Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

Nishit Narang
WILPD-CSIS
(nishit.narang@pilani.bits-pilani.ac.in)

innovate achieve lead

BITS Pilani

Pilani Campus

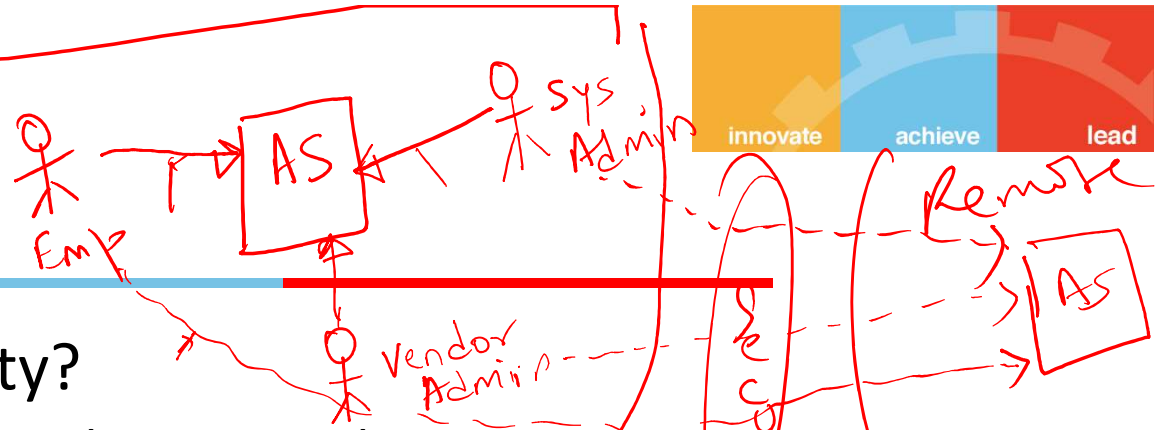
<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 11: Cloud Security

Cloud Security Fundamentals

Source Disclaimer: Content for some of the slides is from the course Textbook:
Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010
Some of the other slides are taken from Microsoft Educator Learn Material (Microsoft Azure Security Technologies)

Overview



- Why Cloud Security?
  - Security is a principal concern when entrusting an organization's critical information to geographically dispersed cloud platforms not under the direct control of that organization
  - Designing security into cloud software during the software development life cycle can greatly reduce the cloud attack surface → Secure SDLC / DevSecOps

- Case Study:
  - On-premise application sever moved to cloud environment.
  - How will the various roles of Web Admin, System Admin etc continue to work in a secure fashion?

Secure Software Lifecycle

Refer "*Security Guidance for Critical Areas of Focus in Cloud Computing*" by the Cloud Security Alliance

- Emphasizes the importance of secure software life cycle in their listing of 15 cloud security domains. Example:
  - Domain 6, Information Lifecycle Management
    - *"Understand cloud provider policies and processes for data retention and destruction and how they compare with internal organizational policy. Be aware that data retention assurance may be easier for the cloud provider to demonstrate, but data destruction may be very difficult. Perform regular backup and recovery tests to assure that logical segregation and controls are effective."*
  - Domain 11, Application Security
    - *"IaaS, PaaS and SaaS create differing trust boundaries for the software development lifecycle, which must be accounted for during the development, testing and production deployment of applications."*
  - Domain 14, Storage
    - *"Understand cloud provider storage retirement processes. Data destruction is extremely difficult in a multi-tenant environment and the cloud provider should be utilizing strong storage encryption that renders data unreadable when storage is recycled, disposed of, or accessed by any means outside of authorized applications."*
- Irrespective of whoever develops the software, the process requires a strong commitment to a formal, secure software development life cycle, including design, testing, secure deployment, patch management, and disposal → Secure SDLC, DevSecOps etc

Cloud Information Security Objectives

- Data and Analysis Center for Software (DACS) requires that software must exhibit the following three properties to be considered secure:
  - **Dependability** — Software that executes predictably and operates correctly under a variety of conditions, including when under attack or running on a malicious host
  - **Trustworthiness** — Software that contains a minimum number of vulnerabilities or no vulnerabilities or weaknesses that could sabotage the software's dependability. It must also be resistant to malicious logic
  - **Survivability (Resilience)** — Software that is resistant to or tolerant of attacks and has the ability to recover as quickly as possible with as little harm as possible
- Seven complementary principles that support information assurance are:
  - Confidentiality, Integrity, Availability (CIA Triad), and
  - Authentication, Authorization, Auditing, and Accountability (AAAA)
- These 7 principles are summarized in the following slides.

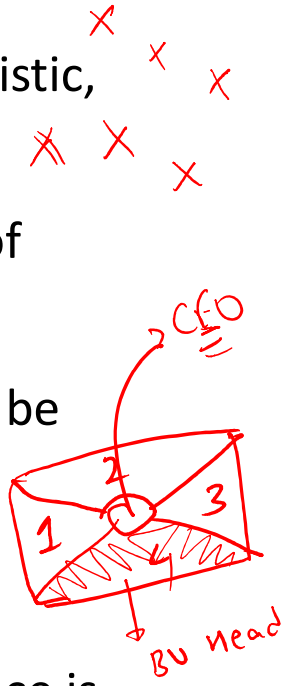
Confidentiality, Integrity, Availability (CIA)

CIA - A way to think about security trade-offs.

- **Confidentiality** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data.
- **Integrity** refers to keeping data or messages correct.
- **Availability** refers to making data available to those who need it.

Confidentiality in Cloud Systems

- Confidentiality in cloud systems is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption, and inference:
  - Intellectual property (IP) includes inventions, designs, and artistic, musical, and literary works
  - Covert channels: A covert channel is an unauthorized and unintended communication path that enables the exchange of information. Covert channels can be accomplished through inappropriate use of storage mechanisms, as example
  - Encryption involves scrambling messages so that they cannot be read by an unauthorized entity, even if they are intercepted
  - Traffic analysis is a form of confidentiality breach that can be accomplished by analyzing the volume, rate, source, and destination of message traffic, even if it is encrypted
  - Inference is usually associated with database security. Inference is the ability of an entity to use and correlate information protected at one level of security to uncover information that is protected at a higher security level



Integrity and Availability in Cloud Systems

- Integrity requires that the following three principles are met:
  - Modifications are not made to data by unauthorized personnel or processes.
  - Unauthorized modifications are not made to data by authorized personnel or processes.
  - The data is internally and externally consistent, i.e. the internal information is consistent both among all sub-entities and with the real/external-world
- Availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. Availability guarantees that
  - the systems are functioning properly when needed.
  - In addition, this concept guarantees that the security services of the cloud system are in working order.
  - A denial-of-service attack is an example of a threat against availability.

The reverse of confidentiality, integrity, and availability is disclosure, alteration, and destruction (DAD)!!

AAAA

- *Authentication* is the testing or reconciliation of evidence of a user's identity. It establishes the user's identity and ensures that users are who they claim to be.
- *Authorization* refers to rights and privileges granted to an individual or process that enable access to computer resources and information assets.
- Auditing: To maintain operational assurance, organizations use two basic methods: system audits and monitoring. These methods can be employed by the cloud customer, the cloud provider, or both, depending on asset architecture and deployment
  - A *system audit* is a one-time or periodic event to evaluate security.
  - *Monitoring* refers to an ongoing activity that examines either the system or the users, such as intrusion detection
  - An *audit trail or log* is a set of records that collectively provide documentary evidence of different cloud operations
- *Accountability* is the ability to determine the actions and behaviors of a single individual within a cloud system
  - Accountability is related to the concept of *nonrepudiation*, wherein an individual cannot successfully deny the performance of an action
  - Audit trails and logs support accountability

Cloud Security Design Principles

- A 1974 paper (***that is still relevant today!***) addresses the protection of information stored in a computer system by focusing on hardware and software issues that are necessary to support information protection
  - "The Protection of Information in Computer Systems" by Saltzer and Schroeder
  - https://www.cs.virginia.edu/~evans/cs551/saltzer/
- The paper presented the following 11 security design principles
  - Least privilege
  - Separation of duties
  - Defense in depth
  - Fail safe
  - Economy of mechanism
  - Complete mediation
  - Open design
  - Least common mechanism
  - Psychological acceptability
  - Weakest link
  - Leveraging existing components
- The following slides summarize these design principles

Principle 1: Least Privilege

- The principle of *least privilege* maintains that an individual, process, or other type of entity should be given the minimum privileges and resources for the minimum period of time required to complete a task.
- This approach reduces the opportunity for unauthorized access to sensitive information.

Principle 2: Separation of Duties

- *Separation of duties* requires that completion of a specified sensitive activity or access to sensitive objects is dependent on the satisfaction of a **plurality** of conditions. For example:
  - an authorization that requires signatures of more than one individual, or
  - the arming of a weapons system that requires two individuals with different keys
- Thus, separation of duties forces collusion among entities in order to compromise the system.

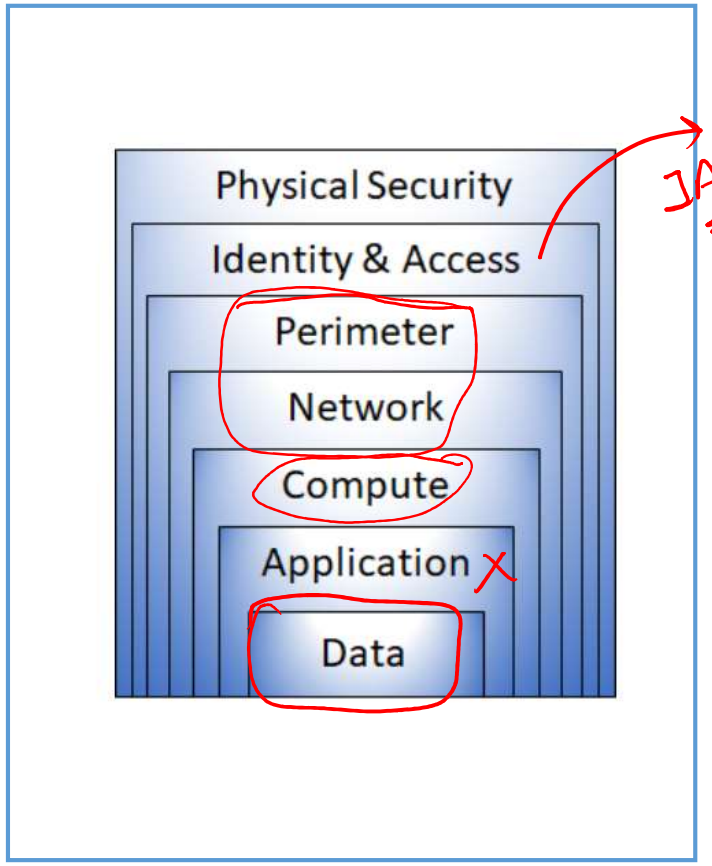
Principle 3: Defense in Depth

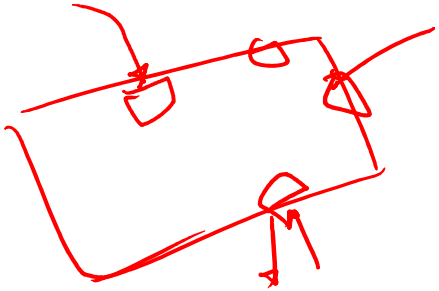
- *Defense in depth* is the application of multiple layers of protection wherein a subsequent layer will provide protection if a previous layer is breached
- The Information Assurance Technical Framework Forum (IATFF), an organization sponsored by the National Security Agency (NSA), has produced a document titled the "Information Assurance Technical Framework" (IATF) that provides excellent guidance on the concepts of defense in depth
  - **Defense in multiple places** — Information protection mechanisms placed in a number of locations to protect against internal and external threats
  - **Layered defenses** — A plurality of information protection and detection mechanisms employed so that an adversary or threat must negotiate a series of barriers to gain access to critical information
  - **Security robustness** — An estimate of the robustness of information assurance elements based on the value of the information system component to be protected and the anticipated threats
  - **Deploy KMI/PKI** — Use of robust key management infrastructures (KMI) and public key infrastructures (PKI)
  - **Deploy intrusion detection systems** — Application of intrusion detection mechanisms to detect intrusions, evaluate information, examine results, and, if necessary, take action

Defense in depth: *Cloud Context*

Defense in depth uses a layered approach to security:

- **Physical** security such as limiting access to a datacenter to only authorized personnel.
- **Identity and access** security controlling access to infrastructure and change control.
- **Perimeter** security including distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- **Network** security can limit communication between resources using segmentation and access controls.
- The **compute** layer can secure access to virtual machines either on-premises or in the cloud by closing certain ports.
- **Application** layer security ensures that applications are secure and free of security vulnerabilities.
- **Data** layer security controls access to business and customer data, and encryption to protect data.





Principle 4: Fail Safe

- *Fail safe* means that if a cloud system fails it should fail to a state in which the security of the system and its data are not compromised.
  - One implementation of this philosophy would be to make a system default to a state in which a user or process is denied access to the system.
  - A complementary rule would be to ensure that when the system recovers, it should recover to a secure state and not permit unauthorized access to sensitive information.
  - In the situation where system recovery is not done automatically, the failed system should permit access only by the system administrator and not by other users, until security controls are reestablished.

Principle 5: Economy of Mechanism

- *Economy of mechanism* promotes simple and comprehensible design and implementation of protection mechanisms, so that unintended access paths do not exist or can be readily identified and eliminated
  - The principle states that Security mechanisms should be as simple and small as possible
  - If the design and implementation are simple and small, fewer possibilities exist for errors
  - The checking and testing process is less complicated so that fewer components need to be tested

Principle 6: Complete Mediation

- *In complete meditation*, every request by a subject to access an object in a computer system must undergo a valid and effective authorization procedure
- This mediation must not be suspended or become capable of being bypassed, even when the information system is being initialized, undergoing shutdown, being restarted, or is in maintenance mode

Principle 7: Open Design

- There has always been an ongoing discussion about the merits and strengths of security designs that are kept secret versus designs that are open to scrutiny and evaluation by the community at large.
  - A good example is an encryption system
- For most purposes, an open-access cloud system design that has been evaluated and tested by a myriad of experts provides a more secure authentication method than one that has not been widely assessed

Principle 8: Least Common Mechanism

- This principle states that in systems with multiple users, the mechanisms allowing resources shared by more than one user should be minimized as much as possible.
  - This principle may also be restrictive because it limits the sharing of resources
  - Shared access paths can be sources of unauthorized information exchange and can provide unintentional data transfers (also known as *covert channels*)
    - Example: If there is a need to access a file by more than one user, then these users should use separate channels to access the resource, as this helps to prevent from unforeseen consequences that could cause security problems
- Thus, the *least common mechanism* promotes the least possible sharing of common security mechanisms
  - Only a minimum number of protection mechanisms should be common to multiple users

Principle 9: Psychological Acceptability

- *Psychological acceptability* refers to the ease of use and intuitiveness of the user interface that controls and interacts with the cloud access control mechanisms
  - The principle states that a security mechanism should not make the resource more complicated to access if the security mechanisms were not present
  - In other words, the principle recognizes the human element in computer security
  - If security-related software or computer systems are too complicated to configure, maintain, or operate, the user will not employ the necessary security mechanisms

Trivia: *When we enter a wrong password, the system normally only tells us that the user id or password was incorrect. It does not tell us that only the password was wrong as this gives the attacker information!!*

Principle 10: Weakest Link

- A chain is only as strong as its weakest link
- In context of cloud-systems, the security of a cloud system is only as good as its weakest component
- Thus, it is important to identify the weakest mechanisms in the security chain and layers of defense, and improve them so that risks to the system are mitigated to an acceptable level

Principle 11: Leveraging Existing Components

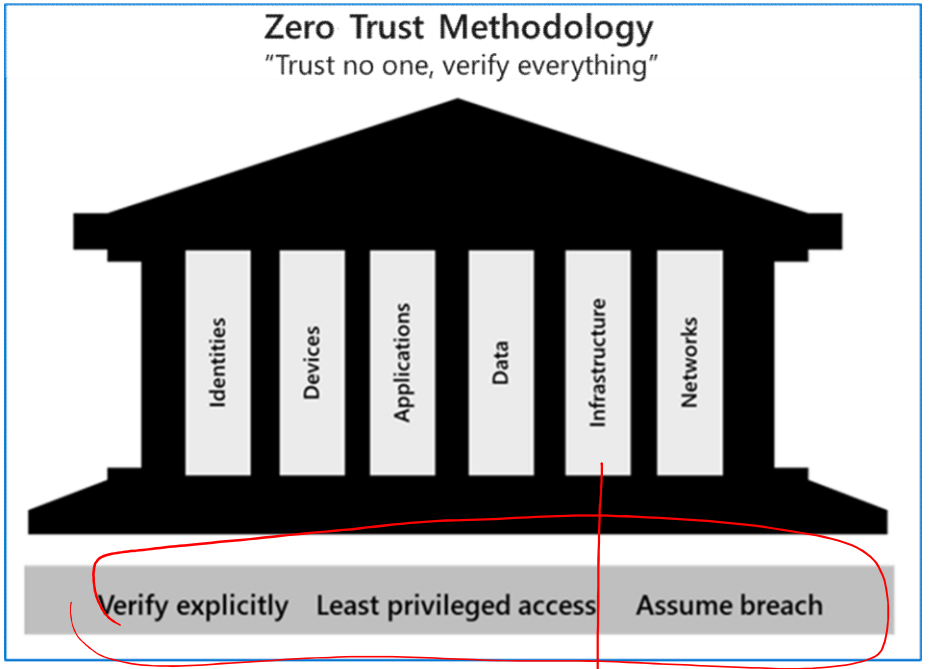
- The principle aims to increase cloud system security by leveraging existing components
- In many instances, the security mechanisms of a cloud implementation might not be configured properly or used to their maximum capability.
- Reviewing the state and settings of the security mechanisms and ensuring that they are operating at their optimum design points will greatly improve the security posture of an information system

"the underlying principles that inform good security practices are well established and quite stable" – IoT SF

Cloud Security:
The Zero-trust methodology

- Zero Trust guiding principles
  - Verify explicitly
  - Least privileged access
  - Assume breach

- Six foundational pillars
  - **Identities** may be users, services, or devices.
  - **Devices** create a large attack surface as data flows.
  - **Applications** are the way that data is consumed.
  - **Data** should be classified, labeled, and encrypted based on its attributes.
  - **Infrastructure** whether on-premises or cloud based, represents a threat vector.
  - **Networks** should be segmented.



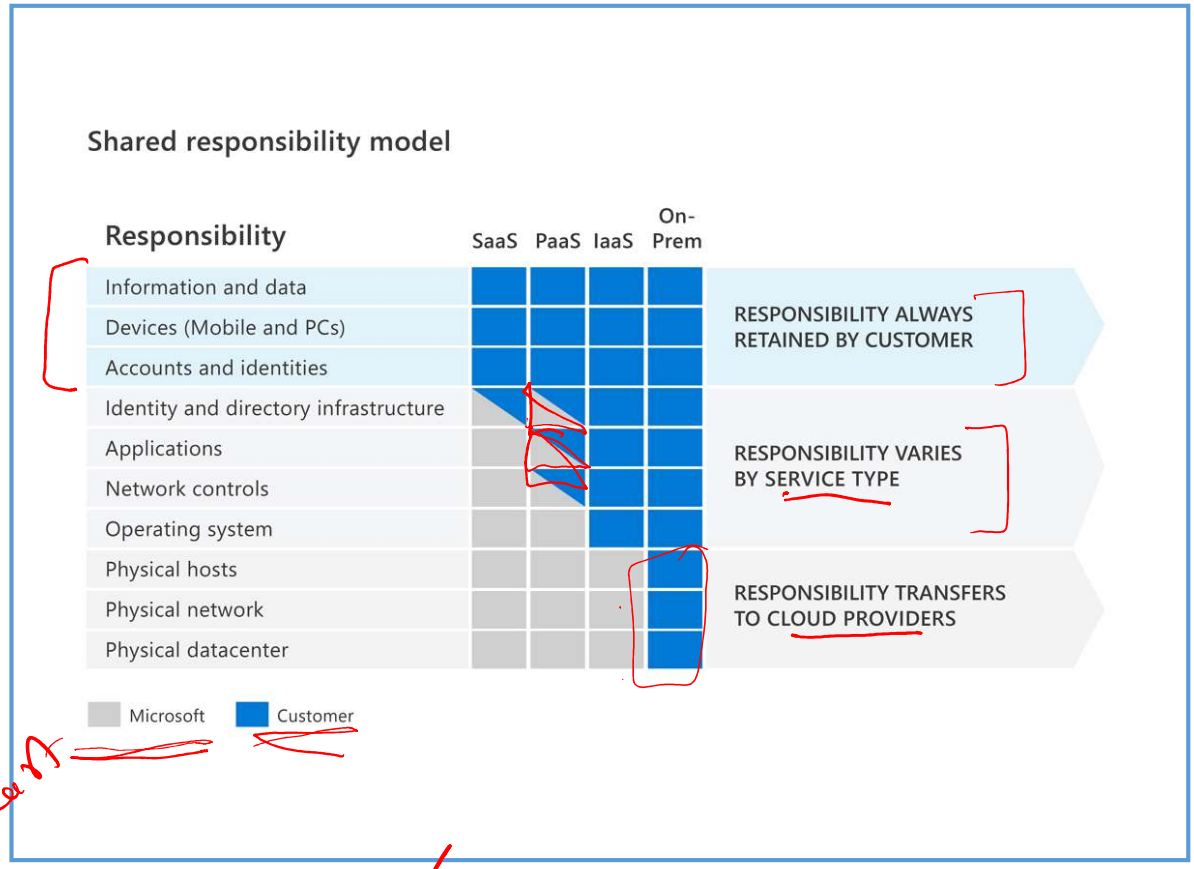
IAM

Data Classif
labeling

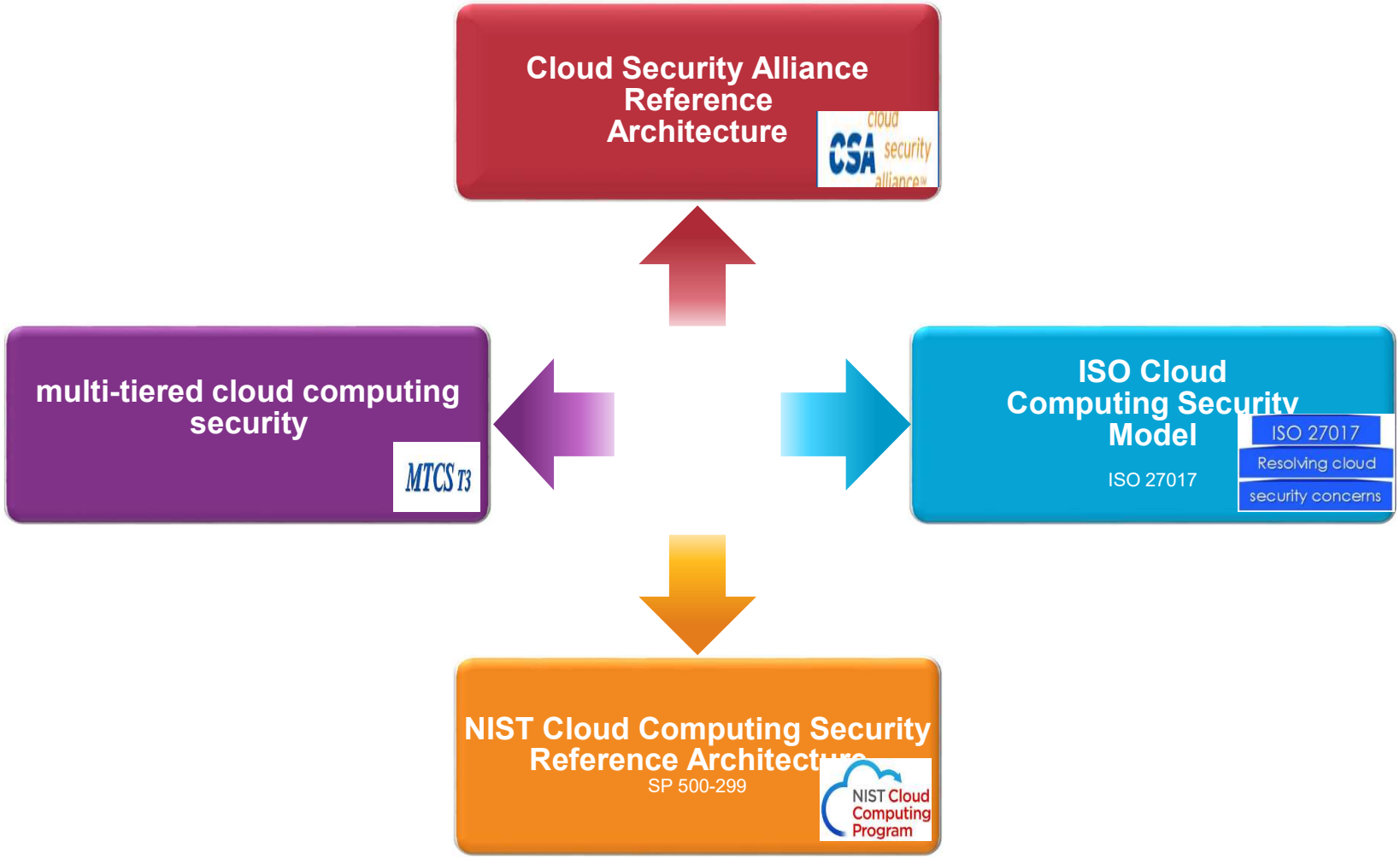
Cloud Security:
The shared responsibility model

The responsibilities vary based on where the workload is hosted:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- On-premises datacenter (On-prem)



RECAP: Cloud Security Reference Architectures & Standards



NIST 33 Security Principles

- NIST Special Publication 800-27
  - "Engineering Principles for Information Technology Security (EP-ITS)
  - It presents 33 security principles that begin at the design phase of the information system or application and continue until the system's retirement and secure disposal
- Some of the 33 principles that are most applicable to cloud security policies and management are as follows:
  - Principle 1 — Establish a sound security policy as the "foundation" for design.
  - Principle 2 — Treat security as an integral part of the overall system design.
  - Principle 3 — Clearly delineate the physical and logical security boundaries governed by associated security policies.
  - Principle 6 — Assume that external systems are insecure.
  - Principle 7 — Identify potential trade-offs between reducing risk and increased costs and decreases in other aspects of operational effectiveness.
  - Principle 16 — Implement layered security; ensure there is no single point of vulnerability.
  - Principle 20 — Isolate public access systems from mission-critical resources (e.g., data, processes, etc.).
  - Principle 21 — Use boundary mechanisms to separate computing systems and network infrastructures.
  - Principle 25 — Minimize the system elements to be trusted.
  - Principle 26 — Implement least privilege.
  - Principle 32 — Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
  - Principle 33 — Use unique identities to ensure accountability

Business Continuity Planning / Disaster Recovery

- Business continuity planning (BCP) and disaster recovery planning (DRP) involve the preparation, testing, and updating of the actions required to protect critical business processes from the effects of major system and network failures
- From the cloud perspective, these important business processes are heavily dependent on cloud-based applications and software robustness and security
- Cloud computing offers an attractive alternative to **in-house** BCP/DRP implementations

DRP

The means of obtaining backup services are important elements in the disaster recovery plan. The typically used alternative services are as follows:

- **Mutual aid agreements** — An arrangement with another company that might have similar computing needs. The other company may have similar hardware or software configurations or may require the same network data communications or Internet access.
- **Subscription services** — Third-party commercial services that provide alternate backup and processing facilities. An organization can move its IT processing to the alternate site in the event of a disaster.
- **Multiple centers** — Processing is spread over several operations centers, creating a distributed approach to redundancy and sharing of available resources. These multiple centers could be owned and managed by the same organization (in-house sites) or used in conjunction with a reciprocal agreement.
- **Service bureaus** — Setting up a contract with a service bureau to fully provide all alternate backup-processing services. The disadvantages of this arrangement are primarily the expense and resource contention during a large emergency.

BCP

- A BCP is designed to keep a business running, reduce the risk of financial loss, and enhance a company's capability to recover promptly following a disruptive event.
- One of the key principle components of the BCP is the BIA:
  - Business impact assessment (BIA) — Assisting the business units in understanding the impact of a disruptive event. This phase includes the execution of a vulnerability assessment.
  - The function of a vulnerability assessment is to conduct a loss impact analysis. Because there are two parts to the assessment, a financial assessment and an operational assessment, it is necessary to define loss criteria both quantitatively and qualitatively

Using the Cloud for BCP/DRP

- Adopting a cloud strategy for BCP/DRP offers significant benefits without large amounts of capital and human resource investments.
- Proper design of a cloud-based IT system that meets the requirements of a BCP and DRP should include the following:
  - Secure access from remote locations
  - A distributed architecture with no single point of failure
  - Integral redundancy of applications and information
  - Geographical dispersion

Redundancy Provided by the Cloud

- Cloud computing offers redundancy in various forms (e.g. physical and virtual infrastructure, data backup etc)
  - Cloud-based BCP and DRP eliminate the need for expensive alternative sites and the associated hardware and software to provide redundancy.
  - Cloud computing provides for low cost and widely available, dynamically scalable, virtualized resources.
  - With a cloud computing paradigm, the backup infrastructure is always in place.
- Another option is to implement a hybrid cloud with collocation of resources and services.
- Cloud service providers also offer organizations the option to support the backup process thorough the use of storage area networks (SANs).
  - Examples of elements that require backup are application data, media files, files that have changed, recent documents, the operating system, and archival files.

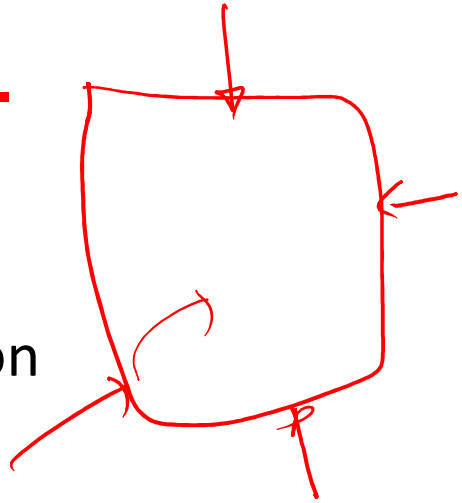
Cloud Security

Identity and Access Management (IAM)

Source Disclaimer:

- Content for some of the slides is from the course Textbook:
  - *Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010*
- Some of the slides are taken from Microsoft Educator Learn Material (Microsoft Azure Security Technologies)
- Material for some of the other slides is from following book:
  - *Authentication: From Passwords to Public Keys, by Richard E. Smith*

IAM: Overview



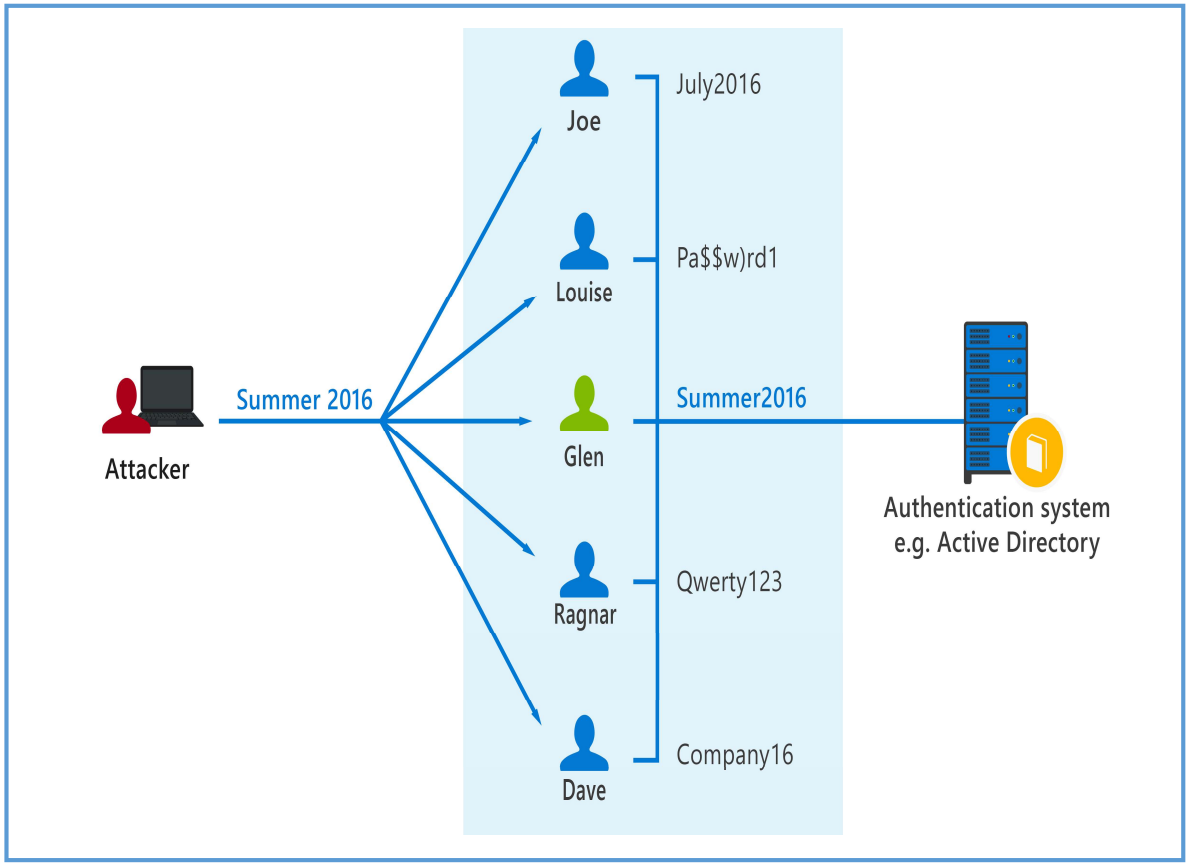
- Why is ***Identity*** important?
  - Concept of identity as a security perimeter
  - Is key behind authentication and authorization

- Why IAM?
  - Improve Operational Efficiency
    - IAM technology and processes can improve efficiency by automating user on-boarding and other repetitive tasks (e.g., self-service for users requesting password resets
  - Regulatory security compliance management
    - Need to comply with various regulatory, privacy, and data protection requirements

Common identity attacks

Types of security threats:

- Password-based attacks
  - Many password-based attacks employ brute force techniques to gain unauthorized access, often using a dictionary
- Phishing
  - hacker sends an email that appears to come from a reputable source, instructing the user to sign in and change their password
- Spear phishing
  - a variant on phishing. Hackers build databases of information about users, which can be used to create highly credible emails



A password-spray attack – attacker sprays a commonly used password against multiple accounts