Network Services Security

Module 12

Introduction

- Having secured the platform's OS in Module 11, it is necessary to address services
- Services were touched on generically, but like OS security there are unique considerations when focusing on a service and its specific implementation.
  - E.g. Web services provided by Apache

Focus

- Tens of services exist
- Focus will be on services mentioned in Module 8
  - DNS
  - Mail
  - Interactive Session Services
  - File Services
  - Web Services

Securing Services

- Protocols and implementation conventions help shape the nature of a service's security
- However, security objectives, functional requirements, configuration, features and vulnerabilities of specific services software govern the actionable details

Approach

- Services applications evolve over time
  - Features come and go, but some are stable
  - Vulnerabilities come and go, but some persist
- Services applications will be chosen
  - E.g. Apache, Sendmail, OpenSSH
- Discussion will avoid being version specific
  - Handouts will address version sensitive details

DNS Service Security

- DNS security is in part addressed by:
  - Architectural design, e.g. “split DNS”
  - Server placement within an IT environment
  - Addressing colocation with other accessible services on same server
  - Service configuration on each server
  - Patching vulnerabilities and running current versions
  - Utilizing authentication, integrity and confidentiality services where and when possible

Threats to DNS

- Provider vs Consumer
  - As a provider of DNS you need to be concerned about
    - Availability – service is accessible
    - Integrity – records are consistent with your intentions
    - Confidentiality – DNS is inherently an unauthenticated publishing mechanism, but there is the idea of “too much” sharing
    - Assurance – The DNS service does not put its host and environment at avoidable risk

Threats to DNS

- As a consumer of DNS you need to be concerned about:
  - Availability – can users access needed local and Internet records
  - Integrity – can users trust the results they are receiving
  - Assurance – are servers or user systems vulnerable to malformed replies

Threats to DNS

- DNS servers are interesting
  - The platform hosts both a DNS provider and a DNS consumer
    - They are subject to both provider and consumer oriented threats

Threats to DNS

- Typosquatting - registering a domain name very similar to a popular domain name (E.g. iastate.edu , iastade.edu, iastate.com)
  - Mistyped email addresses may result in secrets being revealed
  - Receiving mail from a bogus domain is common in phishing, spear phishing

Threats to DNS

- DDoS – Distributed Denial of Service
  - Overloading a domain's name servers with requests
    - Consequence: Users unfamiliar with the actual IP addresses of the systems of interest are unable to connect to those systems even though they are operating properly
- DNS Amplification Attack
  - Publicly available DNS server responds to recursive queries
  - Attacker spoofs source IP of DNS request. Spoofed IP address is of the victim of large unrequested DNS responses originating from open recursive DNS server

Threats to DNS

- Registrar Hijacking
  - Your account with the DNS registrar is compromised allowing the attacker to manage you domain's registration
    - Domain can be moved to another registrar
    - Registered name servers can be changed
      - World will recognize other servers as legitimate
- Compromising the host through exploiting a vulnerability within name server software.

Threats to DNS

- Cache Poisoning
  - DNS caches are temporary storage locations holding frequently used records
    - Localizing popular records speeds up name resolution and reduces the burden on authoritative servers
  - Attackers inject false records into the cache exploiting poor configuration choices or vulnerabilities
    - This attack combined with a good impersonation of the legitimate service will fool many users

Threats to DNS

- ID Guessing and Query Prediction
  - Fooling DNS resolver to accept bogus query results as legitimate via fabricated replies
- Name Chaining
  - A type of cache poisoning
  - Response messages crafted by attacker introduce arbitrary DNS names and provides further information claimed to be relevant to those names

Threats to DNS

- Unauthorized Zone Transfers
  - Zone transfers are used between Primary and Secondary name servers in order for the Secondary name servers to have current zone information
  - A zone transfer gives an attacker a view into all the hosts within the zone reducing their information disadvantage.
  - Zone transfer restrictions must be enabled

Threats to DNS

- Illegitimate zone information in zone transfers
  - Secondary server trusts the primary is providing legitimate information
  - Digital signatures on the zone information allows secondary to verify legitimacy
- Dynamic DNS misuse
  - Dynamic DNS allows the automation of record management
  - The use of DHCP makes hostname to address assignment challenging to maintain
  - Disable DDNS or restrict service to only legitimate sources

Threats to DNS

- Denial of Domain Names
  - Resource records are stripped out of query responses

DNS Configuration Best Practices

- BIND
  - Run BIND in a chroot environment
  - Separate the roles of caching server and authoritative server
  - Prevent recursive queries on external nameservers
  - Prevent recursive queries on authoritative servers
    - Limits the server's to exposure to malformed responses

- Permit recursive queries on caching servers, but do not allow them to serve zones
  - Limit users to only internal users
- Configure forwarders on internal authoritative servers to direct recursive queries to designated caching servers
  - Set conditional forwarding for internal zones not served by a particular authoritative server
    - Prevents an internal query from leaving the environment
      - Split DNS will cause confusion if the query is answered by Internet facing name servers

- BIND 9 supports a feature called “views”
  - Different data is provided to clients based on source IP of the requestor
    - Denying the requestor an answer is a valid option
- Restrict Dynamic DNS (DDNS) to only DHCP servers and require TSIG authentication
  - DDNS enables automated record updating
  - DDNS can be used to inject fake information

Configuration Best Practices

- Prevent DNS Open Resolver configurations
  - Do not provide recursive query support for external users
- Prevent clients from abusing the Resource Record Time To Live in the cache of the DNS
  - Short: Fast-Flux – rapidly distributing addresses to malicious hosts by informing cache servers not to store records very long
  - Long: Promotes long lasting cache poisoning by reducing the purge time for the poised record
  - Modify BIND name server configuration to have a max-cache-ttl
  - Manage the maximum size of the cache
- Segregate Authoritative and Recursive servers
  - Same as not allowing cache and authoritative services to coexist on the same server
- Limit the Zone Transfer servers;
  - Require secondary servers to authenticate with TSIGs
- Restrict the administrator access to the system (including IP and access method)
- Deploy out-of-band management;
- Lock down the underlying operational system (OS)

Internet Mail Service Security

- Email security is in part addressed by:
  - Architectural design
  - Server placement within an IT environment
  - Addressing colocation with other accessible services on same server
  - Service configuration on each server
  - Patching vulnerabilities and running current versions
  - Utilizing authentication, integrity and confidentiality services where and when possible

Threats to Internet Mail

- Eavesdropping
- Traffic Analysis
- Spam
- Modification or Destruction
- Malware – Virus, worm and malicious payloads
- Denial of Service – Email bombs
- Phishing/Spear Phishing
- Impersonation
- Hoaxes
- Repudiation – Denial of: origination, submission, receipt

Threats to Internet Mail

- Exploiting open relays
  - Popular with spammers
  - Also enables reflection attacks
  - Open relay is an MTA that allows Internet users to request the MTA deliver mail on their behalf to destinations beyond the domain in which it resides or it services
    - Uses MTA owner's resources
    - Embarrasses MTA owner for enabling spammers
    - Hides spammers by allowing open relay to be the first server to route the spam

Threats to Internet Mail

- Maliciously redirected mail routing
  - Vulnerability:
    - DNS MX record integrity compromise
    - Lack of DNS record integrity and authenticity checking
  - Consequence:
    - Mail sent to a malicious MTA that either reads and forwards or reads and stops routing
- Subject line information leakage
  - Even with encrypted mail messages, subject line is commonly left readable
  - User puts sensitive information in the subject line

Threats to Internet Mail

- Using SMTP to access vulnerabilities in MTA
  - E.g. Buffer overflow as a gateway to host OS
- Use of SMTP commands for information gathering
  - E.g. VRFY, EXPN, VERB
- Email as a mechanism for data leakage
  - Technically, an environmental threat
  - Automated or manual email composition and sending from within the trusted network

Threats to Internet Mail

- Information Leakage via Error Messages
  - Guess and verify valid user names via error responses
    - Useful for phishing and possibly credential compromise
  - Probe polices and mail architecture by sending messages designed to invoke an error response
    - Useful for mapping the environment behind the firewall

Threats to Internet Mail

- Signed message replay
  - Resending a signed message to unintended recipients intact.
    - Objectives – Spam, reputation damage of sender
- Detection False Positives
  - Anti-spam, anti-virus and other controls improperly categorize legitimate mail as bad.

Interactive Session Services Security

- Interactive session services security is in part addressed by:
  - Architectural design
  - Server placement within an IT environment
  - Addressing colocation with other accessible services on same server
  - Service configuration on each server
  - Patching vulnerabilities and running current versions
  - Utilizing authentication, integrity and confidentiality services where and when possible

Interactive Session Services Security

- Architecturally these services are comparatively simple, however:
  - Sophisticated authentication or centralized user management may complicate things a bit
  - Sequential chaining of interactive sessions complicates things as well
- Basically, the service resides on every host you wish to manage remotely over a network

Interactive Session Services Security

- These services are a convenience in many cases as opposed to being an absolute necessity
  - Some systems may require strictly physical console access only
    - The network may be too dangerous
    - The information contained is highly sensitive
  - Possible compromise, establish a “management” network difficult to enter without physical access
    - Hosts are remote manageable but only from a network that requires controlled physical access
    - Typically this means a second NIC dedicated to the management network and related services only listening on the second NIC

Generic Threats to Interactive Session Services

- Eavesdropping
- Traffic Analysis
- Modification or Destruction
- In-band access to vulnerabilities of service software
- Denial of Service
- Impersonation
- Session Replay
- Session Hijacking
- Man-in-the-middle

Interactive Session Services Security

- Telnet, rlogin, Virtual Network Computing (VNC), and X are insecure session services
  - They will not be discussed.
  - VPNs and SSH are some methods to improve the overall security of these types of connections
- SSH and Remote Desktop Protocol/Remote Desktop Console (RDP/RDC) are the focus

Threats to SSH

- Environmental threat resulting from SSH
  - Persistent attackers use SSH for their communications within the victim's environment
    - Legitimate use of SSH masks or interferes with detection of the attacker’s communications
- Account compromise due to reliance on weak passwords
  - Allowing root to login via SSH exposes this well known account to brute force attacks

Threats to SSH

- Threats to TCP will disrupt SSH sessions
- Attacker can determine source and destination, volume of data transferred and timing (i.e. traffic analysis)
- Carelessness
  - Host authentication messages can be ignored at the user's peril
  - Weak passphrase protecting SSH private key

Threats to SSH

- Advanced attacker inside environment impersonates an authorized user
  - Poor key management practices may allow:
    - Multiple copies of the same user private key to exist
      - Passphrases may be weak or non-existent
    - SSH accounts and related keys persist after people move on
      - Lack of discipline results in lack of visibility into where keys are located
      - People moving on may take a copy of the keys with them

Threats to SSH

- Malware spread between servers enabled by poor key management
  - Malware can take advantage of pervasive trust between servers established by keys located on so many systems
  - Machine-to-machine communication is a very common use for SSH

Threats to RDP

- Credential theft via malware
  - User RDP credentials can be stole by malware, allowing criminal to impersonate
- Remote password guessing enabled if too many guesses are permitted
  - Allowing RDP across the perimeter allows the attacker to be offsite.
- Without Network Level Authentication, RDP is subject to man-in-the-middle attacks
  - Requires server certificate and client to at least warn if authentication fails
  - Certificate needs to be issued by a trusted CA to avoid client side confusion

File Services Security

- File services security is in part addressed by:
  - Architectural design
  - Server placement within an IT environment
  - Addressing colocation with other accessible services on same server
  - Service configuration on each server
  - Patching vulnerabilities and running current versions
  - Utilizing authentication, integrity and confidentiality services where and when possible

Generic Threats to File Services

- Eavesdropping
- Traffic Analysis
- Modification or Destruction
- In-band access to vulnerabilities of service software
- Denial of Service
- Impersonation
- Session Replay
- Session Hijacking
- Man-in-the-middle
- Malware distribution vector
- Exfiltration/ Data Leakage

File Services Security

- Transient file services
  - FTP
  - SFTP
  - HTTP
- Long-term file services
  - NFS
  - Windows File Services

File Services Security

- FTP and HTTP
  - Nearly open to nearly every generic file-services threat
  - Security services are needed if there are concerns regarding:
    - Confidentiality
    - Integrity
    - Availability

File Services Security

- SFTP, a service under the SSH protocol suite, is a secure substitute for FTP
- HTTPS = HTTP + SSL is the common secure substitute for HTTP
  - Secure Hypertext Transfer Protocol (S-HTTP) was never widely adopted
  - SSL provides an encrypted as well as:
    - Server side authentication services
    - Client side authentication services (optional)

Threats to SFTP

- Attacker can exploit previously mentioned SSH key management issues
- Attacker can access plaintext scripts or configuration files used for automated file transfer
  - Script and configuration files may be exposed by web server or whichever host the file resides
    - E.g. sftp-config.json is fairly common file

Threats to HTTPS

- Attackers can implement man-in-the-middle attacks if users ignore SSL certificate warnings
  - Worse is if attacker is successful in getting certificates issued in the name of a target site
    - SSL server authentication will succeed
- Web page design may expose content to non-SSL transmission (i.e. mixed content)
  - Session cookies in the clear are subject to "sidejacking"
  - By only protecting the user authentication process with SSL, session cookie gets exposed on subsequent pages

Threats to HTTPS

- Widgetjacking – Social media widgets (e.g. Facebook, Linkedin, Twitter) may have access to session cookies and other sensitive content and leak over clear connections
- Sophisticated protocol manipulations can gradually determine content of SSL communications (i.e. timing attack)
  - Paterson and Alfardan – Feb. 2013

Threats from HTTPS

- Inappropriate content bypassing content filters due to encryption
  - This is a bidirectional issue.
    - Unable to prevent access to inappropriate remote content including malware
    - Unable to prevent release of information from within environment

File Services Security

- NFS has been historically an insecure protocol and NFSv2 and NFSv3 are still used.
  - NFSv4 addresses many threats
- Windows file sharing or SMB/CIFS has security features like Kerberos based authentication and share ACLs

Issues with NFSv2 & v3

- Service has no communications security
  - No encryption
  - User authentication is entrusted to client host
- Supports file sharing over UDP and TCP
  - Historically sharing relied on UDP
    - Easier to spoof
- Not designed to be used by client hosts outside the trusted network
- NFS is historically an RPC (remote procedure call) based protocol requiring a *portmapper* service
  - Client seeking NFS service contacts the server's portmapper to direct it to the correct TCP or UDP port

Threats to NFSv2 & v3

- If directory is exported with no access list configured, any system on the network is capable of accessing the directory's contents
- An improperly scoped export may expose too much of the host's file system.
- If a directory is exported with root access to a set of identified clients, anyone with superuser privileges on one of the clients can modify exported files owned by root
- Impersonation of NFS users is possible, so long as impersonating user has the same User ID on local system
  - Local system superuser rights makes this very easy
- Designated client hosts can be impersonated by another host using the same IP address
  - Easier to achieve if client host is turned off regularly
  - Use of DNS names in ACL can be exploited by manipulating DNS

Threats to NFS

- Guessing file handles allows remote access to exported files

Threats to Windows File Services

- Microsoft SMB Protocol underlies Windows file sharing
  - Common Internet File System (CIFS) is considered to be a dialect of SMB
- Windows clients support at least six different dialects of Microsoft SMB Protocol
  - First dialect came out around the early 90's
  - Dialects are negotiated between client and server

Threats to Windows File Services

- Protocol security has improved over time
  - A successful negotiation to use an older dialect of SMB may bypass security controls
- Protocol supports two authentication schemes for shares
  - Share-level – a single password shared by all users is sufficient
  - User-level – user credentials are used consisting of a user name and an authenticator (usually a password)
    - Specific user and group ACLs are supported

Threats to Windows File Services

- Over the wire, encrypted challenge-response messages are exchanged
  - A challenge string is issued to the client
  - The client using the password and challenge compute a new string that can be verified by server
  - Both NTLM and LAN Manager encryption are supported
    - LAN Manager was replaced by Windows NT 3.1 around 1994

Threats to Windows File Services

- CIFS supports cryptographic based authentication via Kerberos
  - But no authentication exchange must use Kerberos by default
- Authentication is from client to server
  - Non-Kerberos authentication has no means to protect password from man-in-the-middle
    - Server does not authenticate to client like in SSL or SSH

Threats to Windows File Services

- Password authenticators used by users are subject to brute force
  - Failed authentication tracking and limits are needed

WWW Service Security

- Multifaceted problem
  - Communications security - HTTPS
  - “Data at rest” security – DB security, platform security
  - Service side security
    - Service platform as the target
    - Data as the target
    - Service enables web attack on a different target
  - Client side security

WWW Service Security

- Focus will be on:
  - Service side security
  - ~~Strictly on Web server~~
    - ~~Common commercial web application architecture includes an application server and database server~~

Open Web Application Security Project (OWASP)

- Non-profit organization
- Vendor neutral
- Provide a Top 10 list of vulnerabilities every 3 years
  - List is ranked based on:
    - Prevalence of the vulnerability
    - Estimates of exploitability, detectability and impact
- There are many other issues beyond these 10

OWASP Top 10 - 2013

- A1 – Injection
- A2 – Broken Authentication and Session Management
- A3 – Cross-Site Scripting (XSS)
- A4 – Insecure Direct Object References
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A7 – Missing Function Level Access Control
- A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using Known Vulnerable Components
- A10 – Unvalidated Redirects and Forwards

Vulnerability Explanation

- A1. Injection
  - Commands or data queries submitted by the client should be considered untrusted. Vulnerable logic that processes submitted commands or queries are prone to being tricked to execute unauthorized commands or provide more data than authorized by the user.
    - Common types: SQL injection, OS injection, LDAP injection

Vulnerability Explanation

- A2. Broken Authentication and Session Management
  - Flaws in authentication and session management allow attackers to compromise things like passwords, cryptographic keys, or session tokens. The attacker is able to assume the identity of the true user.

Vulnerability explanation

- A3. Cross-Site Scripting (XSS)
  - Service flaw allows untrusted data to be sent to the client browser without prior validation or data envelopment (rendering any possible executable instructions inert).
  - Consequences of this vulnerability include:
    - session hijacking,
    - web site defacement,
    - directing unsuspecting users to a malicious site for possibly additional attacks

Vulnerability Explanation

- A4. Insecure Direct Object References
  - Objects such as files, directories and database keys are given references or handles within the executing software
  - These references provide linkage between the software logic and the objects.
  - Reference use is not access controlled. Access control kicked in prior to the reference being provided.
  - Software flaws expose these handles allowing attackers unauthorized access to the objects.

Vulnerability Explanation

- A5. Security Misconfiguration
  - Flaw is essentially poor security management practices
  - Services component like development frameworks, application server, web server, database server and their relevant platforms need to be securely configured and deployed
  - Persistent monitoring and maintenance are needed to ensure service components are and remain securely configured
  - Software components should be kept up to date.

Vulnerability Explanation

- A6. Sensitive Data Exposure
  - A broad vulnerability category
  - Services flaws that allow attackers access to sensitive data (e.g. credit cards, tax IDs, auth. credentials)
    - Controls on sensitive data are inadequate
    - Primarily a design and service-management flaw as opposed to software or configuration vulnerability

Vulnerability Explanation

- A7 Missing Function Level Access Control
  - Flaw commonly relates to inadequate protection of service functionality
  - One flaw is to perform access control solely by controlling the functions available on the user interface (UI)
    - Rationale is that if a user is able to request the function then it must be okay because the UI enabled them
    - There is a lack of consideration that an attacker may not use the UI as intended thus bypassing access control
  - In general, function usage authorization should be verified at time of use

Vulnerability Explanation

- A8. Cross-Site Request Forgery (CSRF)
  - Service is vulnerable to “identity piggybacking”
  - While the user has an active session, the attacker exploits the user’s browser to send HTTP requests on behalf of the attacker with the credentials of the user.
    - Service is unable to differentiate the origin of the request and thinks it is servicing the legitimate user.

Vulnerability Explanation

- A9. Using Components with Known Vulnerabilities
  - Flaw is essentially poor security management practices
  - Some number of service components such as libraries, development frameworks, server software, platform are allowed to operate despite their vulnerabilities
    - Short term: Patches and version migration take time to adopt
    - Long term: The lack of adoption is likely due to lack of development and configuration discipline
    - Legacy applications are a possible factor. Legacy applications typically have limited development support needed to accommodate changes in its dependencies (e.g. OS) that result from new versions of supporting software and their patches.
  - Accessible vulnerabilities undermine all other controls in place
    - Outcomes of vulnerability exploitation are wide ranging, like:
      - Platform compromise
      - Loss of data confidentiality
      - Loss of data availability
      - Loss of data integrity

Vulnerability Explanation

- A10. Unvalidated Redirects and Forwards
  - Using untrusted data to determine the destination page of a redirect or forward
    - Server-based redirect is a directive configured on server that informs web server to substitute one page for another
      - Substitute page does not need to be on same server
      - Attack Value – Direct users to a malicious site or compromised page
    - Forwards are essentially redirects but destination page is another page local to the server
      - Attack Value: Bypass access control to access a page normally requiring greater privilege by getting approval to access a lower privileged page

Risk Analysis - REMOVE

- Terminology
  - Asset – An owned resource, product, process, information, system that is valued
  - Threat – The occurrence of an event that will cause an undesirable impact on an asset(s)
  - Vulnerability – A flaw or shortcoming of the asset or its safeguards that provides a means for the asset to be negatively impacted

Threats that OWASP Top 10 Enable

- Unauthorized access to data
  - A1. Injection
  - A2. Broken Authentication and Session Management
  - A3. Cross-Site Scripting (XSS)
  - A4. Insecure Direct Object References
  - A5. Security Misconfiguration
  - A6. Sensitive Data Exposure
  - A7. Missing Function Level Access Control
  - A8. Cross-Site Request Forgery (CSRF)
  - A9. Using Components with Known Vulnerabilities
  - A10. Unvalidated Redirects and Forwards

Threats that OWASP Top 10 Enable

- Compromising the service platform
  - A2. Broken Authentication and Session Management
  - A3. Cross-Site Scripting (XSS)
  - A4. Insecure Direct Object References
  - A5. Security Misconfiguration
  - A6. Sensitive Data Exposure
  - A7. Missing Function Level Access Control
  - A9. Using Components with Known Vulnerabilities
  - A10. Unvalidated Redirects and Forwards

Threats that OWASP Top 10 Enable

- Indirect compromise of a target via the insecure service
  - A3. Cross-Site Scripting (XSS)
  - A5. Security Misconfiguration
  - A7. Missing Function Level Access Control
  - A9. Using Components with Known Vulnerabilities
  - A10. Unvalidated Redirects and Forwards