JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Security Architecture & Tool Sets

Security Architecture & Tool Sets

What does this section cover?

- Security Policies and Compliance
- Adopting a Security Framework
- Defense in Depth Architectures
- Identity and Access Management
- Security in Software Development

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Policy Documents

Security Architecture & Tool Sets

Policy Documents

- Information Security Policy Framework
  - Policies
  - Standards
  - Procedures
  - Guidelines

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Policies

- High-level statements of intent
- Contains broad statements about cybersecurity objectives in the company
- Framework to meet the business goals and to define roles, responsibilities, and terms used in other security documents

Policy Examples

- Information Security
- Acceptable Use
- Data Ownership
- Data Classification
- Data Retention
- Account Management
- Password

Who Approves the Policies?

- The CEO, CISO, CIO, or CSO will approve the policy for the organization
- Without management buy-in, the policy is a waste of your time and effort
- Top-down approach is most effective

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Standards

- Used to implement a policy
- Includes mandatory actions, steps, or rules needed to achieve cybersecurity
- Approved by a lower level than C-Suite, such as Director of Information Systems
- Standards can also exist in industry frameworks (COBIT, ITIL, etc.)

Procedures

- Detailed step-by-step instructions created for people to perform an action
- Actionable steps to create a consistent method for achieving a security objective
- Example:
  - The service desk has a procedure for how to create a new user's account
  - Encompass all the security related policies, standards, and guidelines for action by your front-line employees

Guidelines

- Not required actions, just recommended
- Flexible in nature to allow for exceptions and allowances during a unique situation
- Example:
  - The organization may create a guidelines showing users how to store data files in a cloud service and how to encrypt the files
  - These aren't required, but may be useful to the end user an can be changes quickly

Are the Rules Meant to Be Broken?

- Most of the time, the policies, standards, and procedures should be followed
- How do you get permission to break these established “rules”?
- Your information security framework should include the method for granting any necessary “exceptions”

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Exceptions

- Specific approval to deviate from a policy, standard, procedure
- Approval authority is specified in policy
- Exception request includes:
  - Policy, standard, or procedure requiring exception
  - Reason for exception request
  - Scope and duration of exception
  - Risks associated
  - Description of compensating controls to lower risk

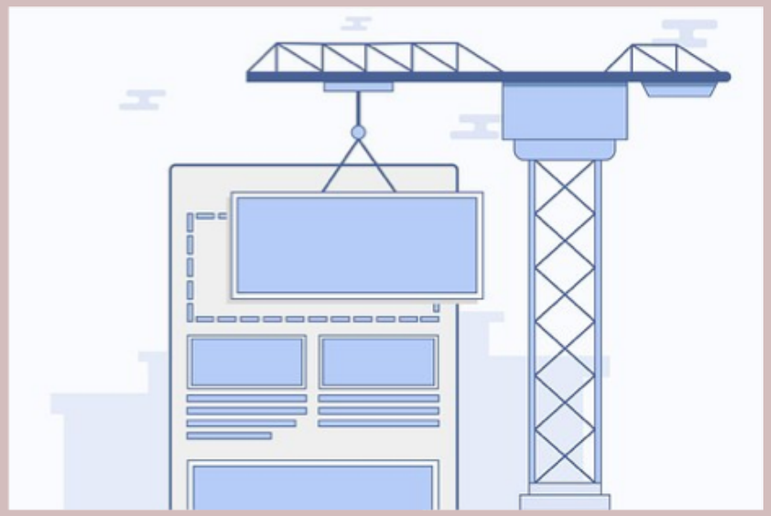
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Standard Frameworks

Security Architecture & Tool Sets

Standard Frameworks

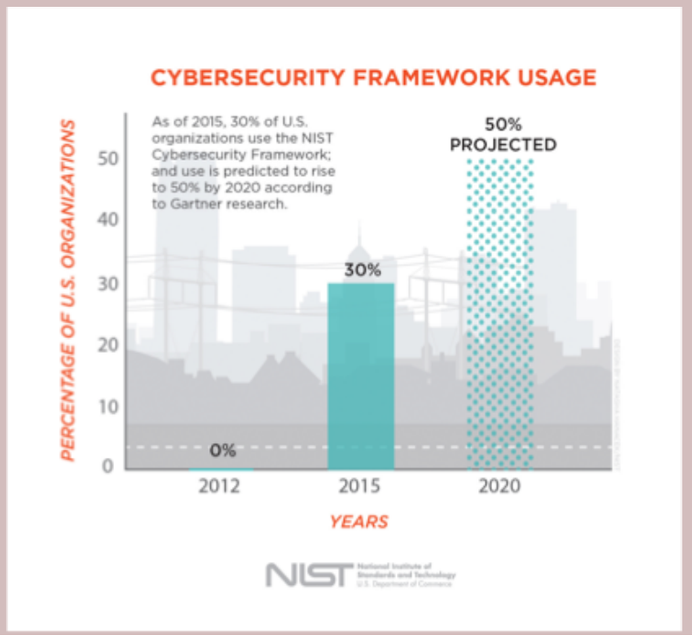
- Creating your own cybersecurity program is daunting task
- Standard frameworks exist to help
- Provide a standardized approach



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

NIST Cybersecurity Framework

- Designed to meet one or more objective
  1. Describe current posture
  2. Describe desired state
  3. Identify and prioritize areas for improvement
  4. Assess progress toward desired state
  5. Communicate risk among internal and external stakeholders



NIST Cybersecurity Framework

- Framework Core is a set of five security functions that apply to all industries
- Framework Implementation Tiers measure how the organization is positioned to meet cybersecurity objectives
- Framework Profiles describe how the organization might approach the functions covered by Framework Core

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

ISO 27001

- Used to be the most commonly used information security standard
- Declining in usage outside of regulated companies that require ISO compliance
- To become ISO 27001 certified, an external accessor validates organizational compliance

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

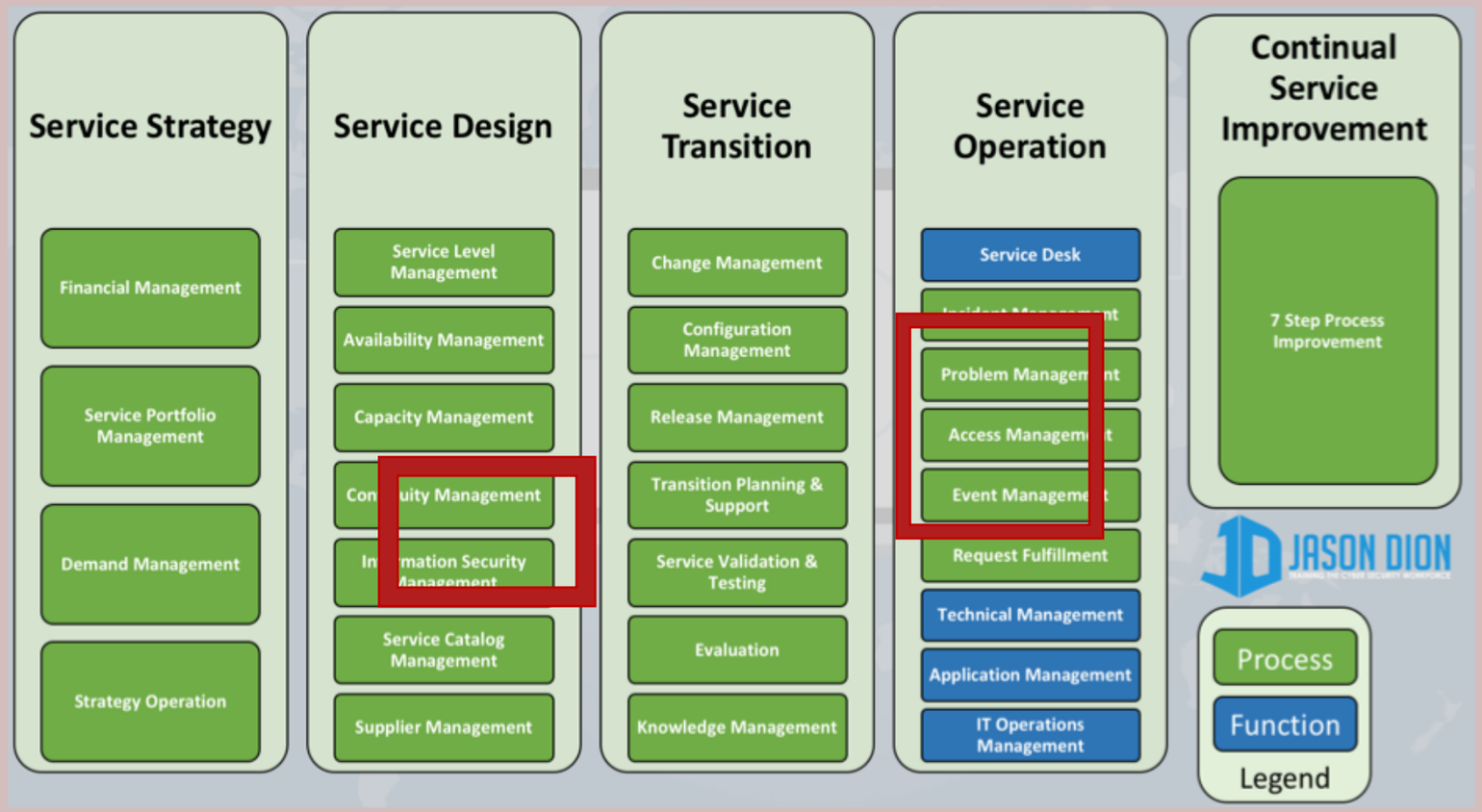
ISO 27001: 14 Categories

- Information Security Policies
- Organization of Information Security
- Human Resource Strategy
- Asset Management
- Access Control
- Cryptography
- Physical and Environment Security
- Communications Security
- System Acquisition
- Information Security Incident Management
- Information Security Aspects of Business Continuity
- Compliance with internal requirements

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Information Technology Infrastructure Library (ITIL)

- Comprehensive approach to ITSM



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

COBIT

- Control Objectives for Information & Related Technologies
- Set of best practices for IT governance developed by ISACA
- Divides IT activities into four domains:
  - Plan and Organize
  - Acquire and Implement
  - Deliver and Support
  - Monitor and Evaluate

COBIT Framework Components

- COBIT framework
- Process descriptions
- Control objectives
- Management guidelines
- Maturity models

COBIT® 5

AN ISACA® FRAMEWORK

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

The Open Group Architecture Framework (TOGAF)

- Widely adopted approach to EA

- Four domains:
  - Business Architecture
    - Integrates EA with business strategy
  - Application Architecture
    - Contains apps/systems used, interaction between systems, and the relation to the business processes
  - Data Architecture
    - Details approach to storing and managing info assets
  - Technical Architecture
    - Details infrastructure needed to support other domains

Sherwood Applied Business Security Architecture (SABSA)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Alternative model for security architecture that maps to architectural layers from different perspectives

- Used in Enterprise Architecture (EA)

View	Architecture Layer
Business	Contextual Security
Architect	Conceptual Security
Designer	Logical Security
Builder	Physical Security
Tradesman	Component Security
Service Manager	Security Service Management

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Policy-Based Controls

Security Architecture & Tool Sets

Policy-Based Controls

- Policies provide the control objectives the organization wants to achieve
- This is the desired end state, not the method or activities to accomplish them
- Security controls are used to achieve the control objectives
  - Physical Controls
  - Logical Controls
  - Administrative Controls

Physical Controls

- Controls that impact the physical world

- Examples:
  - Fences, gates, locks, lighting, alarm systems, fire suppressions systems, etc.

Logical Controls

- Technical controls to enforce confidentiality, integrity, and availability

- Examples:
  - ACLs in firewalls and routers, encryption schemes

Administrative Controls

- Procedural controls to implement good cybersecurity practices

- Examples:
  - Separation of duties, background checks, reviewing of log files, etc.

LogTime	Computer	Protocol Type	Source IP	Destination IP	Access type	Attack
11/16/2015 03:14:30 PM	CISCO-ASA	UDP	182.72.211.60/35445	192.168.2.34/467	interface interface_name	
11/16/2015 03:14:30 PM	CISCO-ASA	UDP	182.72.211.61/789	192.168.1.26/233		
11/16/2015 03:14:30 PM	CISCO-ASA				for icmp	
11/16/2015 03:14:30 PM	CISCO-ASA	UDP	182.72.211.60/35445	192.168.2.34/467	interface interface_name	
11/16/2015 03:14:30 PM	CISCO-ASA				for icmp	
11/16/2015 03:14:30 PM	CISCO-ASA	UDP	182.72.211.61/789	192.168.1.26/233		
11/16/2015 03:14:30 PM	CISCO-ASA	UDP	182.72.211.61/789	192.168.1.26/233		
11/16/2015 03:14:31 PM	CISCO-ASA	ICMP	10.4.1.2	10.2.1.1	interface dmz	
[illegible]6/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.168.1.1	interface outside	Snort attack
11/16/2015 03:14:31 PM	CISCO-ASA	ICMP	10.4.1.2	10.2.1.1	interface dmz	
11/16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.168.1.1	interface outside	Snort attack
11/16/2015 03:14:31 PM	CISCO-ASA	ICMP	10.4.1.2	10.2.1.1	interface dmz	
11/16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.168.1.1	interface outside	Snort attack
11/16/2015 03:14:31 PM	CISCO-ASA	ICMP	10.4.1.2	10.2.1.1	interface dmz	
11/16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.168.1.1	interface outside	Snort attack
11/16/2015 03:14:31 PM	CISCO-ASA	ICMP	10.4.1.2	10.2.1.1	interface dmz	
11/16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.168.1.1	interface outside	Snort attack
11/16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.168.1.1	interface outside	Snort attack
11/16/2015 03:14:31 PM	CISCO-ASA	UDP	10.1.1.1	192.168.1.1	interface outside	Snort attack
11/16/2015 03:14:31 PM	CISCO-ASA	ICMP	10.4.1.2	10.2.1.1	interface dmz	
11/16/2015 03:14:31 PM	CISCO-ASA	ICMP	10.4.1.2	10.2.1.1	interface dmz	

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Combining Control Objectives

- Physical, Logical, and Administrative controls are most effective when they are combined together

- Example:
  - To prevent theft of the data from a server
    - Physical controls for building access
    - Logical controls like encryption
    - Administrative controls like requiring two people

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Audits and Assessments

Security Architecture & Tool Sets

Quality Control

- Louis V. Gerstner, former IBM Chairman

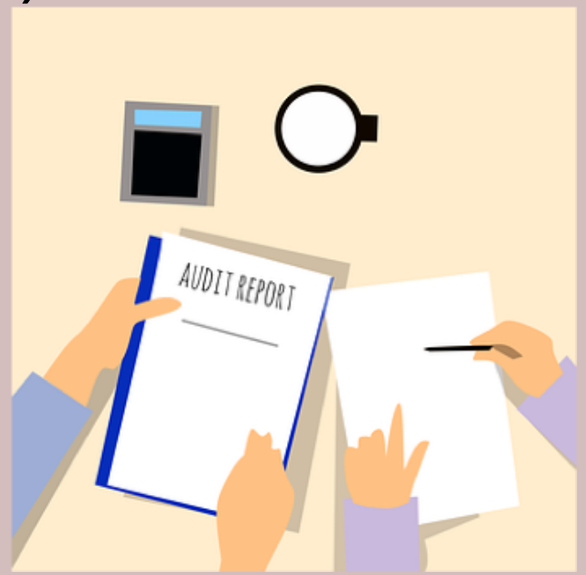
You get what you inspect,
not what you expect…

- Evaluation of your cybersecurity program is essential to it being effectively run

- Evaluation occurs as audits or assessments

Audits

- Formal review of organizational cybersecurity program (internally)
- Or, it can be for a specific compliance requirement (externally), like PCI DSS
- Rigorous, formal testing of controls resulting in formal declaration by the auditor of compliance



Assessments

- Less formal review of security controls
- Usually request by the organization itself for process improvement purposes
- Information gathered through interviews with employees (which is considered the truth) instead of independent verification

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Laws and Regulations

Security Architecture & Tool Sets

Compliance with Laws and Regulations

- United States has various laws and regulations that must be adhered to, based on your industry (CSA+ focus)

- European Union also has broad-ranging data protection regulations

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Health Insurance Portability and Accountability Act (HIPAA)

- Security and privacy rules for healthcare

- Affects healthcare providers, insurers, and others storing health information

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Gramm-Leach-Bliley Act (GLBA)

- Requires financial institutions to have formal security programs in place

- Must designate a “responsible” individual

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

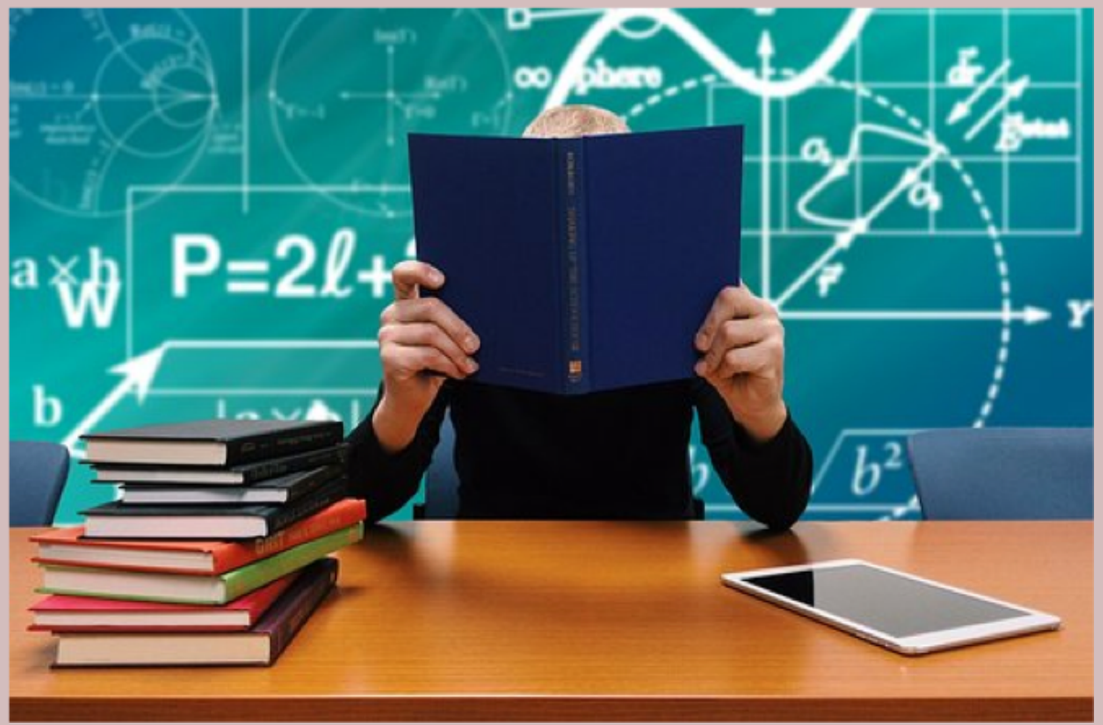
Sarbanes-Oxley (SOX) Act

- Requires publicly traded companies to maintain good security around their IT systems storing and processing their financial records

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Family Educational Rights and Privacy Act (FERPA)

- Requires educational institutions to implement security and privacy controls for educational records



Payment Card Industry Data Security Standard (PCI DSS)

- Rules about storage, processing, and transmission of credit/debit card info

- Not a law, but a contractual obligation

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Data Breach Notifications (Various State Laws)

- Requires companies to notify victims of data breaches in a timely manner

Equifax **data breach**: Don't let your guard down yet
The Denver Channel - 12 hours ago
DENVER — Multiple **data breaches** happened this past year, and the Equifax **data breach** remains the biggest. Nearly 143 million American's had their personal information stolen, according to Equifax. This includes Social Security numbers, addresses, birthdays and names. The dust has settled in these ...

Los Angeles city attorney sues Uber over **data breach**
Local Source - KABC-TV - Dec 4, 2017

View all

Duke Energy says **data breach** may have exposed personal ...
Charlotte Observer - 7 hours ago
About 370,000 Duke Energy customers in the Carolinas, including in Charlotte, may have had addresses, banking data and other personal information exposed in a potential **data breach** stretching back to 2008, a company spokesman said Tuesday. Ryan Mosier said the Charlotte-based utility learned Nov ...

374000 Duke Energy customers potentially affected by **data breach**
Greenville News - 8 hours ago

View all

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

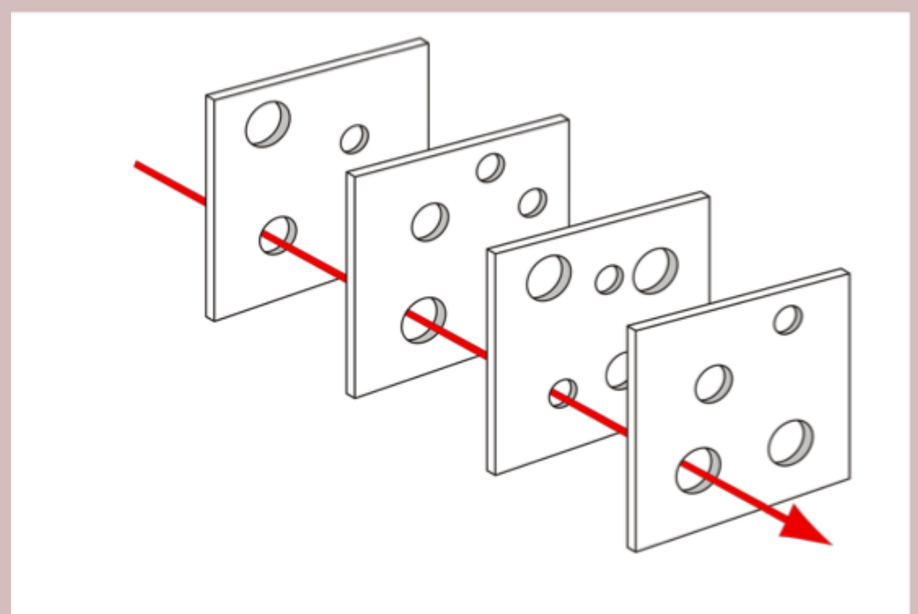
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Defense in Depth

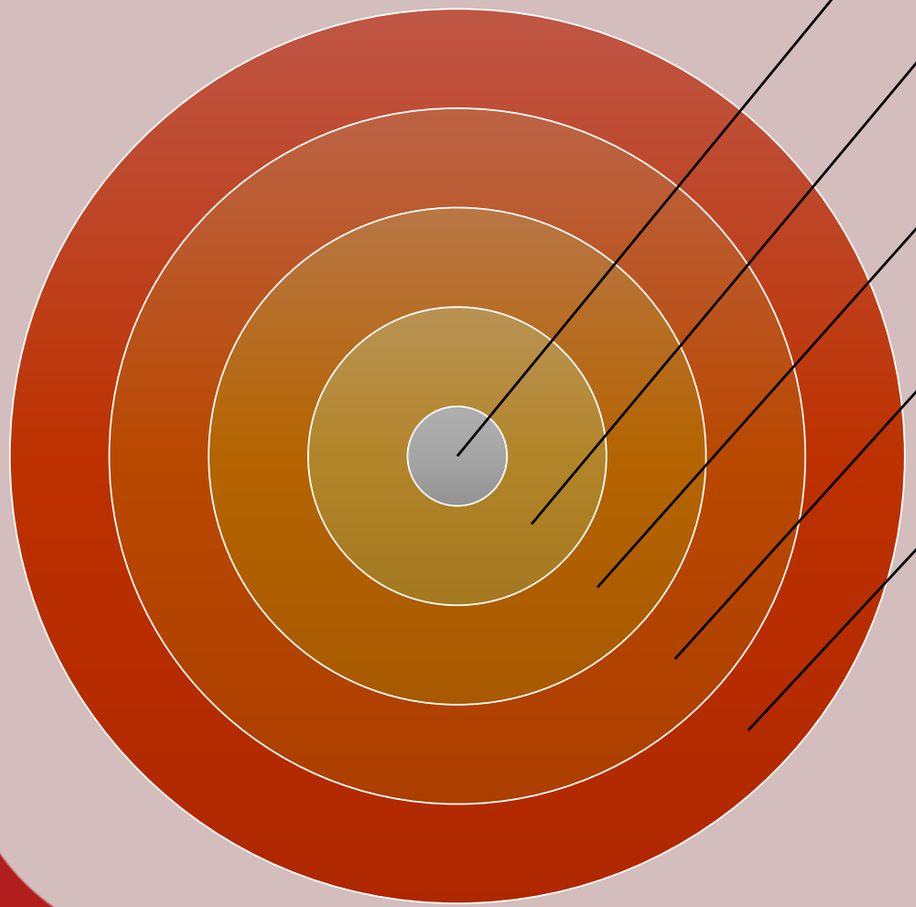
Security Architecture & Tool Sets

Defense in Depth

- Foundation of good security architecture
- Does not rely on a single defensive measure or control for protection



Layered Security Defense



Data

Application

Endpoint Security

Network

Perimeter

JASON DION

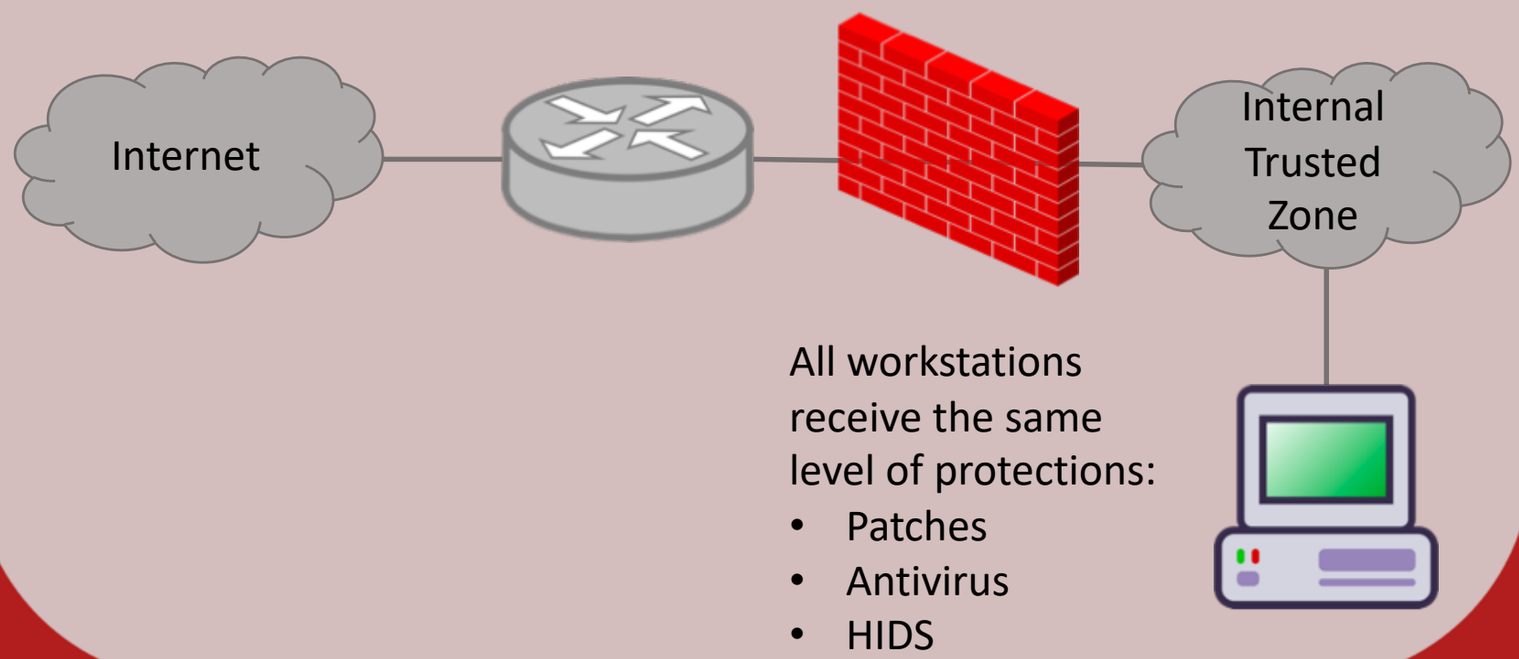
TRAINING THE CYBER SECURITY WORKFORCE

Layered Security Defense

- Difficult to design and implement
- Must consider business needs and usability in the design of layered controls
- Four design models
  - Uniform Protection
  - Protected Enclaves
  - Risk or Threat Analysis-based
  - Information Classification-based

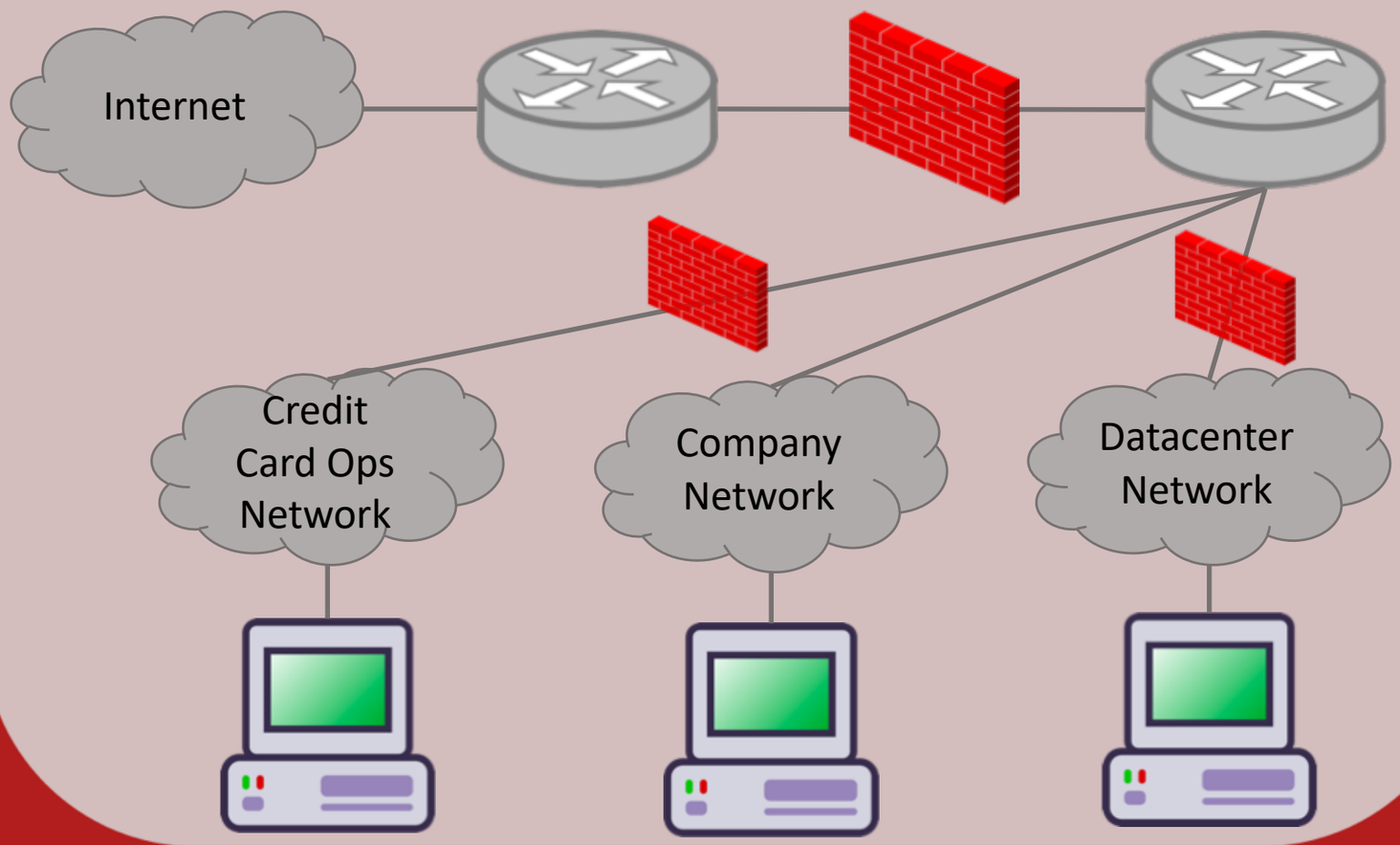
Uniform Protection

- Gives same level of protection to all data, systems, or networks
- Can be expensive for larger networks



Protected Enclave

- Enclaves that house more sensitive data are given additional protections



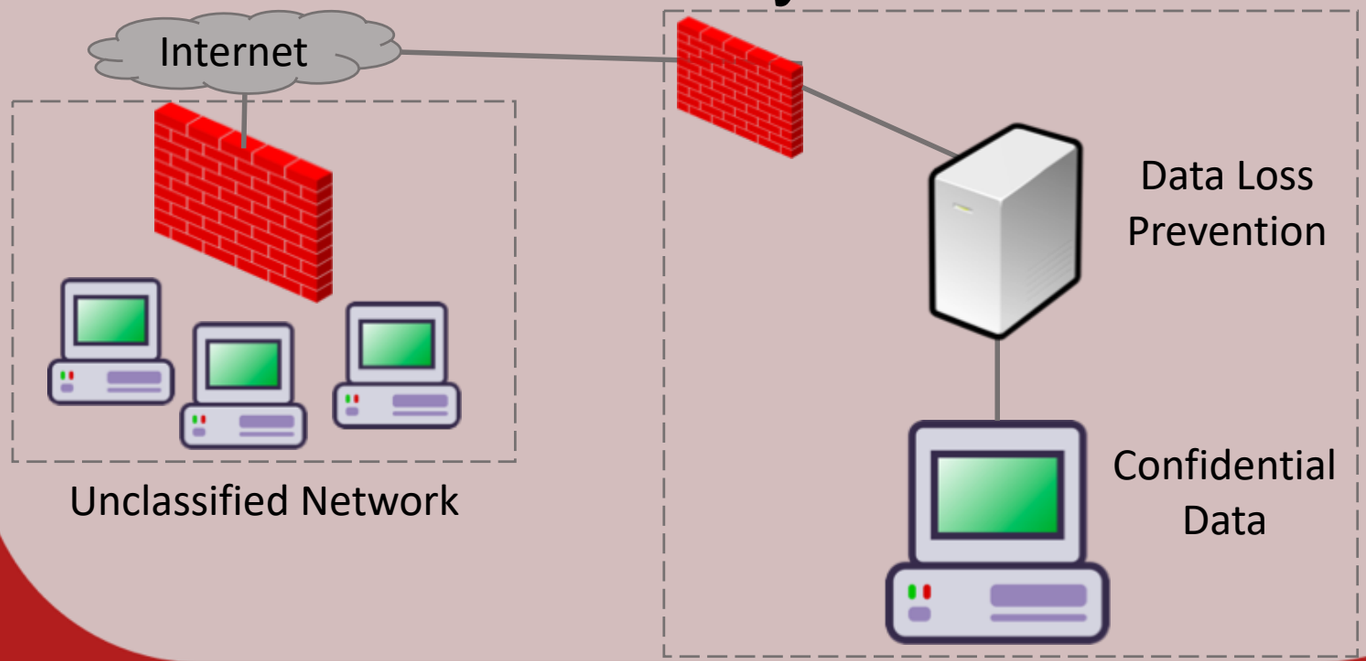
Risk or Threat Analysis-based

- Addresses specific risks or threats in the design of the networks and systems

- Example
  - If you are concerned with phishing as a threat vector, you could employ additional controls to securely scan and filter your incoming emails

Information or Classification-based

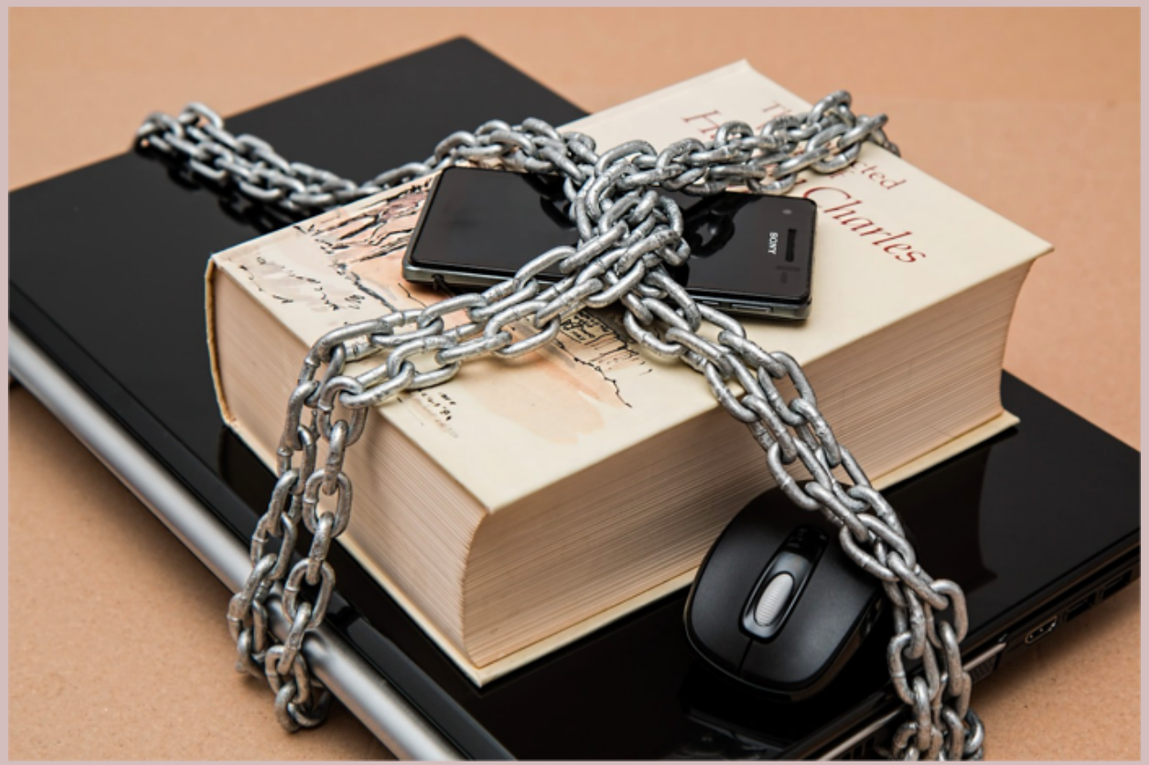
- Map data protection to different classes of information
- Higher classification levels get additional attention and security controls



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Combining Design Models

- Often, these four models are combined as opposed to picking a single model



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Types of Controls

Security Architecture & Tool Sets

Types of Controls

- Controls prevent, detect, counteract, or limit certain security risks
  - Technical Controls
  - Administrative Controls
    - Legal Controls
  - Physical Controls
  - Preventive Controls
  - Detective Controls
  - Corrective Controls
  - Compensating Controls

Based on their Implementation

Based on when the control acts

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Technical Controls

- Designed to provide security through technical measures

- Examples
  - Firewalls
  - IDS/IPS
  - Authentication Systems
  - Network Segmentation

Administrative Controls
(or Procedural Controls)

- Designed to provide security through processes and procedures

- Legal controls are a type of these controls that are put in place by the law

- Examples
  - Incident Response Plans
  - User Awareness Training
  - Account Creation Policy
  - Acceptable Use Policy

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Physical Controls

- Designed to provide security by preventing physical access or harm to the organization's systems or facilities

- Examples
  - Fences
  - Mantraps
  - Security Guards
  - Fire Suppression Systems

Preventative Controls

- Designed to stop an incident before it has occurred
- Proactive measures
- Examples
  - Firewalls
  - Antivirus
  - Training
  - Security Guards

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Detective Controls

- Designed to detect when an incident occurs, capture details about it, and send an alarm/notification so someone can act

- Examples
  - Intrusion Detection System
  - Security Cameras
  - Logs

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Corrective Controls

- Designed to fix an issue after an incident has occurred
- Part of incident response process
- Reactive measures
- Examples
  - Security Patching
  - System Rebuilding
  - Restore from Backups

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Compensating Controls

- Designed to satisfy a security requirement not being met by other controls
- Minimizes threat down to an acceptable level of risk (based on risk appetite)
- Examples
  - Blocking certain ports instead of upgrading all of the operating systems
  - Segmenting vulnerable software to a separate part of the network

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Layered Network Design

Security Architecture & Tool Sets

Layered Network Design

- Combining the network architecture, configuration management, practices, and policies

- Can be accomplished through
  - Network segmentation
  - Firewalls
  - Outsourcing network segments

Network Segmentation

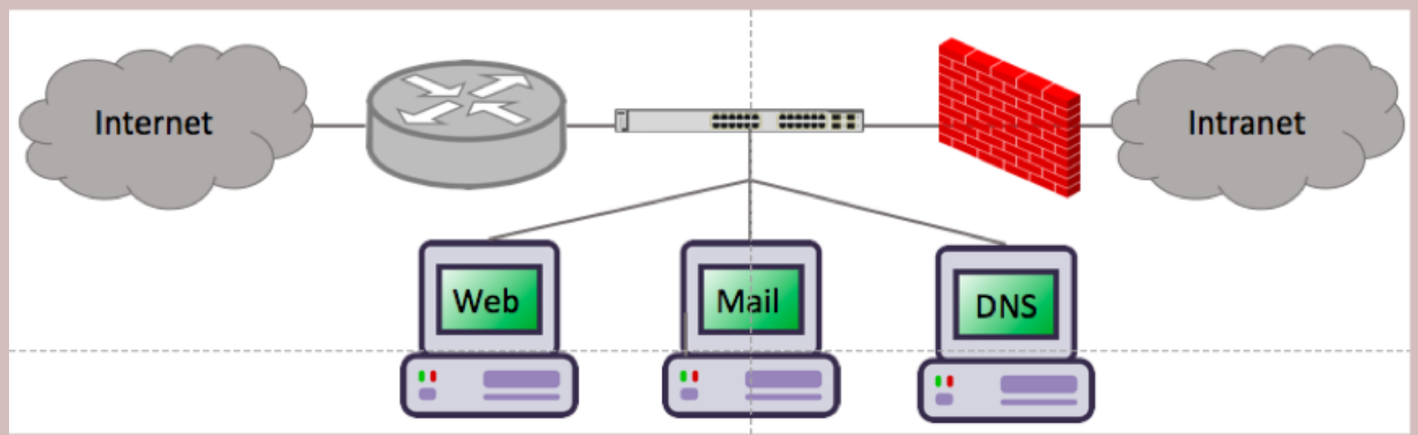
- Compartmentalization of the network
- Benefits
  - Reduces the network's attack surface
  - Limits scope of regulatory compliance
  - Increases availability of critical services
  - Increases network efficiency
- Segmentation is implemented through firewalls, routers, switches, and VLANs

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Single Firewall or Router

- Simplest network design utilized used to create a DMZ for a lower trusted segment of the network

- Ensure you put protections in place between DMZ and intranet

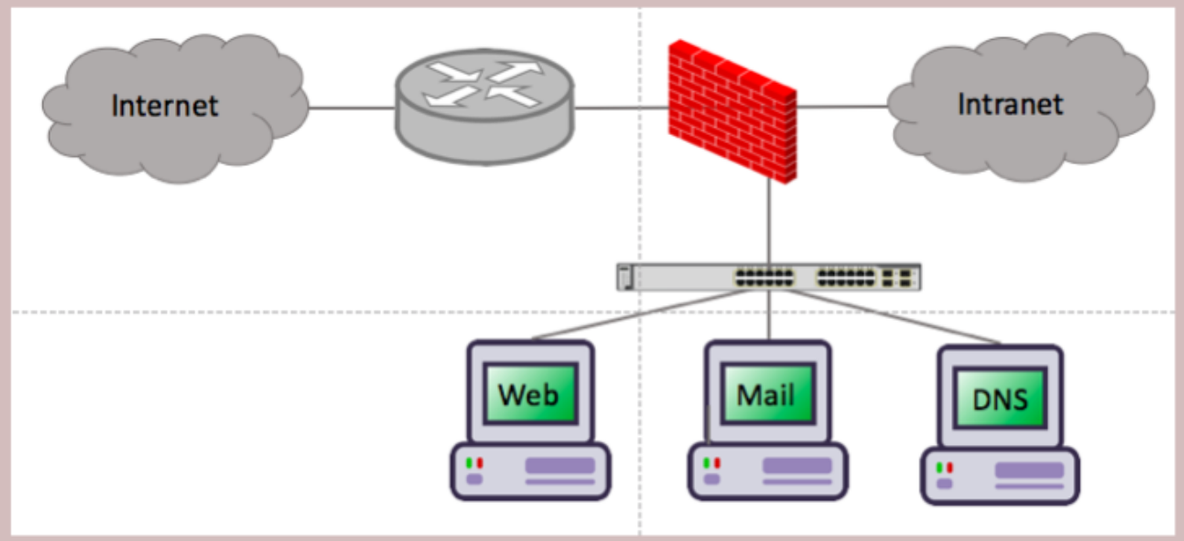


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Multiple Interface Firewalls

- Different ACL and rulesets applied to each interface, creating multiple network segments

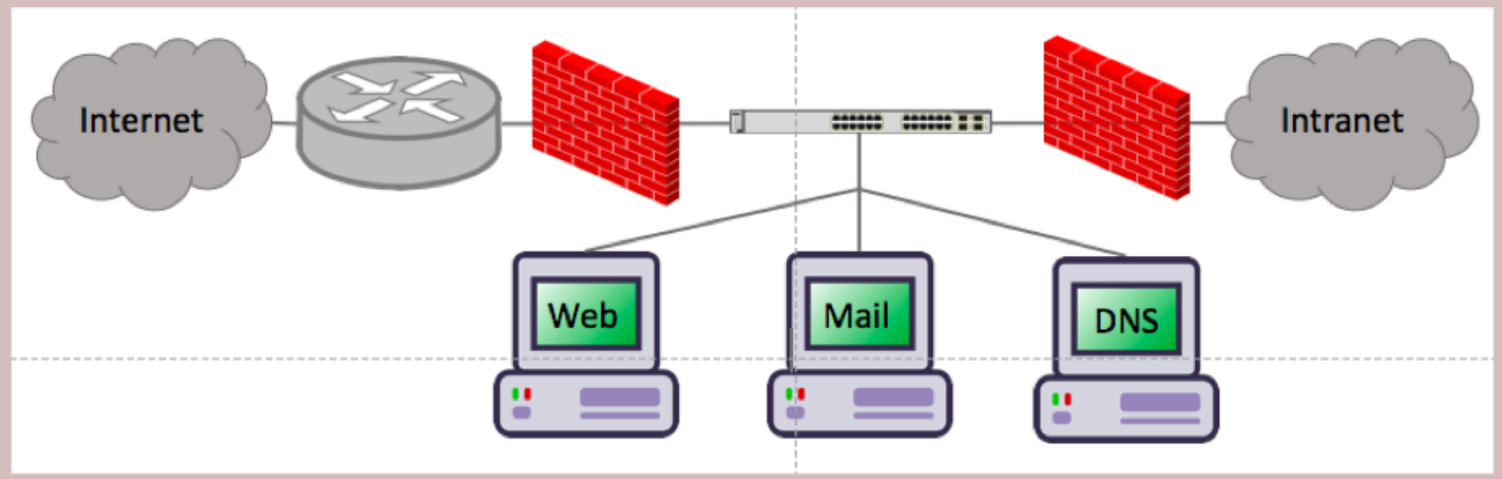
- Often called service-leg DMZ



Multi-Firewall

- Dual-firewalls (or more) puts a firewall at each control point

- Allows for more stringent controls as you move deeper into the network



Outsourcing Segments

- Remote Services
  - SaaS and PaaS rely on providers for security and network designs
- Directly Connected Remote Network
  - Acts as an extension of your intranet
  - Utilizes IaaS with direct point-to-point VPNs
  - To users, it appears the IaaS is just part of your network
  - Low-level host protections at IaaS are still handled by the third-party service provider

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

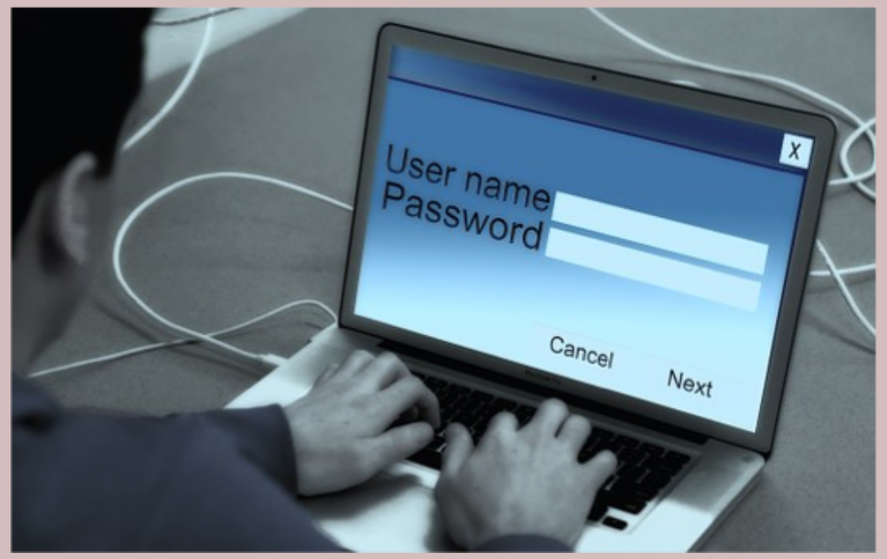
Layered Host Security

Security Architecture & Tool Sets

Layered Host Security

- Servers, desktops, laptops, smartphones are all considered hosts on your network

- Often the most at-risk part of the network since your users directly use them



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Common Security Controls

- Passwords and strong authentication
- Encryption (file or full disk)
- Host firewalls and Host-based IPS
- Data Loss Prevention (DLP) software
- Whitelisting/Blacklisting of software
- Antimalware/Antivirus software
- Patch management
- System hardening
- Configuration management
- File Integrity Monitoring
- Logging of events and issues

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Cryptography: Encryption and Hashing

- Encrypting files or the full disk can protect “data at rest”
- Proper storage of the encryption keys/passphrases is critical to security
- Hashing of files can be used to ensure file integrity, as well

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Logging, Monitoring, and Validation

- Logs must be securely stored and centrally monitored
- Specialized log server or SIEM (Security Information and Event Management)
  - Tripwire, AlienVault, Splunk, …
- Configuration Management (Microsoft SCCM and others) allow validation of system settings and software across the connected hosts

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Data Analytics

Security Architecture & Tool Sets

Data Analytics

- Integrating logs across the devices provides the most value and information
- Manual review of logs is time consuming
- Automated systems can help prioritize items for review based on heuristics and previous signatures created
- You need to conduct data aggregation and correlation, trend analysis, and historical analysis

Data Aggregation and Correlation

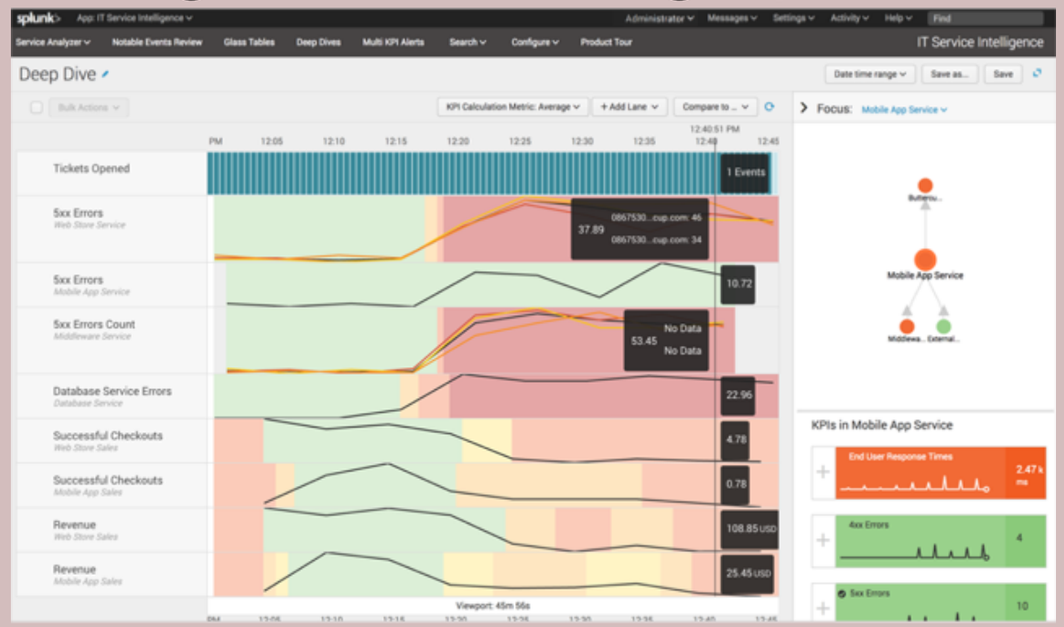
- Combine data from multiple sources to identify events impacting different systems
  - System logs, authentication logs, application logs, event logs, and others into central analysis node

- Effective as a detective control

Trend Analysis

- Analyzes system, events, and devices to detect trends and patterns

- Identifies issues that are outside of expected growth or usage patterns



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Historical Analysis

- Analyzes system, events, and devices over time to detect trends and patterns

- Helpful during incident responses as it looks back over a longer period of time

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Personnel Security

Security Architecture & Tool Sets

Policies, Processes, and Standards

- Foundation of administrative controls

- Includes:
  - Change control
  - Configuration management
  - Monitoring and response
  - **Personnel security controls**
  - Business continuity
  - Disaster Recovery

Separation of Duties

- Requires more than one person to perform a task by breaking the task into additional parts

- Provides a system of checks and balances to prevent fraud and abuse

Dual Control

- Process requiring two individuals to perform the action together

- Example:
  Unlocking a safe or a server room

Succession Planning

- Focuses on ensuring important duties will always have someone who can perform them

- Prevents issues from task not being performed during personnel turnover

- Example:
  A primary and backup administrator

Cross Training of Employees

- Focuses on teaching employees skills to cover tasks other coworkers perform

- On-the-job training is used to ensure you have additional resources for a big project in the future or if someone quits

Background Checks

- Conducted prior to hiring an employee

- Example:
  Bank runs credit check on new hires

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Mandatory Vacation Time

- Staff members must take vacation

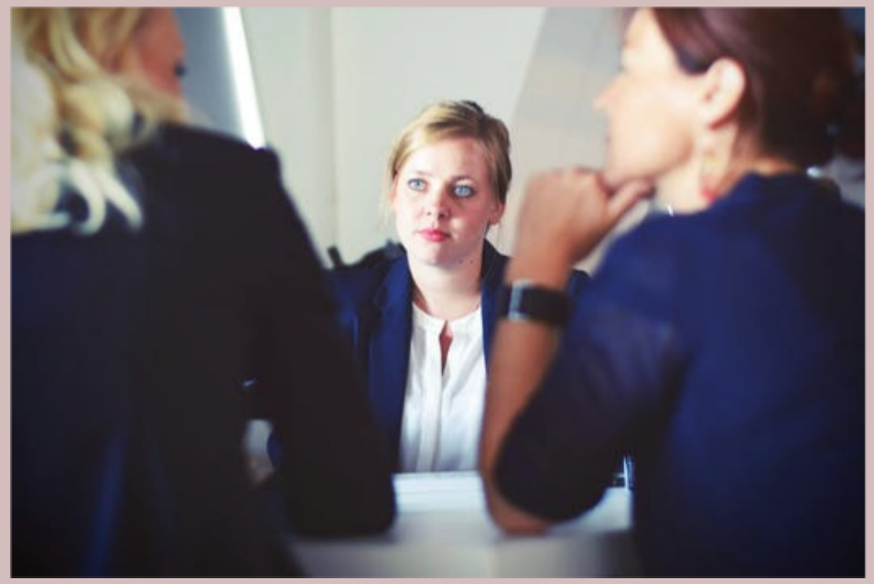
- Allows us to identify any issues being hidden since the person will not maintain continuous access to the systems

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Termination

- Policies and procedures focuses on what to do when an employee is terminated

- Retrieving company property, disabling accounts, changing security codes, etc.



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Outsourcing Concerns

Security Architecture & Tool Sets

Outsourcing Concerns

- If you outsource, there are additional things you need to be concerned with…
  - Proper vetting of the provider
  - Employment practice
  - Access control
  - Data ownership and control
  - Incident response and notification process

Proper Vetting and Employment Practices

- What kind of background checks are you doing on the service provider?
- What kind of background checks are done on their employees?
- What internal personnel controls are used?
- How do they handle employee issues?

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Access Control

- How is access control handled to the system?
- How is your data physically or logically segmented from other organizations that the service provider handles?

Data Ownership and Control

- Who owns the data?
- Is it encrypted when stored?
- Does the service provider have access to just the data, or do they also have the encryption keys?

Incident Response and Notification Processes

- How will you be notified if there is a breach?

- Or, will you even be notified if there is a breach?

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

User Awareness Training

Security Architecture & Tool Sets

User Awareness Training

- Users are the biggest threat to networks
- Proper security training is the most cost effective control that can be applied in an organization
- All the technical controls in the world won't stop a threat if a user lets the bad guys into your network…

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Areas to Discuss

- Acceptable Use Policy
- Threats face by the organization
- How to report a security issue
- Physical security concepts
- BYOD Policy
- Data handling requirements
- Best practices for passwords, emails, remote work, secure web browsing, etc.

Spearphishing and Phishing

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Analyzing Secure Architectures

Security Architecture & Tool Sets

Analyzing Architectures

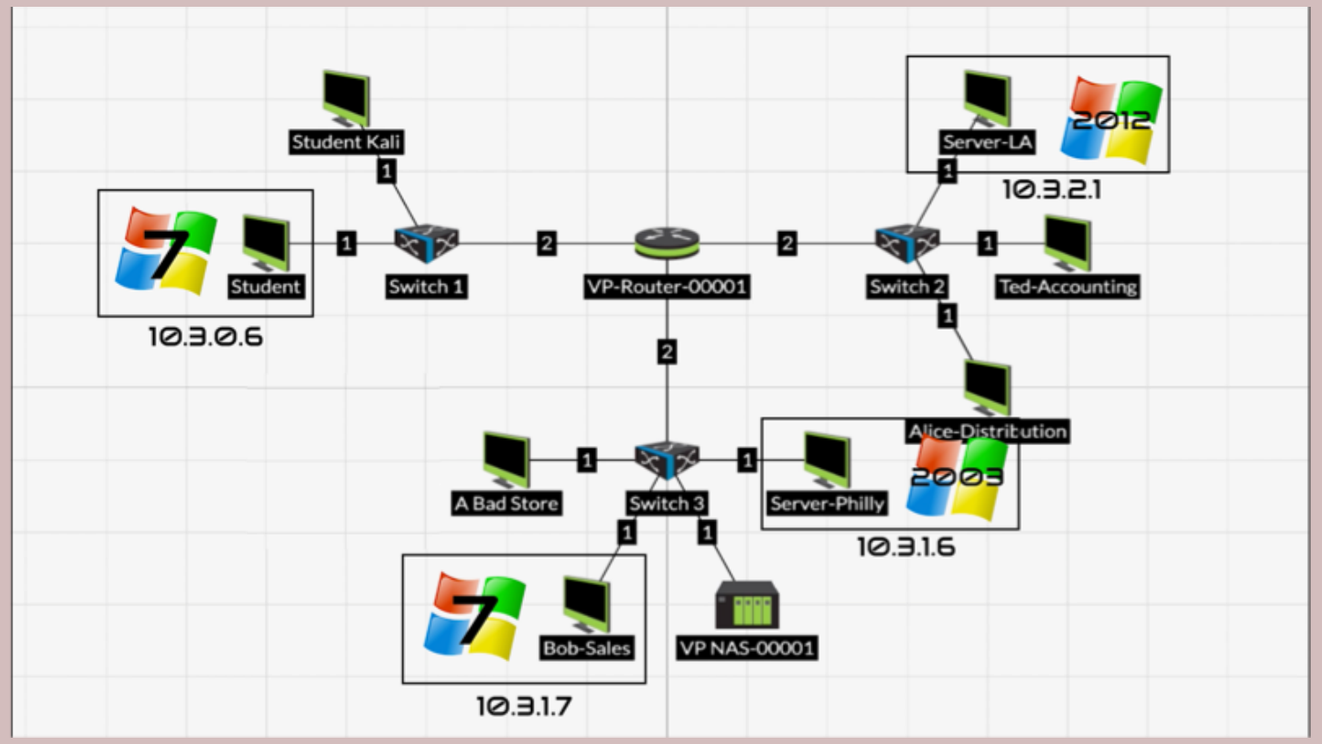
- Attackers always look for the flaw in the architecture's security controls
- Penetration testers act like an attacker to find these flaws, gaps, and single points of failure
- When analyzing security controls, determine if they meet the given requirement or stated goal

Reviewing Architectures

- Operational View
  - Focuses on how a function is performed or is supposed to accomplish
- Technical View
  - Focuses on technologies, configurations, and settings used in an architecture (system or service)
- Logical View
  - Focuses on the interconnections of systems with less technical details than the technical view

Common Issue: Single Points of Failure

- Singular part of the system that could cause the entire system to fail or the desired security level to fail is exploited



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Common Issue: Data Validation and Trust

- Data is commonly assumed to be valid and trustworthy in a system
- Can cause issues, such as trusting input provided to web application will be valid
- Can lead to SQL injections or other issues
- To prevent this, systems should be designed with validation and integrity checking

Common Issue: Users

- The largest cause of a security failure
- Mistakes and abuse can be at fault
- To prevent this:
  - Use automated monitoring to detect error
  - Constrain interfaces to only allow activities
  - Implement procedural checks and balances
  - Provide user awareness training

Common Issue: Authentication & Authorization

- User credentials, passwords, and permissions can cause security failure

- To prevent this:
  - Multifactor authentication
  - Centralized account management
  - Centralized privilege management
  - Monitor privileged account access
  - User awareness training

Architecture Reviews

- Step-by-step analysis of organization security needs
- Begin with the design requirements and then look at technical and logical diagrams
- Identify issues and report them per your organizational processes

Maintaining Secure Architectures

- Threats change over time and systems become outdated
- Conduct scheduled reviews
  - Systems, networks, and processes
- Continual Improvement
  - Incremental improvements over time
- Retirement of processes
  - Policies can become no longer relevant

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

What is Identity?

Security Architecture & Tool Sets

What is Identity?

- Collection of user information, rights, credentials, group memberships, & roles
- Set of claims about an individual or account holder made about one party to another party
- Key part of authentication, authorization, and trust

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Attributes of Identity

- Name, address, title, contact information, identification number, etc…

- Attributes populate the directory and can be used as an authentication process

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

AAA: Authentication, Authorization, and Accounting

- Used to control access to computers, networks, and services

- AAA systems use usernames, passwords, or other attributes of an identity to authorize access

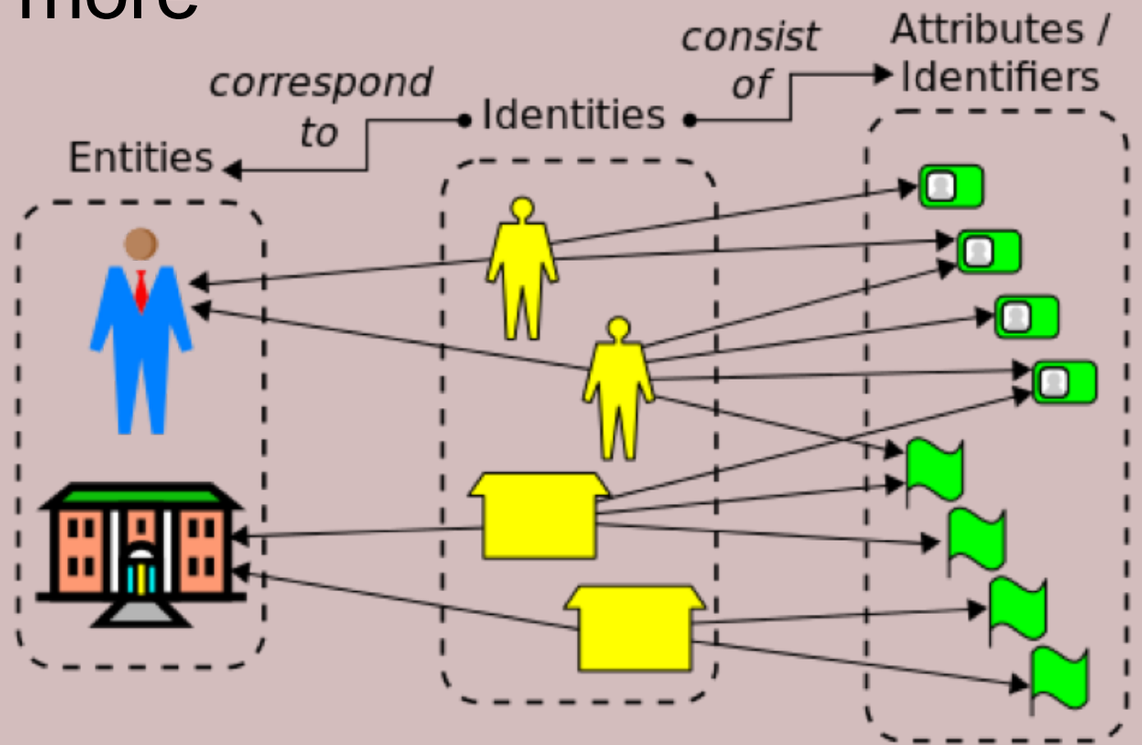
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

AAA: Authentication, Authorization, and Accounting

- Authentication
  - Individual proves who they are
- Authorization
  - Individual is provided access to a given resource
- Accounting
  - Logs and monitors a user when an authentication or authorization attempt is made or completed

Centralized Identity and Access Management (IAM)

- Systems built to create, store, and manage identity information, including group memberships, roles, permissions, and more



What does IAM do for us?

- Provisioning accounts
- Authentication
- Single-Sign-On (SSO)
- LDAP Directory
- Account Maintenance
- Reporting
- Monitoring
- Logging
- Auditing

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identity Systems

Security Architecture & Tool Sets

Identity Systems

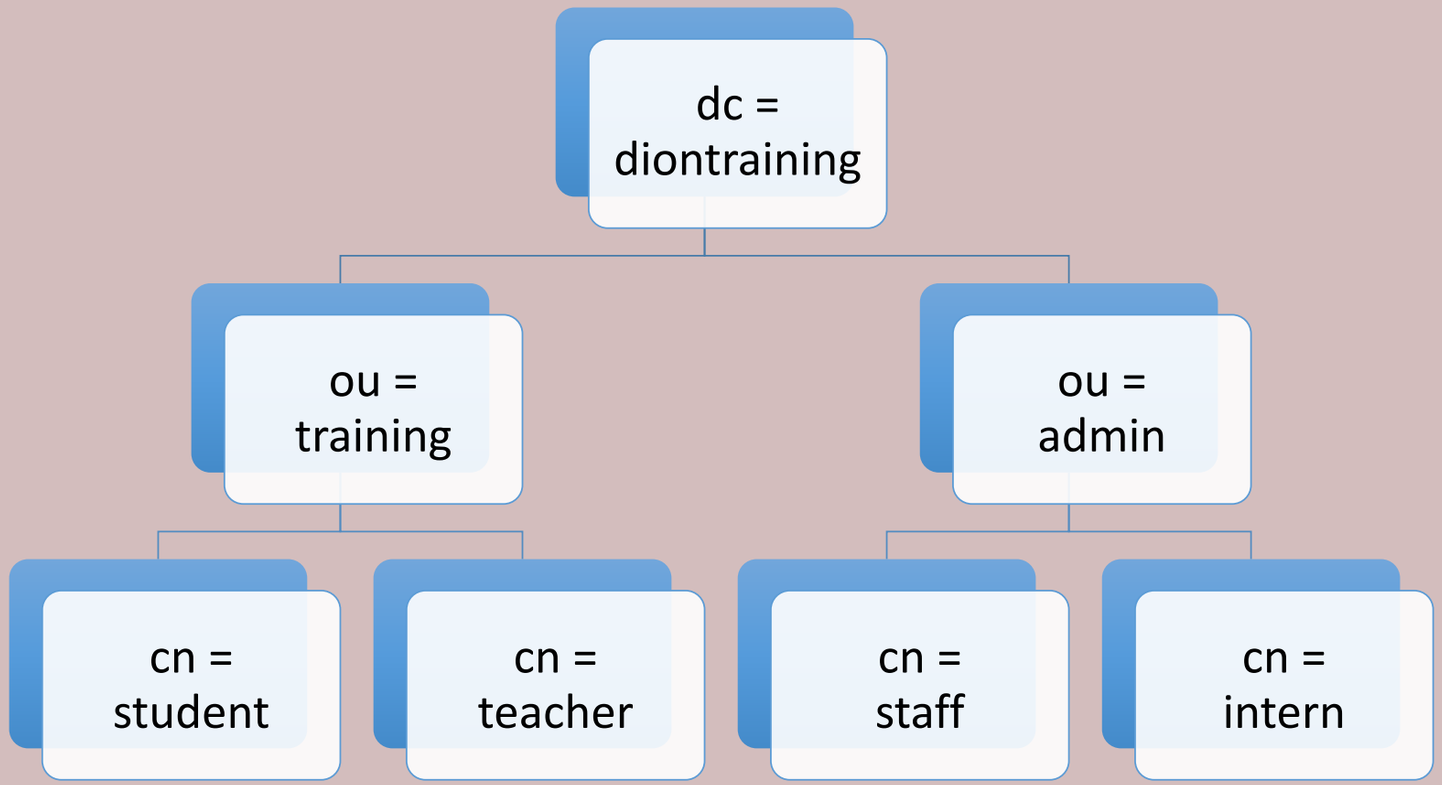
- Provide common functions
  - Identity creation and management
  - Authentication and authorization
  - Federation of identity information

- To provide these functions, we use:
  - Directories
  - Authentication services
  - Identity Management Platforms and federated identity tools

Directory Services

- Used in networks to provide information about systems and users
- LDAP (Lightweight Directory Access Protocol) is commonly used
  - Microsoft's Active Directory, Oracle's Internet Directory, IBM's Security Directory, OpenLDAP, 389 Directory Server, ApacheDS, and OpenDJ
- Can be used to make organizational information available to email and other programs

LDAP Directory Structure



dc = domain name
ou = organizational unit
cn = common name

Securing LDAP

- Enable and require TLS for LDAP query
- Set password storage to use salted hash
- Disable unauthenticated and anonymous LDAP modes (require user/password)
- Replicate LDAP to a redundant server to prevent outages or Denial of Service
- Strong ACLs on LDAP to limit access to objects using least privilege model

LDAP Injection

- Type of attack where improperly filtered input via web applications send arbitrary LDAP queries to the server

- Prevent this by:
  - Escaping all variable using the right LDAP encoding function
  - Use frameworks that automatically protect from injection (*LINQ to Active Directory)*
  - Minimize privileges assigned to LDAP web apps
  - Use input validation to whitelist what is allowed

Authentication Protocols

- Protocols used to supply verification of user's identity to a relying system

- Examples:
  - TACACS+
  - RADIUS
  - Kerberos

TACACS+

- Cisco extension to the Terminal Access Control Access Control System
- Uses TCP to provide AAA services
- Lacks integrity checking of data it sends
  - Subject to replay attacks
- Encryption flaws
  - Encryption key can be discovered by attacker
- Don’t use TACACS+ unless on an isolated network, it is just too flawed…

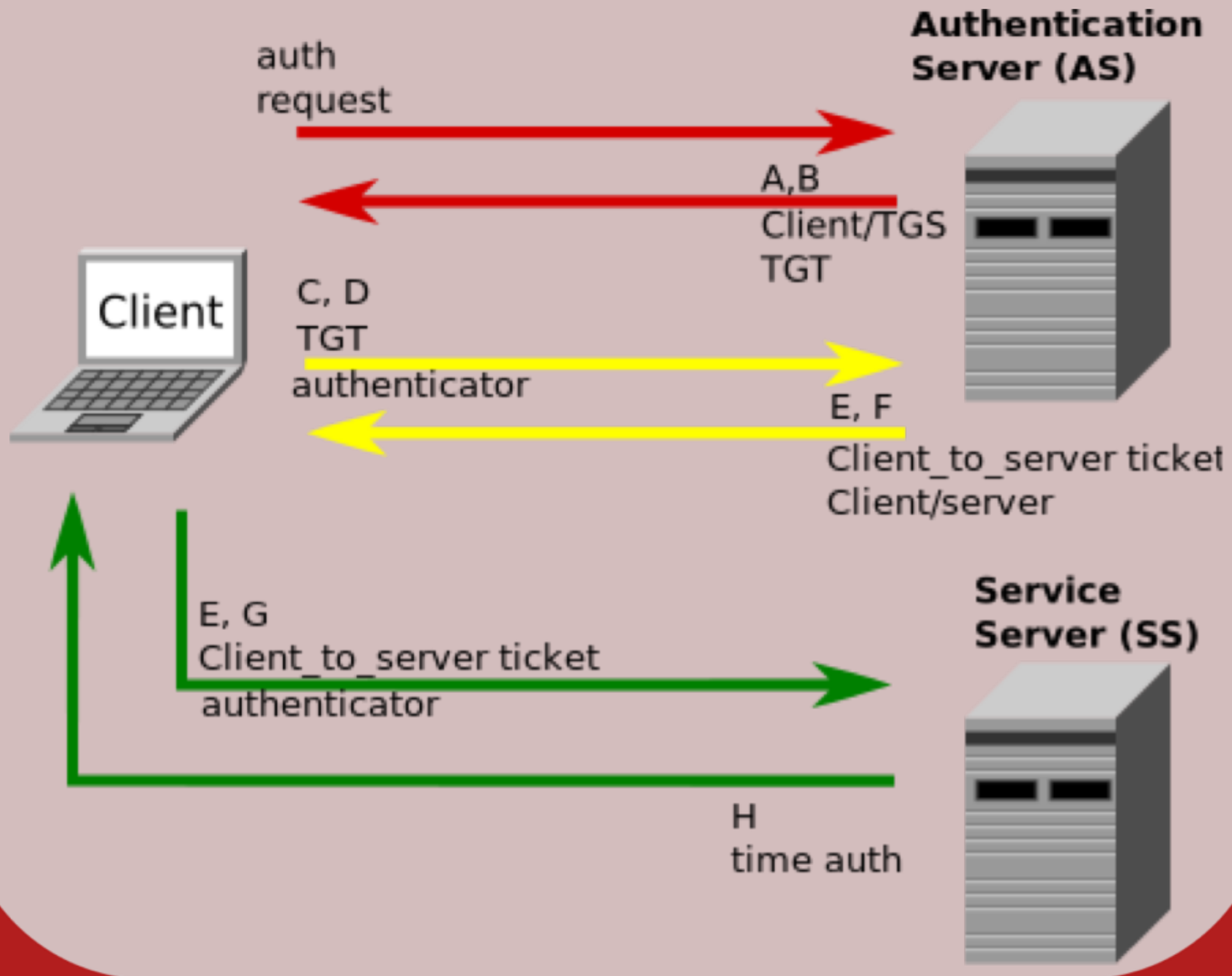
RADIUS

- Remote Authentication Dial-in User Service
- Most common AAA for networks, wireless networks, and other services
- Operates over TCP or UDP in a client-server model
- Password obscured using shared secret and MD5 hash (not considered strong)
- RADIUS traffic should be encrypted using IPSec between endpoints

Kerberos

- Designed with security in mind
- Operates on untrusted networks using encryption of its data
- Principles (users) comprised of three elements:
  - Primary (usually a username)
  - Instance (unique ID incase usernames are similar)
  - Realm (group of primaries)
- Replaced NTLM for AAA in Windows domains

Kerberos Authentication



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Single-Sign-On (SSO)

- Allows users to authenticate once and then be able to use multiple systems

- Examples:
  - LDAP
  - CAS (Central Authentication Service)

- Benefits:
  - Reduce password reuse
  - Fewer password resets and support calls

Shared Authentication

- OpenID
  - Open-source standard for decentralized authentication
  - Uses Google ID to logon to all sites
- OAuth
  - Open authentication standard used to share elements of identify with third-party (ie., Google provides your info)
- OpenID Connect
  - Authentication layer built using OAuth protocol
- Facebook Connect
  - Facebook login to authenticate to other websites and services

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Threats to Identity Systems

Security Architecture & Tool Sets

Threats to Identity Systems

- Threats to the underlying authentication and authorization system
  - Exploit how users login
  - How credentials are handled
  - How users are authorized
- Target account lifecycle
  - Creating credentials
  - Preventing credential removal
  - Elevating privileges of credentials
- Attack the account itself
  - Phishing
  - Compromise systems holding credentials

Personnel-based Threats

- Targets users through phishing or social engineering techniques
- User awareness training helps prevent this
- Insider threat would also fall into this category

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Endpoint Threats

- Targets your endpoints through…
  - Local exploits
  - Keyloggers
  - Local administrative credentials
  - Password stores and tokens

- Protect by using anti-malware and anti-virus

- Protect by using strong authentication stores

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Other Identity Threats

- Sever-based Threats
  - Attacks your servers to send identity and authentication information to AAA servers
- Application/Service Threats
  - Attacks your applications and/or services that rely on identity and authentication
- Roles, Rights, and Permission Threats
  - Threats focused on users or groups roles, rights, and permissions

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Attacking AAA Protocols and Systems

Security Architecture & Tool Sets

Attacking AAA Protocols and Systems

- Directory, authentication, and SSO systems are great targets for attacks to go after
- Attackers use specific vulnerabilities and misconfigurations to target the AAA protocol itself or how a server implements the protocol
- Attempting system compromises of domain controllers and AAA systems is common

Attacking LDAP

- Target unencrypted LDAP traffic to capture traffic for replay attacks
  - Use secure binding to prevent this
- Target improper access controls to harvest directory information or to modify directory
  - Setup good access controls
- Perform LDAP injection against vulnerable web applications that interface with directory
  - Validate web-based input and use least privilege
- Conduct Denial-of-Service against LDAP to cause services to fail which rely on it
  - Design scalable LDAP for redundancy

RADIUS

- Authentication commonly used for network devices and VPNs can be attacked by…
  - Session replay of server or client responses
  - Compromising shared secret key from client machines
  - Brute-force share secret key from a stolen password
  - Denial-of-Service to prevent user authentication

Kerberos

- Relies on central key distribution center (KDC)
- Compromise of KDC allows impersonation as any user

- Common attacks:
  - Stealing administrator account credentials
  - Kerberos ticket reuse
    - Pass-the-ticket allows impersonation for ticket lifespan
    - Pass-the-key allows reusing secret key to get new tickets
  - Ticket Granting Ticket (TGT) attacks
    - “Golden Ticket” allows creation of new tickets, account changes, and creation of new accounts/services

Active Directory

- Core identity store and AAA service for Microsoft Windows domains
  - Many exploits built for clients, servers, and AD
- Many Windows domains contain older systems still…
  - or are at least backward configurations still activated which makes them vulnerable to attack
- Very common target for attackers

Attacks on Active Directory

- Malware focused on stealing credentials
  …or Phishing or social engineering
- Malware focused on Windows server exploit
- Focus on attacking older services like NTLM, LANMAN, NetBIOS, unsigned LDAP, or SMB
- Privilege creep of service accounts
- Overuse of domain admin credentials
- Privilege escalation attacks

OAuth, OpenID, OpenID Connect

- OAuth and OpenID are implemented by each service provider leading to configuration flaws
- Open redirects are a common attack
  - Redirects and forwards aren't validated
  - Untrusted user input can be sent to web apps
  - Users can be redirected to untrusted websites
  - Potential for phishing, pharming, or bypassing of website security
- Original account information will not be compromised, but your web application may allow in untrusted users

OAuth, OpenID, OpenID Connect

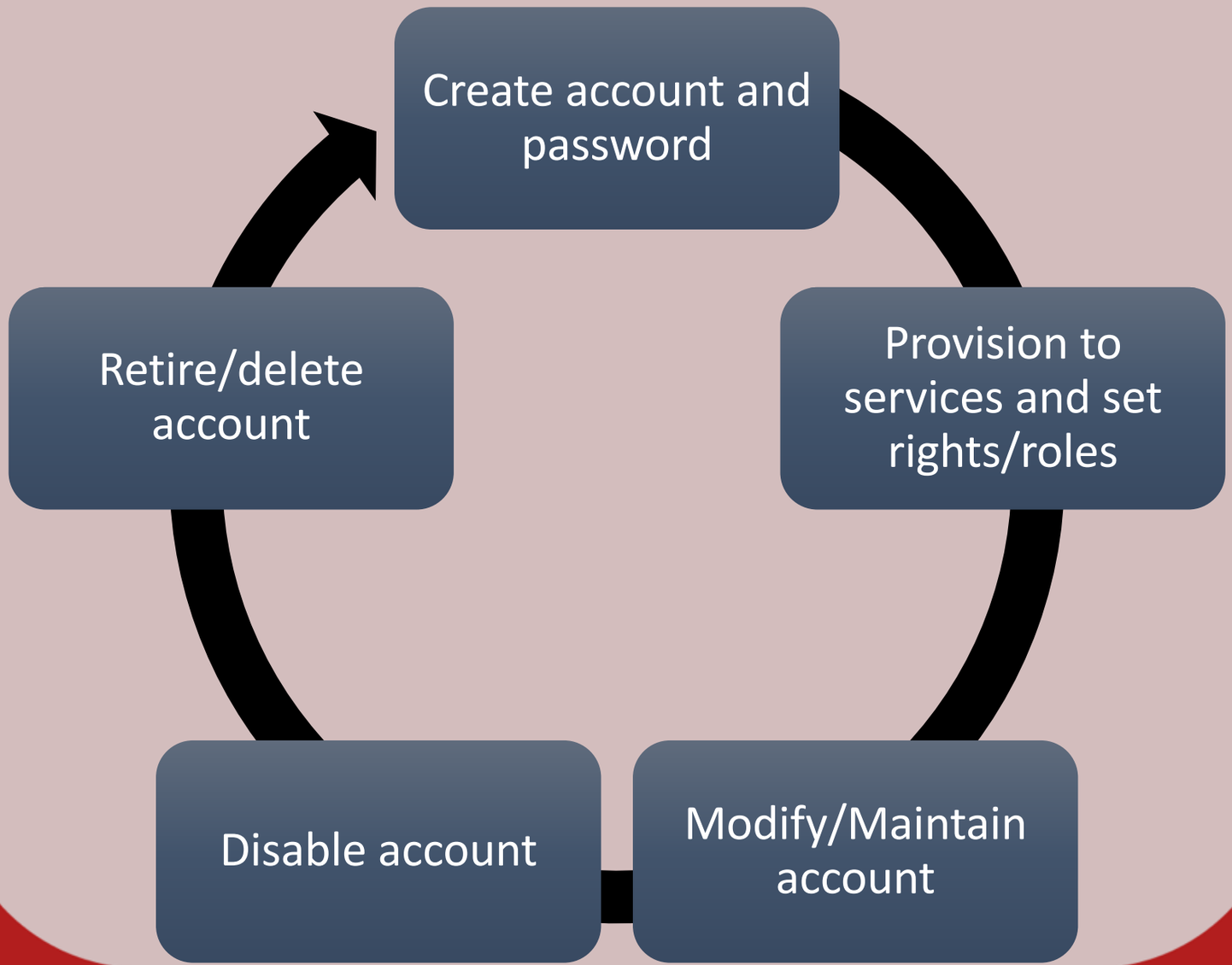
- OpenID attacks have been directed at vulnerabilities in the protocol itself
  - Example:
    - Attackers forged request to gain arbitrary logins
- OAuth2 is vulnerable to cross-site request forgery (CSRF) attacks
  - Attack attempts to get user to click a link so that their browser performs an action as the user
- OpenID Connect provides extra encryption and signing to prevent many of these exploits

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Targeting Account Lifecycle

Security Architecture & Tool Sets

Targeting Account Lifecycle



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Utilize Least Privilege

- Users should only be provided with the lowest set of privileges and access necessary to perform their job functions

Prevent Privilege Creep

- Accounts tend to gain privileges overtime based on rotating job functions a user undertakes

- Always ensure to remove old rights when they are no longer needed
  - Employee get promoted or moved to another job

Identity Lifecycle Management

- Numerous tools exist to help with this
- Centrify, Okta, and Ping Identity provide account lifecycle maintenance and monitoring features

Centrify® PingIdentity® okta

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identity Exploits

Security Architecture & Tool Sets

Impersonation Attacks

- Attacks takes on the identity of a legitimate user
- Usually involves credential theft or open redirects (OAuth)

Session Hijacking

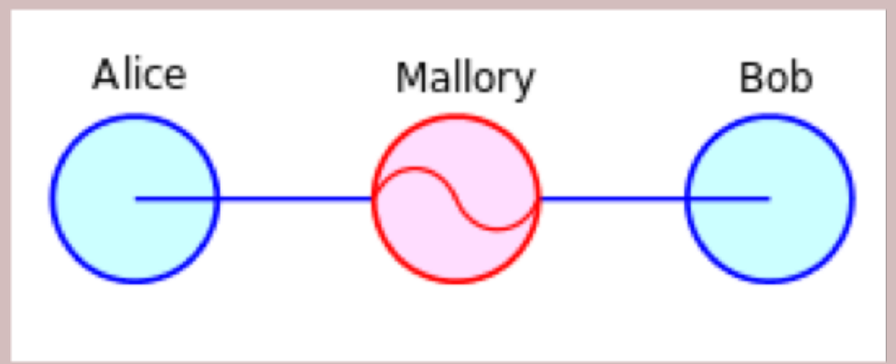
- Attacker takes over an existing session by acquiring or guessing the session key

- Prevented through encrypting sessions

Man-in-the-Middle (MITM)

- Attacker accesses the information flow between systems or services

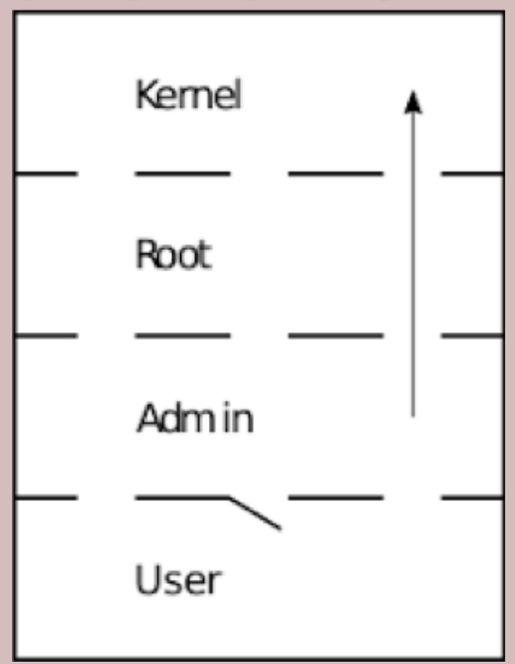
- Prevented through using session or link encryption tunnels



Privilege Escalation

- Attacker elevates their permissions from one level to a higher level

- Usually follows an attack on a normal user account credentials



Rootkits

- Attacker uses malware to provide continued access to a server/client while hiding their own presence

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Credential Theft

Security Architecture & Tool Sets

Credential Theft

- Attackers can target users, services, or simply brute force credentials to compromise them

Phishing

- Aimed at stealing credentials by tricking users into clicking on a link in an email and entering their username/password

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Compromise Other Websites (Password Reuse)

- Aimed at stealing credentials from a less secure server, then reusing them in your organization

- If the other server stored them as MD5 or other weak key stores, it becomes easy to crack the passwords

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Brute-Force Attack

- Login using every different combination until you gain access

- Prevent:
  - Limit number of login attempts
  - Use CAPTCHA-style to prevent automation

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Securing Authentication and Authorization

Security Architecture & Tool Sets

Securing Authentication

- Technical and administrative controls can help secure the authentication process
- Uses strong passwords/passphrases
- Password management is a concern
  - Consider Single-Sign-On
  - Token-based for multifactor
  - Password safes (LastPass, Dashlane, etc)
- Encrypt communications between clients and authenticators using TLS

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Securing Authorization (Users)

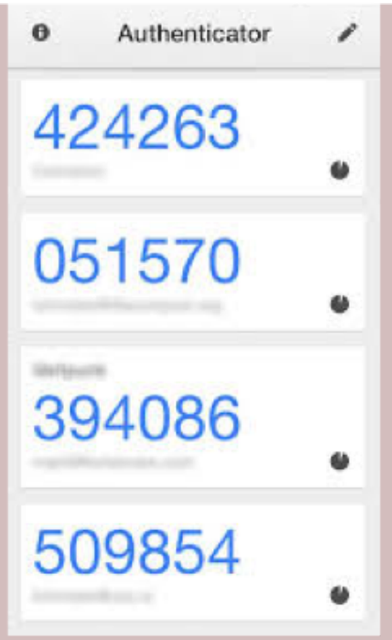
- Access control ensures users are matched with rights/privileges
- Polices to control what rights are given
- Implement management systems for approving rights
- Monitor/report on which accounts have which rights assigned

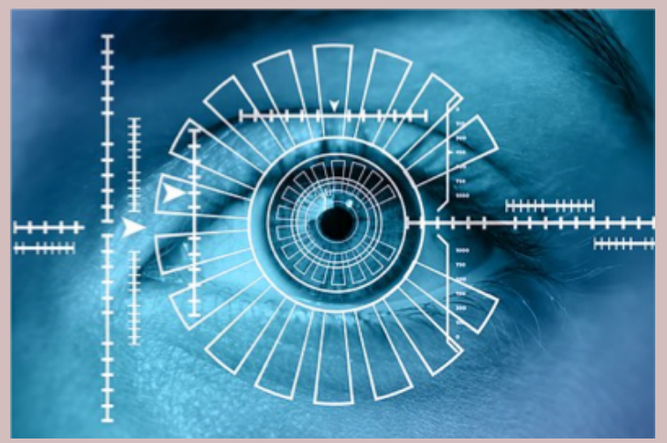
Securing Authorization (Admin)

- Privileged User Management concerns giving admin rights to users
- Use additional monitoring and logging
- Implement separation of duties
- Use appropriate training
- Prevent admin accounts from being used as daily accounts

Multifactor Authentication

- Use two or more factors for authentications
  - Knowledge factors
  - Possession factors
  - Biometric factors
  - Location factors



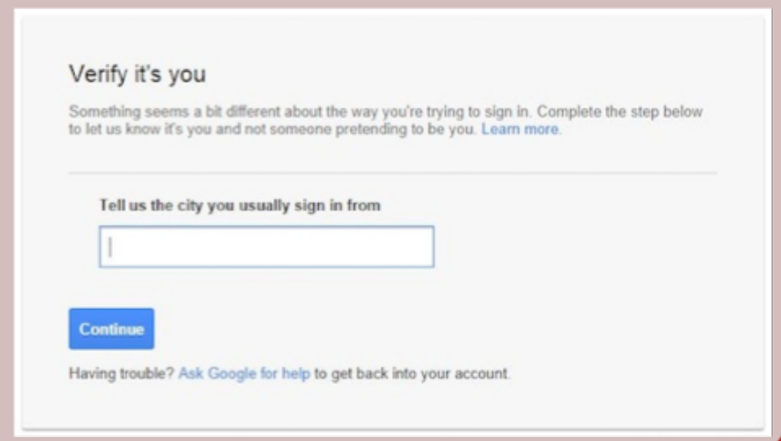


JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Context-Based Authentication

- Authentication decision is based on information about the user, system, etc.

- User's role or group membership
- Time of day in relation to user's hours
- IP address and reputation
- Frequency of access
- Location (IP or GPS)
- Type of device



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Identity as a Service (IDaaS)

Security Architecture & Tool Sets

Identity as a Service (IDaaS)

- Provides authentication services, usually through cloud-based resources
  - Identity lifecycle management
  - Directory services (LDAP, AD, or others)
  - Access management
  - SSO via SAML, OAuth, or other technology
  - Privilege account management/monitoring
  - Reporting, auditing, and other oversight/visibility into the identity lifecycle

Challenges with IDaaS

- Will you centralize your directory services or will internal and external directories be used?
- How about authentication? Centralized or federated?
- Will you use local or cloud-based authoritative credential stores?

IDaaS Benefits

- If your current organization doesn't already have strong identity management, IDaaS can be a big improvement in security…

  …can be better managed

  …can be more capable

  …can be more secure

- Centralized monitoring and reporting can help detect issues sooner than traditional systems

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Detecting Identity Attacks

Security Architecture & Tool Sets

Detecting Identity Attacks

- Identity and Access Management systems should be fed into the SIEM

- Configure your SIEM to detect:
  - Privileged account usage
  - Privilege changes and grants
  - Account creation or modifications
  - Terminated user account usage
  - Lifecycle management events
  - Separation of duty violations

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Active Monitoring

- Knowledgeable technicians should actively monitor identity systems
- Humans should analyze reports to identify issues
- Remember, you must know what normal looks like in order to detect the abnormal

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Federated Identity Systems

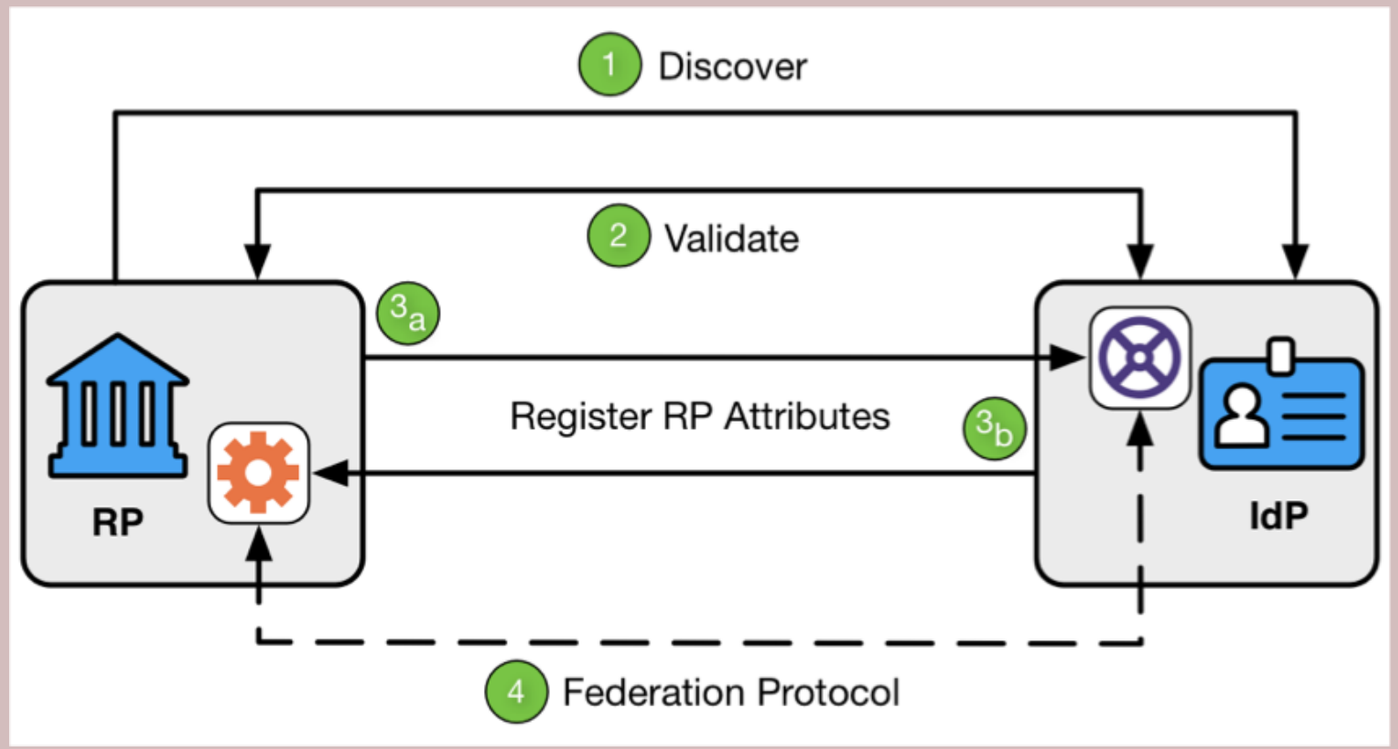
Security Architecture & Tool Sets

Federated Identity Systems

- Moves the trust boundary outside your organization to Google, Facebook, LinkedIn, or other identity providers

- Identity Provider (IDP)
  - Provides identities & release data to relying parties
- Relying Party (RP) or Service Provider (SP)
  - Members of the federation that provides services to the user when identified by identity provider
- Consumer or User
  - Asked to make decision on who to share their identity with by IDP in order to get services from RP/SP

Federated Identity Systems



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Choosing a Federated Identity System

- Do you care that the user says who they are?
  - If not, use Google, Facebook, etc.
  - Otherwise, find identity provider that vets its users

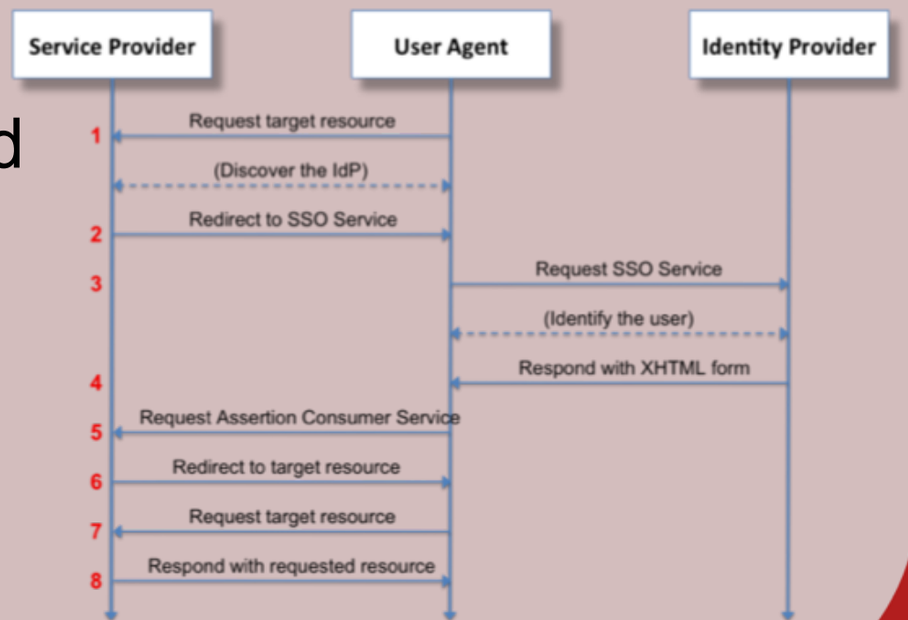
- When users signup for your site using federated ID, you immediately provision a user account on your system mapped to the attributes released by IDP

Federated Identity Systems Technologies

- Security Assertion Markup Language (SAML)
- OAuth and OAuth 2.0
- Active Directory Federation Services (ADFS)
- OpenID Connect

Security Assertion Markup Language (SAML)

- XML-based language to send authentication and authorization data between IDP and RP
- Used to enable SSO for web apps & services
- Allows attribute, authentication, and authorization decisions to be exchanged



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

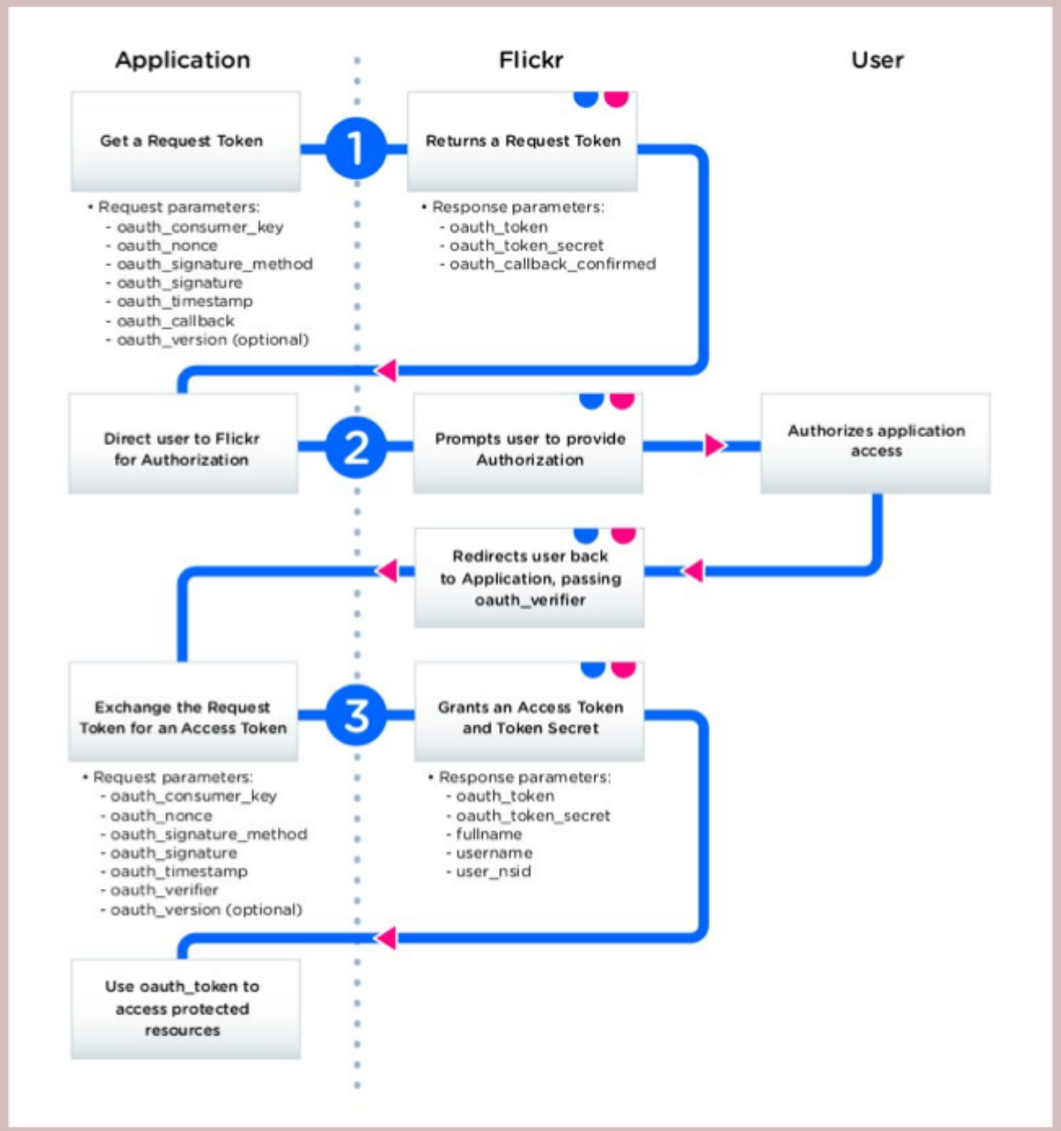
OAuth and OAuth 2.0

- Developed by the Internet Engineering Task Force (IETF) to provide an authorization framework to allow service provider applications to access HTTP-based services
- Provides access delegation to allow service providers to provide actions on behalf of user
- Supports web clients, desktops, mobile devices, and other embedded device types

OAuth and OAuth 2.0

- OAuth has types of four parties served:
  - Clients
    - Applications that the user wants to access/use
  - Resource Owners
    - End user being serviced
  - Resource Servers
    - Servers provided by a service the user wants to access
  - Authorization Servers
    - Servers owned by the identity provider (IDP)

Flickr Federated Example (OAuth Authentication Process)



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Active Directory Federation Services (ADFS)

- Microsoft's answer to federated identities
- Provides authentication and identify data as claims to service providers
- Partner sites use trust policies to match claims to claims supported by their services to make their own authorization decisions
- Works similar to the OAuth authentication process

Incident Response for Federated Identity Systems

- Check your contract (if you have one)
- IDP usually responsible for notifying account owners (users) and RP/SP of a breach and required response (like password resets)
- RP/SP must determine their response if IDP was compromised (what response, if any)
- If your users' accounts are compromised, how will you provide them access?
  - Think about if a Facebook login got stolen…

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

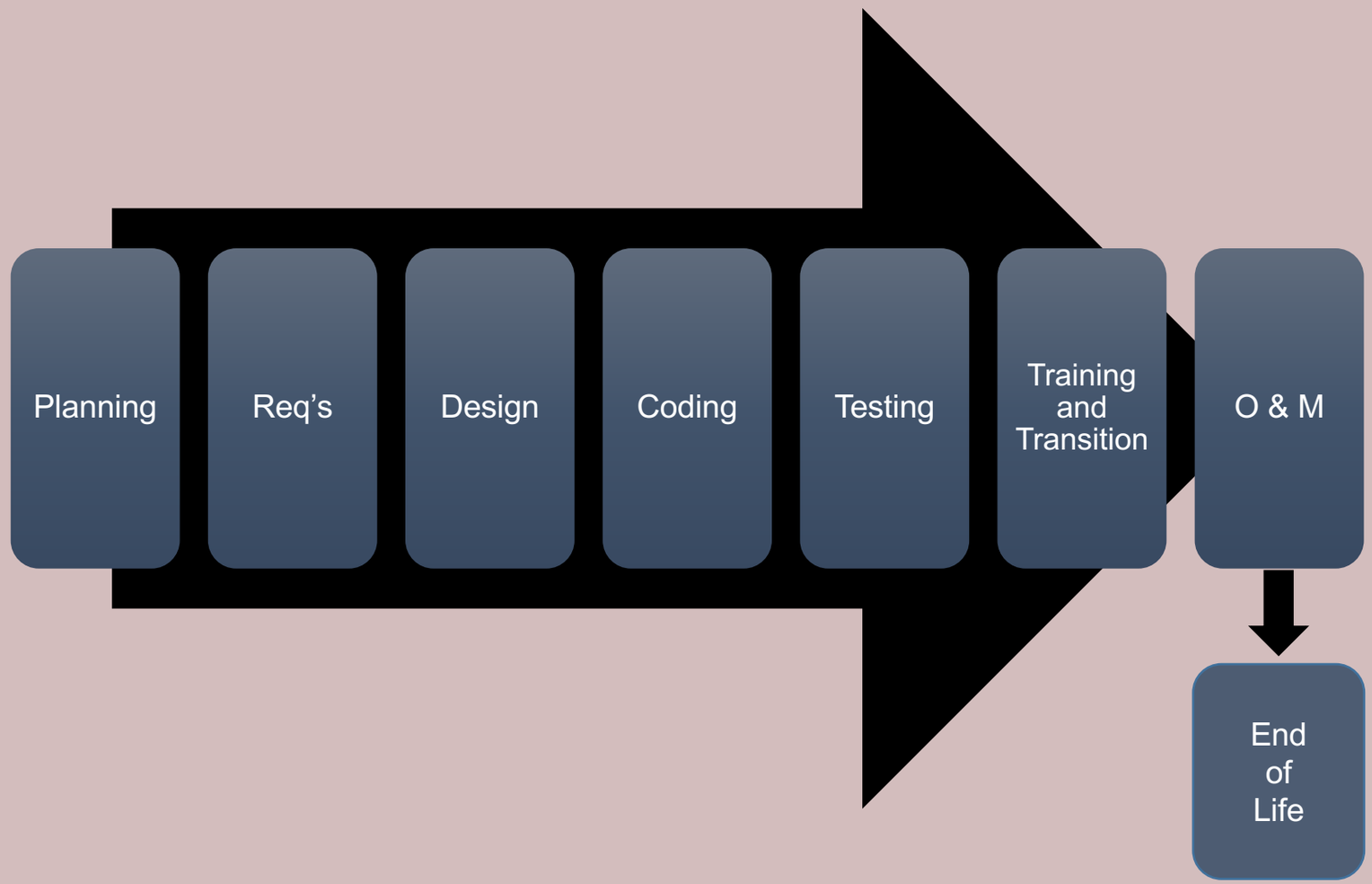
Software Development Life Cycle

Security Architecture & Tool Sets

Software Development Life Cycle (SDLC)

- Software development doesn't always follow formal models
- Many different forms of SDLC…
  but all share 8 basic functions/phases
- SDLC can also be used for applications, services, systems, or other desired outputs
- Planning for security early in the process will provide better security at a cheaper price…

Software Development Life Cycle (SDLC)



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Planning

- Initial investigations into the effort conducted
- Determines feasibility of designing the desired software, costs, and any alternate solutions
- End result: decision to move forward or not

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Requirements

- Gain customer or stakeholder input to determine required functionality
- What should the program do?
- What does your current program not do?

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

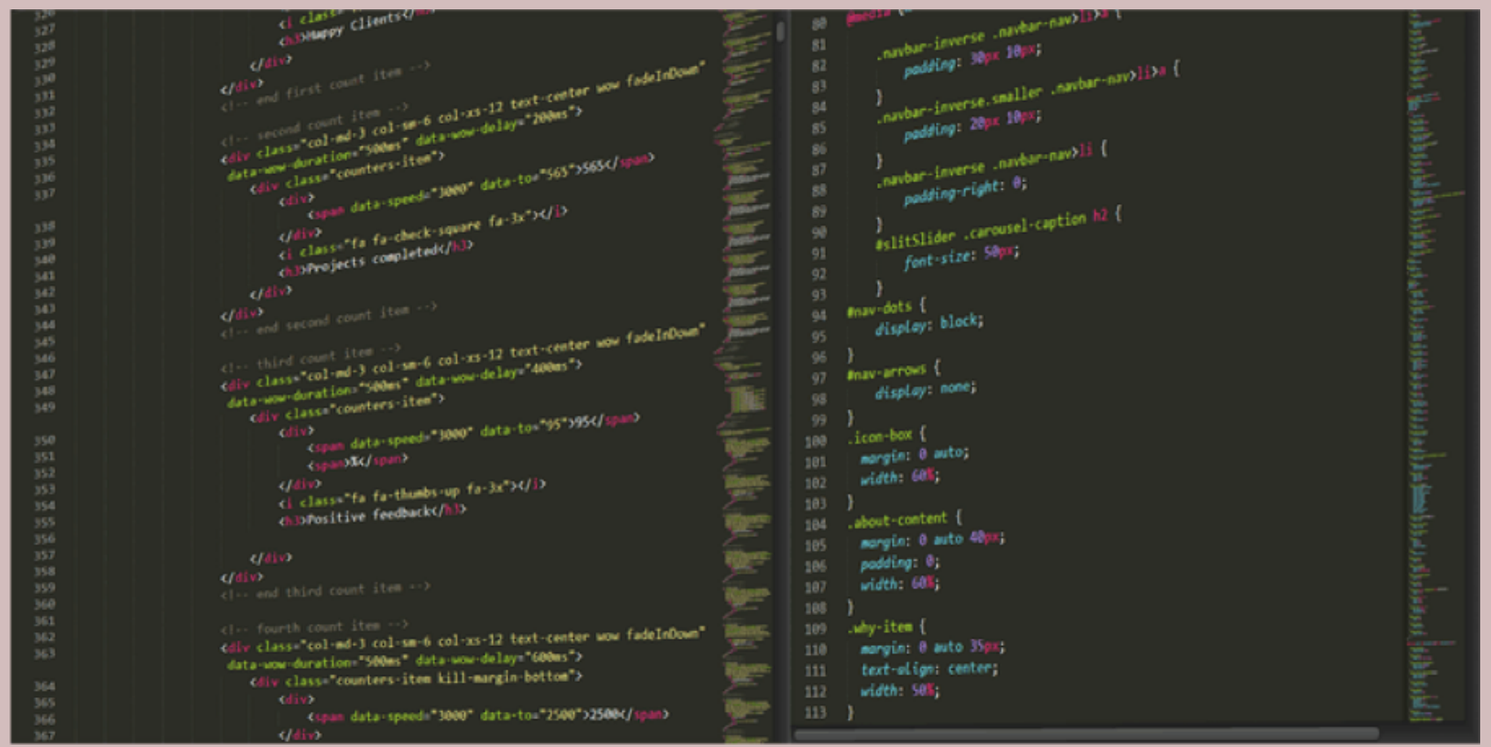
Design

- Creates designs for functionality, architecture, integration points, techniques, data flows, processes, and other elements

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Coding

- Programmers start writing the code for the software and conduct testing of individual units of code and through code analysis



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Testing

- Formal testing with outside development team (stakeholders, customers, beta group, etc)

- User Acceptance Testing ensure users are satisfied with the functionality

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

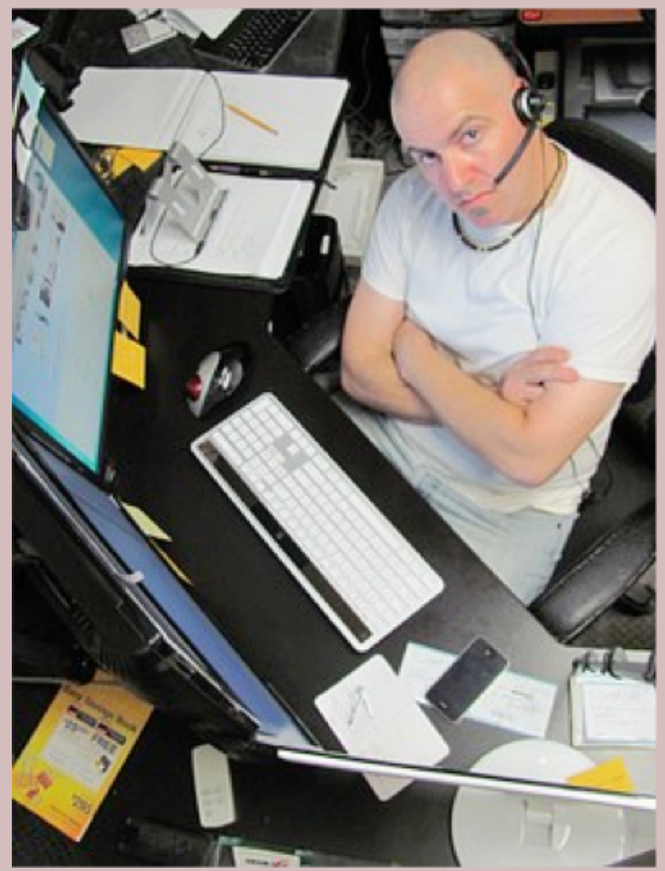
Training and Transition

- Ensures the end users are trained on software
- Consists of acceptance, installation, and deployment of software into live environment

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Operations and Maintenance

- Longest phase of the SDLC
- Patching, updating, modification, and daily support for the new software occurs

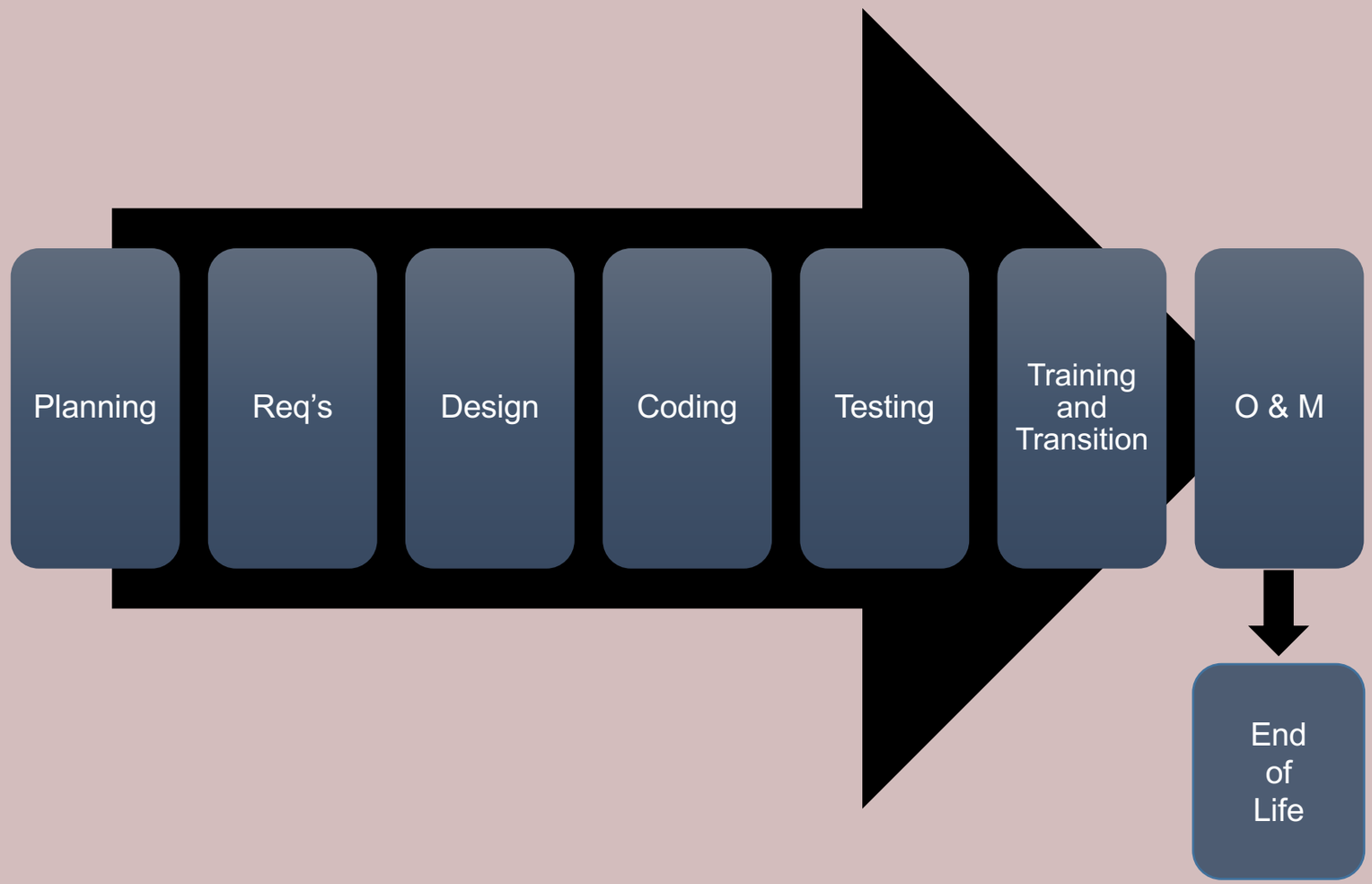


End of Life

- Disposition and retirement of the software
- How will you stop supporting the software?
- Will you migrate users to a new version?

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Software Development Life Cycle (SDLC)



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Software Development Models

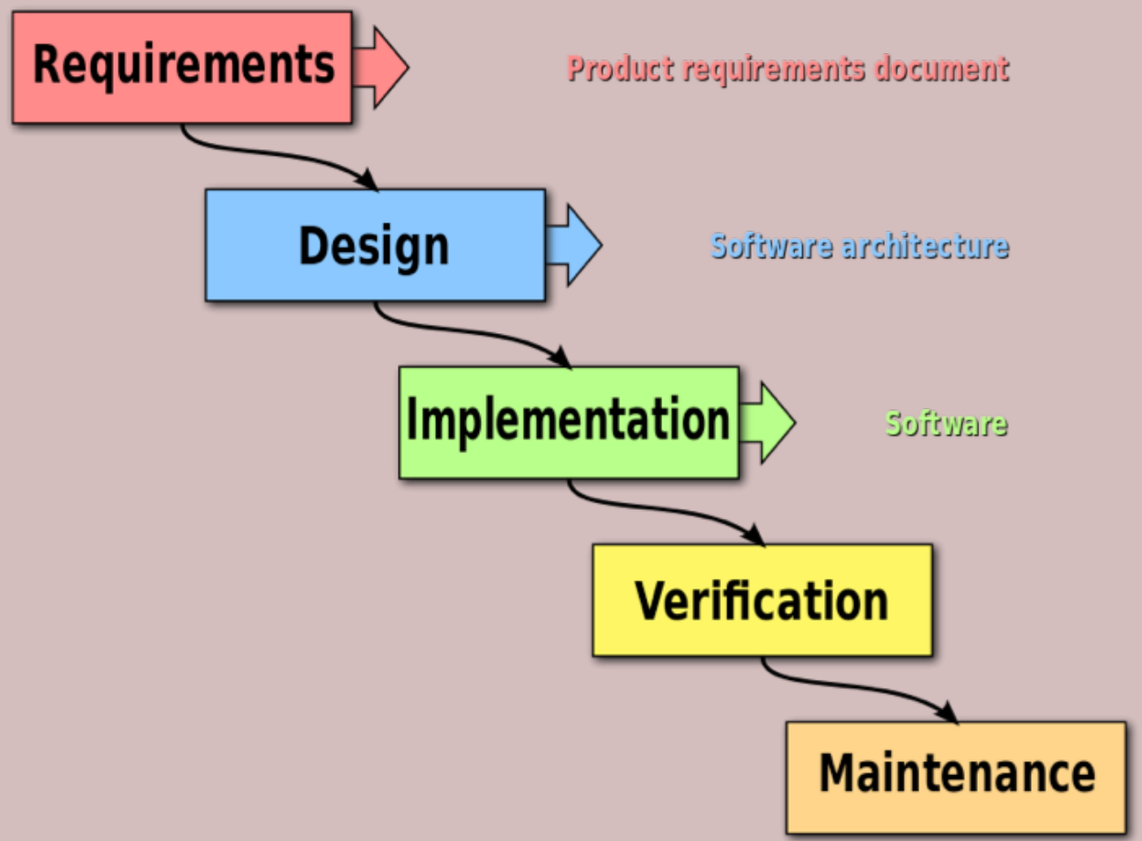
Security Architecture & Tool Sets

Software Development Models

- Many models of software development exist
- Models provide a common framework to use
- Can use detailed practices, procedures, and documentation
- Can also be less formal and haphazard

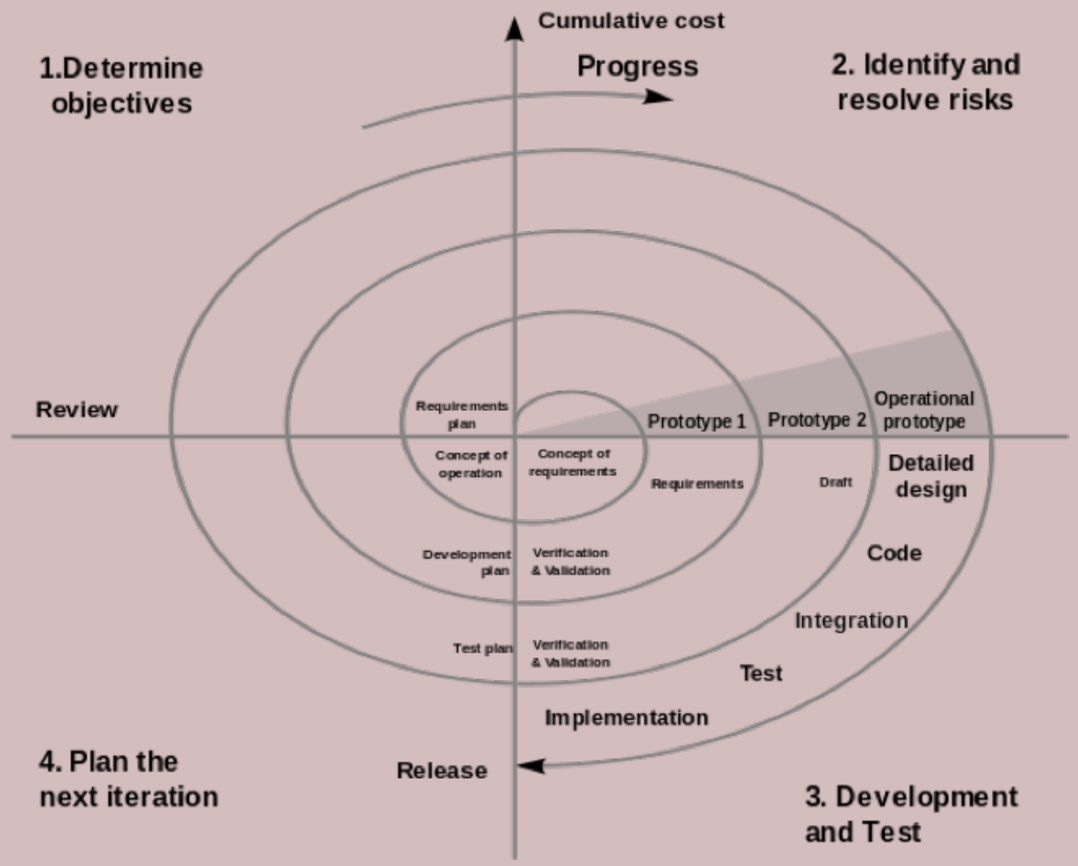
Waterfall Model

- Linear model with each phase following the previous phase



Spiral Model

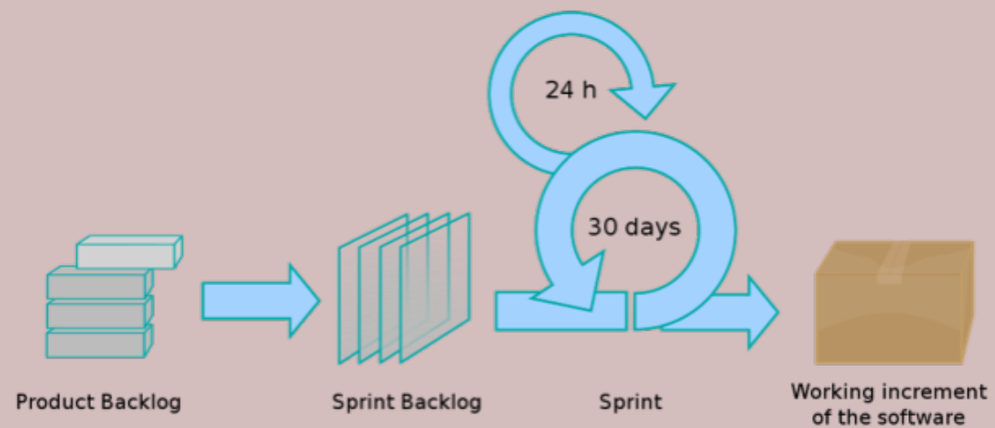
- Modification of Waterfall, it adds iterative process to revisit phases over and over



Agile

- Iterative and incremental process

- Foundations of Agile:
  - Individuals and interactions are most important
  - Working software is better than the documentation
  - Customer collaboration over contract negotiation
  - Responding to changes fast is better than a plan

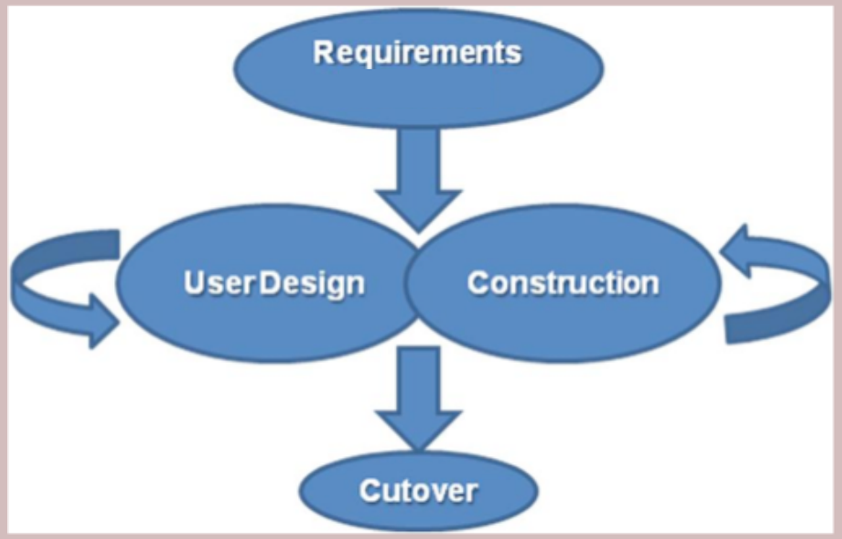


Terms Used in Agile

- Backlogs
  - List of features or tasks to complete
- Planning Poker
  - Estimation tool for planning in Agile
- Timeboxing
  - Agreed upon time to work on specific goal
- User stories
  - Describe high-level user requirements
- Velocity tracking
  - Adds up estimates for current sprint efforts and compares to what was actually complete

RAD
(Rapid Application Development)

- Iterative process relying on building prototypes
- Provides a highly responsive development environment for modularized work
- No planning phase… they just start coding

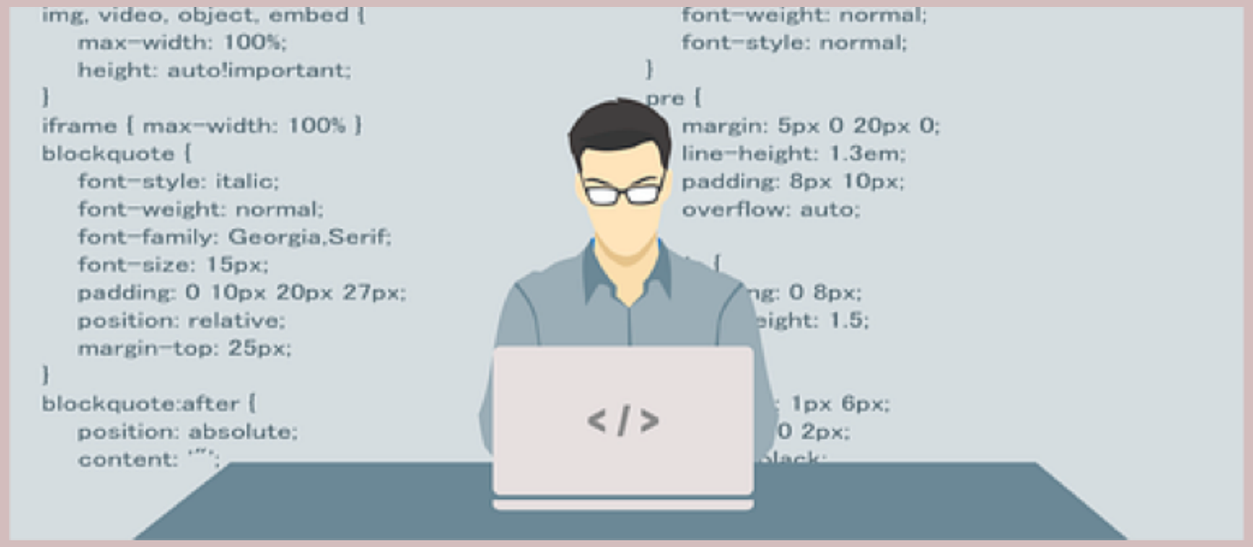


Terms Used in RAD

- Business Modeling
  - Focuses on understanding business processes
- Data Modeling
  - Gather and analyze datasets and the relationships
- Process Modeling
  - Define the processes and data flows
- Application Generation
  - Code & convert data and processes into prototype
- Testing and Turnover
  - Focus on interfaces between components and verifying functionality

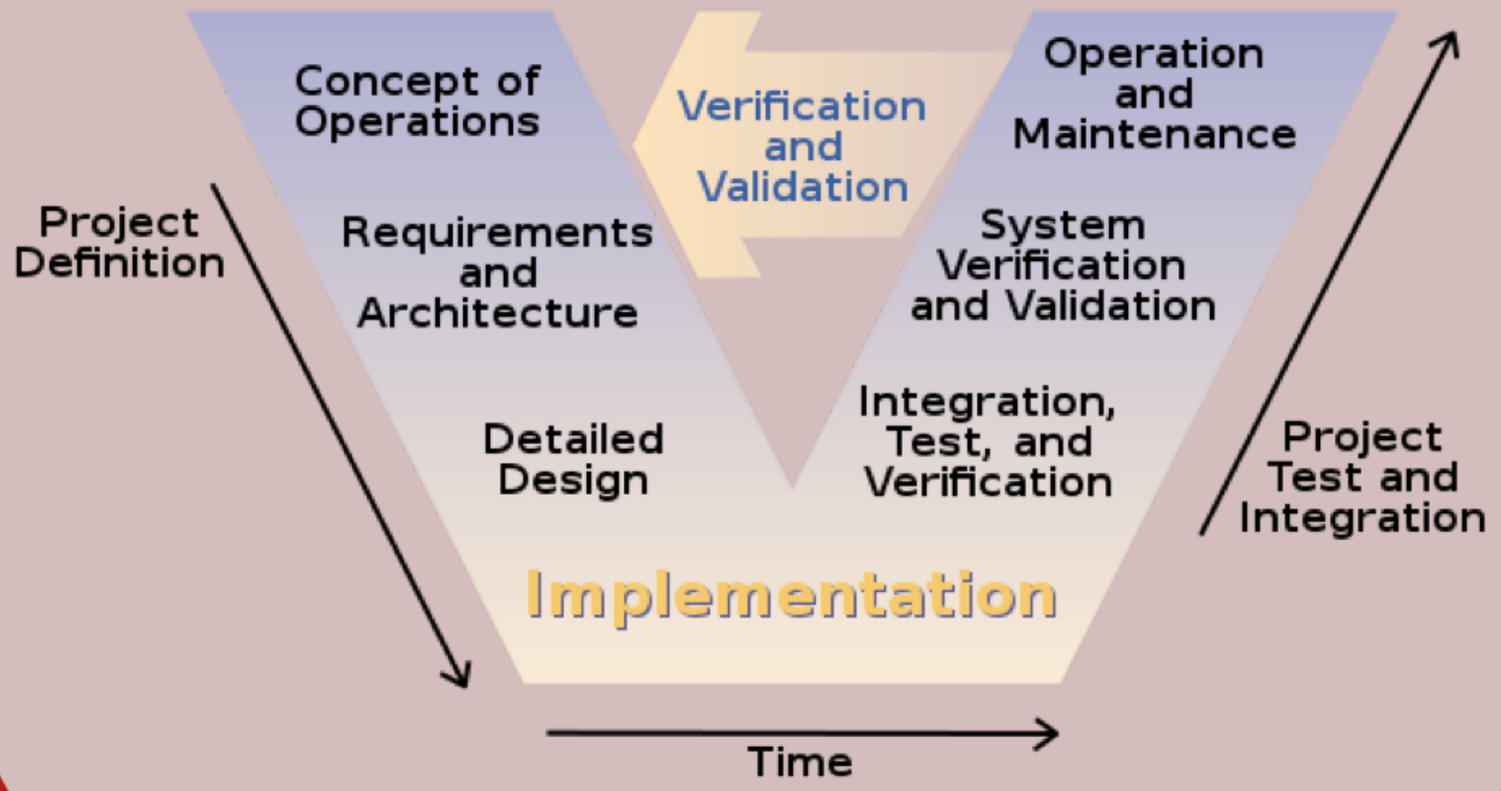
Big Bang SDLC Model

- All coding is based on requirements and making resources available
- Doesn't scale well, works best for single coder
- No planning or process



V Model

- Extension of the waterfall which pairs testing and development phases together



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Coding for Security

Security Architecture & Tool Sets

Coding for Security

- Security should be added in requirements
- Security is built during design and coding
- Security is *then* tested in prototypes and final products

Secure Coding Practices

- Have an organizational secure coding policy
- Conduct risk assessments (and ongoing assessments) to prioritize issues to remediate
- User input validation (prevent XSS/SQL inject)
- Consider your error messages
  - What information is being given? Too much?
- Database security in application and database
  - Prevents data leaks

Secure Coding Practices

- Encrypt sensitive information being stored
- Hash passwords your applications store
- Design for availability and scalability
  - Conduct load and stress testing
- Conduct monitoring and logging
- If possible, utilize multifactor authentication

Secure Coding Practices

- Code for secure session management
  - Prevents session hijacking
- Proper cookie management
  - Secure cookies if used in web applications
- Encrypt network traffic
  - Use TLS to prevent network-based data capturing
- Secure the underlying infrastructure
  - As a cybersecurity analyst, your biggest impact will usually be on the infrastructure and not the code

Open Web Application Security Project (OWASP)

- Community hosting standards, guides, best practices, and open source tools
- Provides updated lists of proactive controls to test your web application's security
- Check out OWASP.org

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Source Code Management

- Use check-in/check-out and revision history to ensure you know what code is current version

- Source Control Management or Version Control tools, like Git, Subversion, or CVS

GitHub

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Testing Application Code

Security Architecture & Tool Sets

Testing Application Code

1. Scanning using a tool
2. Automated vulnerability scanning tools
3. Manual penetration testing
4. Code review

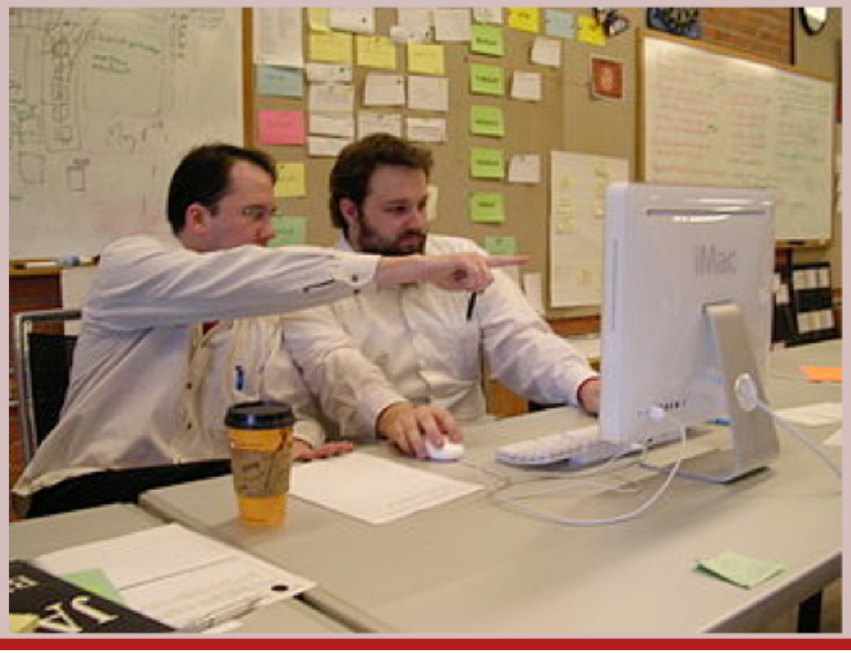
- OWASP considers code reviews the best and most thorough of these options
- “360 Reviews” combined code review with penetration testing, then review’s code again

Code Reviews

- Shares knowledge of the code with others
- More experience is learned across the team
- Detects problems and enforces good coding
- Agile and formal models:
  - Pair Programming
  - Over-the-Shoulder
  - Pass-Around
  - Tool-Assisted
  - Fagan

Pair Programming

- Agile development technique
- Two developers use one workstation
- Provides real-time code review but is costly



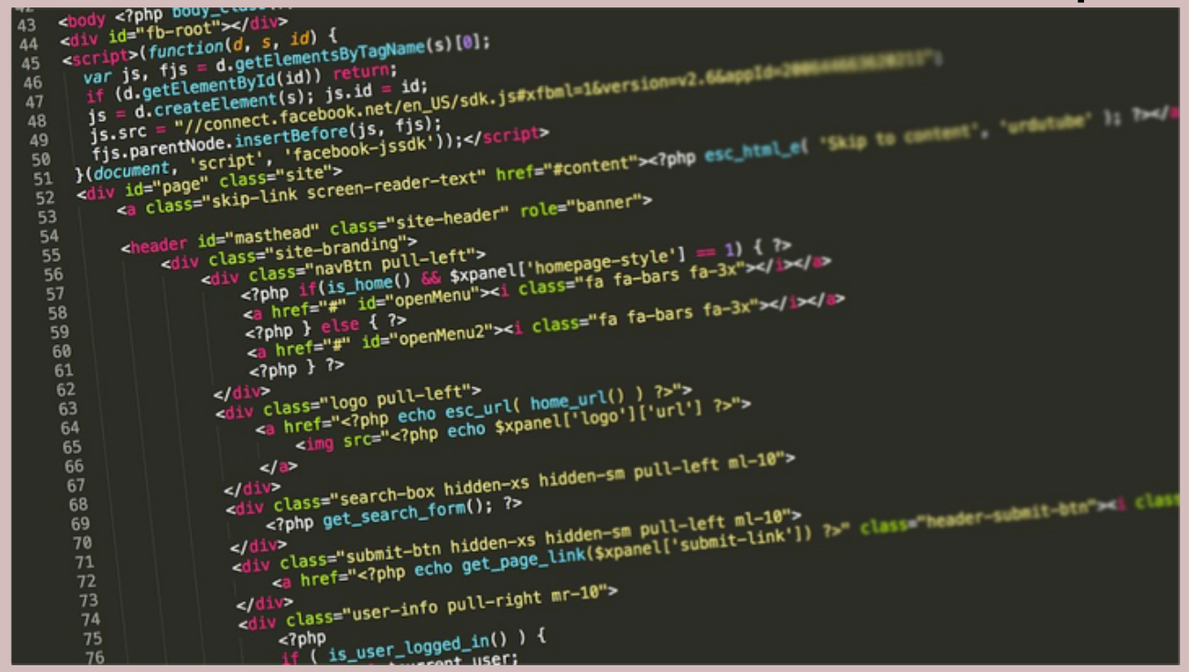
Over-the-Shoulder

- Agile development technique
- Developer who coded software explains it to another developer
- Lower cost than pair programming since it occurs at intervals instead of having a constant review

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Pass-Around

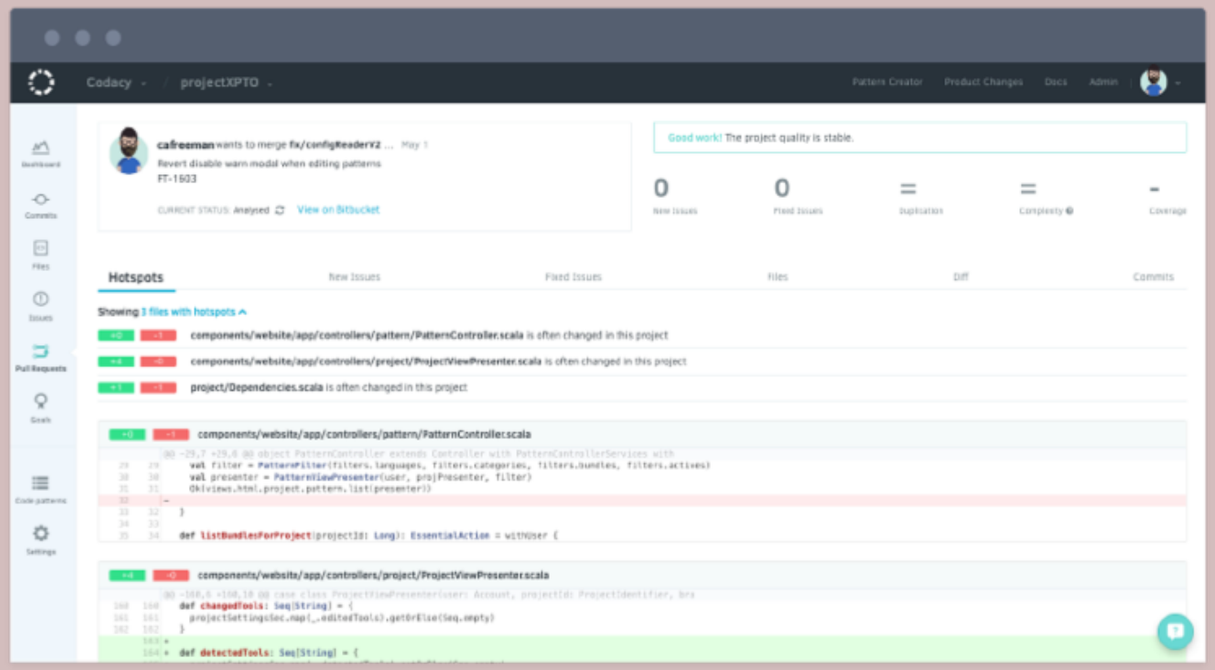
- Form of review with one or more reviewers
- Code is emailed or shared for review
- Code documentation is much more important



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Tool-Assisted

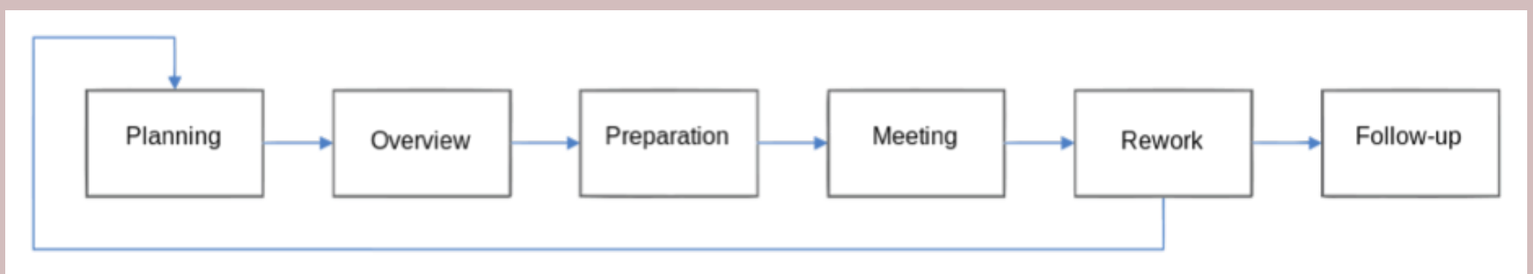
- Formal or informal software-based tools conduct code reviews
- Specialized software allows the reviewers to mark up the code, provide feedback, and more



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Fagan

- Structured formal code review by a team of reviewers
- Specifies entry/exit criteria for each process
- More costly and harder to implement than other types of code reviews



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Finding Security Flaws

Security Architecture & Tool Sets

Finding Security Flaws

- Coding flaws are always going to occur
  - Programming and syntax errors
  - Business logic and process errors
  - Error handling
  - Incorrect integration with other services

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Static Analysis

- Conducted by reviewing the code manually or with an automated tool
- Code is not run during static analysis
- Form of white-box testing

Dynamic Analysis

- Code is executed while providing specific input
- Uses automated tools or manual input
- Types
  - Fuzzing
  - Fault Injection
  - Mutation Testing
  - Stress Testing (Load Testing)
  - Security Regression Testing

Fuzzing

- Sends invalid or random data to an application to test ability to handle unexpected data
- Typically automated to use large datasets
- Used to detect input validation, logic issues, memory leaks, and error handling

Fault Injections

- Directly inserts faults into error handling parts of the code to test them

- Examples:
  - Compile-time injection
    - Injects faults by modifying source code before compiling
  - Protocol software injection
    - Uses fuzzing to send noncompliant data to a protocol
  - Runtime injection
    - Inserts data into running memory of the program or by sending in a fault to the program to deal with it

Mutation Testing

- Makes small changes to the program itself to determine they would cause a failure
- If they cause a failure then they are rejected
- Used to test if code is testing for possible issues with unexpected input types

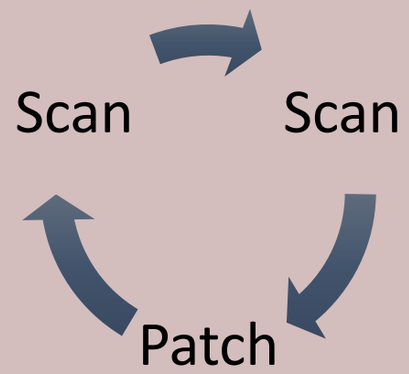
Stress Testing (Load Testing)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

- Ensures applications and systems can support the expected production load
- Uses automated tools to “stress” an expected load and determine if its handled properly
- Test for the worst-case scenario
- Can be conducted against entire system or just a single component

Security Regression Testing

- Ensures that any changes made do not create new problems or issues in the application
- Used most commonly when a new patch or update is added
- Verifies no new vulnerabilities or misconfigurations have been added



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Web App Vulnerability Scanning

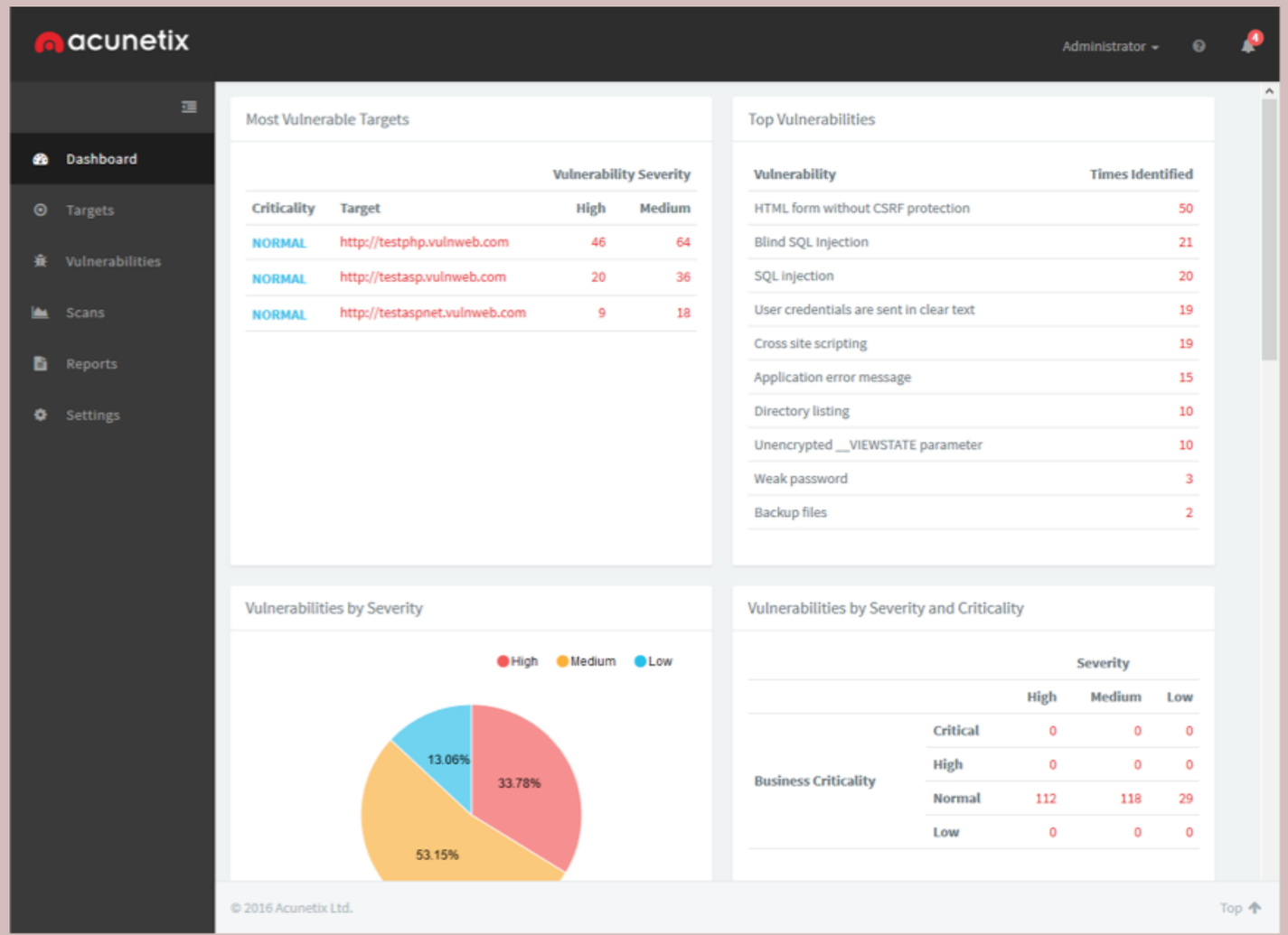
Security Architecture & Tool Sets

Web Application Vulnerability Scanning

- Dedicated web app vulnerability scanners do better than Nessus, Nexpose, and OpenVAS
- Identify problems with applications and the underlying web servers, databases, and infrastructure
- Examples
  - Acunetix WVS
  - Archni
  - Burp Suite
  - IBM's AppScan
  - HP's WebInspect
  - Netsparker
  - QualysGuard's Web Application Scanner
  - W3AF

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Acunetix



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Acunetix

SQL injection (verified)

Severity HIGH

Vulnerability description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This vulnerability affects **/listproducts.php**.

Discovered by: Scripting (Sql_Injection.script).

Attack details

URL encoded GET input **artist** was set to **(select 1 and row(1,1)>(select count(*),concat(concat(CHAR(52),CHAR(67),CHAR(117),CHAR(98),CHAR(52),CHAR(117),CHAR(78),CHAR(77),CHAR(72),CHAR(79),CHAR(55)),floor(rand()*2))x from (select 1 union select 2)a group by x limit 1))**
Injected pattern found:

```
4Cub4uNMHO7
```

- View HTTP headers
- View HTML response
- Launch the attack with HTTP Editor
- Retest alert(s)
- Mark this alert as a false positive

The impact of this vulnerability

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use subselects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

How to fix this vulnerability

Your script should filter metacharacters from user input.
Check detailed information for more information about fixing this vulnerability.

Detailed information

- Click here for more detailed information about this vulnerability

Web references

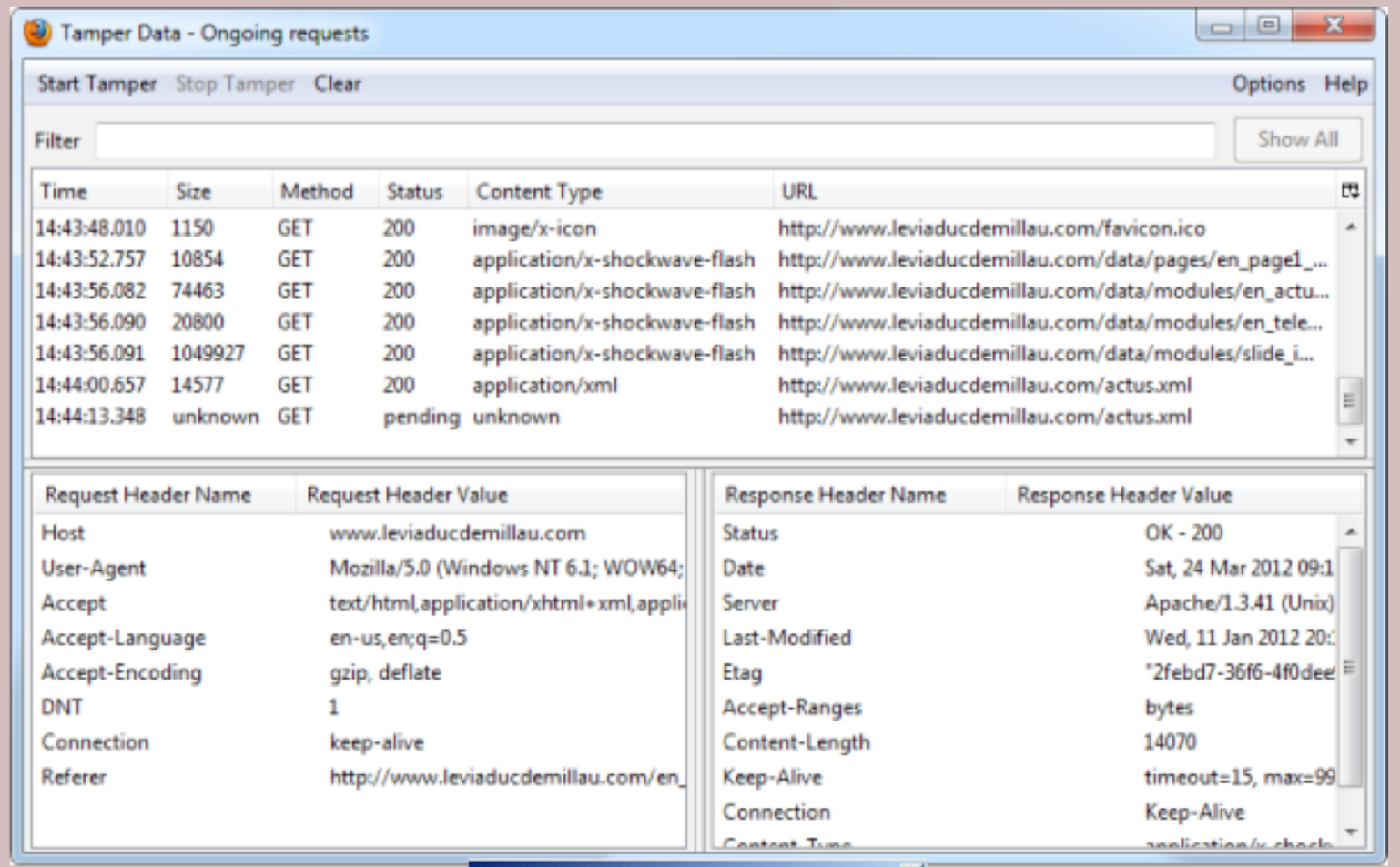
- Acunetix SQL Injection Attack
- Advanced SQL Injection
- Security Focus - Penetration Testing for Web Applications (Part Two)
- More Advanced SQL Injection

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Manual Scanning

- Uses and interception proxy to capture communications between browser and server
- Testers can modify data sent and received
- Examples
  - Tamper Data for Firefox and Chrome
  - HttpFox
  - Fiddler
  - Burp Suite

Tamper Data

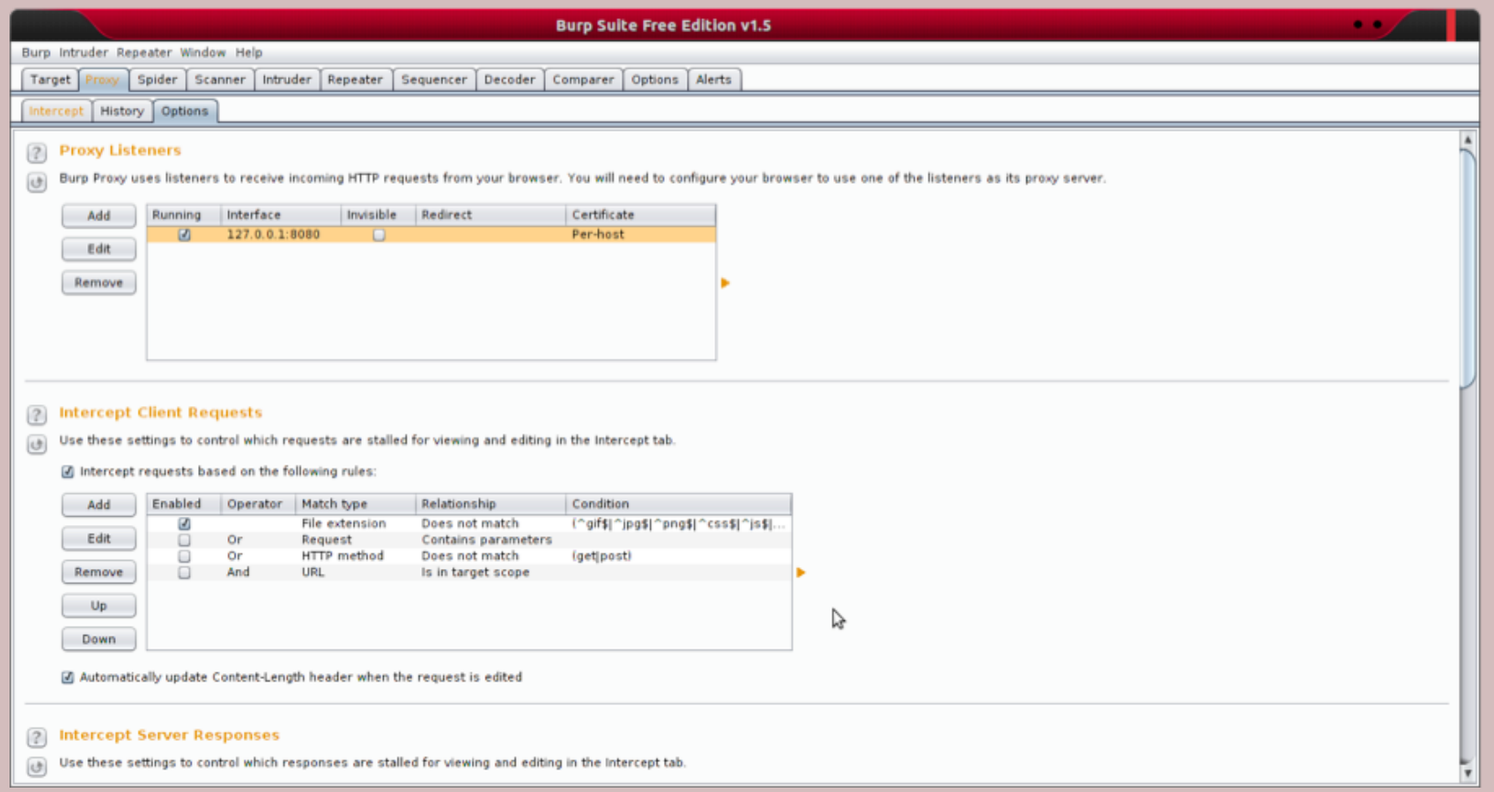


JASON DION

TRAINING THE CYBER SECURITY WORKFORCE

Burp Suite

- Automated and Manual modes



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Outsource Your Scanning

- Even the best vulnerability scanners will miss business logic issues and other flaws
- Outsourcing to a security firm can identify issues that a web application scanner can't
- These firms can provide both static and dynamic analysis of your applications