data to individual subjects (See Note 1 below).  In this case, data storage need only be secure to the extent it can be retrieved easily by the principal investigator in response to a request for ethical review by the IRB Executive Committee.  If stored electronically, the data file must be backed up on an independent storage device.

**B) STORAGE OF SENSITIVE DATA**

Data is sensitive when it contains identifiers that can link any data to individual subjects. In this case, the investigator has a special obligation to maintain more secure data storage that protects the confidentiality of research subjects. When the principal investigator is not a student, sensitive data may be stored on campus or off campus as regulated below.  When the principal investigator is a student, however, sensitive data must be stored on campus by his/her faculty supervisor as regulated below.

* On campus – Hard copies of the data must be stored in a locked cabinet in a locked room. Data must be “de-identified” and the identifiers stored in a separate location.  If stored electronically as well, data must be stored on a password protected hard drive.
* Off campus – Hard copies of the data must be stored in a locked location, under the personal control and supervision of the investigator or to which only the investigator has access.  Data must be “de-identified” and the identifiers stored in a separate location.  If stored electronically as well, the data must be stored on a password protected and encrypted device.

**C) STORAGE DURATION**

Both non-sensitive and sensitive data must be stored for a minimum of three years after the conclusion of the study. Principal investigators and faculty supervisors of student research may extend storage duration beyond the minimum for reasonable cause.  However, research data in either hard copy or electronic form should not be maintained in perpetuity.  The sensitivity of the data and the reasons for maintaining the data should be the primary factors determining the length of retention beyond the minimum.

**D) DISPOSAL OF DATA**

Following the storage period, both non-sensitive and sensitive data must be destroyed in the manner which protects the confidentiality of the research subjects.  Hard copies of the data should be shredded and electronic data files should be deleted from all storage devices including any recycling bins.

**Network Security**

Network security consists of the [policies](https://en.wikipedia.org/wiki/Policies) and practices adopted to prevent and monitor [unauthorized](https://en.wikipedia.org/wiki/Unauthorized) access, misuse, modification, or denial of a [computer network](https://en.wikipedia.org/wiki/Computer_network) and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.  Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

**Firewall:**

A firewall is a network security system designed to prevent unauthorized [access](http://www.webopedia.com/TERM/A/access.html) to or from a private [network](http://www.webopedia.com/TERM/N/network.html). Firewalls can be implemented in both [hardware](http://www.webopedia.com/TERM/H/hardware.html) and [software](http://www.webopedia.com/TERM/S/software.html), or a combination of both.

Network firewalls are frequently used to prevent unauthorized [Internet](http://www.webopedia.com/TERM/I/Internet.html) users from accessing private networks connected to the Internet, especially [intranets](http://www.webopedia.com/TERM/I/intranet.html). All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified [security](http://www.webopedia.com/TERM/S/security.html) criteria.



### Firewall Implementation

The firewall remains a vital component in any network security architecture, and today's organizations have several types to choose from. It's essential that IT professionals [identify the type of firewall](http://searchsecurity.techtarget.com/tip/How-to-choose-a-firewall) that best suits the organization's network security needs. Once selected, one of the key questions that shapes a protection strategy is "Where should the firewall be placed?" There are three common firewall topologies: the bastion host, screened subnet and dual-firewall architectures. Enterprise security depends on choosing the right [firewall topology](http://searchsecurity.techtarget.com/tip/Choosing-the-right-firewall-topology-Bastion-host-screened-subnet-or-dual-firewalls).

The next decision to be made, after the topology chosen, is where to [place individual firewall systems](http://searchsecurity.techtarget.com/tip/Placing-systems-in-a-firewall-topology) in it. At this point, there are several types to consider, such as bastion host, screened subnet and multi-homed firewalls.

Remember that firewall configurations do change quickly and often, so it is difficult to keep on top of routine firewall maintenance tasks. Firewall activity, therefore, must be continuously [audited](http://searchsecurity.techtarget.com/tip/Auditing-firewall-activity) to help keep the network secure from ever-evolving threats.

### Network Layer Firewalls

Network layer firewalls generally make their decisions based on the source address, destination address and [ports](http://searchnetworking.techtarget.com/definition/port) in individual IP packets. A simple [router](http://searchnetworking.techtarget.com/definition/router) is the traditional network layer firewall, since it is not able to make particularly complicated decisions about [what a packet](http://searchnetworking.techtarget.com/definition/packet-filtering) is actually talking to or where it actually came from.

One important distinction many network layer firewalls possess is that they route traffic directly through them, which means in order to use one, you either need to have a validly assigned [IP address](http://searchwindevelopment.techtarget.com/definition/IP-address) block or a private Internet address block. Network layer firewalls tend to be very fast and almost transparent to their users.

### Application Layer Firewalls

[Application layer firewalls](http://searchnetworking.techtarget.com/tip/Application-layer-firewalls-defend-against-attacks-up-the-stack)are hosts that run proxy servers, which permit no traffic directly between networks, and they perform elaborate logging and examination of traffic passing through them. Since proxy applications are simply software running on the firewall, it is a good place to do logging and access control. Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other after having passed through an application that effectively masks the origin of the initiating connection.

However, run-of-the-mill network firewalls can't properly defend applications. As [Michael Cobb](http://searchsecurity.techtarget.com/contributor/Mike-Cobb) explains, [application layer firewalls](http://searchsecurity.techtarget.com/tip/Defending-layer-7-A-look-inside-application-layer-firewalls) offer [Layer 7 security](http://searchsecurity.techtarget.com/video/Balancing-security-and-performance-Protecting-layer-7-on-the-network) on a more granular level, and may even help organizations get more out of existing network devices.

In some cases, having an application in the way may impact performance and make the firewall less transparent. Older application layer firewalls that are still in use are not particularly transparent to end users and may require some user training. However, more modern application layer firewalls are often totally transparent. Application layer firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network layer firewalls.

[Future firewalls](http://searchnetworking.techtarget.com/tip/Set-up-firewalls-for-the-next-generation-What-to-consider) will likely combine some characteristics of network layer firewalls and application layer firewalls. It is likely that network layer firewalls will become increasingly aware of the information going through them, and application layer firewalls have already become more transparent. The end result will be kind of a fast packet-screening system that logs and checks data as it passes through.

### Proxy Firewalls

### [Proxy](http://whatis.techtarget.com/definition/proxy-server) firewalls offer more security than other types of firewalls, but at the expense of speed and functionality, as they can limit which applications the network supports.

Why are they [more secure](http://searchsecurity.techtarget.com/answer/The-benefits-of-application-proxy-firewalls)? Unlike [stateful firewalls](http://searchnetworking.techtarget.com/definition/stateful-inspection%22%20%5Ct%20%22_blank) or application layer firewalls, which allow or block network packets from passing to and from a protected network, traffic does not flow through a proxy. Instead, computers establish a connection to the proxy, which serves as an intermediary, and initiate a new network connection on behalf of the request. This prevents direct connections between systems on either side of the firewall and makes it harder for an attacker to discover where the network is, because they don't receive packets created directly by their target system.

[Proxy firewalls also provide](http://searchsecurity.techtarget.com/answer/Comparing-an-application-proxy-firewall-and-a-gateway-server-firewall) comprehensive, protocol-aware security analysis for the protocols they support. This allows them to make [better security decisions](http://searchsecurity.techtarget.com/essentialguide/Enterprise-firewall-protection-Where-it-stands-where-its-headed) than products that focus purely on packet header information.

**Virtual Private Network**

A remote-access VPN uses a public telecommunication infrastructure like the internet to provide remote users secure access to their organization's network. This is especially important when employees are using a public Wi-Fi hotspot or other avenues to use the internet and connect into their corporate network. A VPN client on the remote user's computer or mobile device connects to a VPN gateway on the organization's network. The gateway typically requires the device to authenticate its identity. Then, it creates a network link back to the device that allows it to reach internal network resources -- e.g., file servers, printers and intranets -- as though it was on that network locally.

A site-to-site VPN uses a gateway device to connect the entire network in one location to the network in another -- usually a small branch connecting to a data center. End-node devices in the remote location do not need VPN clients because the gateway handles the connection. Most site-to-site VPNs connecting over the internet use IPsec. VPNs can also be defined between specific computers, typically servers in separate data centers, when security requirements for their exchanges exceed what the enterprise network can deliver. Increasingly, enterprises also use VPN connections in either remote-access mode or site-to-site mode to connect -- or connect to -- resources in a public infrastructure-as-a-service environment. Newer hybrid-access scenarios put the VPN gateway itself in the cloud, with a secure link from the cloud service provider into the internal network.



**Types of VPN**:-

1. **PPTP VPN**

This is the most common and widely used VPN protocol. They enable authorized remote users to connect to the VPN network using their existing Internet connection and then log on to the VPN using password authentication. They don’t need extra hardware and the features are often available as inexpensive add-on software. PPTP stands for Point-to-Point Tunneling Protocol. The disadvantage of PPTP is that it does not provide encryption and it relies on the PPP (Point-to-Point Protocol) to implement security measures.

1. **Site-to-Site VPN**

Site-to-site is much the same thing as PPTP except there is no “dedicated” line in use. It allows different sites of the same organization, each with its own real network, to connect together to form a VPN. Unlike PPTP, the routing, encryption and decryption is done by the routers on both ends, which could be hardware-based or software-based.

1. **L2TP VPN**

L2TP or Layer to Tunneling Protocol is similar to PPTP, since it also doesn’t provide encryption and it relies on PPP protocol to do this. The difference between PPTP and L2TP is that the latter provides not only data confidentiality but also data integrity. L2TP was developed by Microsoft and Cisco.

1. **IPsec**

Tried and trusted protocol which sets up a tunnel from the remote site into your central site. As the name suggests, it’s designed for IP traffic. IPSec requires expensive, time consuming client installations and this can be considered an important disadvantage.

1. **SSL**

SSL or Secure Socket Layer is a VPN accessible via https over web browser. SSL creates a secure session from your PC browser to the application server you’re accessing. The major advantage of SSL is that it doesn’t need any software installed because it uses the web browser as the client application.

1. **MPLS VPN**

MPLS (Multi-Protocol Label Switching) are no good for remote access for individual users, but for site-to-site connectivity, they’re the most flexible and scalable option. These systems are essentially ISP-tuned VPNs, where two or more sites are connected to form a VPN using the same ISP. An MPLS network isn’t as easy to set up or add to as the others, and hence bound to be more expensive.

1. **Hybrid VPN**

A few companies have managed to combine features of SSL and IPSec & also other types of VPN types. Hybrid VPN servers are able to accept connections from multiple types of VPN clients. They offer higher flexibility at both client and server levels and bound to be expensive.

**Intrusion Detection Systems**

An **intrusion detection system** (**IDS**) is a device or [software application](https://en.wikipedia.org/wiki/Software_application) that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a **security information and event management** (**SIEM**) system. A SIEM system combines outputs from multiple sources, and uses [alarm filtering](https://en.wikipedia.org/wiki/Alarm_filtering) techniques to distinguish malicious activity from false alarms. There is a wide spectrum of IDS, varying from virus scanning software to hierarchical systems that monitor the traffic of an entire backbone network. The most common classification is either in network (NIDS) or host-based (HIDS) intrusion detection systems, in reference to what is monitored by the IDS. A system that monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as [malware](https://en.wikipedia.org/wiki/Malware)) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on [machine learning](https://en.wikipedia.org/wiki/Machine_learning)). Some IDS have the ability to respond to detected intrusions, which are typically referred to as an **intrusion prevention system.**



**Types Of Inrusion Detection Systems**

### Network Intrusion detection systems (NIDS) and Host Intrusion detection systems (HIDS)

Network Intrusion Detection Systems (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

A Host Intrusion Detection Systems (HIDS) and software applications (agents) installed on workstations which are to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host Intrusion detection systems (HIDS) can only monitor the individual workstations on which the agents are installed and it cannot monitor the entire network. Host based IDS systems are used to monitor any intrusion attempts on critical servers.

The drawbacks of Host Intrusion Detection Systems (HIDS) are

• Difficult to analyse the intrusion attempts on multiple computers.

• Host Intrusion Detection Systems (HIDS) can be very difficult to maintain in large networks with different operating systems and configurations

• Host Intrusion Detection Systems (HIDS) can be disabled by attackers after the system is compromised.

### Knowledge-based (Signature-based) IDS and behavior-based (Anomaly-based) IDS

A knowledge-based (Signature-based) Intrusion Detection Systems (IDS) references a database of previous attack signatures and known system vulnerabilities. The meaning of word signature, when we talk about Intrusion Detection Systems (IDS) is recorded evidence of an intrusion or attack. Each intrusion leaves a footprint behind (e.g., nature of data packets, failed attempt to run an application, failed logins, file and folder access etc.). These footprints are called signatures and can be used to identify and prevent the same attacks in the future. Based on these signatures Knowledge-based (Signature-based) IDS identify intrusion attempts.

The disadvantages of Signature-based Intrusion Detection Systems (IDS) are signature database must be continually updated and maintained and Signature-based Intrusion Detection Systems (IDS) may fail to identify a unique attacks.

A Behavior-based (Anomaly-based) Intrusion Detection Systems (IDS) references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

**Access Control**

Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment. In the fields of **access control** is the selective restriction of access to a place or other [resource](https://en.wikipedia.org/wiki/Resource). The act of *accessing* may mean consuming, entering, or using. Permission to access a resource is called [*authorization*](https://en.wikipedia.org/wiki/Authorization). [Locks](https://en.wikipedia.org/wiki/Lock_%28security_device%29) and [login credentials](https://en.wikipedia.org/wiki/Login) are two analogous mechanisms of access control

There are two main types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access limits connections to computer networks, system files and data.

The four main categories of access control are:

* [Mandatory access control](http://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC)
* Discretionary access control
* [Role-based access control](http://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC)
* Rule-based access control

Access control systems perform authorization, identification, [authentication](http://searchsecurity.techtarget.com/definition/authentication), access approval, and accountability of entities through login credentials including [passwords](http://searchsecurity.techtarget.com/definition/password), personal identification numbers (PINs), [biometric](http://searchsecurity.techtarget.com/definition/biometrics) scans, and physical or electronic keys.

**Threat**

In [computer security](https://en.wikipedia.org/wiki/Computer_security) a **threat** is a possible danger that might exploit a [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_%28computing%29) to breach security and therefore cause possible harm.

A threat can be either "[intentional](https://en.wikipedia.org/wiki/Intention)" (i.e. hacking: an individual cracker or a criminal organization) or "[accidental](https://en.wikipedia.org/wiki/Accident)" (e.g. the possibility of a computer malfunctioning, or the possibility of a [natural disaster](https://en.wikipedia.org/wiki/Natural_disaster) such as an [earthquake](https://en.wikipedia.org/wiki/Earthquake), a [fire](https://en.wikipedia.org/wiki/Fire), or a [tornado](https://en.wikipedia.org/wiki/Tornado)) or otherwise a circumstance, capability, action, or event.

Types of threat:

**Viruses**

A computer virus is a [malware](https://en.wikipedia.org/wiki/Malware) that, when executed, [replicates](https://en.wikipedia.org/wiki/Quine_%28computing%29) by reproducing itself or infecting other [programs](https://en.wikipedia.org/wiki/Computer_program) by modifying them. Infecting computer programs can include as well, data [files](https://en.wikipedia.org/wiki/Computer_file), or the [boot sector](https://en.wikipedia.org/wiki/Boot_sector) of the [hard drive](https://en.wikipedia.org/wiki/Hard_disk_drive). When this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as acquisition of [hard disk](https://en.wikipedia.org/wiki/Hard_disk) space or [CPU](https://en.wikipedia.org/wiki/Central_processing_unit) time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, [logging their keystrokes](https://en.wikipedia.org/wiki/Keystroke_logging), or even rendering the computer useless.

**Worms**

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming [bandwidth](https://en.wikipedia.org/wiki/Bandwidth_%28computing%29), whereas viruses almost always corrupt or modify files on a targeted computer. Many worms that have been created are designed only to spread, and do not attempt to change the systems they pass through.

**Trojan Horse**

In [computing](https://en.wikipedia.org/wiki/Computing), Trojan horse, or Trojan, is any [malicious](https://en.wikipedia.org/wiki/Malware) [computer program](https://en.wikipedia.org/wiki/Computer_program) which is used to hack into a computer by misleading users of its true intent. The term is derived from the [Ancient Greek](https://en.wikipedia.org/wiki/Ancient_Greek) story of the [wooden horse](https://en.wikipedia.org/wiki/Trojan_Horse) that was used to help Greek troops invade the city of [Troy](https://en.wikipedia.org/wiki/Troy) by stealth.

Trojans are generally spread by some form of [social engineering](https://en.wikipedia.org/wiki/Social_engineering_%28security%29), for example where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by [drive-by download](https://en.wikipedia.org/wiki/Drive-by_download). Although their payload can be anything, many modern forms act as a [backdoor](https://en.wikipedia.org/wiki/Backdoor_%28computing%29), contacting a controller which can then have unauthorized access to the affected computer.[[6]](https://en.wikipedia.org/wiki/Trojan_horse_%28computing%29#cite_note-6)this infection allows an attacker to access users' personal information such as banking information, passwords, or personal identity (IP address).

Unlike [computer viruses](https://en.wikipedia.org/wiki/Computer_virus) and [worms](https://en.wikipedia.org/wiki/Computer_worm), Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

**Logic Bomb**

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company. Software that is inherently malicious, such as [viruses](https://en.wikipedia.org/wiki/Computer_virus) and [worms](https://en.wikipedia.org/wiki/Computer_worm), often contain logic bombs that execute a certain [payload](https://en.wikipedia.org/wiki/Payload_%28software%29) at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as [Friday the 13th](https://en.wikipedia.org/wiki/Friday_the_13th) or [April Fools' Day](https://en.wikipedia.org/wiki/April_Fools%27_Day). [Trojans](https://en.wikipedia.org/wiki/Trojan_horse_%28computing%29) that activate on certain dates are often called "[time bombs](https://en.wikipedia.org/wiki/Time_bomb_%28software%29)".

**Trapdoors**

Trap doors, also referred to as **backdoors,** are bits of code embedded in programs by the programmer to quickly gain access at a later time, often during the testing or debugging phase. If an unscrupulous programmer purposely leaves this code in or simply forgets to remove it, a potential security hole is introduced. Hackers often plant a backdoor on previously compromised systems to gain later access. Trap doors can be almost impossible to remove in a reliable manner. Often, reformatting the system is the only sure way.

**Spoofs**

A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypasses access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. In the context of [network security](https://en.wikipedia.org/wiki/Network_security), a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.

**E-mail viruses**

An e-mail virus is computer code sent to you as an [e-mail](http://searchmobilecomputing.techtarget.com/definition/e-mail) note attachment which, if activated, will cause some unexpected and usually harmful effect, such as destroying certain files on your hard disk and causing the attachment to be remailed to everyone in your address book. Although not the only kind of computer [virus](http://searchsecurity.techtarget.com/definition/virus), e-mail viruses are the best known and undoubtedly cause the greatest loss of time and money overall. The best two defenses against e-mail viruses for the individual user are:

1. a policy of never opening (for example, double-clicking on) an e-mail attachment unless you know who sent it and what the attachment contains, and
2. installing and using [anti-virus software](http://searchsecurity.techtarget.com/definition/antivirus-software) to scan any attachment before you open it.

**Macro Viruses**

In [computing](https://en.wikipedia.org/wiki/Computing) terminology, a macro virus is a [virus](https://en.wikipedia.org/wiki/Computer_virus) that is written in a [macro](https://en.wikipedia.org/wiki/Macro_%28computer_science%29) [language](https://en.wikipedia.org/wiki/Programming_language): a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as [Microsoft Office](https://en.wikipedia.org/wiki/Microsoft_Office), allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread. This is one reason it can be dangerous to open unexpected [attachments](https://en.wikipedia.org/wiki/E-mail_attachment) in [e-mails](https://en.wikipedia.org/wiki/E-mail). Many [antivirus programs](https://en.wikipedia.org/wiki/Antivirus_software) can detect macro viruses, however they are still difficult to detect.

A macro virus is a computer [virus](http://searchsecurity.techtarget.com/definition/virus) that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. Macro viruses tend to be surprising but relatively harmless. A typical effect is the undesired insertion of some comic text at certain points when writing a line. A macro virus is often spread as an e-mail virus.

**Malicious Software**

Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware and rootkits, etc., which steal protected data, delete documents or add software not approved by a user.

Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. The malware propagation concerns parasitic software fragments that attach themselves to some existing executable content. The fragment may be machine code that infects some existing application, utility, or system program, or even the code used to boot a computer system. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency.

**Denial Of service (DoS)**

A denial of service (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems attack a single target. A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended [users](https://en.wikipedia.org/wiki/User_%28computing%29), such as to temporarily or indefinitely interrupt or suspend [services](https://en.wikipedia.org/wiki/Network_service) of a [host](https://en.wikipedia.org/wiki/Host_%28network%29) connected to the [Internet](https://en.wikipedia.org/wiki/Internet). Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

**Security threats to e-commerce**

There are many threats to e-commerece security, such as acts of human error or failure, forces of nature, deliberate acts of theft or extortion, etc. Because technology and the internet at that are still such a new phenomenon there are many issues with websites and there is still no way to make your e-commerce site completely secure without certain threats. With technology continually changing and new e-commerce sites entering the market using new and improved technology. Other e-commerce sites are always looking for a way to improve and become better than the next, creating a competitive environment. With all this continuous change, this makes it hard to continually keep the current threats away while also staying relevant, keeping employees up to date and trained, keeping cost down, etc.

Five security threats:

## 1. Password Breaches

For starters, make every password in your web hosting system distinct from the others. There should be no repetition of words or phrases at all. Secondly, use lengthy, high entropy words and phrases that even password cracking software can’t break. Your most ideal solution for DIY passwords is to use a passphrase of multiple random words and a couple of numbers in between them. To gauge its strength, you can try this [little tool](https://howsecureismypassword.net/).

Another major security procedure you can follow is to use the two factor authentication systems of major web hosts and data services providers which are sustaining your online business and protect your data in a way that offers an enormous security boost over regular password based login attempts.

## 2. DDOS Attacks

Distributed Denial of Service attacks are a major staple of the internet hackers world. The hijacking of your hosting servers for the sake of crashing them completely or using them to target yet another series of hosting servers is practiced by major online hacking organizations such as Anonymous and by minor criminal hackers with access to smart resources.

In either case, if your servers suffer a DDOS attack, you’re looking at some serious downtime as you try to get your site up and running again and the risk of having the DDOS attack happen again and again in the future.

## 3. RansomWare

One of the latest digital threats to rear its ugly little head in the online landscape, Ransomware, does exactly what its name implies. It hijacks either your actual computer hard drive, or more rarely, your website servers and all the data they contain – and then threatens to erase all of your valuable data within a certain period of time unless you pay a certain amount of money to have free that info again.

## 4. Data Destruction

Right up there with the hijacking of your data and the crushing of your e-commerce website under a torrent of traffic pings, there is the destruction of all your data by hackers who enjoy causing havoc or by some irresponsible accidental action by one of your employees or even you yourself.

Data erasure, whether by accident or on purpose is one of the biggest sources of headaches in a lot of online business websites that handle large volumes of customer information. Usually, the cause of such a breach is negligence by someone working in the company; most of the time, the simplest solution is to have regular and well organized backups of all your data done. This way, an accidental annihilation of information can be quickly remedied by copying again from a backed-up copy.

## 5. Fraud

Finally we get down to fraud, the most common type of digital security threat most small online businesses are going to face in 2014, just like they did in 2013. Fraud costs small businesses in the U.S. nearly 4 billion dollars per year and affects as many as 2 percent of all online sales transactions, meaning that you are extremely likely to suffer a case or two unless you protect yourself robustly.

**Electronic Payment System**

An e-commerce payment system facilitates the acceptance of [electronic payment](https://en.wikipedia.org/wiki/Electronic_payment) for [online transactions](https://en.wikipedia.org/wiki/E-commerce). Also known as a sample of [Electronic Data Interchange](https://en.wikipedia.org/wiki/Electronic_Data_Interchange) (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking.

Over the years, [credit cards](https://en.wikipedia.org/wiki/Credit_card) have become one of the most common forms of payment for e-commerce transactions. In North America almost 90% of online retail transactions were made with this payment type. Increased security measures include use of the [card verification number (CVN)](https://en.wikipedia.org/wiki/Card_Verification_Number) which detects fraud by comparing the verification number printed on the signature strip on the back of the card with the information on file with the cardholder's issuing bank. Also online merchants have to comply with stringent rules stipulated by the credit and debit card issuers ([Visa](https://en.wikipedia.org/wiki/Visa_Inc.) and [MasterCard](https://en.wikipedia.org/wiki/MasterCard)) this means that merchants must have security protocol and procedures in place to ensure transactions are more secure. This can also include having a certificate from an authorized [certification authority (CA)](https://en.wikipedia.org/wiki/Certification_Authority) who provides [PKI (Public-Key infrastructure)](https://en.wikipedia.org/wiki/Public-key_infrastructure) for securing credit and debit card transactions.

**E-cash**

An anonymous electronic cash system; equivalent to "cash" or "printed bank notes" except that it is transferred through networks with bits of information, in essence it is just another representation of monetary value; anonymity is preserved through public key cryptography, digital signatures, and blind signatures.

### How it is used:

E-cash is used over the Internet, email, or personal computer to other workstations in the form of secured payments of "cash" that is virtually untraceable to the user. It is backed by real currency from real banks.

The way e-cash works is similar to that of electronic fund transfers done between banks. The user first must have an e-cash software program and an e-cash bank account from which e-cash can be withdrawn or deposited. The user withdraws the e-cash from the account onto her computer and spends it in the Internet without being traced or having personal information available to other parties that are involved in the process. The recipients of the e-cash send the money to their bank account as with depositing "real" cash.

Other than making purchases on the Internet, e-cash can also be found used in entertainment sites - on "gambling tables" in Internet casinos such as [PAF Casino](http://www.pafcasino.fi/) and [Internet Casino](http://www.casino.org/). E-cash allows the exchange of money to be conducted in the same way as in real casinos.

**Credit Card**

A credit card is a [payment card](https://en.wikipedia.org/wiki/Payment_card) issued to users (cardholders) as a method of [payment](https://en.wikipedia.org/wiki/Payment). It allows the cardholder to pay for [goods and services](https://en.wikipedia.org/wiki/Goods_and_services) based on the holder's promise to pay for them. The [issuer](https://en.wikipedia.org/wiki/Credit_card_issuer) of the card (usually a bank) creates a [revolving account](https://en.wikipedia.org/wiki/Revolving_account) and grants a [line of credit](https://en.wikipedia.org/wiki/Line_of_credit) to the cardholder, from which the cardholder can borrow money for payment to a [merchant](https://en.wikipedia.org/wiki/Merchant) or as a [cash advance](https://en.wikipedia.org/wiki/Cash_advance).

A credit card is different from a [charge card](https://en.wikipedia.org/wiki/Charge_card), where it requires the balance to be repaid in full each month.[[2]](https://en.wikipedia.org/wiki/Credit_card#cite_note-2) In contrast, credit cards allow the consumers a continuing balance of debt, subject to [interest](https://en.wikipedia.org/wiki/Credit_card_interest) being charged. A credit card also differs from a [cash card](https://en.wikipedia.org/wiki/Cash_card), which can be used like currency by the owner of the card. A credit card differs from a charge card also in that a credit card typically involves a third-party entity that pays the seller and is reimbursed by the buyer, whereas a charge card simply defers payment by the buyer until a later date.

**Debit Card**

A debit card (also known as a bank card or check card) is a [plastic](https://en.wikipedia.org/wiki/ISO/IEC_7812) [payment card](https://en.wikipedia.org/wiki/Payment_card) that can be used instead of [cash](https://en.wikipedia.org/wiki/Cash) when making purchases. It is similar to a [credit card](https://en.wikipedia.org/wiki/Credit_card), but unlike a credit card, the money comes directly from the user's bank account when using a debit card. Some cards may bear a [stored value](https://en.wikipedia.org/wiki/Stored-value_card) with which a payment is made, while most relay a message to the cardholder's bank to withdraw funds from a payer's designated bank account. In some cases, the [primary account number](https://en.wikipedia.org/wiki/Primary_account_number) is assigned exclusively for use on the Internet and there is no physical card. Debit cards usually also allow for instant withdrawal of cash, acting as the [ATM card](https://en.wikipedia.org/wiki/ATM_card) for withdrawing cash. Merchants may also offer [cash back](https://en.wikipedia.org/wiki/Debit_card_cashback) facilities to customers, where a customer can withdraw cash along with their purchase.

**Digital Signature**

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message ([authentication](https://en.wikipedia.org/wiki/Authentication) and [non-repudiation](https://en.wikipedia.org/wiki/Non-repudiation)), and that the message was not altered in transit ([integrity](https://en.wikipedia.org/wiki/Data_integrity)).

Digital signatures are a standard element of most [cryptographic protocol](https://en.wikipedia.org/wiki/Cryptographic_protocol) suites, and are commonly used for software distribution, financial transactions, contract, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to implement [electronic signatures](https://en.wikipedia.org/wiki/Electronic_signature), a broader term that refers to any electronic data that carries the intent of a signature,  but not all electronic signatures use digital signatures.

Digital signatures employ [asymmetric cryptography](https://en.wikipedia.org/wiki/Asymmetric_key_algorithm). In many instances they provide a layer of validation and security to messages sent through a nonsecure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital seals and signatures are equivalent to handwritten signatures and stamped seals. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide [non-repudiation](https://en.wikipedia.org/wiki/Non-repudiation), meaning that the signer cannot successfully claim they did not sign a message, while also claiming their [private key](https://en.wikipedia.org/wiki/Private_key) remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a [bit string](https://en.wikipedia.org/wiki/Bitstring): examples include [electronic mail](https://en.wikipedia.org/wiki/Electronic_mail), [contracts](https://en.wikipedia.org/wiki/Contract), or a message sent via some other [cryptographic protocol](https://en.wikipedia.org/wiki/Cryptographic_protocol).



**Public Key Cryptography**

Public-key cryptography, or asymmetric cryptography, is any cryptographic system that uses pairs of [keys](https://en.wikipedia.org/wiki/Cryptographic_key): *public keys* that may be disseminated widely paired with *private keys* which are known only to the owner. There are two functions that can be achieved: using a public key to authenticate that a message originated with a holder of the paired private key; or encrypting a message with a public key to ensure that only the holder of the paired private key can decrypt it.

In a public-key encryption system, any person can encrypt a message using the public key of the receiver, but such a message can be decrypted only with the receiver's private key. For this to work it must be computationally easy for a user to generate a public and private key-pair to be used for encryption and decryption. The strength of a public-key cryptography system relies on the degree of difficulty (computational impracticality) for a properly generated private key to be determined from its corresponding public key. Security then depends only on keeping the private key private, and the public key may be published without compromising security.

Because of the computational complexity of asymmetric encryption, it is usually used only for small blocks of data, typically the transfer of a symmetric encryption key (e.g. a [session key](https://en.wikipedia.org/wiki/Session_key)). This symmetric key is then used to encrypt the rest of the potentially long message sequence. The symmetric encryption/decryption is based on simpler algorithms and is much faster.

Message authentication involves [hashing](https://en.wikipedia.org/wiki/Cryptographic_hash_function) the message to produce a "digest," and encrypting the digest with the private key to produce a [digital signature](https://en.wikipedia.org/wiki/Digital_signature). Thereafter anyone can verify this signature by:

1. computing the hash of the message
2. decrypting the signature with the signer's public key
3. comparing the computed digest with the decrypted digest

