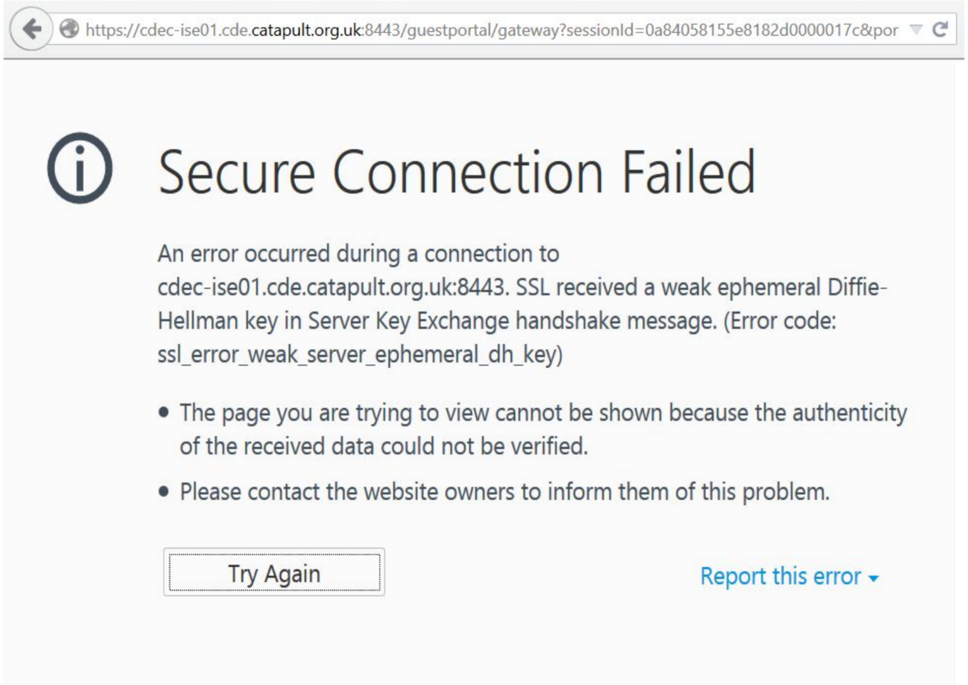
Computer Security Sample Exam Question

Kami Vaniea

August 13, 2024

Analyze a warning

When trying to open a website the instructor received the following warning in her web browser:



https://cdec-ise01.cde.catapult.org.uk:8443/guestportal/gateway?sessionId=0a84058155e8182d0000017c&por

Secure Connection Failed

An error occurred during a connection to cdec-ise01.cde.catapult.org.uk:8443. SSL received a weak ephemeral Diffie-Hellman key in Server Key Exchange handshake message. (Error code: ssl_error_weak_server_ephemeral_dh_key)

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

SSL/TLS supports several cryptographic algorithms and during the initial handshake the browser and the server negotiate which one they will use. Some of these algorithms are older and no longer considered to be secure by the cryptographic community. The warning above is telling the user that the remote server is only willing to use an older insecure protocol, so the browser has blocked the connection for the user's safety.

1. Think about the five properties of the definition of security. Name one property that would be violated if the user were to ignore the warning and view the page. Explain how the property would be violated.

Answer: *One point for naming the property, two points for the explanation. Authenticity is the most obvious as the warning explicitly mentions it. By using a weak key there is no guarantee that the user is communicating with the person/computer they expect to be communicating with. Without Authenticity a man-in-the-middle attack may be happening and there would be no way for the user to know.*

2. Suppose that Alice got the warning above when connecting to a National Health Service (NHS) for the UK website. She is concerned about other people learning about her private health information. For each of the following, would engaging in the described activity protect Alice's information from interception by a third party? Explain why or why not.

   (a) Use a Virtual Private Network (VPN)

   Answer: *No. A VPN will fix the encryption issue from Alice's computer to the end of the VPN, but it will not provide end-to-end encryption and the NHS site is claiming to only support poor encryption.*

   Answer: *Yes. If the attack is being caused by a local router, such as an evil coffee shop router, then the VPN would protect the traffic through the router and therefore protect Alice's health information. Also, because her browser is warning her, if she used a VPN and it turned out the attacker was on the post-VPN connection where the VPN encryption no longer protects the traffic, she would still get this error and could safely decide not to connect.*

   (b) Turn on her browser's Incognito or Private Browsing Mode

   Answer: *No. Incognito has no impact on transport security, it just removes local identifiers.*

   (c) Log in from a different computer

   Answer: *No. If the problem is server-side then changing computers will not help. Similar to the VPN one full marks are possible for a "yes" answer that mentions some sort of local disruption as the cause.*

Protect Bob's Toaster

Bob manages his own home network and he is concerned that his new internet connected toaster has security issues. He has turned to you for help managing the situation.

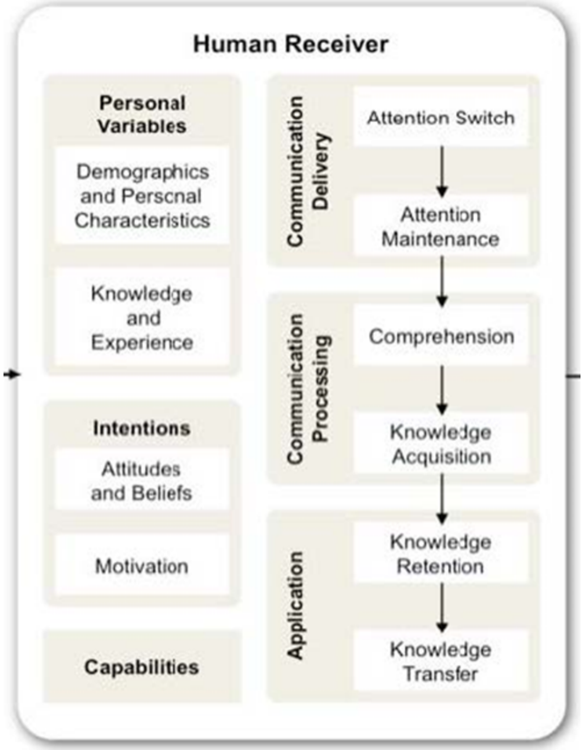
Bob just got the following email:

```
To: Bob <bob@bt.co.uk>
From: Brittish Telecom <bt@bt-customer-service.co.nz>
Subject: Security issues with your home network

Dear Bob,

We have recently detected an issue with your home network
sending malicious internet traffic as part of a large-scale
attack on several major websites including the New York
Times.

To avoid fines or prosecution you must immediately download
and install our anti-virus program which we are providing
free of charge to all customers. Doing so will protect you
and your family in the future.

Please download from:
http://free-anti-virus.moonfruit.com

Sincerly,
The BT Security Team
```

1. Identify two features of this email which indicate that it is likely to be fraudulent.

   Answer: *There are piles of issues, the from address is nz (New Zealand) instead of the UK. The url goes to moonfruit, which is definitely not British Telecom. There is also threatening language about fines to create a sense of urgency.*

2. (Topic not properly covered in ECE 458) While this email seems obviously fraudulent to a skilled computer security student, many people will still click on the provided link and install dangerous software. Use the human-in-the-loop framework discussed in class to analyse the email. Name three components (boxes) of the framework. For each named component, apply it to the above email.



Answer:

Multiple answers possible. Motivation: the threats are intended to be motivating and provide a good reason to comply. Attitudes and Beliefs: popular opinion is that IoT devices have security issues, so it is easy to believe that a home network might be impacted. Knowledge Transfer: if Bob has fallen for this in the past then he may have prior knowlede he can transfer making him less likely to fall for this email.

3. Bob has an internet connected toaster in his house and even though you told him that the above email is fraudulent he is still very concerned that his toaster is attacking other people. Bob only uses his toaster from within his house, he doesn't need to make toast when he is at work. What basic network technology would you recommend Bob use to protect the internet from his toaster?

   Answer: *Firewall. Partial marks: IDS*

4. How would you recommend Bob configure the technology you identified in (c), what properties must you make sure the solution possesses in order to reassure Bob?

Answer: *The firewall needs to block both outgoing and incoming connections from the toaster likely using IP address filtering. While protecting the internet from the toaster only requires blocking outgoing messages, an attacker might be able to remotely tell the toaster to change IP addresses or even change its MAC address which would cause the firewall to bypassed. So its best to block both incoming and outgoing messages.*

5. We learned about STRIDE. If Bob's toaster really is "sending malicious traffic" as the email says, which element of STRIDE best describes what the toaster is doing? State the element and explain how Bob's toaster might be doing that.

Answer: ***D****enial of service is the most natural answer. The attack referenced in the email is describing a DDOS attack on the New York Times. Bob's toaster would be used to send out as much traffic as possible to the victim.*

Answer: *Alternatively, it might be sending traffic to an amplifier, for example,* ***S****poofing the IP of the victim and sending a download request for a large file. Such an attack would allow Bob's toaster to send a relatively small number of packets while the victim receives a very large amount of data, thereby creating a* ***D****enial of Service attack.*