True & False

2015:

1. True False Kerberos authentication protocol requires clock synchronization for the client to authenticate with the server.
2. True False Secure BGP would protect against some control plane routing attacks.
3. True False IPSec in Authentication Header (AH) mode provides confidentiality of IP packets.
4. True False SSL/TLS uses X509 certificates to provide replay attack protection.
5. True False DNSSEC provides integrity of domain name to IP resolutions.
6. True False An anomaly based IDS can detect previously unknown attacks

2016:

1. **True False** Secure BGP routing would protect again attacks at the data plane level, such as dropping IP packets.
2. **True False** With properly validated, unforged certificates, HTTPS security guarantees of confidentiality, integrity, and authentication hold even if DNS has been compromised.
3. **True False** Stateless packet-filter firewalls are able to reconstruct fragmented IP packets to make filtering decisions.
4. **True False** IPSec provides source IP address authentication.
5. **True False** 802.11i provides confidentiality for the source and destination hardware MAC address of data packets.

2017:

1. **True False** Stateless firewalls are able to perform Deep Packet Inspection (DPI) and detect and block attacks attempting to exploit application vulnerabilities.
2. **True False** TLS provides protection against replay attacks by including fresh random numbers in the handshake.
3. **True False** HTTPS protects against eavesdropping attacks from both a passive and active network attacker.
4. **True False** Signature based IDS are able to detect previously unknown attacks.
5. **True False** Cross-Site Request Forgery (CSRF) attacks are mitigated by the browser's Same Origin Policy (SOP).

Authentication:

2015

1) **Authentication (50 points)**

a) What is the current Certificate Authority (CA) trust model for HTTPS in terms of the domain names that CAs included in the browser can validly sign certificates for? (15 Points)

Any CA that is trusted by a browser can sign a valid certificate for any domain name.

b) How does this Certificate Authority (CA) trust model differ from DNSSEC in terms of the scope of domain names that registrars can validly sign? (20 points)

For DNSSEC the '.' root CAs can sign valid domain name resolutions for any domain, but CAs lower down in the DNS hierarchy can only sign valid resolutions for domain names below them in the DNS naming hierarchy. This limits their scope of trust unlike HTTPS.

c) What is two-factor authentication and what are the advantages of using this in place of password authentication? (15 Points)

Two-factor authentication requires a user to validate his identity using two different form of authentication: Something you have, Something you know, Somewhere you are, or Something you are(biometrics). If a user is required to produce a password and an RFID tag then an attacker will need to know his password and have access to or be able to clone the tag. Two-factor authentication prevents an attacker from successfully authenticating unless they can compromise both types of authentication. Password authentications should be paired with another factor because they are susceptible to eavesdropping, insecure storage, and possibility of a successful guess.

2016:

Secure Network Protocols (30 points)

a） At a high level a Public Key Infrastructure (PKI) and Certificate Authority (CA) are required to enable establishment of trust (i.e. authentication). Describe the PKI frameworks for DNSSEC and HTTPS and who the root Certificate Authorities are and what their scope of trust is (i.e. what domain names can they sign certificates for?) in DNSSEC and HTTPS? [**20 points**]

For DNSSEC the PKI is a hieratically scoped naming structure where ICANN the root CA can sign a valid DNS record for any domain name. ICANN then signs the CA keys for Top Level Domain (TLD) registrars, such as Verisign that manages the .com TLD. This CA key for Verisign is only valid for signing domains beneath .com. Verisign then will sign CA keys for the owner of a .com domain that are only valid for that domain and subdomains. In the case of HTTPS each browser includes a set of CA keys that are valid for signing certificates for any domain name. This means that any trusted CA can sign domains globally.

b） Describe one technique used by secure protocols, such as TSL and IPSec, to protect against replay attacks and one technique used to protect against man-in-the-middle attackers. [**10 points**]

In order to protect again replay attacks a protocol must include some form of freshness, such as a random nonce, sequence number, or time stamp. To protect against man-in-the middle attacks the protocol must provide some form of authentication, integrity, and optionally confidentiality if that is required for the protocol.

DNS:

An interesting feature of DNS is that a 60-byte UDP query to a (recursive) DNS server can result in a 512-byte UDP response or even—in the case of the EDNS(DNSSEC) extension—a 4000-byte UDP response to the source IP address.

a. Can you think of a way to abuse this feature in order to stage denial of service attacks? **[10 points]**

The most straight forward way for an attacker to mount a DoS attack is by spoofing DNS resolution request messages for a domain that is known to reply with a larger DNSSEC resolution where the IP address is spoofed to that of the intended victim. The DNS server will then reply with with the larger DNSSEC resolution with the destination IP address of the intended victim allowing the attacker to amplify the amount for bandwidth consumed.

b. How would you redesign the DNS request-response protocol to prevent this particular attack? What are the trade-offs in terms of usability and performance of the redesign? **[15 points]**

There are several ways to redesign DNS to mitigate DoS attacks. The first would be to add an additional challenge message sent in reply to a DNS resolution request that included a cookie. The requestor would then have to reply with the correct cookie value before the actual large reply would be sent. This would add an extra round trip time to the DNS resolution process and consume additional bandwidth in the none spoofed case. The other defense might be to rate limit the number of responses sent to a single IP address. This would not completely mitigate the problem since the attacker could make uses of more DNS resolvers to compensate. It also might cause legitimate DNS resolution requests to be suppressed due to rate limiting.

c. Which of the security properties of authentication, availability, confidentiality, and integrity does DNSSEC provide for signed DNS to IP address records? [**10 points**]

DNSSEC provides authentication and integrity to DNS to IP address resolution records.

Routing:

a) Describe how BGP IP address prefixing attacks are currently detected. [15 points]

Currently BGP as deployed does not have any formal security model. It is secured by ad-hoc trust between BGP routers, which results in accepting all, some, or none of the routes advertised by a peer BGP router. There are collective, such as the BGP looking glass, that share BGP route announcements that are seen by their routers. This data can be analyzed to detect anomalous routes. However, these anomalies must be manually investigated since there is a chance for false positives.

b) Describe what would be required to provide secure IP address origin authentication in BGP routing. [10 points]

The core requirement for secure IP address origin authentication would be an authoritative database of IP address prefix ownership.

c) Describe an extension to BGP routing assuming secure IP address origin authentication is deployed that could validate the authenticity and integrity of every hop of a BGP routing announcement to mitigate hop deletion attacks. [15 points]

If this authoritative database of IP address prefix ownership existed it could also include public keys for each IP address prefix owner. Then every BGP route advertisement could be signed using a secure MAC based on asemestric cryptography (i.e., RSA, DSA, Elliptical Curves) that would provide authentication and integrity. Assuming all BGP route announcements were signed, then peer BGP routers could verify the information using the public key from the database.

Firewall：

2015

2) Firewall (50 points)

Louis Reasoner has just discovered a new firewall program called Ipchairs, but he is so excited about Ipchairs' simple rule format that he neglects to read the entire manual. He installs the following rules on his firewall:

No Action Prot. Source Destination Source port Destination port
1 ACCEPT TCP 0.0.0.0/0 129.174.1.10/32 * 22
2 ACCEPT TCP 0.0.0.0/0 129.174.1.10/32 * 80
3 ACCEPT ALL 0.0.0.0/0 129.174.1.10/32 * 53
4 DENY ALL * 192.0.0.1 * 1:2000
5 ALLOW ALL * 192.0.0.1 * *

Louis' machine is 129.174.1.10. He wants ssh (TCP 22), web (TCP 80), and DNS (TCP/UDP 53) services running on his machine to be accessible to everybody, all other ports below 2000 blocked, and he doesn't care about ports above 2000. Later that day, Louis notices incoming traffic to port 135 is not being blocked.

(a) What was Louis' mistake? Show how he can fix his rules. (30 Points)

Louis set to destination to 192.0.0.1 instead of 129.174.1.10, change these two rules to fix it.

4 DENY ALL * 129.174.1.10 * 1:2000

5 ALLOW ALL * 129.174.1.10 * *

(b) How should Louis modify his rules if he installs a print daemon that only listens on port 7701? The print daemon should only be accessible to others on his local network, 129.174.1.0/24, and to his friend Max, whose computer is at 128.59.15.63. (20 Points)

1 ACCEPT TCP 0.0.0.0/0 129.174.1.10/32 * 22
2 ACCEPT TCP 0.0.0.0/0 129.174.1.10/32 * 80
3 ACCEPT ALL 0.0.0.0/0 129.174.1.10/32 * 53
4 ACCEPT TCP 129.174.1.0/24 129.174.1.10 * 7701
5 ACCEPT TCP 128.59.15.63 129.174.1.10 * 7701
6 DENY ALL * 129.174.1.10 * 1:2000
7 ALLOW ALL * 129.174.1.10 * *

IDS:

2015:

a) Wolf Security released an intrusion detection system that can detect Syn floods and SQL injection attacks. The boast a low false positive rate and high accuracy rate, rates are in the following table:

How connection is classified

Type of connection	Syn flood	SQL Injection	Normal
Syn flood	85%	5%	10%
SQL Injection	5%	90%	5%
Normal	5%	5%	90%

For example, when the IDS observes a Syn flood, it correctly classifies it as a Syn flood with probability 85%, misclassifies it as an SQL Injection attack with probability 5%, and misclassifies it as a normal connection with probability 10%.

For the purposes of this problem, assume that Syn floods are 3% of all connections, and that SQL Injection attacks are 1% of all connections, while 96% of traffic consists of normal connections.

Also assume that a connection cannot be both a Syn flood and an SQL injection attack at the same time.

When the IDS announces that it detected a Syn flood, what is the probability that the connection is, in fact, normal? Give your calculations. (40 points)

P(normal | Syn flood) = (P(Syn flood | normal) * P(normal)) / P(Syn flood) =

(P(Syn flood | normal) * P(normal))/ (P(Syn flood | normal) * P(normal) + P(Syn flood | SYN flood) * P(SYN flood) + P(Syn flood | SQL Injection) * P(SQL Injection))

(.05 * .96) / (.05 * .96 + .85 * .03 + .05 * .01) = .6486 =

65% chance that the traffic is normal.

b) Explain how an anomaly based IDS functions and what trade-off is makes in terms of false positive rates and detection of unknown attacks compared to a signature-based IDS. (10 points)

Any anomaly-based IDS uses a supervised statistical model based on network traffic features to determine what is normal and what is anomalous. This tends to result in higher false positive rates compared to signature-based IDSs. It also enables anomaly-based IDSs to detect previously unknown attacks that a signature-based IDS can't detect.

2016:

a) Wolf Security released an intrusion detection system that can detect Syn floods and SQL injection attacks. They boast a low false positive rate and high accuracy rate, rates are in the following table:

How connection is classified

Type of connection	Syn flood	SQL Injection	Normal
Syn flood	90%	5%	5%
SQL Injection	5%	90%	5%
Normal	5%	0%	95%

For example, when the IDS observes a Syn flood, it correctly classifies it as a Syn flood with probability 90%, misclassifies it as an SQL Injection attack with probability 5%, and misclassifies it as a normal connection with probability 5%.
For the purposes of this problem, assume that Syn floods are 1% of all connections, and that SQL Injection attacks are 4% of all connections, while 95% of traffic consists of normal connections.
Also assume that a connection cannot be both a Syn flood and an SQL injection attack at the same time
When the IDS announces that it detected a Syn flood, what is the probability that the connection is, in fact, normal? Give your calculations. [**25 points**]
(.05*.95)/((.05*.95)+(.04*.05)+(.01*.90)) = 0.811965 81.2%

b) Define what a false positive and false negative is in the context of an IDS and one reason why each is costly for operators of these systems. [**10 points**]

A false positive is when an event that is benign is detected as an alert and a false negative is then malicious activity is classified as benign. The cost of false positives is the resources required to investigate alerts that are actually benign. The cost of false negatives is that an attack might occur without being detected.

2017:
Wolf Security released an intrusion detection system that can detect Syn floods and SQL injection attacks. They boast a low false positive rate and high accuracy rate, rates are in the following table:

How connection is classified

Type of connection	Syn flood	SQL Injection	Normal
Syn flood	91%	4%	5%
SQL Injection	5%	90%	5%
Normal	5%	0%	95%

For example, when the IDS observes a Syn flood, it correctly classifies it as a Syn flood with probability 91%, misclassifies it as an SQL Injection attack with probability 4%, and misclassifies it as a normal connection with probability 5%.
For the purposes of this problem, assume that Syn floods are 1% of all connections, and that SQL Injection attacks are 4% of all connections, while 95% of traffic consists of normal connections.
Also assume that a connection cannot be both a Syn flood and an SQL injection attack at the same time.
When the IDS announces that it detected a Syn flood, what is the probability that the connection is, in fact, normal? Give your calculations. [**25 points**]
Describe how anomaly based IDS systems function and why this enables them to detect previously unknown attacks. [**10 points**]
Anomaly based system are built using a supervised statistical model that can differentiate between normal and anomalous behavior. Since unknown attacks might be classified as anomalous it might be able to detect them.