3

NETWORK SECURITY

Last Name:

First Name:

# Directions

**You must do all Test Your Understanding questions in bold**.

To answer a questions, place your cursor at the end of its line and hit Enter.

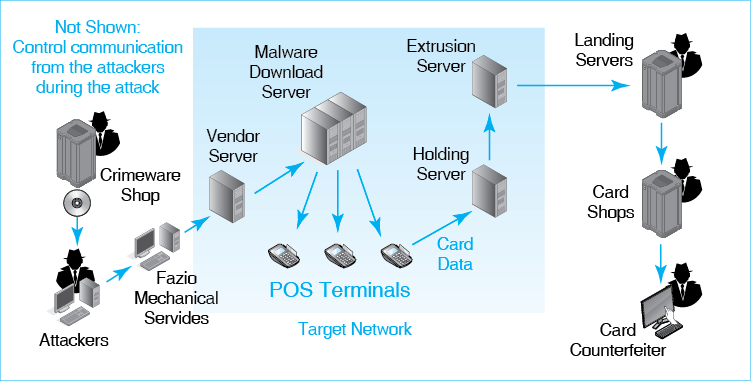
You are responsible for other Test Your Understanding questions on tests, unless they care ~~crossed out~~.

Do all End-of-Chapter questions unless they are crossed out.

# The Target Breach

## The POS Attack

Figure 3-: The Target Breach



Test Your Understanding

1. a) List the steps taken by the attackers.

**b) How did the attackers gain access to Target’s network**?

c) List the internal Target servers the attackers compromised.

d) How did the attackers exfiltrate the card data?

e) **List the criminal groups, besides the main attackers, who were involved in the overall process**.

f) What benefit did the attackers seek to obtain from their actions?

g) **Critique (positively or negatively) the fact that Target knew that fraud was already occurring with the stolen card data but did not reveal this when it announced the breach**.

## Damages

Test Your Understanding

2. a) How was Target damaged by the breach?

**b) Were banks and credit card bureaus damaged by the breach**?

**c) How were consumers damaged by the breach**?

**d) How were retailers damaged by the breach**?

e) What can retailers do to defend themselves against counterfeit credit cards?

f) **What individual victim or group of individual victims suffered the most harm**?

# Introduction

Test Your Understanding

3. How does security thinking differ from network thinking?

# TYPES OF ATTACKS

## Malware Attacks

4. a) What is malware?

**b) What are the most frequent attacks on companies**?

## **Vulnerabilities and Patches**

5. a) What is a vulnerability?

b) How can users eliminate vulnerabilities in their programs?

**c) What name do we give to attacks that occur before a patch is available**?

## Social Engineering: No Vulnerability Necessary

5a. **a) What kind of attack may succeed against a system with no technological vulnerabilities**?

**b) What is the goal of social engineering**?

c) What is a phishing attack?

d) Distinguish between phishing and spear phishing attacks.

## Types of Malware

6. a) How do viruses and worms differ?

b) How do viruses and worms propagate using social engineering?

**c) What other propagation method do some worms use**?

d**)** **Why is it especially dangerous**?

e) What are Trojan horses?

**f) How do Trojan horses propagate to computers**?

## Payloads

7. a) What are payloads?

b) What is spyware?

**c) What is the difference between the two types of spyware mentioned in the text**?

d) What is ransomware?

e) **Discuss your choices are if you are hit by ransomware.**

f) Distinguish between credit card number theft and identity theft.

**g) Which is more harmful to the victim? Why**?

## Human Break-Ins (Hacking)

8. **a) What is the definition of hacking**?

**b) If you see a username and password on a Post-It note on a monitor, is it hacking if you use this information to log in? Explain in terms of the definition**.

**c) You discover that you can get into other e-mail accounts after you have logged in under your account. You spend just a few minutes looking at another user’s mail. Is that hacking? Explain in terms of the definition**.

**d) If you click on a link expecting to go to a legitimate website but are directed to a website that contains information you are not authorized to see. Is that hacking? Explain in terms of the definition**.

## Denial-of-Service (DoS) Attacks

9. **a) What is the purpose of a denial-of-service attack**?

b) Which programs directly attack the victim in a distributed denial-of-service attack?

c**) What is a collection of compromised computers called**?

d) What is the person who controls them called?

**e) To what computer does the attacker send messages directly**?

f) Explain the steps of a distributed DoS attack.

## Advanced Persistent Threats (APTs)

10. a) **Explain “advanced” in the term *advanced persistent threat***.

**b) Explain “persistent” in the context of APTs**.

c) How do adversaries often enter the system and then expand to other parts of it?

d) Who mounts APTs today?

# TYPES OF ATTACKERS

## Cybercriminals

11. a**) What type of adversary are most hackers today**?

**b) Why is this type of attacker extremely dangerous**?

**c) What resources can they purchase and sell over the Internet**?

## Employees, Ex-Employees, and Other Insiders

12. **a) Why may employees attack**?

**b) For what four reasons are employees especially dangerous**?

**c) Who are the most dangerous employees**?

d) Why may ex-employees attack?

e**) What should be done when an employee leaves the firm**?

f) Why are contractor firms more dangerous than other outside firms?

## Cyberterrorists and National Governments

13. a) What are cyberterror and cyberwar attacks?

b**) Why are cyberwar attacks especially dangerous**?

# PROTECTING DIALOGUES CRYPTOGRAPHY

## Encryption for Confidentiality

14. **a) What is a cipher**?

**b) What protection does confidentiality provide**?

c**) What is the minimum size for encryption keys to be considered strong in most encryption ciphers**?

## Electronic Signatures: Message Authentication and Integrity

15. **a) What two protections do electronic signatures provide**?

**b) What three protections are typically given to each packet**?

## Host-to-Host Virtual Private Networks (VPNs)

16. **a) Distinguish between private networks and virtual private networks**.

**b) Why is SSL/TLS attractive for VPNs to connect browsers to webserver**?

# OTHER FORMS OF AUTHENTICATION

## Terminology and Concepts

17. a) What is authentication?

b) Distinguish between the supplicant and the verifier.

c) What are credentials?

d) Who is the true party?

e) What is the specific goal of authentication?

**f) Is the supplicant the true party or is the supplicant an impostor**?

**g) Why must authentication be appropriate for risks to an asset**?

## Reusable Passwords

18. a**) Why are passwords widely used**?

**b) What three types of passwords are susceptible to dictionary attacks**?

**c) Can a password that can be broken by a dictionary attack be adequately strong if it is very long**?

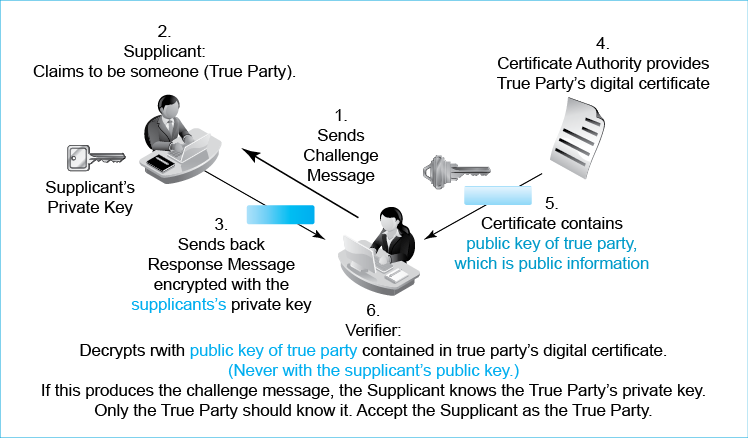
d) What types of passwords can be broken only by brute-force attacks?

**e) What are the two characteristics of passwords that are safe from even brute-force attacks**?

**f) Why is it undesirable to use reusable passwords for anything but the least sensitive assets**?

## Other Forms of Authentication

Figure 3-: Digital Certificate Authentication



19. a) How do you authenticate yourself with an access card?

b) **What is biometrics**?

c) **Why may fingerprint recognition be acceptable for user authentication to a laptop**?

d) Why is iris recognition desirable?

e) Why is face recognition controversial?

20. **a) In digital certificate authentication, what does the supplicant do**?

**b) What does the verifier do**?

**c) Does the verifier decrypt with the true party’s public key or the supplicant’s public key? Why is this important**?

d) How does the verifier get the true party’s public key?

21. Why is two-factor authentication desirable?

# FIREWALLS

## Dropping and Logging Provable Attack Packets

22. a) What does a firewall do when a definite attack packet arrives?

**b) Does a firewall drop a packet if it probably is an attack packet**?

c) Why is it important to read firewall logs daily?

## Stateful Packet Inspection (SPI) Firewalls

23. **a) Why are stateful firewalls attractive**?

**b) What type of firewalls do most corporations use for their main border firewalls**?

c) What are the two states in connections for SPI firewalls?

d) Which state needs the most security protection?

e) Which state gets the most security?

f) What is the big limitation of stateful packet inspection firewall? Don’t just name it. Explain it.

## Next-Generation (Application Aware) Firewalls (NGFWs)

24. **a) Why are SPI firewalls limited in their ability to detect attack packets**?

b) How do NGFWs address this problem?

c) Give specific examples of how application information can be used to increase security.

d) Why are NGFWs expensive.?

## Intrusion Detection Systems

25. a) Do IDSs stop packets?

b) Why are they painful to use?

c) How do they offer a broader picture of the threat environment than NGFWs?

# Box: Antivirus Protection

26. **a) Distinguish between what firewalls look at and what antivirus programs look at**.

b) Are AV programs used to detect more than viruses? Explain.

c) Distinguish between signature detection and behavioral pattern detection.

**d) Why is signature detection not enough**?

# CONCLUSION

## END-OF-CHAPTER QUESTIONS

### Thought Questions

3-1. a) What form of authentication would you recommend for relatively unimportant resources? Justify your answer.

b) What form of authentication would you recommend for your most sensitive resources?

3-2. What is the promise of newer authentication systems?

3-3. In digital certificate authentication, the supplicant could impersonate the true party by doing the calculation with the true party’s private key. What prevents impostors from doing this?

3-4. What are the implications for digital certificate authentication if the true party’s private key is stolen?

3-5. a) If someone in your firm gives you their password and you log into their account, is this hacking? Go back to the definition.

b) If you think someone in your office is sending slanderous e-mail about you, is it hacking if you break into their e-mail account to see if this is true? Go back to the definition.

c) If you log into a server at your bank to test their security, is this hacking. Go back to the definition.

Harder Thought Questions (You May Not Get These, but Try)

3-6. When a sales clerk accepts a credit card payment, he or she should type the last four digits of the credit card into the terminal in order for the terminal to verify that the last four digits on the card are the same as on the magnetic stripe. How do you think sales clerks may enter the last four digits yet still make the crosscheck worthless?

3-7. Keys and passwords must be long. Yet most personal identification numbers (PINs) that you type when you use a debit card are only four or six characters long. Yet this is safe. Why?

Perspective Questions

3-8. What was the most surprising thing you learned in this chapter?

3-9. What was the most difficult part of this chapter for you?