Daniel Willard
CS 433 Network Security
29FEB2024

Textbook, Chapter 6 Exercises, (3 points each.)

16) A 32-bit IP addressing scheme affords approximately 4 billion addresses. Compare this number to the world's population. Every additional bit doubles the number of potential addresses. Although 32 bits is becoming too small, 128 bits seems excessive, even allowing for significant growth. But not all bits have to be dedicated to specifying an address. Cite a security use for a few bits in an address.

- Traffic Filtering and Access Control Lists: This allows network administrators to filter traffic based on various criteria such as source or destination IP address, protocol, and port numbers. This enables fine-grained control over network access, helping to prevent unauthorized access, block malicious traffic, and enforce security policies.
- Geolocation and Geo-blocking: Assigning bits in the IP address for geolocation purposes enables organizations to implement geo-blocking strategies to restrict access to certain services or content based on the geographic location of users.
- Virtual Private Network Identification: Incorporating bits in the IP address to identify VPN connections can facilitate secure remote access to corporate networks. VPN-specific bits can indicate whether traffic originates from a trusted VPN client, allowing network devices to apply appropriate encryption, authentication, and access controls to ensure the confidentiality and integrity of data transmitted over the VPN.
- Intrusion Detection and Prevention Systems: Utilizing bits in the IP address for tagging packets with intrusion detection and prevention information enables IDPS devices to efficiently analyze network traffic for signs of suspicious or malicious activity. By embedding relevant metadata within the IP address, IDPS systems can quickly identify and respond to potential security threats, helping to safeguard network assets and data.

17) When a new domain is created, for example, yourdomain.com, a table in the .com domain has to receive an entry for yourdomain. What security attack might someone try against the registrar of .com (the administrator of the .com table) during the creation of yourdomain.com

- DNS hijacking or DNS cache poisoning attack:
In a DNS hijacking attack, an attacker aims to gain unauthorized access to the DNS records of a domain, such as "yourdomain.com", by compromising the registrar's systems or exploiting vulnerabilities in the DNS infrastructure. By doing so, the attacker can manipulate the DNS records associated with "yourdomain.com" and redirect traffic intended for that domain to malicious servers controlled by the attacker.
- They could attempt to intercept communication between the registrar and the authoritative DNS servers responsible for the .com domain zone. Through various means such as DNS spoofing, phishing attacks, or exploiting vulnerabilities in the registrar's infrastructure, the attacker could modify the DNS records for "yourdomain.com" before they are officially registered.

25) How can a website distinguish between lack of capacity and a DoS attack? For example, websites often experience a tremendous increase in volume of traffic right after an advertisement displaying the site's URL is shown on television during a popular broadcast. How can a site administrator determine when high traffic is reasonable?

- Monitoring Traffic Patterns: Sudden and sustained spikes in traffic that are abnormal compared to historical data may suggest the presence of an attack.
- Analyzing Traffic Sources: DDoS traffic often originates from a limited number of IP addresses or exhibits characteristics such as identical user-agents or abnormal request patterns.
- Behavioral Analysis: By analyzing request rates, request payloads, and session behavior, administrators can detect anomalous patterns associated with DDoS attacks.
- Application Layer Monitoring: Monitoring the performance and responsiveness of web applications can provide insights into whether the increase in traffic is overwhelming the server's capacity or is a result of malicious activity. Legitimate traffic following an advertisement may result in increased but manageable server load, whereas DDoS attacks often lead to degradation or unavailability of services due to resource exhaustion.
- Implementing DDoS Mitigation Solutions: These solutions use a combination of traffic analysis, rate limiting, IP reputation filtering, and behavioral analysis techniques to distinguish between legitimate and malicious traffic and mitigate the effects of DDoS attacks without disrupting legitimate user access.

27) A DDoS attack requires zombies running on numerous machines to perform part of the attack simultaneously. If you were a system administrator looking for zombies on your network, what would you look for?

- Unusual Network Traffic Patterns: DDoS zombies typically generate high volumes of outbound traffic as they participate in the attack.
- Abnormal Behavior of Networked Devices: Look for signs of abnormal behavior or performance degradation in networked devices, such as increased CPU or memory utilization, unusually high network activity, or unexplained crashes or reboots.
- Anomalous DNS Queries: Unusual DNS query patterns may indicate the presence of DDoS zombies attempting to contact their command-and-control servers.
- Endpoint Security Alerts: Look for indicators of malware infections, such as the presence of known DDoS botnet malware or unusual network communications, and investigate any alerts or anomalies detected by endpoint security tools.
- Analyze Firewall and Intrusion Detection System logs: Review firewall and IDS logs for indications of suspicious traffic patterns, such as repeated connection attempts or SYN floods targeting specific IP addresses or network segments.
- Behavioral Analysis: Use anomaly detection algorithms to identify patterns of behavior that are inconsistent with typical network activity, such as sudden spikes in traffic volume or unusual communication patterns between internal hosts and external destinations.

34) Can link and end-to-end encryption both be used on the same communication? What would be the advantage of that? Cite a situation in which both forms of encryption might be desirable.

- Yes, link-layer encryption and end-to-end encryption can be used together in the same communication. Link-layer encryption typically encrypts data at the network interface level, while end-to-end encryption encrypts data at the application layer, ensuring that data remains encrypted throughout its entire journey from the source to the destination.
- The advantage of using both forms of encryption is enhanced security and privacy protection. Link-layer encryption protects data as it traverses the network infrastructure, preventing unauthorized access or interception by malicious actors within the network. End-to-end encryption ensures that data remains encrypted even if it passes through intermediary nodes or is stored on intermediate servers, providing robust protection against eavesdropping and unauthorized access throughout the communication path.

38) What is the security purpose for the sequence number field of an IPsec packet?

- The sequence number field in an IPsec packet serves a crucial security purpose: it helps prevent replay attacks.
- The sequence number field in the IPsec packet header ensures the integrity and freshness of transmitted data by assigning a unique sequence number to each packet. This sequence number is incremented for each packet sent, providing a monotonically increasing value that allows the recipient to detect and reject duplicate or out-of-order packets.

40) What information might a stateful inspection capability of a firewall want to examine from multiple packets?

- Source and Destination IP Addresses
- Source and Destination Ports
- Sequence and Acknowledgment Numbers
- TCP Flags: Analyzing TCP flags, such as SYN, ACK, FIN, and RST, allows the firewall to identify the state of TCP connections (e.g., connection establishment, data transfer, connection termination) and enforce security policies accordingly.
- Connection State: The firewall maintains information about the state of active connections, including whether a connection is in the process of being established, established, or terminated.
- Session Timeout Information
- Application Layer Data: HTTP headers or DNS queries, to enforce application-specific security policies and detect suspicious or malicious activity.

8. In the SSL protocol we discussed in class, Bob presents his certificate to Alice, but Alice does not present her certificate to Bob. Enhance the SSL protocol so that Alice presents her certificate to Bob as well. Draw the new diagram to illustrate how the enhanced SSL works, and explain what this enhancement achieves. (5 points)

```
-   Alice                               BOB
  (Client)                            (Server)
     |                                       |
     |         ClientHello                   |
     |------------------------------------------>|
     |                                       |
     |          ServerHello                  |
     |<------------------------------------------|
     |         Certificate                   |
     |<------------------------------------------|
     |    ClientKeyExchange                  |
     |------------------------------------------>|
     |        CertificateRequest             |
     |<------------------------------------------|
     |          Certificate                  |
     |------------------------------------------>|
     |        ServerKeyExchange        |       |
     |<------------------------------------------|
     |       CertificateVerify               |
     |------------------------------------------>|
     |              Finished                 |
     |------------------------------------------>|
     |       CertificateVerify               |
     |<------------------------------------------|
     |              Finished                 |
     |<------------------------------------------|
```

- Mutual Authentication: By requiring both Alice and Bob to present their certificates during the handshake, the enhanced SSL protocol achieves mutual authentication. Alice verifies Bob's identity by validating his certificate, and Bob verifies Alice's identity by validating her certificate. This ensures that both parties can trust the identity of the other before proceeding with the secure communication.
- Increased Security: Mutual authentication strengthens the security of the communication channel by mitigating the risk of impersonation attacks and unauthorized access. It prevents malicious entities from masquerading as either Alice or Bob and provides assurance that only authenticated parties can participate in the communication.
- Enhanced Trust: Mutual authentication enhances trust between Alice and Bob. By independently verifying each other's identities using digital certificates signed by trusted Certificate Authorities

9. Worm detection can be either signature-based or anomalous-behavior-based. List three reasons/scenarios when anomalous-behavior-based worm detection is preferred. (3 points)

- Zero-day Worms: Anomalous-behavior-based detection is effective for identifying zero-day worms, which are malicious software that exploits vulnerabilities for which no patch or signature exists. Since zero-day worms exploit unknown vulnerabilities, signature-based detection systems may fail to detect them.
- Polymorphic Worms: Polymorphic worms are malicious software that continuously change their code or behavior to evade detection by signature-based antivirus or intrusion detection systems. Signature-based detection relies on predefined patterns or signatures to identify threats, making it ineffective against polymorphic worms that mutate to avoid detection.
- Stealthy Worms: Some worms are designed to spread stealthily and avoid detection by traditional security mechanisms. These worms may exhibit subtle or low-volume behavior that does not trigger alarms in signature-based systems. Anomalous-behavior-based detection can detect stealthy worms by analyzing deviations from baseline network behavior.
-

10. One often deploys layered encryption to secure a routing protocol. For example, a routing update originated from router A to B and then to C before reaching the last hop X will be protected as follows:
update when leaving A: {A, sig_by_A}
update when leaving B: {B, {A, sig_by_A}, sig_by_B}
update when leaving C: {C, {B, {A, sig_by_A}, sig_by_B}, sig_by_C}

(1) Explain how B, C, and X will verify the integrity of the update. (3 points)

- Router B:
Verify the signature (sig_by_B) attached to the update when it received it from router A.
Once verified, router B removes the signature (sig_by_B) and the router identifier (B) from the update.
Verify the signature (sig_by_A) attached to the inner update. This verifies that the update originated from router A and has not been tampered with since it left router A.
- Router C:
Verify the signature (sig_by_C) attached to the update when it received it from router B.
Once verified, router C removes the signature (sig_by_C) and the router identifier (C) from the update.
Verify the signature (sig_by_B) attached to the inner update. This verifies that the update originated from router A through router B and has not been tampered with since it left router B.
- Router X:
Verify the signature (sig_by_X) attached to the update when it received it from router C.
Once verified, router X removes the signature (sig_by_X) and the router identifier (X) from the update.
Verify the signature (sig_by_C) attached to the inner update. This verifies that the update originated from router A through routers B and C and has not been tampered with since it left router C

(2) There is actually a vulnerability with this design; for example, C could replace {B, {A, sig_by_A}, sig_by_B} with {A, sig_by_A}, thus literally removing B from the path. How would you fix this vulnerability? (4 points)

- To fix the vulnerability where router C could replace the inner update with {A, sig_by_A}, thus removing router B from the path, one possible solution is to include the identity of the next-hop router in each layer of encryption. This ensures that each router along the path can verify the identity of the router that forwarded the update to them.
- Update leaving A: {A, sig_by_A}
  Update leaving B: {B, {A, sig_by_A, B}, sig_by_B}
  Update leaving C: {C, {B, {A, sig_by_A, B}, sig_by_B, C}, sig_by_C}
- With this modification, router C cannot remove the inner update from router B without invalidating the outer signature from router B. Router C must forward the entire update from router B, including the inner update with router B's identity, to maintain the integrity of the update along the path.

11. Discuss how you would protect a DNS client from receiving a spoofed DNS response from a malicious attacker, instead of an authentic response from a legitimate DNS server. (4 points)

- Domain Name System Security Extensions: DNSSEC is a suite of security extensions that adds cryptographic integrity and authentication to DNS responses.
- DNS Response Rate Limiting: DNS Response Rate Limiting is a technique used to mitigate DNS amplification attacks and reduce the impact of DNS reflection attacks.
- DNS Query ID Randomization: DNS query ID randomization involves randomizing the query ID field in DNS queries sent by DNS clients. By using random query IDs, DNS clients make it more difficult for attackers to predict and spoof valid DNS responses.
- DNS Response Validation: DNS clients can perform additional validation checks on DNS responses to detect and prevent spoofed responses. DNS clients can compare the source IP address of DNS responses with the IP addresses of known legitimate DNS servers. DNS clients can also verify the consistency of DNS responses across multiple authoritative DNS servers to detect discrepancies or anomalies that may indicate DNS spoofing attacks.
- Use of Secure DNS Resolvers: DNS clients can use secure DNS resolvers that implement additional security features to protect against DNS-based attacks. Secure DNS resolvers may utilize DNS filtering, anomaly detection, and threat intelligence to identify and block malicious DNS traffic. DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) are encrypted DNS protocols that provide confidentiality and integrity protection for DNS queries and responses, reducing the risk of eavesdropping and tampering by attackers.

sources outside of the book:
https://www.csoonline.com/article/569685/dnssec-explained-why-you-might-want-to-implement-it-on-your-domain.html