SENG 460

Practice of Information Security and Privacy

Operations Security

Overview

- Operations Security Concepts
- Operations Security Responsibilities
- Media Control Technologies
- Redundancy and Fault-tolerant Systems
- Backup Systems

Operations Security Concepts

- **Security Administrator (SA) vs Network administrator (NA): SA** performs backups and recovery procedures, setting permissions, add and remove users, and develop user profiles. **NA** ensures high availability and performance of the network resources and provide the users with the functionality they request.
- **Need-to-Know vs Least Privilege**: *Need to know* requires that users should have access only to the information and resources necessary to complete their tasks that fulfill their roles; *Least privilege* means an individual should have just enough permissions and rights to fulfill his role in the company and no more.
- an organization.Give users access only to resources required to do their job.
- **Clipping Levels:** a predefined threshold for the number of certain types of errors that will be allowed before the activity is considered suspicious.
- **Mean Time Between Failures (MTBF):** the estimated lifespan of a piece of equipment.
- **Mean Time to Repair (MTTR):** the amount of time it will be expected to take to get a device fixed and back into production.
- **Single Point of Failure:** a part of a system that, if it fails, will stop the entire system from working.

Operations Security Responsibilities

- Administrative Management
- Asset Management
- Incidental Response Management
- Change Management
- Configuration Management
- Audit and Review

Operations Security Responsibilities

- Administrative Management

- Personnel Administration
  - Separation of duties, Job rotation, Mandatory vacation, etc.

- Security Administration
  - Implements and maintains security devices and software
  - Carries out security assessments
  - Creates and maintains user profiles and implements and maintains access control mechanisms
  - Configures and maintains security labels in mandatory access control (MAC) environments

Operations Security Responsibilities

- Asset Management

- Know all the asset—hardware, firmware, operating system, applications, and individual libraries—in the overall environment.
  - Inventory tools
- Protect all the asset.
  - Identity and Access Management Systems
- Ensure asset availability.
  - Redundancy and Fault Tolerance Systems
  - Backup and Recovery Systems

Tangible Asset & Intangible Asset

Tangible Asset *is the asset we can see and touch.* ***Intangible Asset****: asset is the asset we can't see and touch.*

Operations Security Responsibilities

- Incidental Response Management

- The incident response team should have the following basic items available:
    - A list of outside agencies and resources to contact or report to.
    - Roles and responsibilities outlined.
    - A call tree to contact these roles and outside entities.
    - A list of computer or forensics experts to contact.
    - Steps on how to secure and preserve evidence.
    - A list of items that should be included on a report for management and potentially the courts.
    - A description of how the different systems should be treated in this type of situation. (For example, the systems should be removed from both the Internet and the network and powered down.)

- The incident response steps include the following:
    1. Detect
    2. Respond
    3. Report
    4. Recover\Remediate
    5. Review

Event vs. Incident

An ***event*** is a negative occurrence that can be observed, verified, and documented, whereas an ***incident*** is a series of events that negatively affects the company and/or impacts its security posture.

Operations Security Responsibilities

- Change Management

- Numerous changes can take place in a company, some of which are as follows:
  - New computers installed
  - New applications installed
  - Different configurations implemented
  - Patches and updates installed
  - New technologies integrated
  - Policies, procedures, and standards updated
  - New regulations and requirements implemented
  - Network or system problems identified and fixes implemented
  - Different network configuration implemented
  - New networking devices integrated into the network
  - Company acquired by, or merged with, another company

- Although the types of changes vary, a standard list of procedures can help keep the process under control and ensure it is carried out in a predictable manner (samples procedures introduced in Software Development Security topic) .

Operations Security Responsibilities

- Configuration Management

- A subset of Change Management, but focuses on establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design and operational information throughout its life.

- The functions of configuration management includes:
  - Report the status of configuration changes
  - Document the characteristics of each configuration item.
  - Perform version control
  - Control the changes to the configuration items

- Four procedures normally defined for Configuration Management:

  - Configuration identification
  - Configuration control
  - Configuration status accounting
  - Configuration audits

Patch Management *is part of Configuration management.*

Operations Security Responsibilities

- Audit and Review

- Capturing and monitoring audit logs helps determine if a violation has actually occurred or if system and software reconfiguration is needed.
- Auditing needs to take place in a routine manner.
- Logs can be reviewed through either manual or automatic methods.
- Log reviews should focus on the users, their actions, and the current level of security and access:
  - Are users accessing information and performing tasks that are not necessary for their job description?
  - Are repetitive mistakes being made?
  - Do too many users have rights and privileges to sensitive or restricted data or resources?

Media Control Technologies

- Media Control Concepts

- "**Media**" include both electronic (disk, CD/DVD, tape, Flash devices such as USB "thumb drives," and so on) and non-electronic (paper) forms of information.
- **Data Remanence:** the residual physical representation of information that was saved and then erased in some fashion
- **Data Purging:** making information unrecoverable even with extraordinary effort such as physical forensics in a laboratory.
  - ***Zeroization:*** overwriting with a pattern designed to ensure that the data formerly on the media are not practically recoverable.
  - ***Degaussing:*** magnetic scrambling of the patterns on a tape or disk that represent the information stored there.
  - ***Destruction:*** shredding, crushing, burning.

Not all clearing/purging methods are applicable to all media—for example, optical media is not susceptible to degaussing, and overwriting may not be effective against Flash devices.

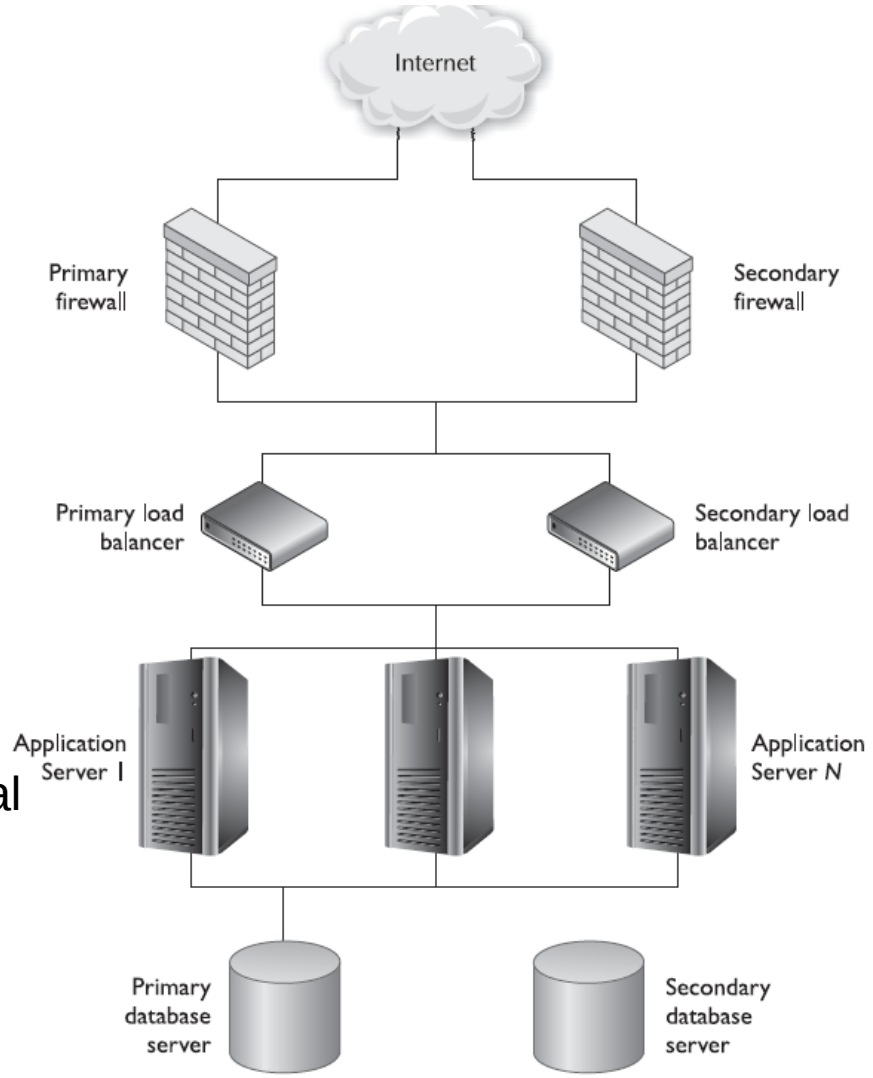
Media Control Technologies

- Media Control Practices

- Tracking (audit logging)
- Effectively implementing access controls
- Tracking the number and location of backup versions
- Documenting the history of changes to media
- Ensuring environmental conditions do not endanger media
- Ensuring media integrity
- Inventorying the media on a scheduled basis
- Carrying out secure disposal activities
- Internal and external labeling

Redundancy and Fault-tolerant Systems

- Backup and redundant systems make sure that when something happens, users' productivity will not be drastically affected.
- Device backup solutions and other availability solutions are chosen to balance the value of having information available against the cost of keeping that information available.
- Each critical device may require a redundant partner to ensure availability.
- Fault tolerance is among the most expensive possible solutions, and is justified only for the most mission-critical information.



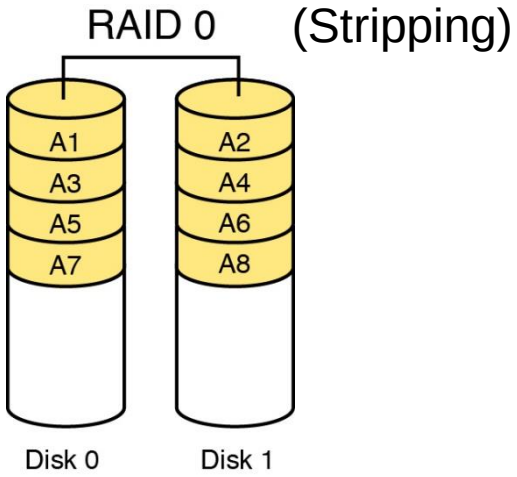
Redundancy and Fault-tolerant Systems

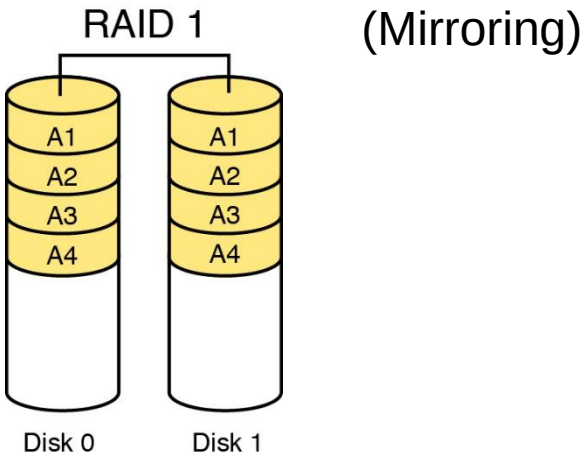
- Redundant array of independent disks (RAID)

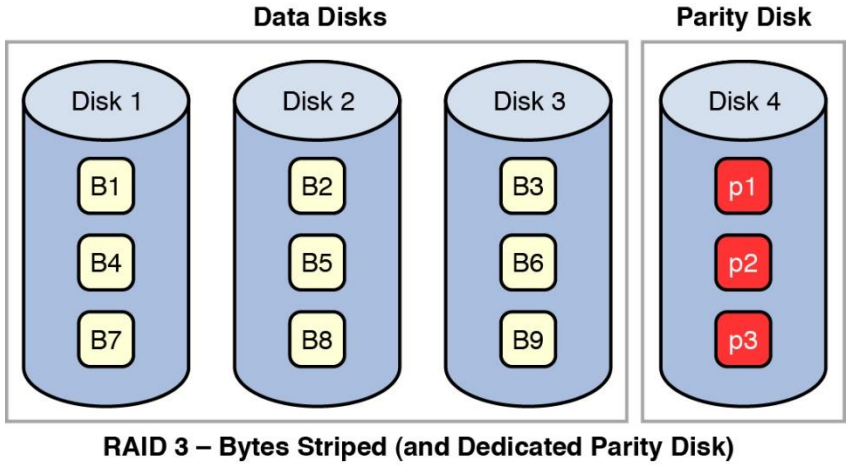
- RAID is a technology used for redundancy and/or performance improvement. It combines several physical disks and aggregates them into logical arrays. When data are saved, the information is written across all drives. A RAID appears as a single drive to applications and other devices.
    - **Striping:** breaking up the data and writing it across several disks so different disk heads can work simultaneously to retrieve the requested information.
    - **Parity:** *control data (data about the data)* are spread across each disks, so that if one disk fails, the other disks can work together and restore its data.
    - **Hot-swapping:** Replace the failed disk automatically while system is running.

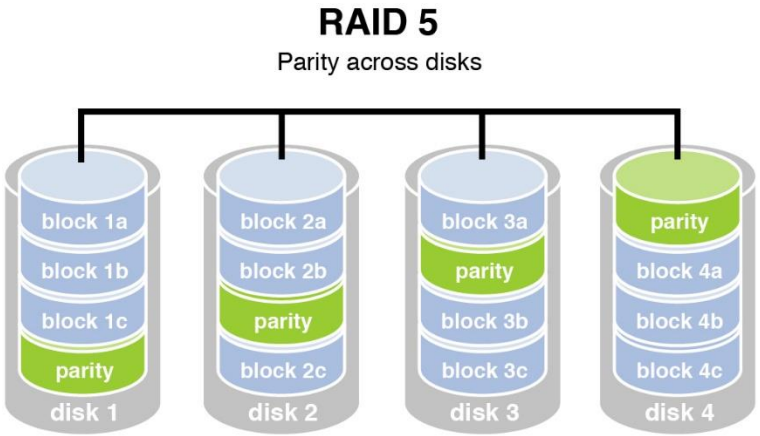
Redundancy and Fault-tolerant Systems

- Redundant array of independent disks (RAID)









Redundancy and Fault-tolerant Systems

- Redundant array of independent disks (RAID)

RAID Level	Activity	Name
0	Data striped over several drives. No redundancy or parity is involved. If one volume fails, the entire volume can be unusable. It is used for performance only.	Striping
1	Mirroring of drives. Data are written to two drives at once. If one drive fails, the other drive has the exact same data available.	Mirroring
2	Data striping over all drives at the bit level. Parity data are created with a hamming code, which identifies any errors. This level specifies that up to 39 disks can be used: 32 for storage and 7 for error recovery data. This is not used in production today.	Hamming code parity
3	Data striping over all drives and parity data held on one drive. If a drive fails, it can be reconstructed from the parity drive.	Byte-level parity
4	Same as level 3, except parity is created at the block level instead of the byte level.	Block-level parity
5	Data are written in disk sector units to all drives. Parity is written to all drives also, which ensures there is no single point of failure.	Interleave parity
6	Similar to level 5 but with added fault tolerance, which is a second set of parity data written to all drives.	Second parity data (or double parity)
10	Data are simultaneously mirrored and striped across several drives and can support multiple drive failures.	Striping and mirroring

Redundancy and Fault-tolerant Systems

- Other Systems

- **Redundant Array of Independent Tapes (RAIT):** similar to RAID, but uses tape drives instead of disk drives. Tape storage is the lowest-cost option for very large amounts of data, but is very slow compared to disk storage.
- **Massive Array of Inactive Disks (MAID):** In a MAID, rack-mounted disk arrays have all inactive disks powered down, with only the disk controller alive. When an application asks for data, the controller powers up the appropriate disk drive(s), transfers the data, and then powers the drive(s) down again. By powering down infrequently accessed drives, energy consumption is significantly reduced, and the service life of the disk drives may be increased.
- **Storage Area Networks (SAN):** consists o large amounts of storage devices linked together by a high-speed private network an storage-specific switches. SANs provide redundancy, fault tolerance, reliability, and backups, and allow the users and administrators to interact with the SAN as one virtual entity.
- **Clustering:** a fault-tolerant server technology that is similar to redundant servers, except each server takes part in processing services that are requested.
- **Grid Computing:** Another load-balanced parallel means of massive computation, similar to clusters, but implemented with loosely coupled systems that may join and leave the grid randomly.

Backup Systems

- Hierarchical Storage Management (HSM)

- provides continuous online backup functionality.
- combines hard disk technology with the cheaper and slower optical or tape jukeboxes.
- dynamically manages the storage and recovery of files, which are copied to storage media devices that vary in speed and cost