Final Exam

Network Security

Instructor: Shiuhpyng Shieh Dec. 13, 2022

You are required to write your answers in the sequential order. Failing to comply with this requirement will be subject to 5-point penalty. Your answer to a question must be brief and concise.

1. (20%) The supplicant (station) derives PTK by using the following equation. PTK=PRF(PMK, "Pairwise key expansion", min(AP-Addr, STA-Addr) || max(AP-Addr, STA-Addr) || min(Anonce, Snonce) || max (Anonce, Snonce), 384), where PTK consists of KEK, KCK, TK. (A) Describe all terms and their functions in the equation, including PTK, PRF, PMK, AP-Addr, STA-Addr, Anonce, Snonce. (B) How does the supplicant get PMK, Anonce, Snonce?

2. (20%) Some electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction, PGP provides the service of converting the raw 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is called radix-64 conversion. (A) In this conversion, how many octets of binary data is mapped into four ASCII characters? Explain the conversion mapping. (B) What's the percentage of size expansion for using Radix-64? (C) DNSSEC is the extension of DNS. Take ".org" as an example. In the DNS hierarchy, "root" is the top-level domain of the hierarchy and ".org" is the sub-domain of root. Where is the key of ".org" stored, at "root" or ".org"? (D) Where are the hash value and signature of ".org" key stored in the DNS hierarchy, at ".org" or root"?

3. (20%) Security association (SA) is uniquely identified by three parameters: Security Parameter Index, security protocol identifier, and IP destination address. Each SA of the security association database has a sequence number counter, and anti-replay window. The fixed window size is W and the largest packet number in the window is N. How does the receiver handle the incoming packet with packet number M if
(A) $N-W < M < N+1$
(B) $N < M$,
(C) $M < N-W+1$

4. (20%) There are two approaches to intrusion detection: anomaly detection and rule-based detection. (A) Elaborate these two approaches. (B) Are they able to handle unknown attacks?

5. (20%) Describe the following four types of firewalls: packet filtering firewall, stateful inspection firewalls, application proxy firewall, and circuit-level firewall. (B) Among the four types, which type of firewalls may use SOCKS?