IMPLEMENT AND OPERATE ENDPOINT DEVICE SECURITY

SSCP®

Systems Security
Certified Practitioner

(ISC)²®

Trusted Platform Module (TPM)

TPM is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop)

Mobile Device Management (MDM)

The intent of MDM is to optimize the functionality and security of mobile devices within the enterprise, while simultaneously protecting the corporate network

Bring Your Own Device (BYOD)

- BYOD is where employees bring non-company IT into the organization and demand to be connected to everything — without proper accountability or oversight
- Challenges:
  - BYOD Governance and Compliance
  - Risk
  - Control

BYOD Policy Considerations

- Specify what devices are permitted
- Establish a stringent security policy for all devices
- Define a clear service policy for devices under BYOD criteria
- Make it clear who owns what apps and data
- Decide what apps will be allowed or banned
- Set up an employee exit strategy

OPERATE AND CONFIGURE CLOUD SECURITY

SSCP®

Systems Security
Certified Practitioner

(ISC)²®

The Five Essential Characteristics of Clouds

- On-Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

Public

The service available to the general public over the Internet, in which a customer can access cloud service provider resources either in the form of a free service or offered on a pay-per-usage model

Private

A proprietary network, or data center, owned and architected for use by a specified entity utilizing cloud technologies to provide services behind a firewall

Hybrid

A hybrid cloud is built by combining two forms of cloud computing deployments, typically a public and private cloud

Community

Offer a valuable and cost-effective manner for specified groups or entities with a similar focus, or with common compliance and requirements to operate in a multi-tenant infrastructure

SaaS

Distributed model where software applications are hosted by a vendor or cloud service provider and made available to customers over network resources

PaaS

A way for customers to rent hardware, operating systems, storage, and network capacity over the Internet from a cloud service provider

IaaS

A model where the customer can provision equipment "as a service" to support operations, including storage, hardware, servers, and relevant networking components

Virtualization

The foundation for an agile, scalable cloud

The first practical step for building cloud infrastructure

Abstracts and isolates the underlying hardware as VMs

Hypervisor

A hypervisor or virtual machine monitor (VMM) is a piece of computer software, firmware, or hardware that creates and runs virtual machines

- Type-1: native or bare-metal hypervisors
- Type-2: hosted hypervisors

Types of Virtualization

- Server virtualization
- Network virtualization
- Desktop virtualization
- Application virtualization
- Storage virtualization

Country-Specific Legal Considerations

- United States
- EU member states
- Latin America
- Asian-Pacific Economic Cooperation (APEC)

Jurisdiction and Applicable Law

- **Applicable law:**
  - Determines the legal regime applicable to a certain matter
- **Jurisdiction:**
  - Usually determines the ability of a national court to decide a case or enforce a judgment or order

Typical Meaning for Common Privacy Terms

Data Subject

Personal Data

Processing

Controller

Processor

who or what data is about

Data Dispersion in Cloud Storage

Data Dispersion techniques are used to provide high availability, assurance, and performance when writing data into cloud-based storage systems

Threats to Storage Types

- Administrators for the cloud provider can technically access your volumes and storage
- Private volume storage can easily become publically available
- Volumes and their snapshots can be used as an invaluable resource for troubleshooting purposes
- Object-level storage typically lacks comprehensive security controls
- Multi-tenancy issues

Data Loss Prevention (DLP)

Controls to protect data form the foundation of organizational security, along with enabling the organization to ensure the ability to meet regulatory requirements and relevant legislation

DLP Components

- Discovery and classification
- Monitoring
- Enforcement

DLP Architecture

Network based

Storage based

Client based

Cloud-Based DLP Considerations

Data in the cloud tends to move and replicate

Administrative access for enterprise data in the cloud could be tricky

DLP technology can affect overall performance

Best Practices

Cloud DLP policy should address the following:

- What kind of data is permitted to be stored in the cloud?
- Where can the data be stored (jurisdictions)?
- How should it be stored? Encryption and storage access consideration
- What kind of data access is permitted? Which devices and what networks? Which applications? Which tunnel?
- Under what conditions is data allowed to leave the cloud?

Best Practices

- Encryption methods should be carefully examined based on the format of the data
- When implementing controls to block data items, create procedures that will prevent business process damage due to false positive events
- DLP can be an effective tool when planning or assessing a potential migration to cloud applications

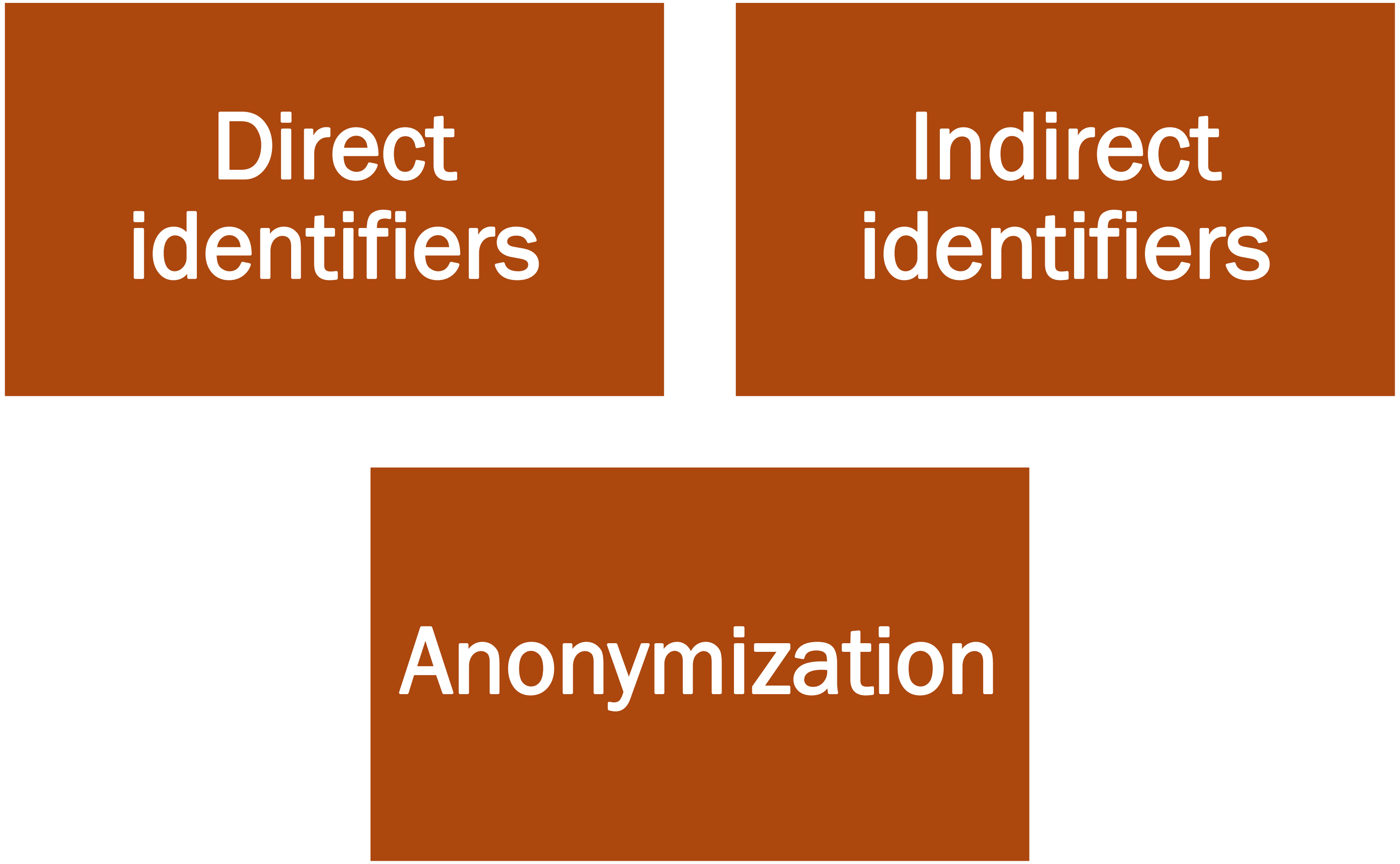
Key Management in Software Environments

Typically, cloud service providers protect keys using software-based solutions to avoid the additional cost and overhead of hardware-based security models

Common Approaches for Data Masking

- Random substitution
- Algorithmic substitution
- Shuffle
- Masking
- Deletion

Data Anonymization



Direct identifiers

Indirect identifiers

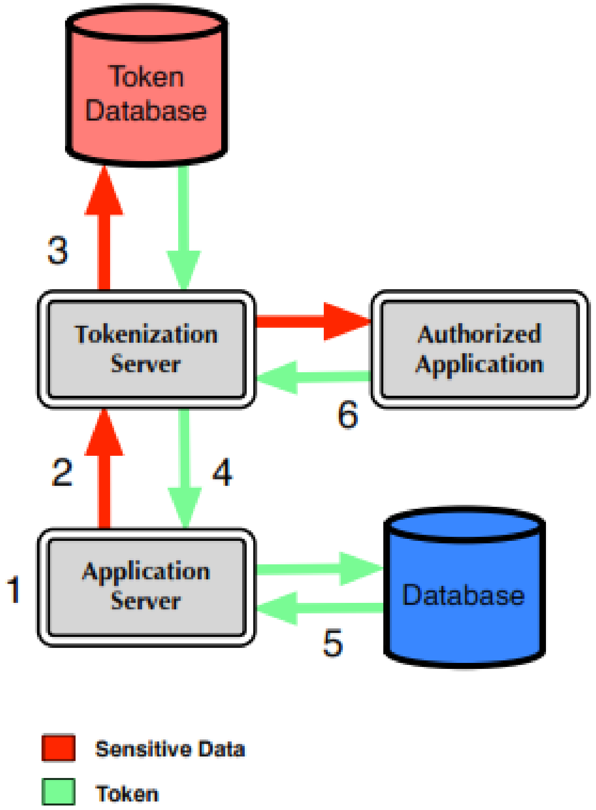
Anonymization

Tokenization

- Tokenization is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token

- Tokenization can assist with:
  - Complying with regulations or laws
  - Reducing the cost of compliance
  - Mitigating risks of storing sensitive data and reducing attack vectors on that data

Basic Tokenization Architecture



Tokenization and Cloud Considerations

- Ensure the provider and solutions protect your data
- Pay special attention authenticating the application when storing or retrieving the sensitive data
- Evaluate your compliance requirements before considering a cloud-based tokenization solution

Security and Information Event Management (SIEM)

Security Information Management (SIM)

Security Event Management (SEM)

SIEM Capabilities

- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Retention
- Forensic analysis

SIEM Challenges

- Turning over internal security data to a cloud provider requires trust
- Targeted attack detection requires in-depth knowledge of internal systems, the kind found in corporate security teams

SECURE BIG DATA SYSTEMS

SSCP®

Systems Security
Certified Practitioner

(ISC)²®

Trends

Mountains of data that contain valuable information

The abundance of cheap commodity computing resources

“Free” analytics tools

Securing the Organization’s Big Data

Identify owners for the outputs of Big Data processes, as well as the raw data

Data ownership will be distinct from information ownership

Deploying Big Data for Security

The challenge of detecting and preventing advanced persistent threats may be answered using Big Data style analysis

Big Data provides the opportunity to consolidate and analyze logs automatically from multiple sources rather than in isolation

OPERATE AND SECURE VIRTUAL ENVIRONMENTS

SSCP®

Systems Security
Certified Practitioner

(ISC)²®

Software-Defined Network (SDN)

SDN enables organizations to accelerate application deployment and delivery, dramatically reducing IT costs through policy-enabled workflow automation

Virtual Appliances

Virtual appliances are prebuilt software solutions comprising one or more virtual machines that are packaged, updated, maintained, and managed as a unit

Virtual Appliances Compared to Virtual Machines

Virtual Appliances

Virtual Machines

Host Clustering Concepts

Within a host cluster, resources are allocated and managed as if they are pooled, or jointly available to all members of the cluster

- Reservations
- Limits
- Shares

VMware Distributed Resource Scheduling (DRS)

Provide your workloads highly available resources

Optimize performance by balancing workload

Scale and manage computing resources without service disruption

Provide optimized performance for hosts and virtual machines by balancing computing capacity by cluster

VMware vSphere High Availability (HA)

- VMware vSphere High Availability (HA) provides uniform, cost-effective failover protection against hardware and operating system
- HA can:
  - Detect hardware and guest operating system failures
  - Restart virtual machines on other vSphere hosts in the cluster when a server outage is detected

Scalability and Reliability

- Scalability
  - Master-slave note relationship
- Reliability
  - No external dependencies
  - Multiple communication paths
  - VM-VM anti-affinity rules

Windows Failover Clustering

System Center Operations Manager (SCOM)

System Center Virtual Machine Manager (SCVMM)

Performance Resource Optimization (PRO)

Attacks and Countermeasures

- To secure a server, it is essential to first define the threats that must be mitigated
- Threats:
  - Intentional actors
  - Unintentional actors

General Guidelines

- Use an asset management system that has configuration management capabilities
- Use system baselines to enforce configuration management throughout the enterprise
- Develop and use of a robust change management system
- Use an exception reporting system
- Use vendor-specified configuration guidance and best practices

Security Benefits of Virtualization

Centralized storage used in virtualized environments prevents a loss of important data

When VMs and applications are isolated, only one application on one OS is affected by an attack

When configured properly, a virtual environment provides flexibility

If a VM is infected, it can be rolled back to a prior “secure” state that existed before the attack

Hardware reductions that occur due to virtualization improve physical security

Security Challenges, Risks, and Issues with Virtualization

- File sharing between hosts and guests
- Snapshots
- Network storage
- Hypervisor
- Virtual machines
- Separation of duties and administrator access
- Time synchronization
- Partitions

Common Virtualization Attacks

Denial of Service (DoS)

VM Jumping

Host Traffic Interception

Mitigation Strategies

Firewalls

VLANs

Agent-based antivirus approaches

Recommendations and Best Practices for Secure Virtualization

- Administrator access and separation of duties
- Give administrators the right to deploy new VMs but not modify existing VMs

Desktop Virtualization and Security

Update Acceptable Use Policy

Limit the use of VMs to the users who need them

Keep virtualization and security software up to date

Choose security policies that support virtualization

Create and maintain a library of secure VM builds

Network Security

- Disconnect any unused NICs
- Make sure that the host platform that connects the hypervisor and guests to the physical network is secure
- Encrypt all traffic between clients and hosts, management systems and the hypervisor, and the hypervisor and hosts using SSL/TLS
- Secure IP communications between two hosts
- Do not use default self-signed certificates
- Place virtual switches into promiscuous mode

Storage Networks

- iSCSI and NFS traffic should be placed on dedicated storage networks or non-routable VLANs
- Use IPSec to encrypt iSCSI traffic to prevent snooping
- When using iSCSI or NFS, use physical switches to detect and disallow IP or MAC address spoofing
- All traffic to and from storage repositories needs to be isolated from non-storage traffic

Virtual Machine Security

- Turn off any unused VMs
- Use IPSec between the host and VM
- Employ VLANs within a single vSwitch
- When VMs move, active memory and state are sent over the network to the new host in clear text. Isolate this traffic from the production network
- Policies can be used to make sure that a new VM is not allowed to join a VM group or cluster unless it has a specific configuration

Virtual Machine Security

- Do not place workloads with different trust levels in the same security domain
- Restrict access to archived VMs
- Consider placing virtual firewalls on these VLANs with two or more VMs
- Place a CPU limit on any VMs that can access the Internet
- If users are allowed to create VMs, consider an authorized template

Virtual Machine Security

- Consider deploying a security VM or virtual appliance to eliminate an agent on each VM
- Disable any copy-paste functionality
- A virtual firewall attached to a VM travels with it at all times to ensure that security policy is enforced before, during, and after any moves
- A security gateway can be employed to inspect traffic between VMs
- Make sure that any VMs that process protected information are isolated from other VMs

Management Systems

- Secure your communications between management systems and the hosts
- Do not allow a management server to be accessible from all workstations
- Separate management servers from database servers

Hypervisor Security

- Install vendor-supplied patches and updates
- Disable any unused virtual hardware that connects to the hypervisor
- Disable unneeded services
- Perform constant monitoring of the hypervisor
- Disable all local administration of the hypervisor
- Require a centralized management application
- Require multi-factor authentication for any admin functions on the hypervisor

Remote Access

- Remote access management should be limited
- Any remote access should ask for a username and a password backed
- Remote communication to any management tools should be encrypted and authenticated.
- When using SSH:
  - Disable version 1 protocol and the admin or root SSH login
  - Require users to use role-based access control

Configuration and Change Management

- Make sure that any physical or virtual servers are hardened before putting them into deployment
- Harden physical and virtual switches and virtual appliances and gateways before deployment
- Do not allow changes to the infrastructure without documentation and testing in a lab environment
- Track VM configurations and issue alerts for any changes to a desired configuration

Clustered Storage Spaces Hardware Requirements

Two or more systems running Windows Server 2012

SAS Host Bus Adapter (HBA)

A Windows Server 2012-certified SAS JBOD enclosure

A minimum of three physical drives

Key Features of vSphere Storage DRS

- Resource aggregation
- Initial placement
- Load balancing
- Affinity rules
- Datastore maintenance mode