Computer Security

2017 Exam 3 Review

Paul Krzyzanowski
Rutgers University
Spring 2017

Question 1

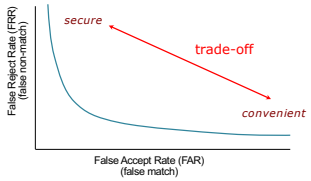
A high False Reject Rate (FRR):
(a) Makes the authentication process less secure.
(b) Makes the user experience more annoying.
(c) Indicates that security has been compromised.
(d) Indicates that the biometric is easy to forge..

(a) No – it's more secure

(b) YES!

(c) No

(d) No



Question 2

An advantage of biometric authentication over keys is that biometric data:
(a) Is more secure.
(b) Cannot be stolen.
(c) Cannot be shared.
(d) All of the above.

(a) It's less secure:
Fuzzy comparisons, possible multiple matches, no ability to hash
(b) Reconstruct a fingerprint from a photo; play a voice recording, …
(c) Cannot be shared legitimately
– requires replicating the biometric (effectively stealing)
– unlike passwords or cards, will not work well in supervised environments

I will accept (b) or (c)

Question 3

Which is an example of behavioral biometrics?
(a) Voice.
(b) Fingerprint.
(c) Iris.
(d) Hand geometry.

Behavioral biometrics – not an intrinsic part of the body

Includes voice, signature, keystrokes, gait analysis

- Not as precise but can be useful (e.g., CAPTCHA)

Question 4

Google's NOCAPTCHA reCAPTCHA *enhances* normal CAPTCHA by:
(a) Asking the user to solve a puzzle.
(b) Asking the user to recognize specific items in an image.
(c) Having the user recognize distorted characters.
(d) Measuring randomness in user actions.

CAPTCHA started started off with distorted text

Other versions, such as reCAPTCHA, had users text in images and identify images

Others tried Math CAPTCHA and puzzle pieces (Puzzle CAPTCHA)

NoCAPTCHA reCAPTCHA: uses behavioral analysis to identify a human – don't even present images.

Question 5

DHCP spoofing does not allow you to:
(a) Tell a system to use a different DNS server.
(b) Change the Ethernet MAC address of a system.
(c) Set the IP address of a computer.
(d) Redirect Internet-targeted traffic from a computer onto a specific system.

A DHCP server tells the system its:
IP address
network mask
gateway (router for addresses outside the local network)

It does not reconfigure the MAC address. That's a feature of each network transceiver and often cannot be changed.

Question 6

A CAM switch table overflow:
(a) Forces traffic to be sent to all ports of the switch.
(b) Causes all traffic to be dropped.
(c) Results in all traffic to unknown addresses to be dropped.
(d) Adds latency to frames since the output port needs to be resolved.

The switch table tells an ethernet switch what ports traffic should be directed to based on the destination ethernet address of a packet

If a packet with an unknown destination address is received, it is sent to all ports.

Question 7

A computer can grab network traffic from multiple VLANs by:
(a) Setting the host's Ethernet card to promiscuous mode.
(b) Initiating a CAM overflow attack.
(c) Sending spoofed ARP messages.
(d) Pretending to be a trunk-connected switch.

This is a VLAN Hopping attack

By pretending to be a trunked witch and speaking the VLAN trunking protocol (802.1Q), the computer can receive the entire stream of ethernet packets

Question 8

ARP cache poisoning can be used to:
(a) Modify the contents of IP packets.
(b) Change the IP address associated with a domain name.
(c) Redirect traffic that is targeted to a specific IP address.
(d) Redirect all traffic that originates from a specific system.

An ARP cache poisoning attack gives computers a false *IP address → MAC address* mapping

This allows a malicious host to get traffic that is destined to other systems.

Question 9

How are source addresses validated in IP packets?
(a) They are protected with an encrypted checksum.
(b) The packet contains a digital signature for the entire header.
(c) The sender can only use the IP address assigned to it as a source address.
(d) They aren't.

Question 10

SYN flooding attacks can be relieved by:
(a) Using random initial sequence numbers in a TCP handshake.
(b) Using an initial sequence number that can be derived a second time.
(c) Validating the source address at the start of a TCP handshake.
(d) Sending a cookie to the client for authentication.

(a) This makes TCP sequence number attacks difficult – throwing bogus data into a TCP stream

(b) Yes. Instead of a random number, use a SYN cookie =
f(client's IP address and port, Secret)
Don't allocate any state upon receiving the SYN message – no SYN queue

(c) No – there's no way to validate the source address

(d) The client does not authenticate the cooke

I will accept (b) or (d)

Question 11

BGP, the *Border Gateway Protocol*, can be used maliciously to:
(a) Assign incorrect IP addresses to hosts on a network.
(b) Impersonate hosts on the Internet.
(c) Block data traffic from entering another network.
(d) Inform routers of better routes.

BGP cannot change the contents of IP packets or block them.

It cannot impersonate hosts.

The protocol simply exchanges routing information among hosts

A malicious host, acting as a router, can give a connected router misleading information about its ability – or cost – to route to a set of IP addresses

Question 12

IPsec's Authentication Header (AH) protocol does not provide:
(a) Tunneling.
(b) Packet integrity.
(c) Payload encryption.
(d) Authentication.

AH simply ensures integrity

ESP – Encapsulating Security Protocol – is the IPsec protocol that provides integrity + encryption

Tunneling and authentication are done by both protocols

Question 13

Tunneling is a form of:
(a) Source address spoofing.
(b) Packet encapsulation.
(c) Message authentication.
(d) Payload encryption.

Question 14

TLS, *Transport Layer Security*, uses:
(a) Source address authentication.
(b) Encryption of the TCP header.
(c) Packet encapsulation.
(d) Hybrid cryptography.

(a) TLS doesn't care about the source or destination addresses

(b) TLS encrypts the payload, not TCP headers

(c) TLS does not encapsulate packets

(d) TLS uses public key cryptography to authenticate & exchange a key and symmetric cryptography to communicate.

Question 15

A screening router will not be able to:
(a) Accept external TCP packets targeted to an internal SMTP server (port 25).
(b) Drop all UDP DNS queries from internal hosts that are directed to other internal hosts.
(c) Drop packets entering from the external network that have an internal source address.
(d) Drop all incoming UDP packets.

A router does not get to filter packets within the network.

Question 16

Which systems belong in an organization's DMZ?
(a) General-purpose user computers.
(b) Payroll database.
(c) Web server.
(d) DHCP server.

The DMZ is a place for externally-facing services

(a), (b), (d) are internal systems

Question 17

A signature-based IDS (Intrusion Detection System) can block:
(a) A sudden increase in IP traffic to a server in Quebec.
(b) An improper sequence of SMTP requests.
(c) Zero-day attacks.
(d) Attempted root FTP logins.

(a) This requires statistical analysis, not pattern matching

(b) This requires maintaining the state of the protocol, not pattern matching

(c) This requires recognizing a never-before-seen bit pattern as an exploit

(d) This requires matching a string "user root"

Question 18

Snort is primarily:
(a) A signature-based IDS.
(b) An anomaly-based IDS.
(c) A protocol-based IPS.
(d) An application proxy.

(a) Snort matches patterns at the network, transport, & application layer

(b) Snort cannot detect anomalies – although some companion software tries to

(c) Snort is really bad at protocols – you can fake some if it by triggering additional rules but that's really unreliable

(d) Snort does not present a protocol interface to applications

Question 19

Which URL has the same origin as **http://www.poopybrain.com/419/exam**?
(a) http://www.poopybrain.com/news
(b) https://www.poopybrain.com/419/exam
(c) http://www.poopybrain.com:8080/419/exam
(d) http://poopybrain.com/419/exam

For two URLs to have the same origin, they must have the same:
1. Scheme (http/https)
2. domain
3. port

(b) Different scheme

(c) Different port

(d) Different domain name

Question 20

JavaScript code on a browser runs with the *authority* of:
(a) The ID of the user who is running the browser.
(b) The URL of the frame in which it was loaded.
(c) The URL of the outermost frame.
(d) The URL of the source of the JavaScript.

Question 21

Cross-Origin Resource Sharing (CORS) allows:
(a) Browsers to send messages to servers.
(b) Apps running in browsers on different systems to communicate.
(c) A web page to load content from multiple places.
(d) Multiple origins to be treated as one.

It's a way for the server to define hosts that should be considered as equivalent

Servers define the set of origins that are permitted to access information

Question 22

A way to keep a browser script *from inspecting a cookie* associated with the page's URL is to:
(a) Associate the script with a different origin.
(b) Mark it Secure.
(c) Mark it HttpOnly.
(d) Run the script in a separate frame.

(a) You can't explicitly set the origin of a script

(b) This just ensures the cookie goes over an HTTPS link

(c) YES – this disallows scripts from accessing the cookie

(d) Yes – BUT the frame has to have a different origin and the script may be useless since it won't be able to operate on elements in the page

Question 23

Cross-Site Resource Forgery (XSRF) *cannot* be prevented by:
(a) Adding unique state or unique per-request content to a URL.
(b) Having the server check where the request was referred from.
(c) Using HTTP POST requests.
(d) Using secure cookies.

XSRF: get a user's browser to issue a request to a web application that trusts the user (e.g., URL to add a video to your Netflix queue)

(a) Makes it impossible for the attacker to create a useful URL

(b) Ensures that the request came from a legitimate site (e.g., netflix.com)

(c) Parameters are sent in the body of the POST message, not in the URL

(d) This just uses HTTPS

Question 24

Clickjacking is an attack where:
(a) The attacker tricks the user into clicking on a link they did not intend to click.
(b) JavaScript simulates a click operation on a link.
(c) JavaScript intercepts and logs keystrokes.
(d) JavaScript disables the ability of a user to click anywhere on a page.

Clickjacking: get the user to click on one thing that's really another – e.g., a transparent overlay

Question 25

Persistent Cross-Site Scripting (XSS) attacks can be prevented by:
(a) Using secure cookies.
(b) Sanitizing all user-entered data.
(c) Using HTTPS instead of HTTP.
(d) Using HTTP PUT operations instead of HTTP GET.

Two types of XSS

Persistent: website stores user input and presents it to other users

Reflected: employs user input in HTML pages returned to the browser without validating them (e.g., user name)

(a) This just sends the cookies if HTTPS is used

(b) XSS is a problem only because user data becomes part of HTML

(c) That just makes the channel encrypted

(d) Useful for reflected XSS but not persistent

Question 26

Extended Validation (EV) certificates improve over Domain Validated (DV) ones because they:
(a) Work across multiple related domains.
(b) Are more secure since they use a 2048-bit key rather than a 1024-bit key.
(c) Use a more extensive process to validate the owner before issuing the certificate.
(d) Use a more rigorous authentication process when establishing a TLS connection.

The CA uses a more in-depth verification process prior to *issuing* the certificate

(a) No – a certificate identifies the owner – EV certificates do nothing different
- There are Universal Communication Certificates that encode multiple domain names

(b) No – the key length has nothing to do with it

(c) Yes

(d) No – the authentication process for connecting is no different

Question 27

Permission re-delegation is the vulnerability where an app:
(a) Is granted a default set of permissions without user involvement.
(b) Inherits a set of permissions from another app.
(c) Asks the user for permission to access a resource after it has been installed.
(d) Without a certain permission makes a request for the resource via another app.

Called the "confused deputy problem"

Privileged app is the deputy. Authority is given by the user's permission.

Violates the user's expectation of safety

A huge # of Android apps request permissions for sensitive resources and also expose public interfaces – they are at risk of permission re-delegation

Question 28

Apps in Android are *isolated* from each other by:
(a) Using address space layout randomization (ASLR) and stack canaries.
(b) Having the operating system run only one app at a time in most cases.
(c) Using the sandboxing capabilities of the Dalvik virtual machine.
(d) Running each app under a different user ID even through the system has only one user.

Android does not use sandboxing at the Dalvik layer like Java does with JVM

Question 29

A *masque attack* in iOS is:
(a) When a malicious app is installed and replaces a legitimate one because it has the same ID.
(b) When one app tries to access resources from another app without the user noticing.
(c) An attack where an app covertly installs other apps.
(d) A network attack that tries to find open ports on a remote system.

Doesn't work with App Store apps – need enterprise certificate

Question 30

ARM *TrustZone* enables:
(a) Prevention of buffer overflow attacks.
(b) The ability to tag a portion of a program as trusted while the rest of it is untrusted.
(c) Storage of keys in a way that even the operating system kernel cannot access them.
(d) Two trusted apps to communicate securely.

Question 31

Digital Video Broadcast (DVB) relies on:
(a) Pre-configuring each player with a common secret key that can decode encrypted video.
(b) Broadcasting a key that is encrypted separately for every single subscriber.
(c) Having a subscriber authenticate with the provider and download a decryption key.
(d) Encoding a set of keys within the video that is being broadcast.

(a) Each trusted player is preconfigured with a key – but it cannot decode video

(b) Yes – lots of encrypted keys are sent out, one per subscriber

(c) No – the subscriber does not contact the provider

(d) Keys are transmitted (b) but not encoded within the video

Question 32

Chaffing and winnowing is a cryptographic technique where multiple messages are sent:
(a) But only trusted parties can validate their signatures to determine which ones are legitimate.
(b) But only trusted parties can decrypt the contents of those messages.
(c) And some messages contain information about the validity of future messages.
(d) But only trusted parties know the pattern of which sequences of messages are valid.

Question 33

Steganography differs from *watermarking* because:
(a) Watermarking must be more robust.
(b) Steganography usually supports one-to-many communication while watermarking is one-to-one.
(c) Watermarks must be hidden while steganography can be visible.
(d) Steganography encrypts embedded content while watermarking does not.

The end