

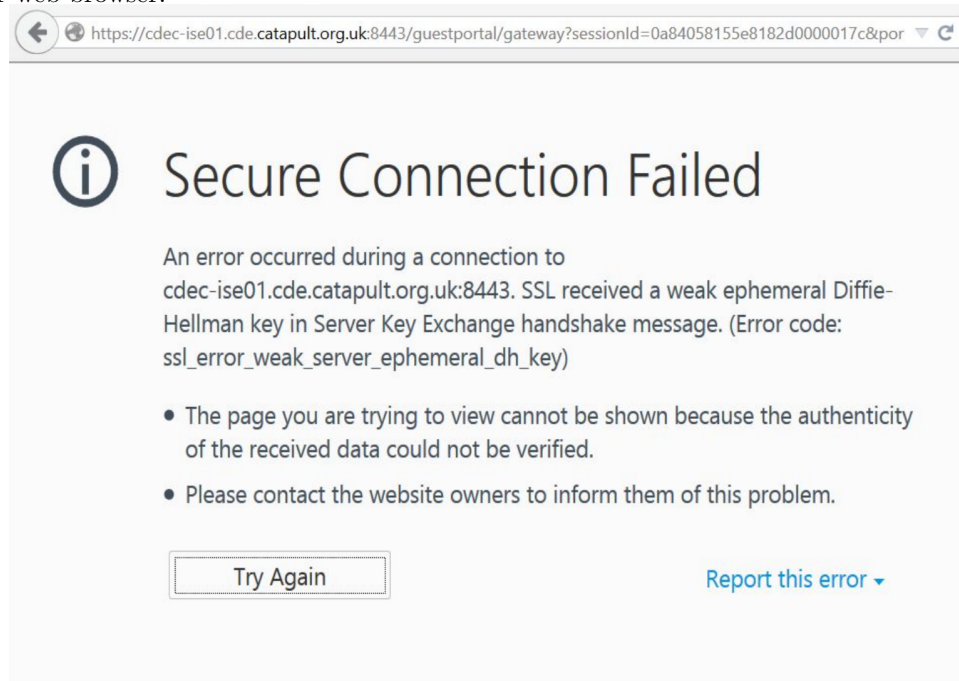
Computer Security Sample Exam Question

Kami Vaniea

August 13, 2024

Analyze a warning

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



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.

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)
 - (b) Turn on her browser's Incognito or Private Browsing Mode
 - (c) Log in from a different computer

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.
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.
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?

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?
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.