Certified Software Security
Sample Material
VS-1086

1. SECURITY CONCEPTS

Security consists of the measures and policies to prevent and monitor unauthorized access, misuse, modification, or denial of a computer resources.

Security is usually implemented by authenticated user name and password, which is something the user 'knows' and called one-factor authentication. With two-factor authentication, something the user 'has' is used (like a security token or 'dongle', an ATM card, or a mobile phone) and with three-factor authentication, something the user 'is' is also used (like fingerprint or retinal scan).

1.1. Digital Asset

A digital asset, in essence, is anything that exists in a binary format and comes with the right to use. Data that do not possess that right are not considered assets. Digital assets include but are not exclusive to: digital documents, audible content, motion picture, and other relevant digital data that are currently in circulation or are, or will be stored on digital appliances such as: personal computers, laptops, portable media players, tablets, storage devices, telecommunication devices, and any and all apparatuses which are, or will be in existence once technology progresses to accommodate for the conception of new modalities which would be able to carry digital assets; notwithstanding the proprietorship of the physical device onto which the digital asset is located.

Types of digital assets include, but are not exclusive to: photography, logos, illustrations, animations, audiovisual media, presentations, spreadsheets, word documents, electronic mails, and a multitude of other digital formats and their respective metadata. The number of different types of digital assets is exponentially increasing due to the rising number of devices that are a conduit for digital media, e.g., smartphones. Due to this steadfast growth of software applications and immense diversity of user touchpoints covering a wide span of devices, our view of the total digital assets universe is growing. In Intel's presentation at the company's "Intel Developer Forum 2013" they named several new types of digital assets including: medical, education, voting, friendships, conversations and reputation amongst others. In 2015, Forbes and other sources characterized bitcoin as a digital asset.

There are 3 key elements that make any single file a digital asset. A digital asset must:

- ✓ Be a digital file
- ✓ Provide value to the company
- ✓ Be searchable and discoverable (usually with metadata)

Metadata

Metadata means data about data. In this regard, data refers to the asset you are dealing with, for instance an image. Metadata is important because it allows users to manage assets more efficiently.

Metadata is the collection of all the data available for this image, but that is not necessarily contained in that image, for instance:

- ✓ the name of the asset
- ✓ the time and date it was last modified
- ✓ the size of the image as it was stored in the repository
- ✓ the name of the folder it is contained in

These are the basic metadata properties to manage for assets, which allow users to see all assets, for example, ordered by their last modification date - useful when trying to discover what assets have recently been added to the repository.

You can add more high-level data to digital assets, for example:

- ✓ the type of asset (is it an image, a video, an audio clip or a document?)
- ✓ the owner of the asset
- ✓ the title of the asset
- ✓ the description of the asset
- ✓ the tags that have been assigned to an asset

More metadata helps you further categorize assets and is helpful as the amount of digital information grows. While it is possible for a single person to manage a list of a few hundred files simply based on their file names, this approach falls short when the number of people involved and the number of assets managed grows.

As metadata is added to assets, the value of the asset grows, because the asset becomes

- ✓ more accessible - people can find it much easier
- ✓ easier to manage - you can find assets with the same set of properties easier and apply changes to them
- ✓ more complex - the more metadata you have added to an asset, the more important managing metadata becomes

There are two basic types of metadata:

- ✓ Technical metadata - Technical metadata is useful for software applications that are dealing with digital assets and should not be maintained manually. The available technical metadata of an asset depends largely on the file type of the asset.
- ✓ Descriptive metadata - Descriptive metadata is metadata concerned with the application domain, for example, the business that an asset is coming from. Descriptive metadata cannot be determined automatically. It has to be created manually or semi-automatically. For instance, a GPS-enabled camera can automatically track the latitude and longitude an image was taken at and add this information to the image's metadata.

Data at Use and Rest

Data at rest in information technology means inactive data that is stored physically in any digital form (e.g. databases, data warehouses, spreadsheets, archives, tapes, off-site backups, mobile devices etc.).

There is some disagreement as to the boundary between data at rest and data in use. Data at rest generally refers to data stored in persistent storage (disk, tape) while data in use generally refers to data being processed by a computer central processing unit (CPU) or in random access memory (RAM, also referred to as main memory or simply memory). Definitions include:
"...all data in computer storage while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated."

Data in use has also been taken to mean "active data" in the context of being in a database or being manipulated by an application. For example, some enterprise encryption gateway solutions for the cloud claim to encrypt data at rest, data in transit and data in use.

While it is generally accepted that archive data (i.e. which never changes), regardless of its storage medium, is data at rest and active data subject to constant or frequent change is data in use, "inactive data" could be taken to mean data which may change, but infrequently. The imprecise nature of terms such as "constant" and "frequent" means that some stored data cannot be comprehensively defined as either data at rest or in use. These definitions could be taken to assume that Data at Rest is a superset of data in use; however, data in use, subject to frequent change, has distinct processing requirements from data at rest, whether completely static or subject to occasional change.

The division of data at rest into the sub-categories "static" and "inconstant" addresses this distinction

Because of its nature data at rest is of increasing concern to businesses, government agencies and other institutions. Mobile devices are often subject to specific security protocols to protect data at rest from unauthorised access when lost or stolen and there is an increasing recognition that database management systems and file servers should also be considered as at risk; the longer data is left unused in storage, the more likely it might be retrieved by unauthorized individuals outside the network.

- ✓ Encryption - Data encryption, which prevents data visibility in the event of its unauthorized access or theft, is commonly used to protect data in motion and increasingly promoted for protecting data at rest. The encryption of data at rest should only include strong encryption methods such as AES or RSA. Encrypted data should remain encrypted when access controls such as usernames and password fail. Increasing encryption on multiple levels is recommended. Cryptography can be implemented on the database housing the data and on the physical storage where the databases are stored. Data encryption keys should be updated on a regular basis. Encryption keys should be stored separately from the data. Encryption also enables crypto-shredding at the end of the data or hardware lifecycle. Periodic auditing of sensitive data should be part of policy and should occur on scheduled occurrences. Finally, only store the minimum possible amount of sensitive data.
- ✓ Tokenization - Tokenization is a non-mathematical approach to protecting data at rest that replaces sensitive data with non-sensitive substitutes, referred to as tokens, which have no extrinsic or exploitable meaning or value. This process does not alter the type or length of data, which means it, can be processed by legacy systems such as databases

that may be sensitive to data length and type. Tokens require significantly less computational resources to process and less storage space in databases than traditionally encrypted data. This is achieved by keeping specific data fully or partially visible for processing and analytics while sensitive information is kept hidden. Lower processing and storage requirements makes tokenization an ideal method of securing data at rest in systems that manage large volumes of data.

- ✓ Federation - A further method of preventing unwanted access to data at rest is the use of data federation especially when data is distributed globally (e.g. in off-shore archives). An example of this would be a European organisation which stores its archived data off-site in the USA. Under the terms of the USA PATRIOT Act the American authorities can demand access to all data physically stored within its boundaries, even if it includes personal information on European citizens with no connections to the USA. Data encryption alone cannot be used to prevent this as the authorities have the right to demand decrypted information. A data federation policy which retained personal citizen information with no foreign connections within its country of origin (separate from information which is either not personal or is relevant to off-shore authorities) is one option to address this concern.

1.2. Security Principles

All information security measures try to address at least one of three goals:

- ✓ Protect the confidentiality of data
- ✓ Preserve the integrity of data
- ✓ Promote the availability of data for authorized use

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs. Information security professionals who create policies and procedures (often referred to as governance models) must consider each goal when creating a plan to protect a computer system.

The CIA Triad

The CIA triad of confidentiality, integrity, and availability is at the heart of information security. There is continuous debate about extending this classic trio. Other principles such as Accountability have sometimes been proposed for addition – it has been pointed out that issues such as Non-Repudiation do not fit well within the three core concepts.

In 1992 and revised in 2002, the OECD's Guidelines for the Security of Information Systems and Networks proposed the nine generally accepted principles: Awareness, Responsibility, Response, Ethics, Democracy, Risk Assessment, Security Design and Implementation, Security Management, and Reassessment. Building upon those, in 2004 the NIST's Engineering Principles for Information Technology Security proposed 33 principles. From each of these derived guidelines and practices.
In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

In 2013, based on a thorough analysis of Information Assurance and Security (IAS) literature, the IAS-octave was proposed as an extension of the CIA-triad. The IAS-octave includes Confidentiality, Integrity, Availability, Accountability, Auditability, Authenticity/Trustworthiness, Non-repudiation and Privacy. The completeness and accuracy of the IAS-octave was evaluated via a series of interviews with IAS academics and experts. The IAS-octave is one of the dimensions of a Reference Model of Information Assurance and Security (RMIAS), which summarizes the IAS knowledge in one all-encompassing model.

Confidentiality - In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes" (Excerpt ISO27000).

Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories.

Sometimes safeguarding data confidentiality may involve special training for those privy to such documents. Such training would typically include security risks that could threaten this information. Training can help familiarize authorized people with risk factors and how to guard against them. Further aspects of training can include strong passwords and password-related best practices and information about social engineering methods, to prevent them from bending data-handling rules with good intentions and potentially disastrous results.

A good example of methods used to ensure confidentiality is an account number or routing number when banking online. Data encryption is a method of ensuring confidentiality. User IDs and passwords constitute a standard procedure; two-factor authentication is

becoming the norm. Other options include biometric verification and security tokens, key fobs or soft tokens. Users can also take precautions to minimize the number of places where the information appears and the number of times it is actually transmitted to complete a required transaction. Extra measures may be taken for sensitive documents, precautions such as storing only on air gapped computers, disconnected storage devices or, for highly sensitive information, in hard copy form only.

Integrity - Data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity in addition to data confidentiality.

Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls. Version control maybe used to prevent erroneous changes or accidental deletion by authorized users becoming a problem. In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. Some data might include checksums, even cryptographic checksums, for verification of integrity. Backups or redundancies must be available to restore the affected data to its correct state.

Integrity models keep data pure and trustworthy by protecting system data from intentional or accidental changes. Integrity models have three goals:

- ✓ Prevent unauthorized users from making modifications to data or programs
- ✓ Prevent authorized users from making improper or unauthorized modifications
- ✓ Maintain internal and external consistency of data and programs

An example of integrity checks is balancing a batch of transactions to make sure that all the information is present and accurately accounted for.

Availability - For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It's also important to keep current with all necessary system upgrades. Providing adequate communication bandwidth and preventing

the occurrence of bottlenecks are equally important. Redundancy, failover, RAID even high-availability clusters can mitigate serious consequences when hardware issues do occur. Fast and adaptive disaster recovery is essential for the worst case scenarios; that capacity is reliant on the existence of a comprehensive disaster recovery plan (DRP). Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire. To prevent data loss from such occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe. Extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to malicious actions such as denial-of-service (DoS) attacks and network intrusions.

Availability models keep data and resources available for authorized use, especially during emergencies or disasters. Information security professionals usually address three common challenges to availability:

- ✓ Denial of service (DoS) due to intentional attacks or because of undiscovered flaws in implementation (for example, a program written by a programmer who is unaware of a flaw that could crash the program if a certain unexpected input is encountered)
- ✓ Loss of information system capabilities because of natural disasters (fires, floods, storms, or earthquakes) or human actions (bombs or strikes)
- ✓ Equipment failures during normal use

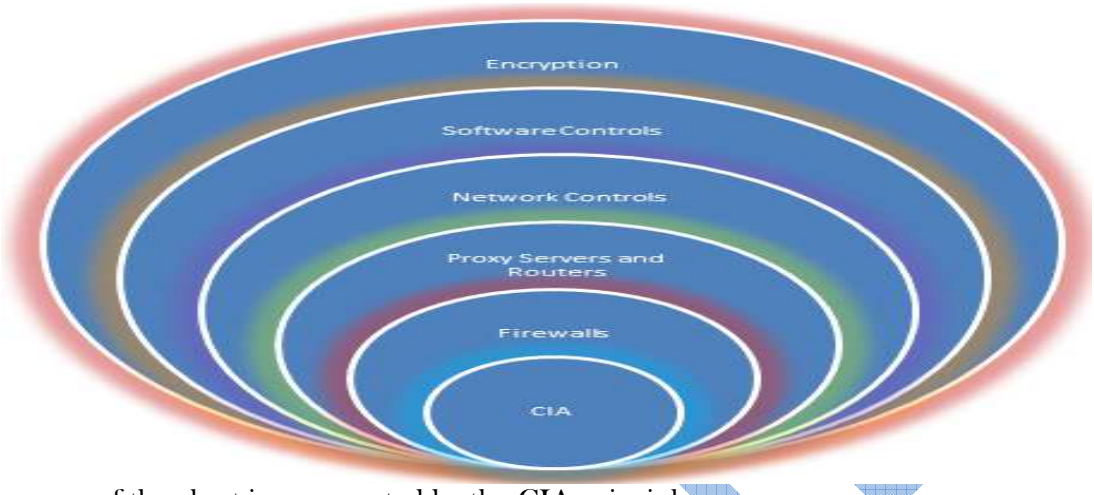
Some activities that preserve confidentiality, integrity, and/or availability are granting access only to authorized personnel, applying encryption to information that will be sent over the Internet or stored on digital media, periodically testing computer system security to uncover new vulnerabilities, building software defensively, and developing a disaster recovery plan to ensure that the business can continue to exist in the event of a disaster or loss of access by personnel.

Non-repudiation - In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. Note: This is also regarded as part of Integrity.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

Methods for abiding by the CIA principles.

Below is an illustration of the top five layers that information security offers in terms of attaining the goals laid out in the CIA triad. It is presented in order to reveal the most commonly used manners of safeguarding the CIA principles and defending any system from a potential data breach.



The core of the chart is represented by the CIA principles

- ✓ Firewalls can be hardware-based and software-based. Firewalls are a piece of equipment or software that are designed to block unsolicited connections, protocols, unwanted network activity and block spam and other malicious requests while you are connected a third-party network (usually the Internet). The hardware firewall utilizes packet filtering to examine the header of a packet and decide if the packet should be forwarded or dropped. Firewalls serve as an intermediary between your computer and the Internet connection. Thus, firewalls can block connections that their user did not wish to make, filter out bad data and prevent outside endeavors to gain control or access to your machine. They have a set of predefined rules that enable them to allow, deny or drop connections and as such their function is of a filtering gateway.
- ✓ A server, through hardware such as proxy server can regulate what the external world sees of the network, this could be a type of protection by providing a "smoke screen" on the network. It can disguise the real network and display a minimal connection to the Internet
- ✓ Routers, another piece of hardware, can regulate access to the network, just like firewalls, it may have access lists that allow or deny access into the network. Nonetheless, they route IP packets to the other networks, a thing which is neither performed by firewalls, nor by any other appliance on the network or the Internet.
- ✓ Network controls are implemented at local level, they involve authentication like logins and passwords.
- ✓ Software controls are software that prevent malware from penetrating the machines. Should a malware infest the system, software controls are in charge of removing the infection and returning the system to the pre-infestation state. Unlike firewalls, software controls can remove existent malware, malware that has already affected the machine, whereas firewalls cannot deal with malware that has already been loaded on your computer.
- ✓ Encryption of data

Certifications

Accounting, Banking & Finance
- Certified GST Professional
- Certified AML-KYC Compliance Officer
- Certified Business Accountant
- Certified BASEL III Professional
- Certified GAAP Accounting Standards Professional
- Certified Treasury Markets Professional

Big Data
- Certified Hadoop and Mapreduce Professional

Cloud Computing
- Certified Cloud Computing Professional

Design
- Certified Interior Designer

Digital Media
- Certified Social Media Marketing Professional
- Certified Inbound Marketing Professional
- Certified Digital Marketing Professional

Foreign Trade
- Certified Export Import (Foreign Trade) Professional

Health, Nutrition and Well Being
- Certified Fitness Instructor

Hospitality
- Certified Restaurant Team Member (Hospitality)

Human Resources
- Certified HR Compensation Manager
- Certified HR Staffing Manager
- Certified Human Resources Manager
- Certified Performance Appraisal Manager

Office Skills
- Certified Data Entry Operator
- Certified Office Administrator

Project Management
- Certified Master in Project Management
- Certified Scrum Specialist

Real Estate
- Certified Real Estate Consultant

Marketing
- Certified Marketing Manager

Quality
- Certified Six Sigma Green Belt Professional
- Certified Six Sigma Black Belt Professional
- Certified TQM Professional

Logistics & Supply Chain Management
- Certified International Logistics Professional
- Certified Logistics & SCM Professional
- Certified Supply Chain Management Professional

Legal
- Certified IPR & Legal Manager
- Certified Labour Law Analyst
- Certified Business Law Analyst
- Certified Corporate Law Analyst

Information Technology
- Certified Angular JS Professional
- Certified Basic Network Support Professional
- Certified Business Intelligence Professional
- Certified Core Java Developer
- Certified E-commerce Professional
- Certified IT Support Professional
- Certified PHP Professional
- Certified Selenium Professional

Mobile Application Development
- Certified Android Apps Developer
- Certified iPhone Apps Developer

Security
- Certified Ethical Hacking and Security Professional
- Certified Network Security Professional

Management
- Certified Corporate Governance Professional
- Certified Corporate Social Responsibility Professional
- Certified Leadership Skills Professional

Life Skills
- Certified Business Communication Specialist
- Certified Public Relations Officer

Media
- Certified Advertising Manager
- Certified Advertising Sales Professional

Sales, BPO
- Certified Sales Manager
- Certified Telesales Executive

& many more job related certifications

Contact us at:
V-Skills
011-473 44 723 or info@vskills.in
www.vskills.in