CompTIA Security+

4.0 Application, Data, and Host Security

Objective 4.1

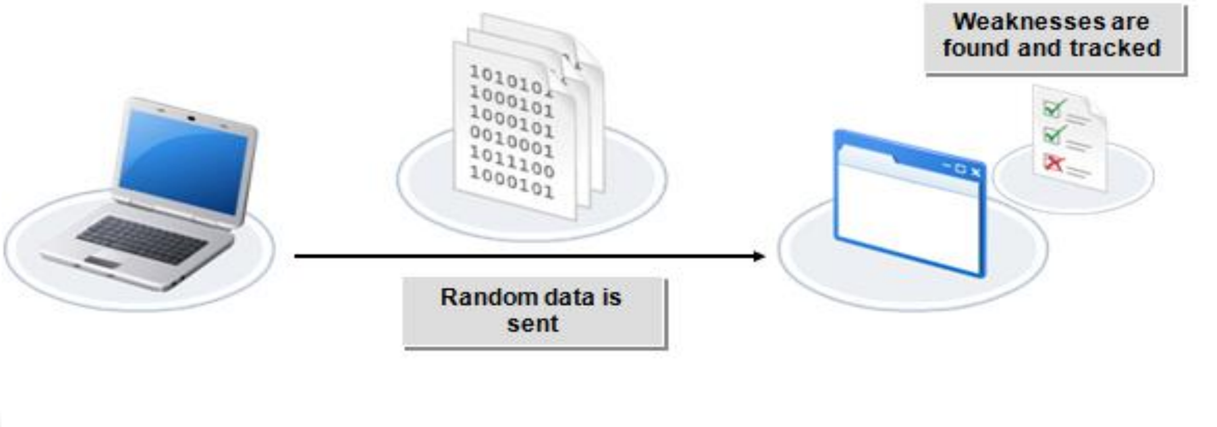
- Explain the importance of application security

Fuzzing

- A process by which semi-random data is injected into a program or protocol stack for detecting bugs

- Application, Protocol, File Format

- Looking for something out of the ordinary
  - Application crash, server error, exception



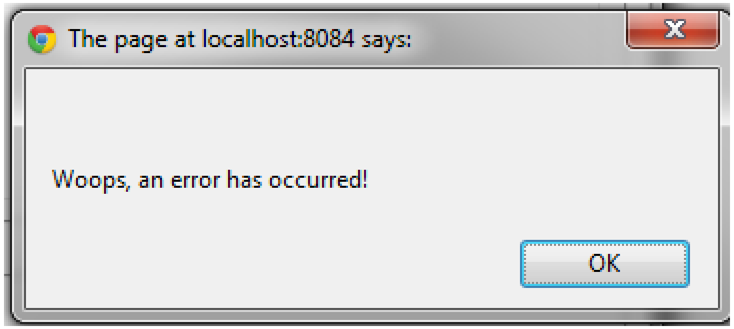
Secure coding concepts

- Examine all written code for security holes
- Should be done by software developer
- A balance between time and security
- Testing is key
  - Should be a Quality Assurance (QA) process
- Usually vulnerabilities will be found at some point
  - Patches, updates, hotfixes, etc…

Error and Exception Handling

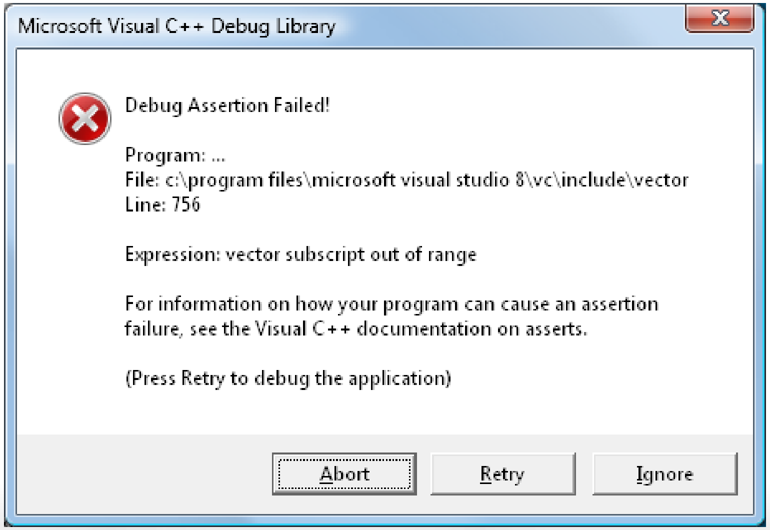
- What happens when an error occurs?
  - “Graceful” exceptions

- Errors should also provide minimal information to visitors and users, especially outside/external visitors and users



The page at localhost:8084 says:

Woops, an error has occurred!



Microsoft Visual C++ Debug Library

Debug Assertion Failed!

Program: ...
File: c:\program files\microsoft visual studio 8\vc\include\vector
Line: 756

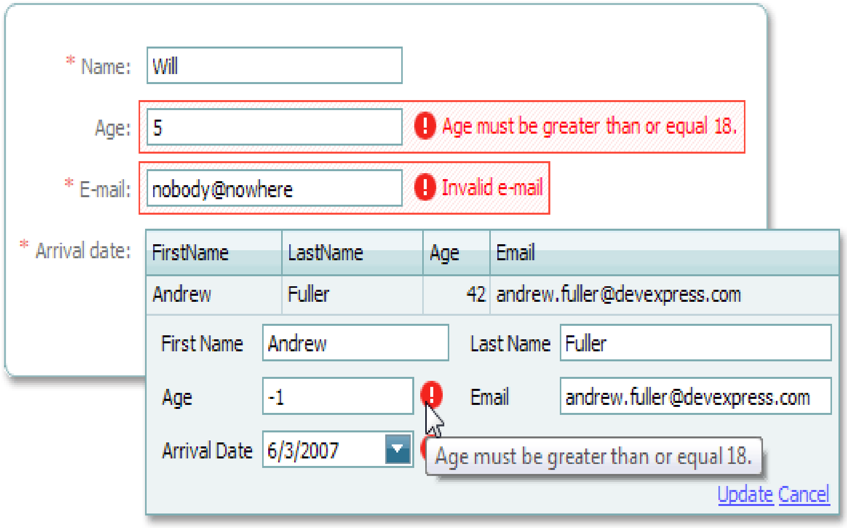
Expression: vector subscript out of range

For information on how your program can cause an assertion failure, see the Visual C++ documentation on asserts.

(Press Retry to debug the application)

Input validation

- What is the expected input?
  - Validate actual input vs. expected input



* Name: Will

Age: 5 ❗ Age must be greater than or equal 18.

* E-mail: nobody@nowhere ❗ Invalid e-mail

* Arrival date:

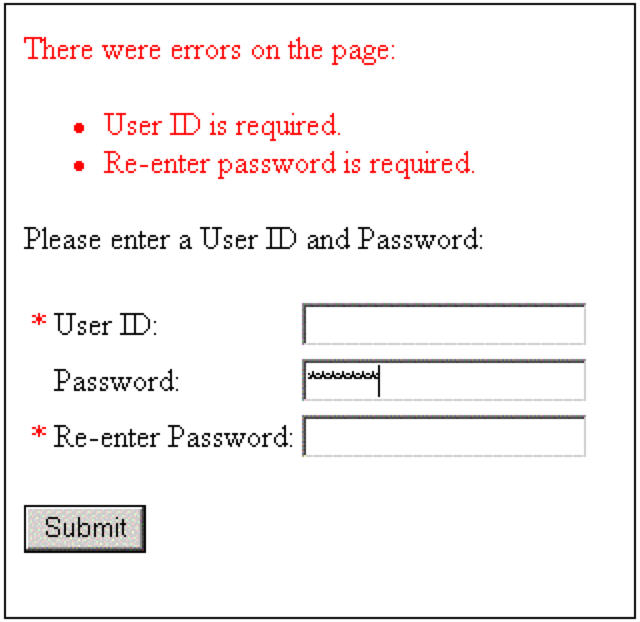
FirstName	LastName	Age	Email
Andrew	Fuller	42	andrew.fuller@devexpress.com

First Name: Andrew Last Name: Fuller

Age: -1 ❗ Email: andrew.fuller@devexpress.com

Arrival Date: 6/3/2007

Age must be greater than or equal 18.



There were errors on the page:

- User ID is required.
- Re-enter password is required.

Please enter a User ID and Password:

* User ID:

Password: ********

* Re-enter Password:

XSS and XSRF Prevention

- XSS
  - Disable running of scripts (Java Script)
  - Check the input for embedded scripts
  - Validate the input prior to storing
- XSRF
  - Authentications should be protected and/or encrypted
  - Always log off from sites instead of closing the browser, closing the tab, or moving on to another URL

Exam Alert

- When presented with a question that relates to **mitigating the danger of any Injection attack, buffer overflows, or XSS attacks, look for answers that relate to input validation**

- By restricting the data that can be input, application designers can reduce the threat posed by maliciously crafted URL references and redirected web content.

Application Configuration Baseline

- Determine a security baseline for every application
  - What browser version? OS service pack? patches?
- Security baseline will change every time something related to the application changes
    - changes with SPs
- Established patterns of use can be used to identify variations that may identify unauthorized access attempts

Application Hardening

- Default application admin accounts, standard passwords, and common services installed by default should also be reviewed and changed or disabled as required
- Use least privilege guidelines
    - Examples: Web, email, ftp, DNS, DHCP, file, print, database services

Application Patch Management

- Describes the method for keeping computers up-to-date with new software releases that are developed after an original software product is installed

- Requires checking for updates regularly

- Install latest updates, patches, service packs to fix bugs and security holes
  - How is this going to be accomplished?

- Don’t forget to update baseline!

- WSUS – Windows Server Update Service

NoSQL vs SQL Databases

- It is noteworthy that SQL is not a database type, but is rather a language to interact with the database.

- A RDBMS – Relationship Database Management System is a way to organize and structure data in a flat two-dimensional table

- A NoRDBMS based system uses hierarchical structuring rather then relationship

- Databases that are labeled as NoSQL may actually support SQL commands, and thus instead should be labeled as NoRDBMS

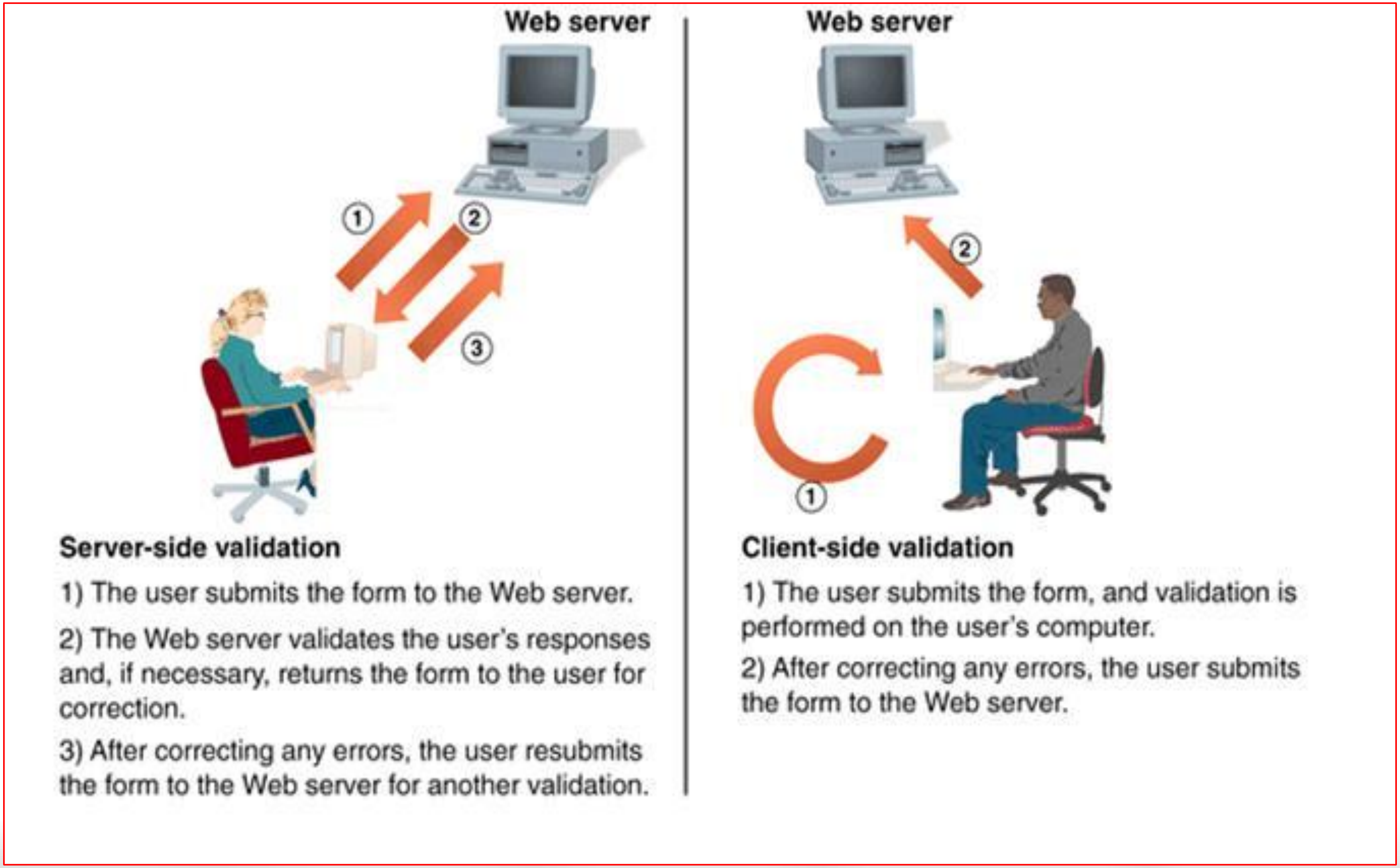
- An advantage to using a SQL database (RDBMS) is the ACID test

- ACID stands for:
  - Atomicity—Each transaction occurs in an all-or-nothing state.
  - Consistency—Each transaction maintains valid data and a valid state of the database.
  - Isolation—Each transaction occurs individually without interference.
  - Durability—Each transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

Exam Alert

- Software exploitation is a method of searching for specific problems, weaknesses, or security holes in software code
- It takes advantage of a program’s flawed code

Server-side vs. Client-side Validation



Server-side validation

1) The user submits the form to the Web server.

2) The Web server validates the user's responses and, if necessary, returns the form to the user for correction.

3) After correcting any errors, the user resubmits the form to the Web server for another validation.

Client-side validation

1) The user submits the form, and validation is performed on the user's computer.

2) After correcting any errors, the user submits the form to the Web server.

Student Check

Which of the following is a process by which semi-random data is injected into a program or protocol stack for detecting bugs?

- ○ A. Cross-site scripting
- ○ B. Fuzzing
- ○ C. Input validation
- ○ D. Cross-site request forgery

Student Check

Which of the following is a process by which semi-random data is injected into a program or protocol stack for detecting bugs?

- ○ A. Cross-site scripting
- ○ B. Fuzzing
- ○ C. Input validation
- ○ D. Cross-site request forgery

Student Check

Which of the following is not a way to prevent or protect against XSS?

○ A. Input validation
○ B. Defensive coding
○ C. Allowing script input
○ D. Escaping metacharacters

Student Check

Which of the following is not a way to prevent or protect against XSS?

- ○ A. Input validation
- ○ B. Defensive coding
- ○ C. Allowing script input
- ○ D. Escaping metacharacters

Student Check

Which of the following is not true in regards to NoSQL (NoRDBMS)?

○ **A. Can support SQL expressions**
○ **B. It is a relational database**
○ **C. Supports hierarchies or multilevel nesting/referencing**
○ **D. Does not support ACID**

Student Check

Which of the following is not true in regards to NoSQL (NoRDBMS)?

- ○ A. Can support SQL expressions
- ○ B. It is a relational database
- ○ C. Supports hierarchies or multilevel nesting/referencing
- ○ D. Does not support ACID

Objective 4.2

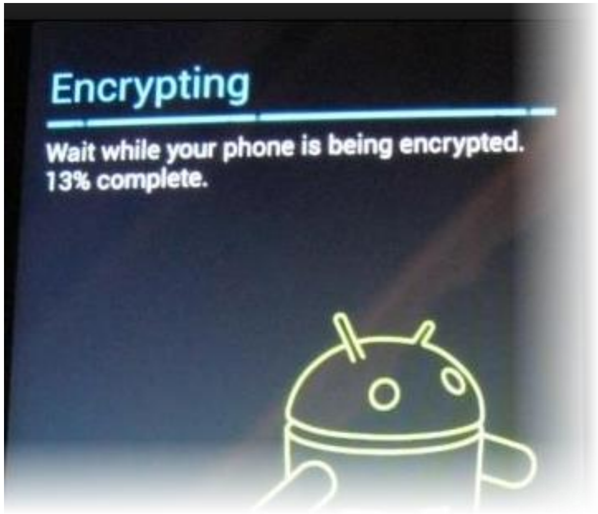
- Mobile security concepts and technologies

Device Security

- Why secure a Portable Electronic Device (PED)?

Full Device Encryption

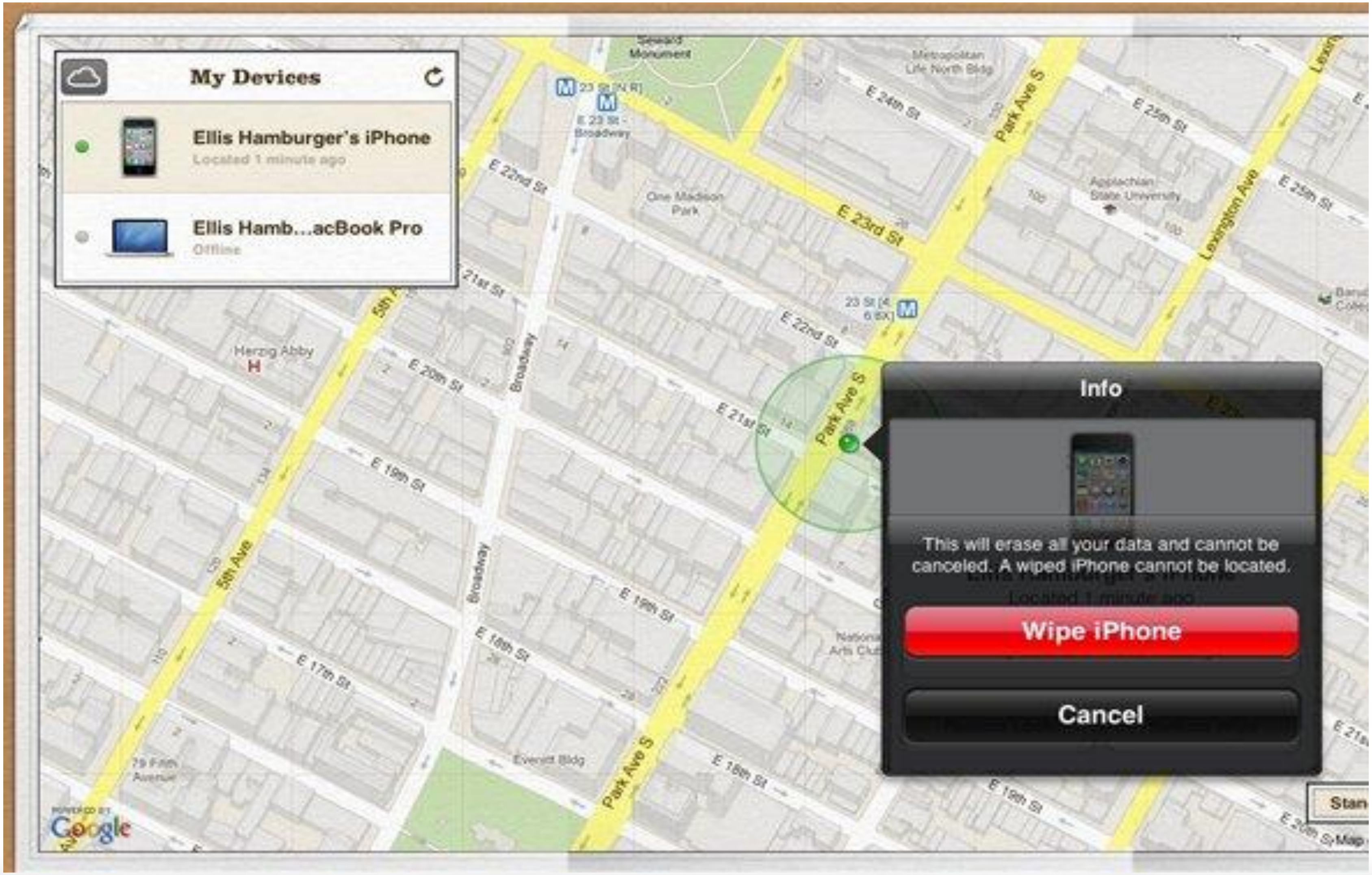
- Full Device Encryption (FDE)
  - Some mobile devices, including portable computers, tablets, as well as mobile phones, may offer device encryption
  - It only protects the data if the mobile device is locked or off
- Voice encryption
  - may be possible on mobile devices when voice over IP (VOIP) services are used



Encrypting

Wait while your phone is being encrypted. 13% complete.

Remote Wiping



This will erase all your data and cannot be canceled. A wiped iPhone cannot be located.

*Screen Locks & Lockout

- Screen Locks
  - Slide
  - Near Field Communication (NFC)
  - Face
  - Pattern
  - PIN
  - Password
- Lockout
  - Disable Device
  - Threshold

Identification
Ticketing
Time & Attendance
NFC
Loyalty & Membership
Physical Access
Cashless Payment
Secure PC Log-on
Transit

GPS

- Many mobile devices include a GPS chip to support and benefit from localized services, such as navigation, so it's possible to track those devices.

Application Control

- A device-management solution that limits which applications can be installed onto a device.

Application Control

How to protect your system and prevent the introduction of unauthorized applications and malware

Storage Segmentation

- To segregate data on a disk from other sectors.
- An example on a mobile device would be to logically segment the OS from the Apps.

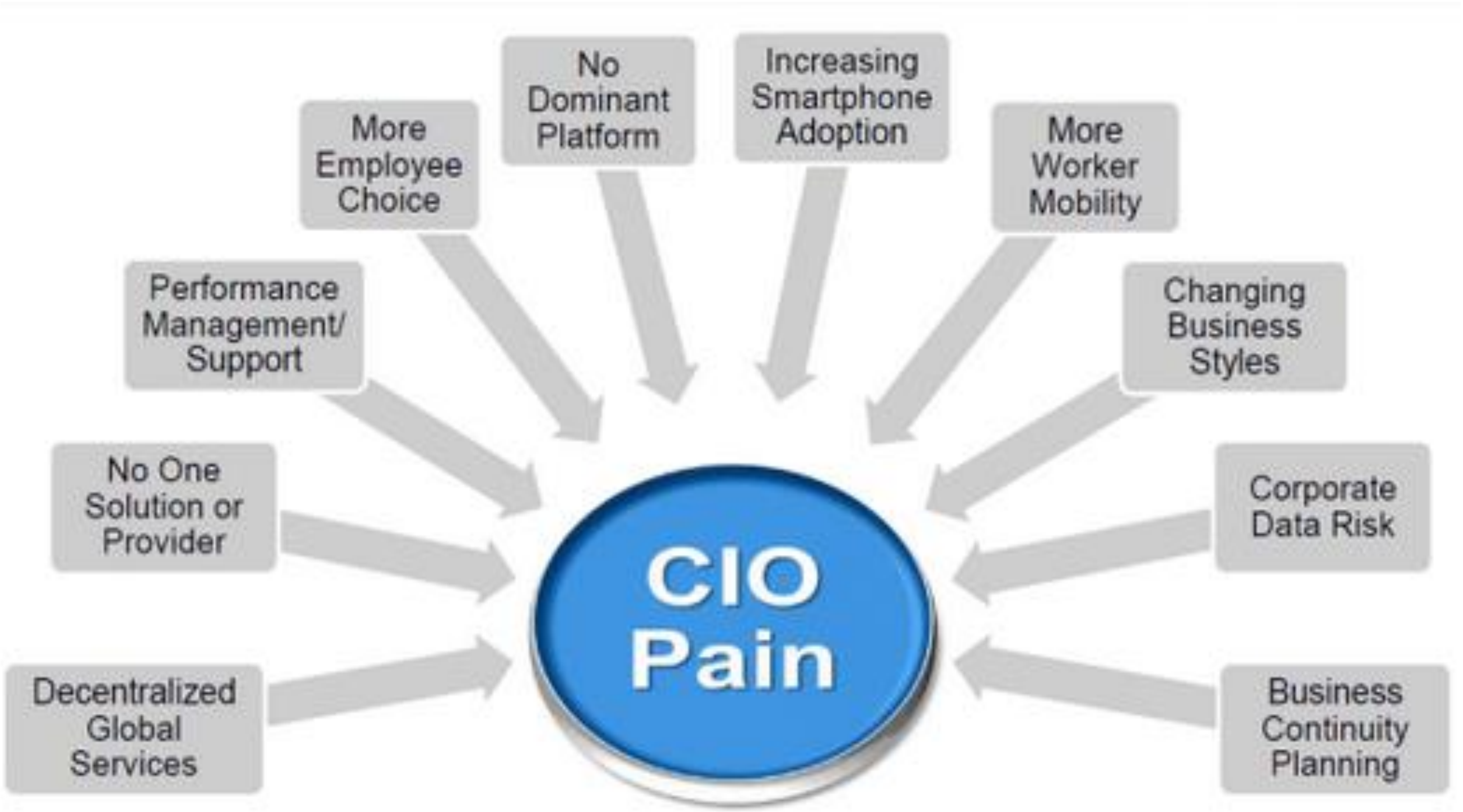
Asset Tracking

- Active
  - A system will push out a request for the device to respond.
- Passive
  - The device will attempt to contact the management service on a regular basis.

Inventory Control

- RFID
- NFC
- QR
- Barcode

Mobile Device Management



No Dominant Platform

Increasing Smartphone Adoption

More Employee Choice

More Worker Mobility

Performance Management/ Support

Changing Business Styles

No One Solution or Provider

Corporate Data Risk

Decentralized Global Services

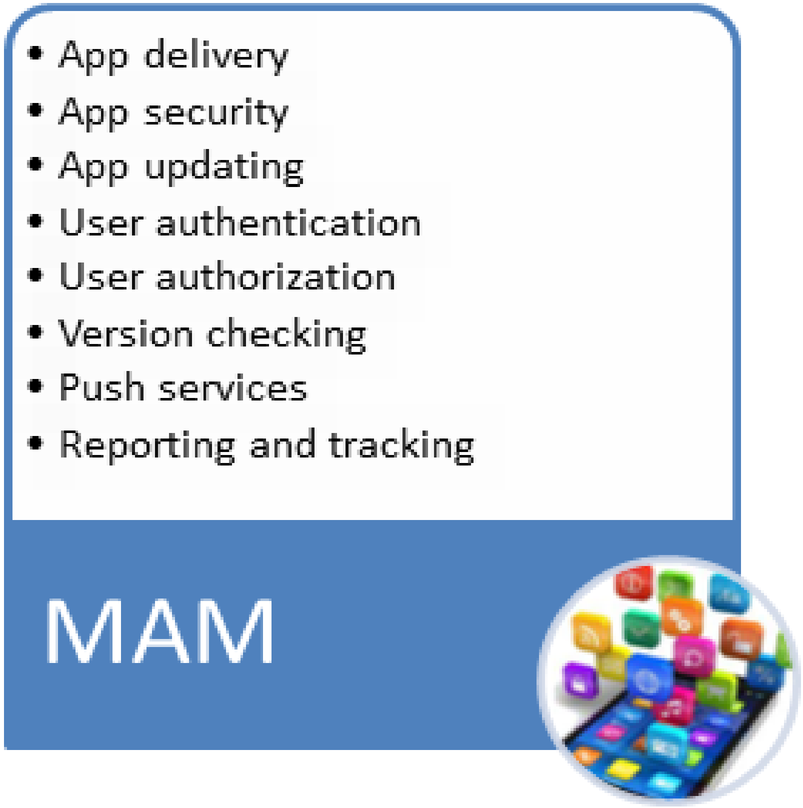
Business Continuity Planning

CIO Pain

Device Access Control

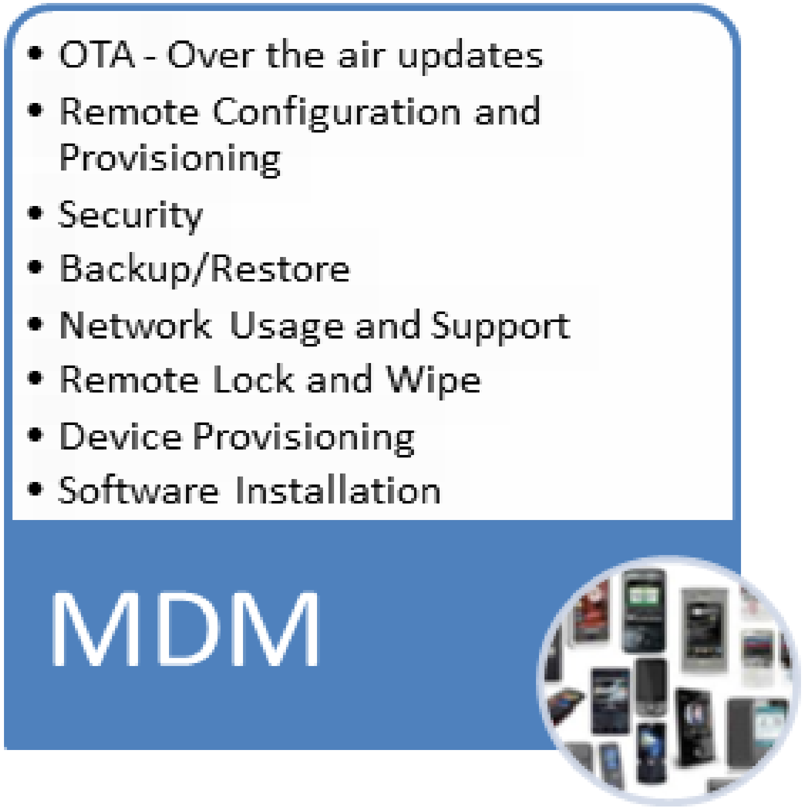
Mobile Application Management

Mobile Device Management



- App delivery
- App security
- App updating
- User authentication
- User authorization
- Version checking
- Push services
- Reporting and tracking

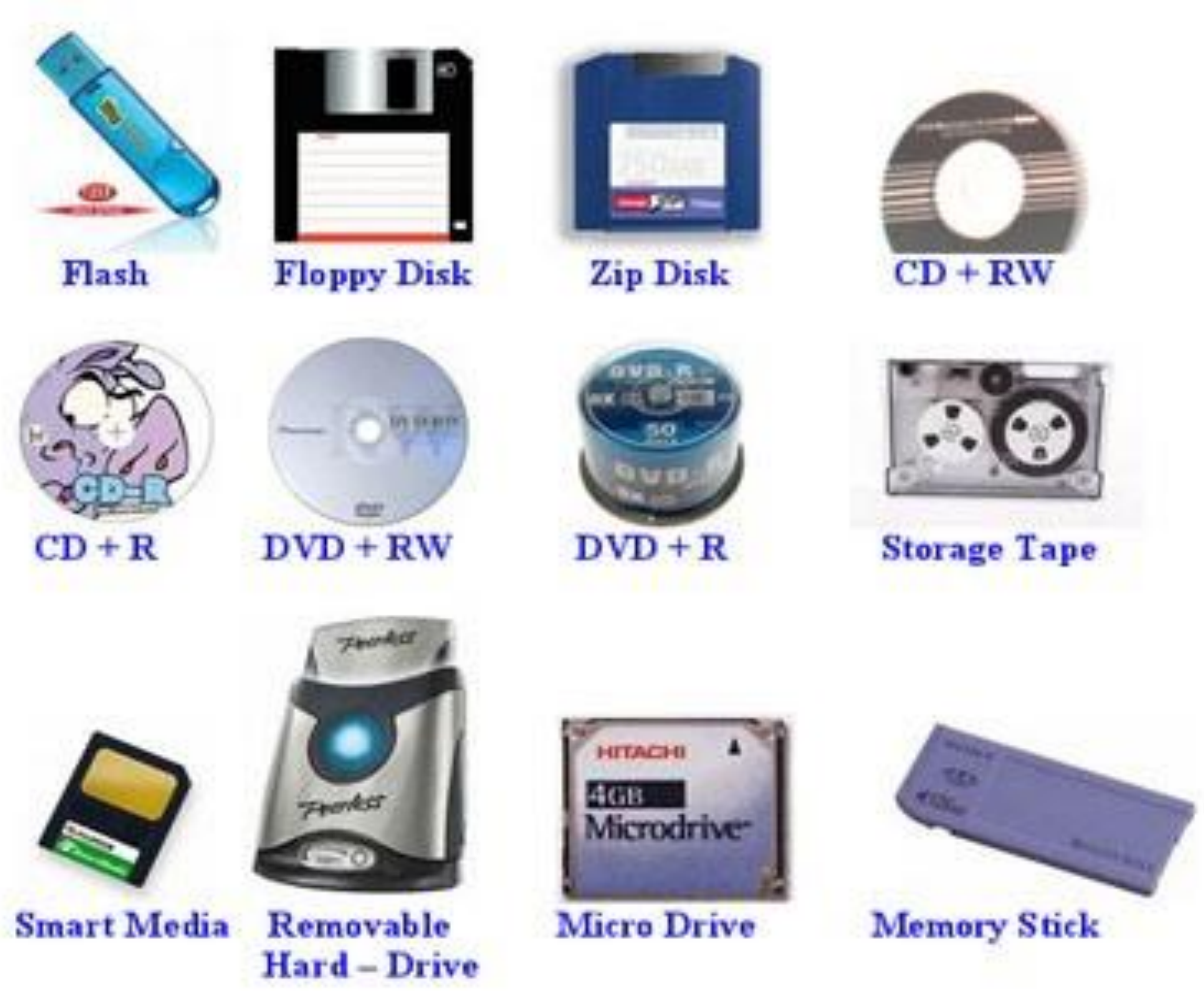
MAM



- OTA - Over the air updates
- Remote Configuration and Provisioning
- Security
- Backup/Restore
- Network Usage and Support
- Remote Lock and Wipe
- Device Provisioning
- Software Installation

MDM

Removable Storage



Application Security

- Key management
- Credential management
- Authentication
- Geo-tagging
- Encryption
- Application whitelisting
- Transitive trust/authentication

Covered on the next slides

Key Management

- Key management is always a concern when cryptography is involved.
- Most of the failures of a cryptosystem are based on the key management rather than on the algorithms
- Good key selection is based on the quality and availability of random numbers
- Most mobile devices must rely locally on poor random-number-producing mechanisms or access more robust random number generators (RNGs) over a wireless link
- Once keys are created, they need to be stored in such a way as to minimize exposure to loss or compromise

Credential Management

- The storage of credentials in a central location is referred to as *credential management*
- Given the wide range of Internet sites and services, each with its own particular logon requirements, it can be a burden to use unique names and passwords
- Credential management solutions offer a means to securely store a plethora of credential sets
- These often employ a master credential set

Authentication

- Whenever possible, use a password, provide a PIN, offer your eyeball or face for recognition, scan your fingerprint, or use a proximity device such as an NFC or RFID ring or tile
- These means of device authentication are much more difficult for a thief to bypass
- It’s also prudent to combine device authentication with device encryption

Geo-tagging

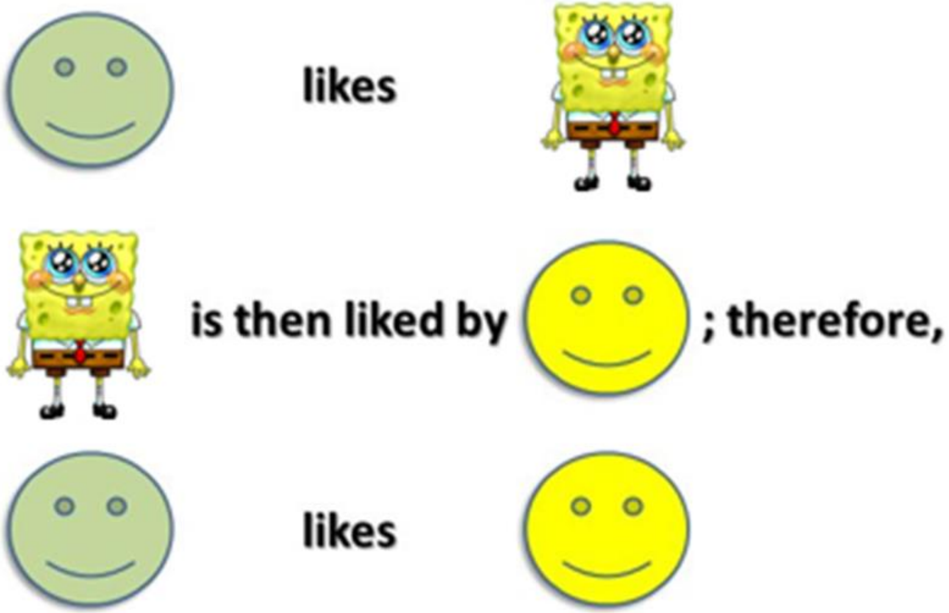
- Mobile devices with GPS support enable the embedding of geographical location in the form of latitude and longitude as well as date/time information on photos taken with these devices.
- This allows a would-be attacker to view photos from social networking or similar sites and determine exactly when and where a photo was taken
- This geo-tagging can be used for nefarious purposes, such as determining when a person normally performs routine activities
- Once a geo-tagged photo has been uploaded to the Internet, a potential cyber-stalker may have access to more information than the uploader intended.
- This is prime material for security-awareness briefs for end users.

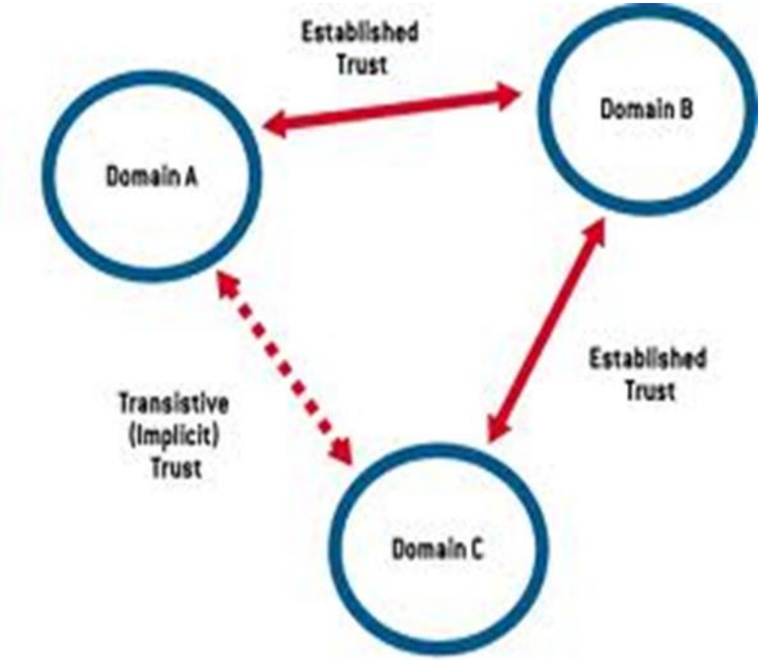
Application Whitelisting

- *Application whitelisting* is a security option that prohibits unauthorized software from being able to execute
- Whitelisting is also known as *deny by default* or *implicit deny*
- Whitelisting prevents any and all software, including malware, from executing unless it's on the preapproved exception list: the whitelist

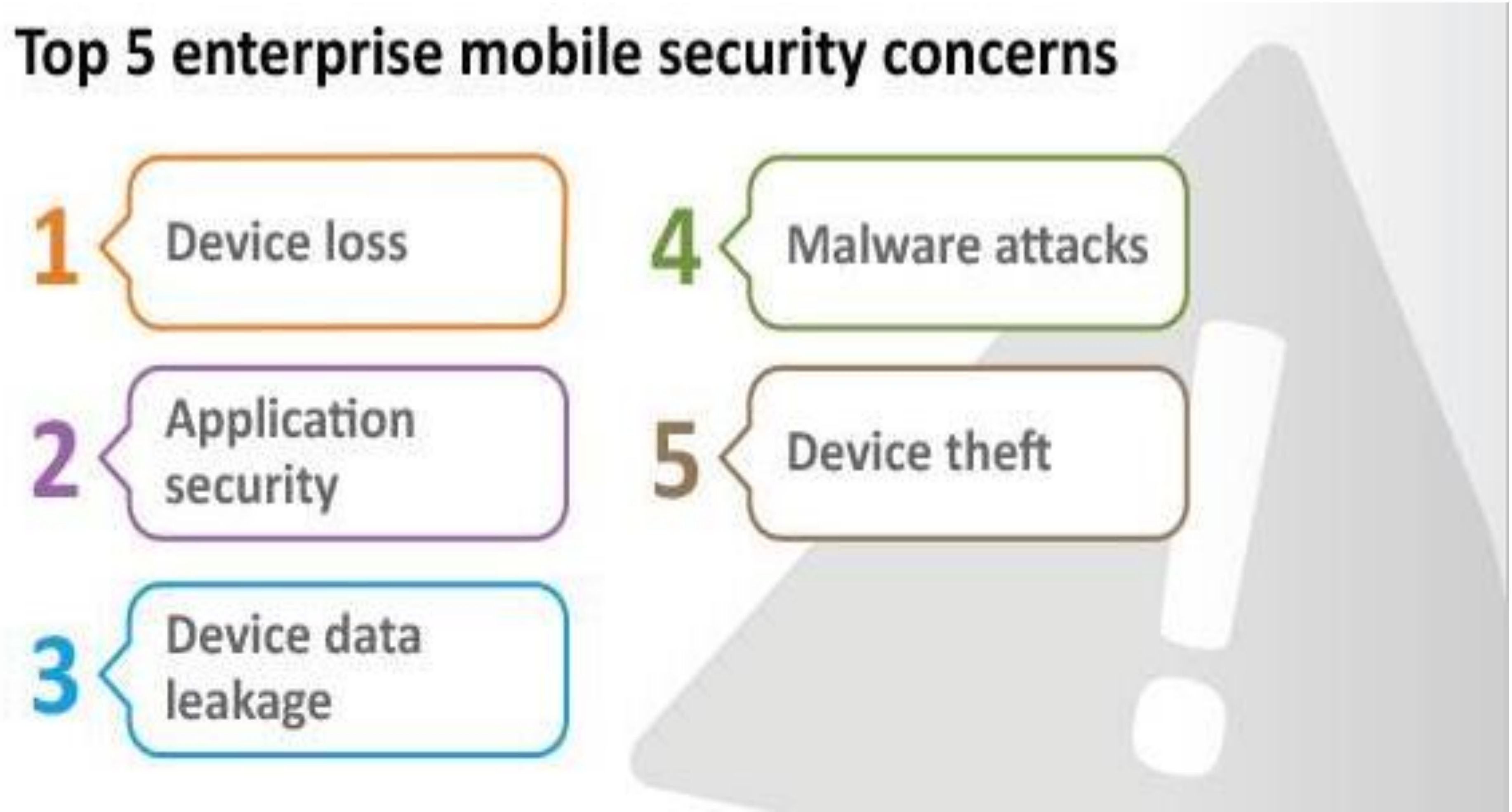
Transitive Trust / Authentication

- *Transitive access, trust, or authentication* are potential backdoor or ways to work around traditional means of access control





BYOD Concerns



Top 5 enterprise mobile security concerns

1 Device loss

2 Application security

3 Device data leakage

4 Malware attacks

5 Device theft

Data Ownership

- If a BYOD mobile device is stolen and corporate data resided on this equipment, can the company submit a remote wipe legally to prevent spillage?
  - YES

Support Ownership

- If a BYOD mobile device is damaged, who is ultimately responsible for replacing or fixing the equipment?
  - It all depends on what the user has signed with their employer.

Patch Management

- Who is responsible for providing updates to the BYOD?

Antivirus Management

- Your BYOD policy should dictate what level of AV or Malware support is required in order to join the Enterprise network.

Forensics

- Digital forensics is a multifaceted process for streamlining and simplifying discovery to uncover issues and increase investigation, litigation, and regulatory readiness.
- It can include a number of steps and impact various stages of an investigation.

Forensics

- Data collection
- Data processing
- Maintaining chain of custody records
- Hosting
- Review
- Production
- E-mail analytics
- Social networking and timeline analysis

Privacy

- Tracking the device even after work hours would be a simple scenario.
- This type of tracking would need to be identified in the BYOD Privacy Policy.

On-boarding/Off-boarding

- On-boarding
  - What type of image or settings are applied to the device when you bring the new Asset into the Enterprise?

- Off-boarding
  - What type of procedures are conducted when the devices is removed from BYOD assets for the Enterprise?

Corporate Policies

- Ensure you provide a policy which ensures the employee treats their BYOD equipment as if it was the company's.

User Acceptance

- A user needs to sign the User Acceptance prior to On-boarding their device within the Enterprise.
- The User Acceptance will cover restrictions, security settings, and MDM tracking.

Architecture/Infrastructure

- The IT department needs to consider the excessive amount of devices which will be connected to the network with implementing a BYOD architecture.
  - Bandwidth
  - IP Space
  - QOS
  - Wireless Infrastructure

Legal Concerns

- Always check with your Legal department when looking at implementing any BYOD architecture.
- This will ensure all of your corporate policies will not violate your staff or allow for your staff to take advantage of your corporation.

AUP

- An acceptable usage policy or fair use policy, is a set of rules applied by the owner or manager of a network, website, service, or large computer system that restrict the ways in which the network, website or system may be used.

On-board Camera/Video

- You need to ensure your policy covers the use of On-board Camera/Video hardware.
- This will prevent theft of corporate data.

Student Check

The most commonly overlooked aspect of mobile phone eavesdropping is related to __________.

- ○ **A. Wireless networking**
- ○ **B. Storage device encryption**
- ○ **C. Overhearing conversations**
- ○ **D. Screen locks**

Student Check

The most commonly overlooked aspect of mobile phone eavesdropping is related to __________.

○ A. Wireless networking

○ B. Storage device encryption

○ C. Overhearing conversations

○ D. Screen locks

Student Check

What technology provides an organization with the best control over BYOD equipment?

- ○ **A. Encrypted removable storage**
- ○ **B. Mobile device management**
- ○ **C. Geo-tagging**
- ○ **D. Application whitelisting**

Student Check

What technology provides an organization with the best control over BYOD equipment?

- ○ A. Encrypted removable storage
- ○ [✓ B. Mobile device management]
- ○ C. Geo-tagging
- ○ D. Application whitelisting

Student Check

Which security stance will be most successful at preventing malicious software execution?

○ A. Deny by exception
○ B. Whitelisting
○ C. Allow by default
○ D. Blacklisting

Student Check

Which security stance will be most successful at preventing malicious software execution?

- ○ A. Deny by exception
- ○ B. Whitelisting
- ○ C. Allow by default
- ○ D. Blacklisting

Objective 4.3

- Carry out appropriate procedures to establish host security

Operating system security and settings

- Systems installed in default configurations often include many unnecessary services that are configured automatically
- These provide many potential avenues for unauthorized access to a system or network

Hardening

- Disable unnecessary services
- Implement file–level security (NTFS permissions)
- Configure log files and auditing
- Configure security settings using Group Policies
- Close unused ports

Anti-malware

- All host devices must have some type of malware protection

- Study done by anti-malware company in 2011 stated that there was over 200 million malicious programs detected and neutralized on host devices

- Examples:
    - Anti-virus
    - Anti-spam
    - Anti-spyware
    - Pop-up blockers
    - Host-based firewalls

Anti-virus

- Always install an anti-virus application
  - Always keep definitions current
  - No anti-virus software application will stop everything
  - Stay diligent

Anti-Spam

- If you have email, you have spam
- Easy way to reach a very large number of people
- Could be legitimate sales attempt but can also be malicious
- Most email clients have anti-spam app built-in
- ISP may provide spam filter in the cloud
- Roughly 90% of all email in 2010 was spam

Anti-spyware

- It’s watching you and sending information back

- Browsing activity, key logs, usernames/passwords

- Need a local anti-spyware app to monitor for spyware

Pop-up Blockers

- Pop-ups are popular way to advertise
- Also known as adware
- Can be annoying, even cause a DoS condition
- Alt + F4 closes the active window
- Some pop-ups are legitimate an you need to adjust the pop-up blocker in your web browser accordingly
- Most web browsers you can hold CTRL+ Click on the link to bypass the pop-up blocker

Patch Management

- Install latest updates, patches, service packs to fix bugs and security holes

White/Black Listing Applications

- Whitelist
  - Is an approved list of software
- Blacklist
  - Is an unauthorized list of software

Trusted OS

- Common Criteria (CC) for Information Technology Security Evaluation.
  - An international computer security certification standard and reference for the US Government
  - ISO/IEC 15408
- Evaluation Assurance Level (EAL)
  - EAL1 – 7
  - EAL4 is the most accepted minimum level
  - Trusted Solaris, Mac OS X10.6, HP-UX 11i v3, AIX 5L, SELinux and SUSE Linix, Windows 7, 8, 8.1, 10

Host-Based Firewalls

- Protect against others on the network
- Restricts access to your host device
- Example: Windows Firewall

Host–based Intrusion Detection

- A host–based IDS monitors all or parts of the dynamic behavior and the state of a computer system
- A HIDS might look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected, e.g. have not been changed by intruders.

Hardware security

- Physical access to a system creates many avenues for a breach in security

- Basic input/output system (BIOS)
  - Identifies and initiates the basic system hardware components

- Universal Serial Bus (USB)

Cable Locks

- Good temporary security for mobile devices

Safe

- Secure important hardware and media
- Protect against elements
    - Fire, water, etc…
- Difficult to steal

Locking Cabinets

- Data centers hardware is generally managed by different groups
- Enclosed cabinets with locks

Host software baselining

- The measure of normal activity is known as a baseline
- This gives you a point of reference when something on the computer goes bonkers
- Without a baseline, it is harder to see what is wrong because you don’t know what is normal
- Baselines must be updated on a regular basis and certainly when the computer has changed or new technology has been deployed

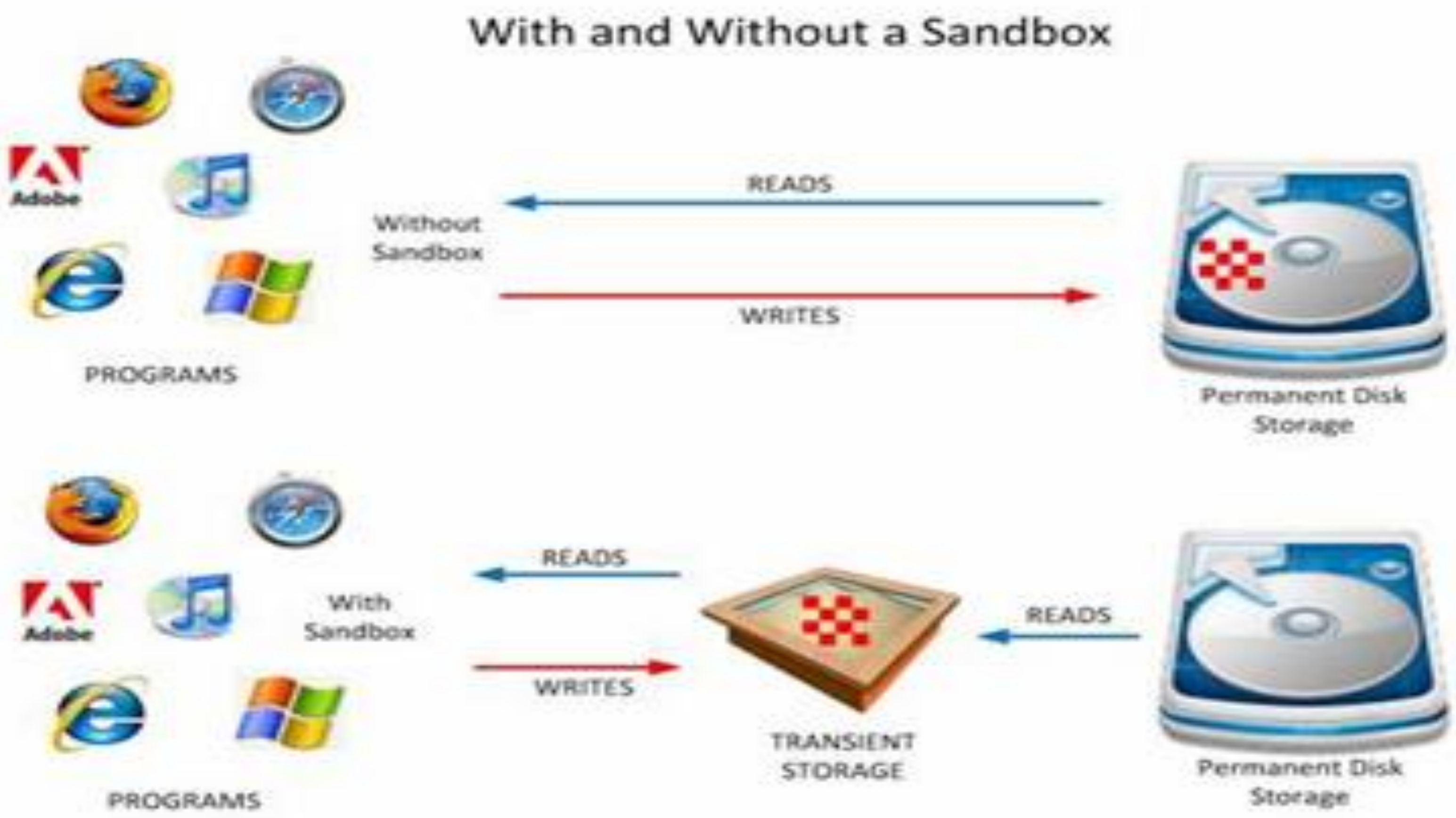
Patch Compatibility

- You need to update your virtual machines just like you would your physical servers.

Host Availability

- Ensuring your Baremetal Hypervisor or Host OS is up and running is essential to your virtual environments health.

Security Control Testing / Sandboxing



Student Check

An organization is looking for a mobile solution that will allow executives and employees alike to discuss sensitive information without having to travel to secure company locations.

Which of the following fulfills this requirement?

- ○ **A. GPS tracking**
- ○ **B. Remote wipe**
- ○ **C. Voice encryption**
- ○ **D. Passcode policy**

Student Check

An organization is looking for a mobile solution that will allow executives and employees alike to discuss sensitive information without having to travel to secure company locations.

Which of the following fulfills this requirement?

- ○ A. GPS tracking
- ○ B. Remote wipe
- ○ C. Voice encryption
- ○ D. Passcode policy

Student Check

Which of the following procedures should be used to properly protect a host from malware? (Select two correct answers.)

○ A. Web tracking software
○ B. Antivirus software
○ C. Content filtering software
○ D. Pop-up blocking software

Student Check

Which of the following procedures should be used to properly protect a host from malware? (Select two correct answers.)

- ○ A. Web tracking software
- ○ B. Antivirus software
- ○ C. Content filtering software
- ○ D. Pop-up blocking software

Student Check

When a vendor releases a patch, which of the following is the most important?

- ○ **A. Installing the patch immediately**
- ○ **B. Setting up automatic patch installation**
- ○ **C. Allowing users to apply patches**
- ○ **D. Testing the patch before implementation**

Student Check

When a vendor releases a patch, which of the following is the most important?

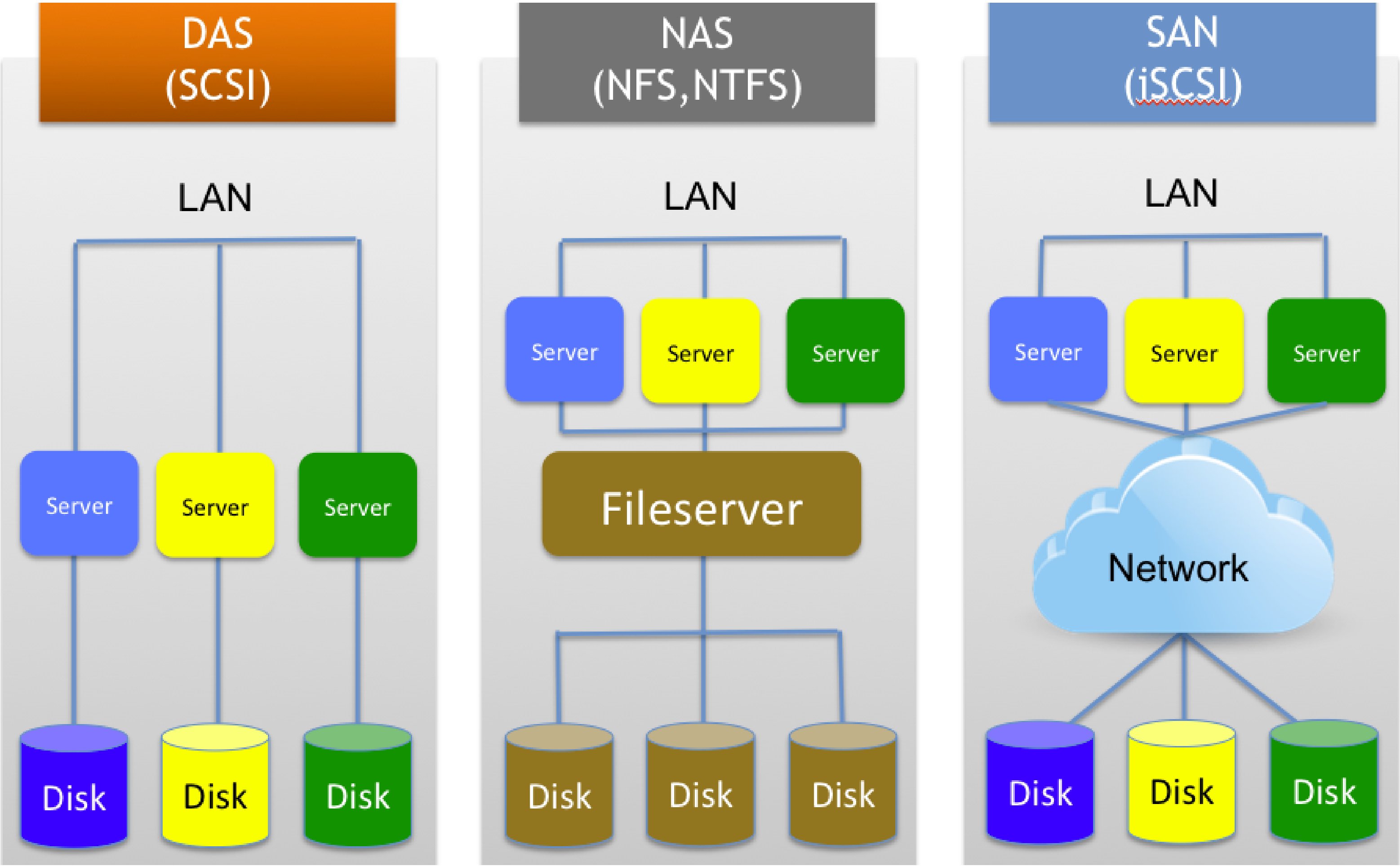
- ○ A. Installing the patch immediately
- ○ B. Setting up automatic patch installation
- ○ C. Allowing users to apply patches
- ○ D. Testing the patch before implementation

Objective 4.4

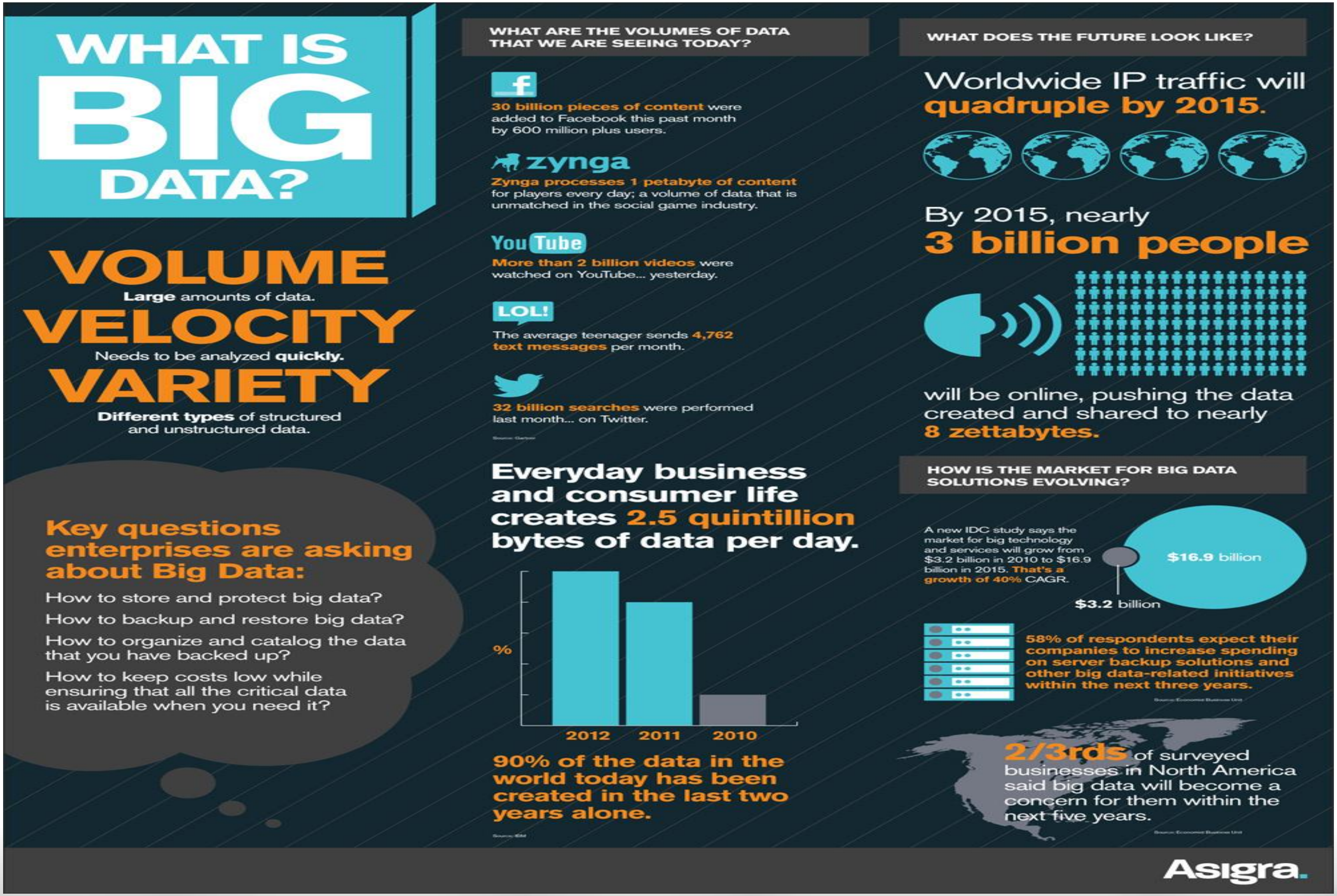
- Explain the appropriate controls to ensure data security.

Cloud Storage

DAS/NAS/SAN


DAS
(SCSI)
LAN
Server
Server
Server
Disk
Disk
Disk
NAS
(NFS,NTFS)
LAN
Server
Server
Server
Fileserver
Disk
Disk
Disk
SAN
(iSCSI)
LAN
Server
Server
Server
Network
Disk
Disk
Disk

Big Data



WHAT IS BIG DATA?

VOLUME
Large amounts of data.

VELOCITY
Needs to be analyzed **quickly.**

VARIETY
Different types of structured and unstructured data.

Key questions enterprises are asking about Big Data:

How to store and protect big data?

How to backup and restore big data?

How to organize and catalog the data that you have backed up?

How to keep costs low while ensuring that all the critical data is available when you need it?

WHAT ARE THE VOLUMES OF DATA THAT WE ARE SEEING TODAY?

30 billion pieces of content were added to Facebook this past month by 600 million plus users.

Zynga processes 1 petabyte of content for players every day; a volume of data that is unmatched in the social game industry.

More than 2 billion videos were watched on YouTube... yesterday.

The average teenager sends **4,762 text messages** per month.

32 billion searches were performed last month... on Twitter.

Source: Gartner

Everyday business and consumer life creates 2.5 quintillion bytes of data per day.

90% of the data in the world today has been created in the last two years alone.

Source: IBM

WHAT DOES THE FUTURE LOOK LIKE?

Worldwide IP traffic will **quadruple by 2015.**

By 2015, nearly **3 billion people** will be online, pushing the data created and shared to nearly **8 zettabytes.**

HOW IS THE MARKET FOR BIG DATA SOLUTIONS EVOLVING?

A new IDC study says the market for big technology and services will grow from $3.2 billion in 2010 to $16.9 billion in 2015. **That's a growth of 40%** CAGR.

58% of respondents expect their companies to increase spending on server backup solutions and other big data-related initiatives within the next three years.

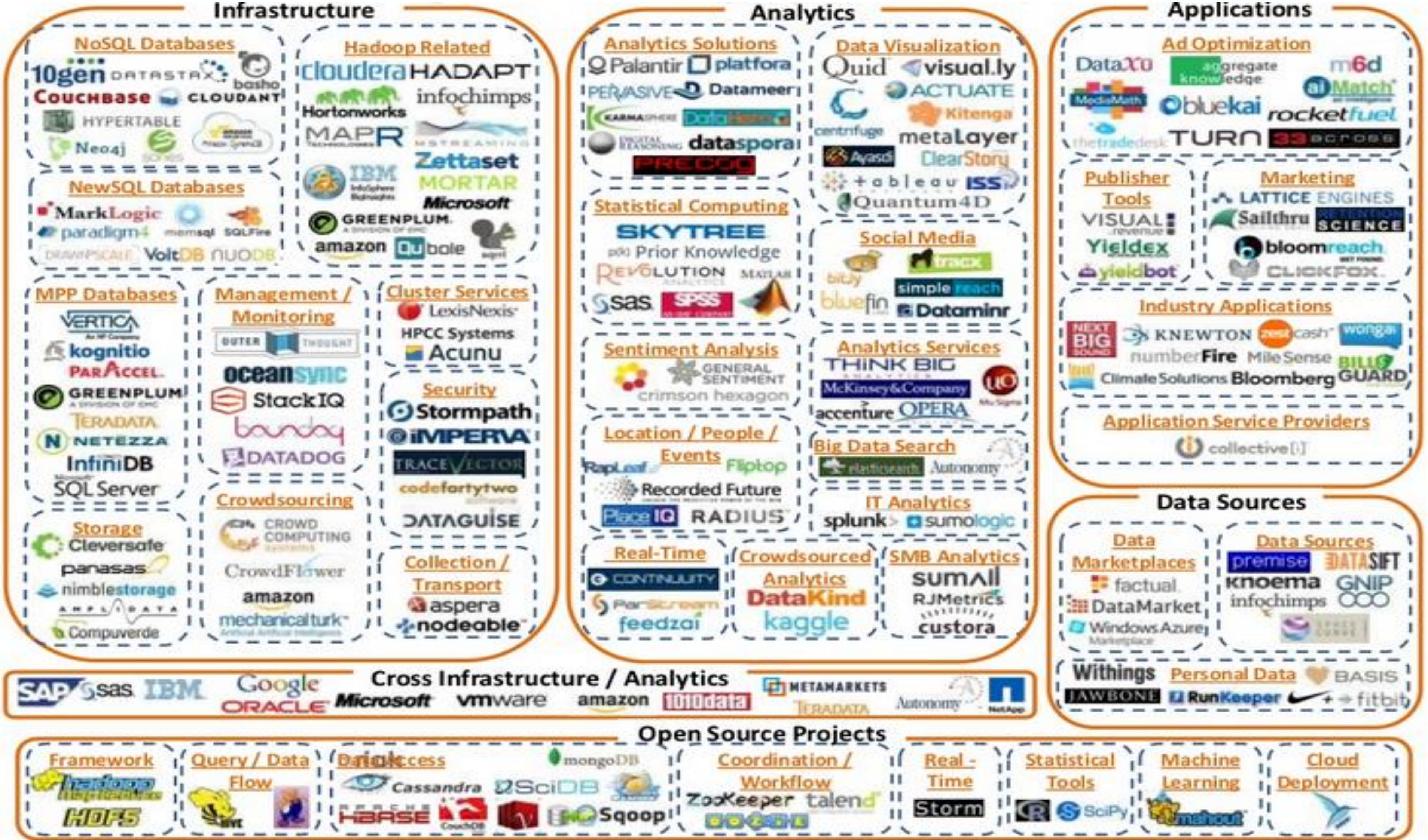
Source: Economist Business Unit

2/3rds of surveyed businesses in North America said big data will become a concern for them within the next five years.

Source: Economist Business Unit

Asigra.

Big Data Landscape



Data Loss Prevention (DLP)

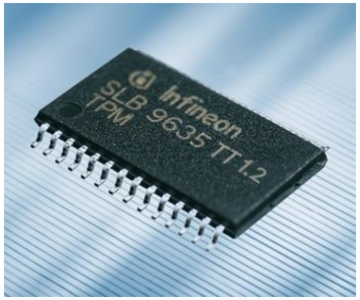
- Ensuring that data does not get outside of your organization or in the hands of people who should not have access to that data
- Prevent data “leakage”
- Think about all of the sources of data
  - Data in motion and data at rest

Data encryption

- Full disk or whole disk
  - Every bit is encrypted
  - BitLocker
- Database
  - Difficult to encrypt entire DB due to the amount files
  - Encrypt only sensitive information (credit card numbers)
- Individual files
  - Encrypted File System (EFS)
- Removable media
  - BitLocker To Go
- Mobile devices

Hardware based encryption devices

- Trusted Platform Module
  - A secure crypto processor used to authenticate hardware devices such as PC or laptop
  - Internal

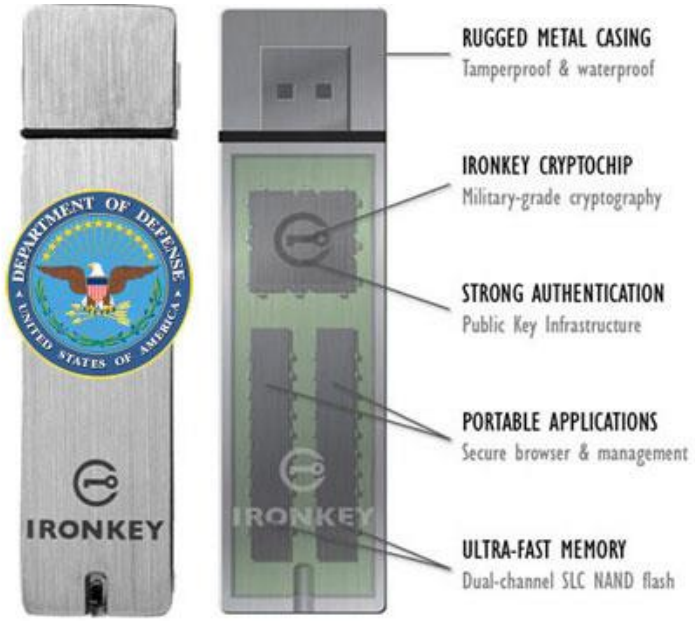


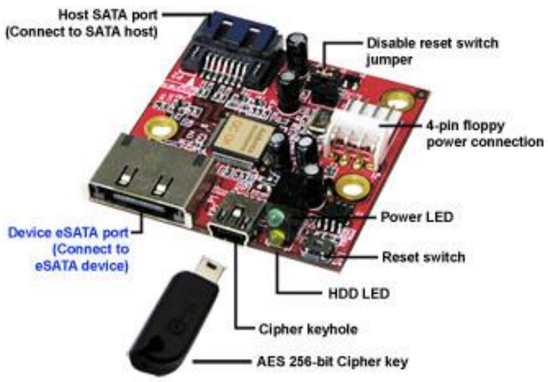
- Hardware Security Module (HSM)
  - High-end cryptographic hardware
  - External

Hardware based encryption devices

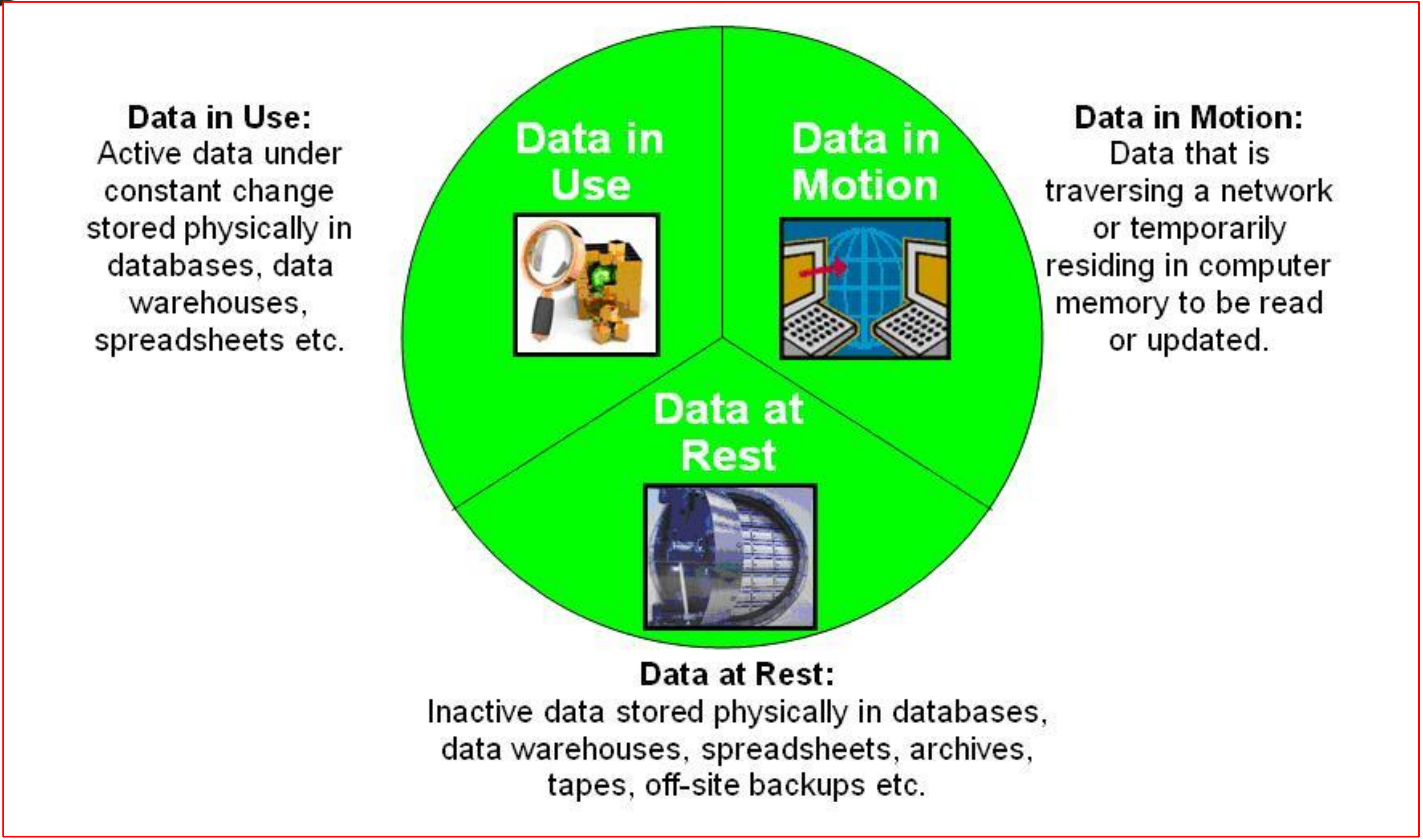
- USB encryption

- Hard drive





Data



Data in Use:
Active data under
constant change
stored physically in
databases, data
warehouses,
spreadsheets etc.

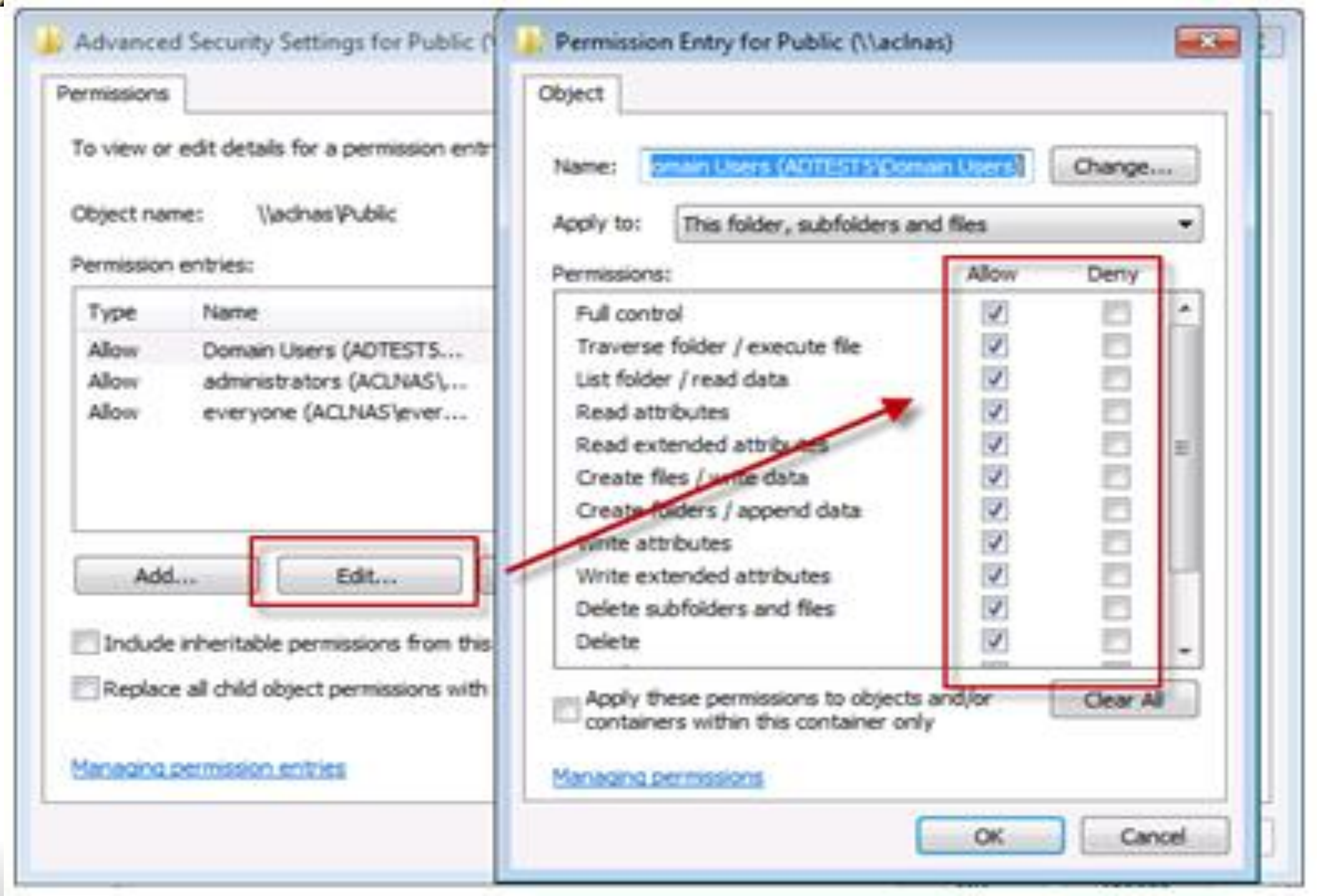
Data in Motion:
Data that is
traversing a network
or temporarily
residing in computer
memory to be read
or updated.

Data at Rest:
Inactive data stored physically in databases,
data warehouses, spreadsheets, archives,
tapes, off-site backups etc.

Permissions/ACL

- Every object in a DAC (Discretionary Access Control) environment has an ACL.
- An ACL is a collection of ACE (Access Control Entries).
- Each ACE focuses on either one user account or a group and then grants or denies an object-specific permission, such as read, write, or execute
- Least privilege means users should only have sufficient permissions to accomplish their work.

Permissions/ACL



Advanced Security Settings for Public (\

To view or edit details for a permission entr

Object name: \\aclnas\Public

Permission entries:

Type	Name
Allow	Domain Users (ADTEST5...
Allow	administrators (ACLNAS\...
Allow	everyone (ACLNAS\ever...

□ Include inheritable permissions from this

□ Replace all child object permissions with

Permission Entry for Public (\\aclnas)

Name: omain Users (ADTEST5\Domain Users)

Apply to: This folder, subfolders and files

Permissions:

	Allow	Deny
Full control	☑	□
Traverse folder / execute file	☑	□
List folder / read data	☑	□
Read attributes	☑	□
Read extended attributes	☑	□
Create files / write data	☑	□
Create folders / append data	☑	□
Write attributes	☑	□
Write extended attributes	☑	□
Delete subfolders and files	☑	□
Delete	☑	□

□ Apply these permissions to objects and/or containers within this container only

Data Policies

- Wiping
  - Degaussing or Random data overwriting
- Disposing
  - Incineration/Acid Bath/Crushing
- Retention
  - Keep financial records for x amount of time
  - Make sure you meet Federal/State law
- Storage
  - Off site

Student Check

The most effective means to reduce the risk of losing the data on a mobile device, such as a notebook computer, is _________________.

○ A. Encrypt the hard drive
○ B. Minimize sensitive data stored on the mobile device
○ C. Use a cable lock
○ D. Define a strong logon password

Student Check

The most effective means to reduce the risk of losing the data on a mobile device, such as a notebook computer, is ________________.

○ A. Encrypt the hard drive

○ B. Minimize sensitive data stored on the mobile device

○ C. Use a cable lock

○ D. Define a strong logon password

Student Check

In order to ensure that whole–drive encryption provides the best security possible, which of the following should not be performed?

○ A. Screen lock the system overnight
○ B. Require a boot password to unlock the drive
○ C. Lock the system in a safe when it is not in use
○ D. Power down the system after use

Student Check

In order to ensure that whole-drive encryption provides the best security possible, which of the following should not be performed?

○ A. Screen lock the system overnight
○ B. Require a boot password to unlock the drive
○ C. Lock the system in a safe when it is not in use
○ D. Power down the system after use

Student Check

Which of the following uses a secure cryptoprocessor to authenticate hardware devices such as PC or laptop?

○ **A. Trusted Platform Module**
○ **B. Full disk encryption**
○ **C. File–level encryption**
○ **D. Public key infrastructure**

Student Check

Which of the following uses a secure cryptoprocessor to authenticate hardware devices such as PC or laptop?

- ○ A. Trusted Platform Module
- ○ B. Full disk encryption
- ○ C. File-level encryption
- ○ D. Public key infrastructure

Objective 4.5

- Explain the appropriate methods to mitigate security risks in static environments.

Environments

- A *static IT environment* is any system that is intended to remain unchanged by users and administrators.
- The goal is to prevent or at least reduce the possibility of a user implementing change that could result in reduced security or functional operation.

SCADA

- *Supervisory control and data acquisition (SCADA)* is a type of *industrial control system (ICS)*
- SCADA is used across many industries, including manufacturing, fabrication, electricity generation and distribution, water distribution, sewage processing, and oil refining.
- A SCADA system can operate as a stand-alone device, be networked together with other SCADA systems, or be networked with traditional IT systems

Embedded Devices

- An *embedded system* is a computer implemented as part of a larger system
- The embedded system is typically designed around a limited set of specific functions in relation to the larger product of which it’s a component

- Examples: Printer, Smart TV, HVAC Control

Android

- *Android* is a mobile device OS based on Linux, which was acquired by Google in 2005.
- In 2008, the first devices hosting Android were made available to the public.
- The use of Android in phones and tablets isn't a good example of a static environment
- Whether static or not, Android has numerous security vulnerabilities
- These include exposure to malicious apps, running scripts from malicious websites, and allowing unsecure data transmissions
- Rooting increases a device's security risk, because all running code inherits root privileges

iOS

- *iOS* is the mobile device OS from Apple that is available on the iPhone, iPad, iPod, and Apple TV
- Unlike Android, Apple is in full control of the features and capabilities of iOS
- Jailbreaking an iOS device reduces its security and exposes the device to potential compromise

Mainframe

- *Mainframes* are high-end computer systems used to perform highly complex calculations and provide bulk data processing
- Modern mainframes are much more flexible and are often used to provide high-speed computation power in support of numerous virtual machines
- Each virtual machine can be used to host a unique OS and in turn support a wide range of applications

Game Consoles

- *Game consoles*, whether home systems or portable systems, are potentially examples of static systems
- The OS of a game console is generally fixed and is changed only when the vendor releases a system upgrade
- The more flexible and open-ended the app support, the less of a static system it becomes

In-vehicle Computing Systems

- *In-vehicle computing systems* can include the components used to monitor engine performance and optimize braking, steering, and suspension, but can also include in-dash elements related to driving, environment controls, and entertainment
- Modern in-vehicle systems may offer a wider range of capabilities, including linking a mobile device or running custom apps

Methods

- Static environments, embedded systems, and other limited or single-purpose computing environments need security management
- Although they may not have as broad an attack surface and aren’t exposed to as many risks as a general-purpose computer, they still require proper security government

Network Segmentation

- *Network segmentation* involves controlling traffic among networked devices
- Complete or physical network segmentation occurs when a network is isolated from all outside communications, so transactions can only occur between devices within the segmented network

Security Layers

- *Security layers* exist where devices with different levels of classification or sensitivity are grouped together and isolated from other groups with different levels
- *Logical isolation* requires the use of classification labels on data and packets, which must be respected and enforced by network management, OSs, and applications
- *Physical isolation* requires implementing network segmentation or air gaps between networks of different security levels

Application Firewalls

- An *application firewall* is a device, server add-on, virtual service, or system filter that defines a strict set of communication rules for a service and all users
- Examples: Comodo or Windows Firewall

Manual Updates

- *Manual updates* should be used in static environments to ensure that only tested and authorized changes are implemented
- Using an automated update system would allow for untested updates to introduce unknown security reductions

Firmware Version Control

- Firmware updates should be implemented on a manual basis, only after testing and review

Wrappers

- A *wrapper* is something used to enclose or contain something else
- Wrappers are well known in the security community in relation to Trojan horse malware
- Some static environments may be configured to reject updates, changes, or software installations unless they’re introduced through a controlled channel

Control Redundancy and Diversity

- As with any security solution, relying on a single security mechanism is unwise
- *Defense in depth* uses multiple types of access controls in literal or theoretical concentric circles or layers

Student Check

What is a security risk of an embedded system that is not commonly found in a standard PC?

○ A. Power loss

○ B. Access to the Internet

○ C. Control of a mechanism in the physical world

○ D. Software flaws

Student Check

What is a security risk of an embedded system that is not commonly found in a standard PC?

○ A. Power loss

○ B. Access to the Internet

○ C. Control of a mechanism in the physical world

○ D. Software flaws