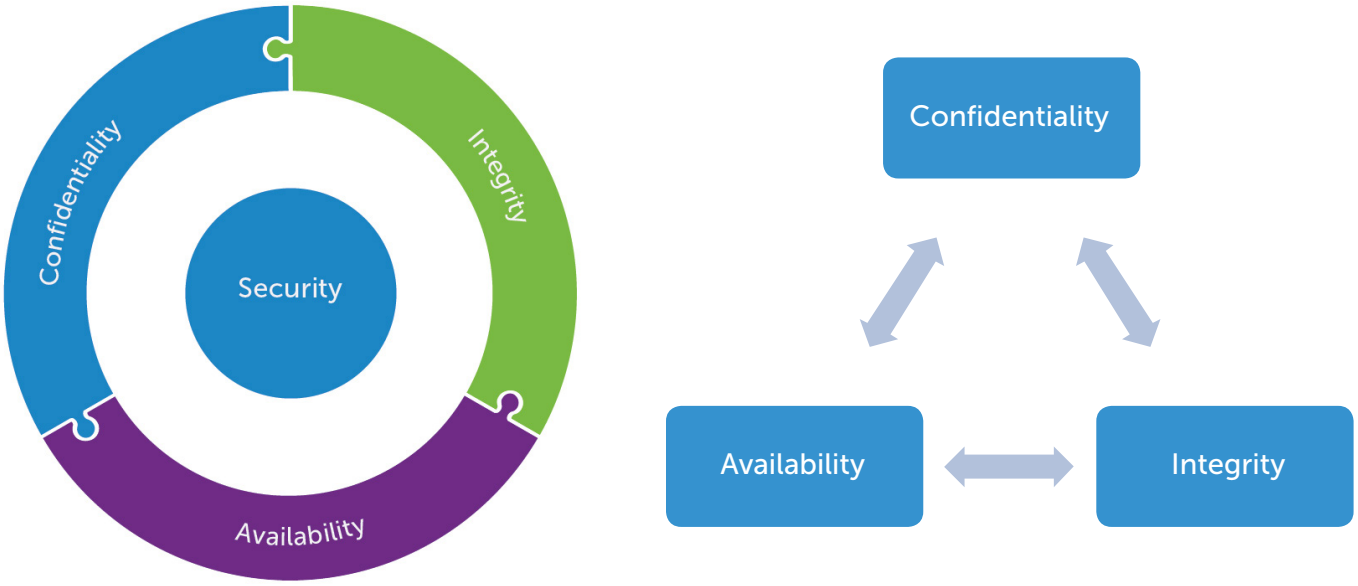
Selecting a framework – the CIA Triad

The CIA Triad of Information Security is the logical concept for planning and implementing robust security solutions. The pillars of the CIA Triad provide a significant foundation of security in an information system. The decisions and implementations of each of these pillars will impact the overall security posture. Pillars are incremental so an increase or decrease in implementation of a given pillar will have a cumulative effect.

The CIA Triad includes the following three pillars of security:



Confidentiality

Confidentiality is the property which ensures that data is not made available to unauthorized individuals, entities or programs. Methods of increased confidentiality include challenge response authentication and certificate signature verification processes.

A robust confidentiality system implements proper access control mechanisms and secure authentication methods to properly obtain and evaluate credentials to be evaluated.

Integrity

Integrity is the property of information security which ensures that the accuracy and completeness of data is maintained secured throughout the lifecycle of the data. Integrity maintains protection of the data from origination, evaluation, storage and transfer. Methods of increased integrity include encrypted hard drives (should this read: physical or secure physical ex. CV or SED storage??), virtualization methods and transport encryption.

Integrity implementation systems rely on reliable authentication systems to ensure that data is properly and securely evaluated and processed.

Availability

Availability is the final property of the Information Security Triad which ensures that the data and security ecosystem is fully available when it is needed. Security systems must be available to be exercised and evaluated against. Availability protections focus on ensuring that denial of service attacks and similar methods are adequately protected against.

Authentication implementation within the CIA Triad

Authentication is a key component to enable Confidentiality within the CIA Triad. A robust and secure authentication system will ensure that the data and access being requested will only be released to a verified user. Advanced authentication can influence the integrity of the security posture due to the secure evaluation of a user's credential and access to stored credentials which are needed for verification.

Identification vs. Authentication vs. Authorization

- **Authorization** is the process of providing to the user access to the resource requested.
    - Authentication is required before authorization
- **Authentication** is the process of verifying the credentials used to request access to a resource.
    - Identification is required before authentication.
- **Identification** is the process of identifying the entity which is going to be requesting authentication.
    - Identification must occur before any authentication or authorization attempts can occur.

Methods for user identification

User Authentication and Authorization Methods

- **What you know?** Requires on the knowledge of data to be verified. Passcode, password, PIN are all examples of **"what you know"**.
- **What you have?** Requires a token to be presented to be verified. Smartcard, Bluetooth device, etc. are examples of **"what you have"** authentication methods.
- **Who you are?** Requires a verification of the user by a biometric factor. Fingerprint, Iris, facial, voice, etc. are examples of **"who you are"** factors.

The following are additional methods to authenticate and provide input to additional authorization routines. These factors are routinely used for enhanced verification for releasing secure data and are used in conjunction with the **"what you know"**, **"what you have"** and **"who you are"** factors.

- **Where you are** – factors verify the location of the user. GPS, Connected Network, etc.
    - Where you are factors are not used for identification but are used for authorization of resource usage after user authentication.
- **What you do** – Factors analyze the behavior of a user and determines if that behavior is indicative of the user. Typing behavior, touchpad behavior, etc.
- **Are you there** – A factor of authentication which detects the physical presence of a user for determination of retained access.

Secure Provisioning factors

The security of a user authentication system requires a secure method for user credentials to be obtained and deployed for future evaluation. Without trusted acquisition of reference credentials, the entire security posture of a system can be compromised.

Some examples of secure provisioning environments include:

- Segregated central enrollment stations
    - User performs all enrollment at a dedicated station at company's HR department. This implementation allows security by physical presence at a trusted site.
- Process secured operating environments
    - Trusted execution environments on a client system. This implementation allows for security based on only running provisioning applications within a secured environment.
- Time based authentication factors
    - OTP password delivered in multiple operating modes. This implementation focuses on a trusted secondary band of communication to the customer to provide information to the user.

Secure Credential Evaluation factors

After credentials are securely acquired, they must be evaluated and stored in a trusted manner to ensure confidentiality and protect against runtime attacks.

- Hardware segregated evaluation environments
    - Hardware segregation environments allow for credential evaluation and comparison operations to occur in a separate operating space to ensure evaluation is not compromised. Examples include hardware security modules (HSM) and match on chip fingerprint readers.
- Software segregation
    - Software segregation concepts focus on ensuring that data being accessed and evaluated are only performed within the confines of a software component that has the right to know and view the data.
- Virtualized segregated environments.
    - Virtualized environments provide operating segregation by using platform capabilities to perform evaluations on a single processor and memory space that is logically segregated from the main processing unit.

Primary vs. Secondary Authentication Factors

- **Primary factors** are those factors which can be used for authentication by themselves.
    - Examples include: password, fingerprint, smartcard
- **Secondary factors** are those factors which require additional factors to be presented to ensure that authentication is reliable and secure.
    - Examples include: location, physical presence, etc.
- The determination if an authentication factor is primary or secondary is the responsibility of the resource granting entity.

Multifactor authentication

- The combination of two or more authentication methods to verify the user's identity and ability to access a resource.
    - Smartcard and PIN
    - Iris and Bluetooth watch.
- Multifactor authentication also allows for the ability for the user to present multiple candidate credentials and then generate a new credential which will be derived for final authorization.

Authorization Methods

- **Static hash comparison** – Static hash comparisons are comparisons of a static value against a stored value. E.g. Password, PIN, etc.
- **Public Key Infrastructure (PKI)** – Public Key Infrastructure uses asymmetric encryption to verify sender and receiver of user identification material.
- **One-time password** – One time passwords are static hash comparisons which update the stored static value for which a presented hash will be compared against.

User Authentication security paradigms

- **Host level security** – All authentication functions are run at the host level with no protection
- **Software protected security** – Authentication functions are run in software protected environments. MSCAPI encryption, Virtualization etc.
- **Hardware segmented security** – Authentication functions are run in common hardware but segmented for limited operating times. Intel SGX, etc.
- **Hardware isolated security** – All authentication functions are run in a separate operating environment which is not accessible from other operating environments. Dell ControlVault, etc.

Authentication Session Management Methods

- **Single Session request** – Session Authentication methods are those which a user presents credentials and authentication is maintained and allowed for that resource until the request is explicitly terminated by the user. Windows login is an example of this.
- **Persistent** – Persistent Authentication is a method which the user's presence and authentication is constantly detected and evaluated to ensure that the user is still present to allow detection.
- **Consumption** – Consumption Authentication session management is a method which upon any authentication request and use of an authenticated credential, the session is limited in availability. The only way for a consumption session to be extended is to present additional authentication factors.

Attacks

There are many types of attacks which target authentication processes. Compromise of the authentication system can generate a vulnerability into the security system. Below are several common types of attacks which impact authentication attempts.

- **Replay** – this type of attack is one which the presented credential is copied and then used again for future authorization attempts.
- **Shoulder Surfing** – this is one type of social engineering attack which the user's presented credential is obtained by a third party from visual manners
    - Additional Social engineering attacks include, phishing, baiting, dumpster diving, etc.
- **Man in the Middle** – this type of attack is which a component is inserted into the middle of the authentication flow and that component stores the presented credential for replay or attack.
- **Dictionary/Brute Force Attacks** – this type of attack is which a user or application uses dictionaries or a list of all possible passwords to request access to a resource.

Security vs. Usability

In today's business environment, IT departments must take into consideration the organization's users' (including IT) ability to maintain high usability while maintaining a high security posture. Authentication factor decisions are determined by infrastructure costs, manageability and usability. Often security is compromised in the name of usability and lower costs. This is common practice when passwords are used for user authentication and authorization events. Increasing Security often raises infrastructure costs and usability thresholds. Determining the company's posture is vital to providing a robust authentication ecosystem. Additionally, value add solutions which provide easy to use manageability and easy to use solutions, at a low infrastructure cost, like Dell Data Protection, can provide extensive protection to a company's infrastructure.

Technology	Cost	Usability	Manageability	Security
Smartcard *	High cost	High	High	High
Password	Low cost	High	Low	Low
Fingerprint to password backend	Medium cost	Low	High	Medium

* - PKI based smartcard

For more information visit Dell.com/DataSecurity