Security Design

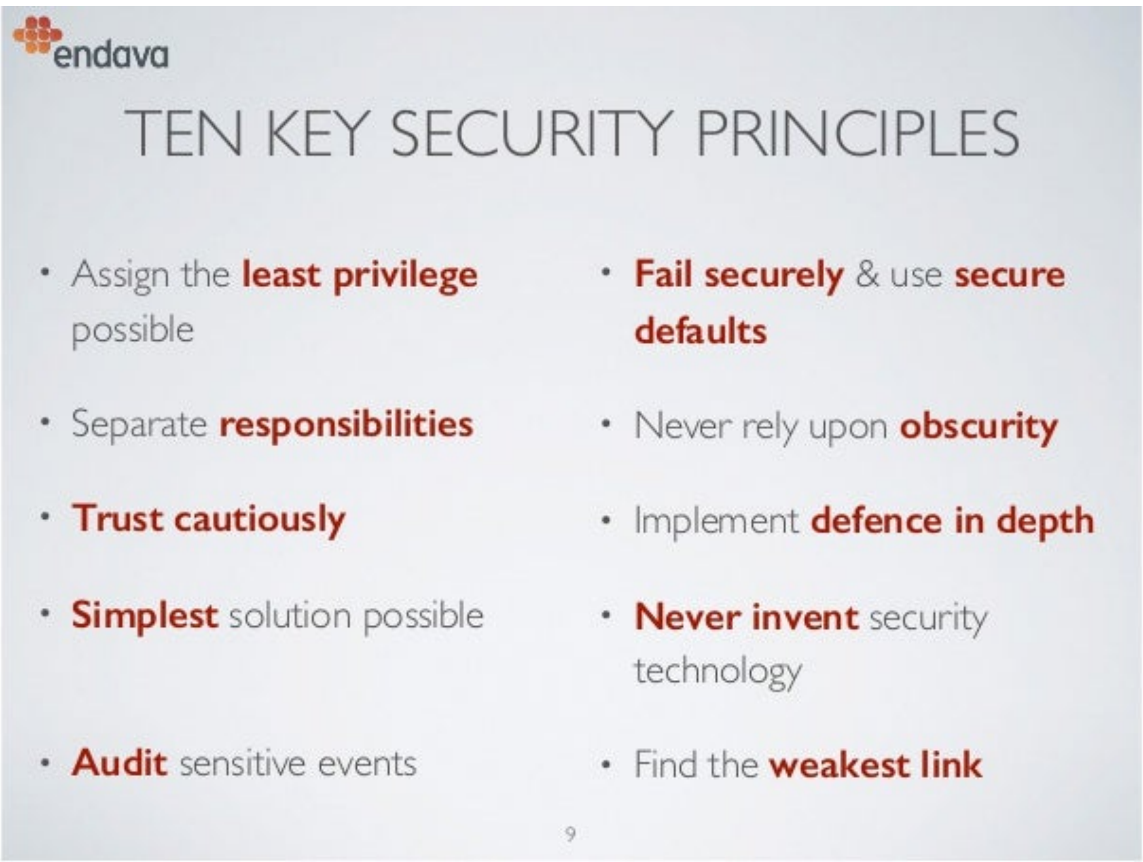
- Security Design
- System Examination
- System Configuration
- Firewalls and Filters
- Hardening Software
- Backups and Change Management
- Access Control and Authentication
- Virtual Private Networking
- Logging and Monitoring
- Security Policy and Management Support
- SELinux

Linux Systems Security

Security Design vs. Architecture

- Security architecture refers to the hardware and software in a system that implements security risk mitigation
- Security design refers to a specification of risks and describes the mitigation strategies that will be undertaken for those risks, if any
- Security design documents are typically policy documents

https://www.freepik.com/free-vector/security-design-concept_3976506.htm



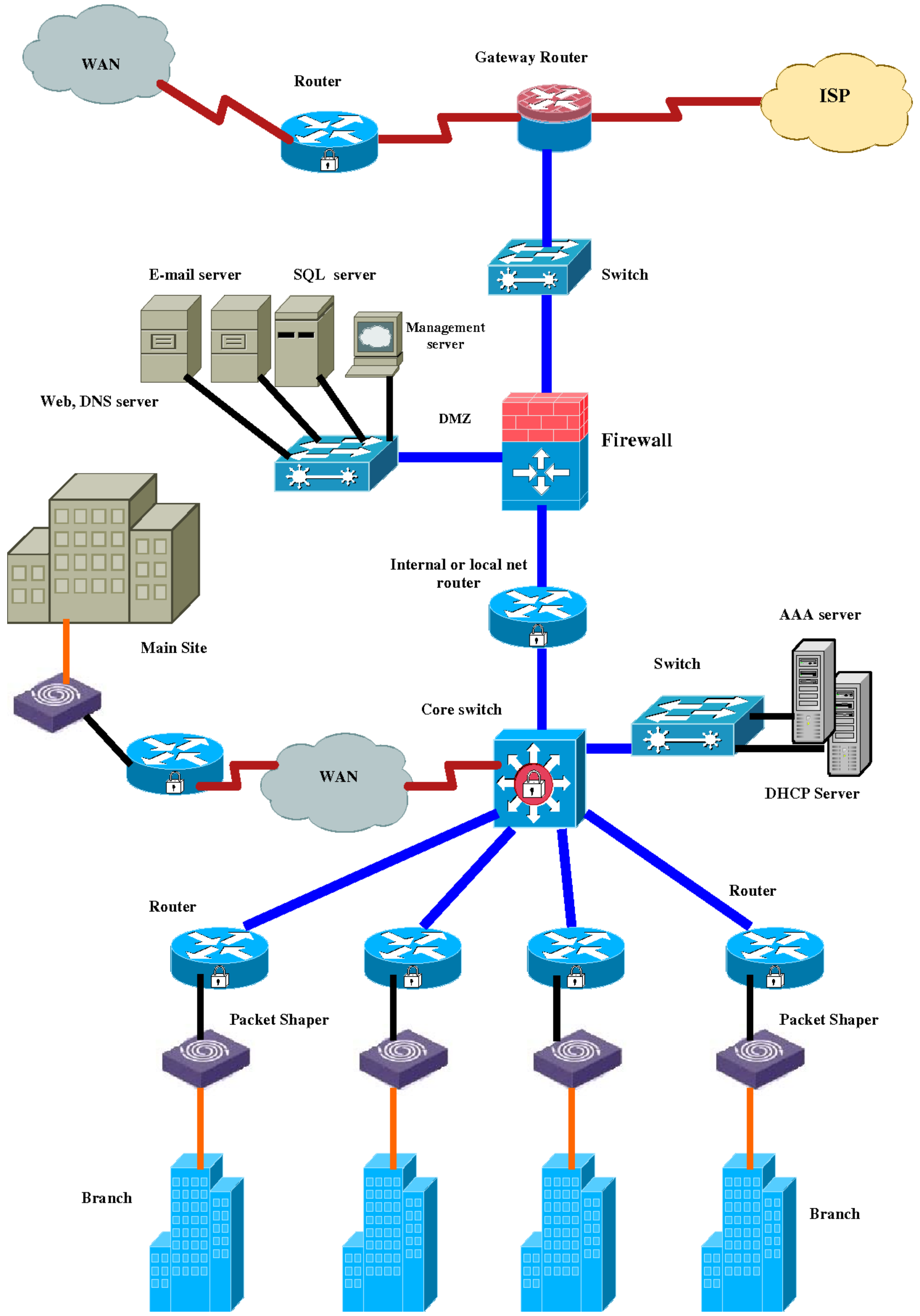
endava

TEN KEY SECURITY PRINCIPLES

- Assign the **least privilege** possible
- Separate **responsibilities**
- **Trust cautiously**
- **Simplest** solution possible
- **Audit** sensitive events
- **Fail securely** & use **secure defaults**
- Never rely upon **obscurity**
- Implement **defence in depth**
- **Never invent** security technology
- Find the **weakest link**

9

https://www.slideshare.net/EoinWoods1/secure-by-design-security-design-principles-for-the-rest-of-us



https://www.semanticscholar.org/paper/Design-and-Implementation-of-a-Network-Security-for-Alabady/a4a5ef4f2e937dc407a4089019316b054e8e3043

Security Risks

- Physical access
- Boot control
- Service availability and control
- User access
- Change control
- Data protection and backup
- Management support

Physical Access Risks

- Simple DOS (denial of service) through damage, disconnection, power down
  - Filesystem corruption can result, hardware damage may be possible
  - A server taken offline this way can cause ripple corruption around the network, particularly if the clients are using state-dependent file access mechanisms
- Copying, modifying, or adding devices, particularly storage
- CTRL-ALT-DEL risks with PC hardware - service interruptions

Physical Access Risks

- Attaching devices may autoload unexpected driver software
- Removable media can be used to get files on or off a system, bypassing network-based security and monitoring
- Alternate boot scenarios using removable media are a concern if physical access is permitted
- Designing around this means a physically secure location and physical access controls, and securing boot control

Hardware Boot Risks

- BIOS/System Firmware should only boot specific devices
- BIOS/System Firmware should be password protected

Boot Loader Risks

- Boot loaders typically offer user intervention at boot
- Most boot loaders have configuration files which must be protected (should be readable only by root) and have any available password options enabled, locations and file names can vary by distro
- Remove old boot options after kernel updates if your OS doesn't do it automatically
- Remove old kernel files if update was done for security concerns

Installed Software Risks

- Distro selection and installation affects how much work you have to do after the installation completes
- The GUI is a luxury, not a necessity, don’t install it unless your server's purpose cannot be achieved without it
- Non-essential software that is installed offers opportunities to attackers, even if that software does not run automatically

Service Software Risks

- Remove innocuous but unnecessary service programs to reduce logfile clutter and eliminate attack vectors
- Remove services you do not require
- Secure service control programs
- Containerized or cloud-based services may be an option but have additional security risks

Service Logging Risks

- Services may or may not log startup/shutdown and activities
- Services may have custom logfiles directly written by the service programs, or may use system logging services

Side Effects Risks

- Resource and capacity limits may be non-existent or have inappropriate defaults allowing unexpected loads to exhaust or incapacitate system resources
- Users who shouldn’t be able to affect running services often can
  - By running service programs manually
  - By interfering with resources those programs use

System Account Risks

- System (sometimes called service) accounts can be dangerous, consider where and how they might be used for access, and what they can do once commandeered
- Service program configuration files commonly provide parameters to limit what those programs do
- Web servers, email servers, database servers, etc. usually are capable of managing private user lists and controls
  - per-service user lists may not be used in favour of simpler unix account linkage and reuse
  - this can result in unexpected user account names being valid for services

User Data Risks

- There are separate risks for data at rest and data in flight
- Where is it stored and how it is stored may enable users to impact availability of a filesystem for other users
- What access rights do users have the ability to give away (DAC vs. MAC vs. RBAC)
- Removable media, network copying, sharing tools, backup tools are all potential data exposure and exfiltration avenues
- Data labelling is relevant, file names can be misleading

User Access Risks

- Password policies are only helpful if they are enforced
- Draconian policies drive users to circumvent them
- Remote access comes in many forms, and does not always require inbound network connections, think malware C&C
- Social engineering to create confused deputies can defeat any password policy or data access control method - tracking access can be forensically helpful

Change Control

- Differentiating between expected and unexpected system behaviour can be enhanced with well-orchestrated and consistent change control
- System updates, upgrades, or configuration changes can introduce new exposures or break existing protections
- Well-orchestrated changes are planned, tested, logged, and verified
- Software installation and update tools do not normally record what they do in a human-friendly change log - human-friendly logs are needed for admins to evaluate changes in system behaviour
- Business practices should be examined for possible impacts

Software Upgrades and Patches

- Automated updates are generally discouraged for servers because they can break things
- Upgrades and patches may also invalidate or ignore configuration options including security-related options
- Automated patch/upgrade installations may not be sufficient, update documentation should be reviewed
- Testing patches and upgrades on virtual duplicates of production machines is an option, remember to check changes to configs in new versions of software

Data At Rest

- Data at rest can be protected using access control and encryption
- Data container access controls such as file permissions and ACLs, or storage control mechanisms such as database permissions are the basic tools
- Encrypting data in storage can be a substantial overhead for the system unless it has encryption hardware
- Encrypting root filesystems is possible, but maintenance becomes more difficult, better to cleanly separate root filesystem from any sensitive data storage

Data In Flight

- Encrypting data in flight may require more than one solution
- SSL/TLS and SSH are trusted tools for protecting individual data transfers, but have been successfully compromised in the past necessitating new versions and deprecation of specific algorithms
- VPNs can encrypt the entire connection between computers, making recon more difficult for bad actors
- Version control systems require extra attention because they do not usually encrypt their data in flight or at rest
- Data replicates and backups should have encryption enabled both in transit and at rest

Backup Risks

- Backup of systems and data may have different requirements and risks
- Backup media may be mobile, or may be offsite
- Restoration must include tamper detection
- Encrypting a backup while it is being written is an extra layer of protection, even if it is being stored on encrypting media
- Automated backup versioning/aging must preserve encryption

Management Support

- Security requires tools, hardware, and personnel
- Those normally require funding and allocation of resources
- The security role may not include making the business decisions, but may be limited to lobbying for them
- Security must be part of the business strategy and plan

Setup of Linux VM
Examine defaults
Review Design Choices

Lab 01 Security Design