Management Information Systems 13e

KENNETH C. LAUDON AND JANE P. LAUDON

CHAPTER 8 SECURING INFORMATION SYSTEMS

CASE 3 IBM Zone Trusted Information Channel (ZTIC)

VIDEO CASE

SUMMARY More and more attacks on online banking applications target the user’s home PC, changing what is displayed to the user while logging and altering key strokes. In order to foil these threats, the IBM Zurich Research Lab has introduced the Zone Trusted Information Channel (ZTIC), a hardware device that can counter these attacks in an easy-to-use way. L=3:07.

URL http://www.youtube.com/watch?v=mPZrkeHMDJ8

CASE Online banking is growing in popularity due to its convenience and ease of use. However, as with any transactions that take place over the Internet, online banking transactions are vulnerable to multiple types of malicious attacks. Although phishing is still a common method that hackers use to commit bank fraud, another method that is difficult to combat is a “man-in-the-middle” attack, referred to in the video as a “man-in-the-browser”’ attack.

Banking transactions are traditionally conducted via two-factor authentication (T-FA). An authentication factor is a piece of information or process used to verify the identity of a person (or other entity) requesting access to a restricted asset or area. Authentication factors are classified into three groups: human factors (biometrics, for example, “something you are”), personal factors (“something you know”), and technical factors (“something you

continued

have”). Two-factor authentication is a system in which two different factors are used in conjunction to authenticate. An example of a traditional two-factor authentication method is the use of a bank card and a PIN number to access a bank account from an ATM.

However, if a transaction is initiated on a computer with malware installed, the security of the transaction is compromised. Not even “padlocked” areas of the Internet that would otherwise be secure can protect against this.

IBM’s Zone Trusted Information Channel (ZTIC, pronounced similarly to “stick”) protects against this. The device sets up a secure link between the ZTIC and the bank’s server. Because there’s a direct connection between the user and the back-end banking server, and because this session is protected by keys that reside on the device itself (and not on the user’s hard drive, where malware can find it), the ZTIC guarantees that banking transactions are secure.

Additionally, the user must press “OK” on their ZTIC to legitimate any banking transaction. So if a user suddenly sees that their ZTIC is asking them to authorize a very large payment to an unknown account, he or she can cancel the transaction before it takes place.

According to IBM, “Various alternatives exist for protecting users against state-of-the-art attacks to online authentication, such as chip card technology or special browser software. The core difference between the ZTIC and these alternatives is that the ZTIC does not rely whatsoever on any software running on the PC, such as device drivers or user interface elements, as these can in principle be subverted, e.g., painted over, by attackers’ malware.”

Hackers and malware are continually developing new tools to commit identity theft and fraud, so it’s important that new advances like the ZTIC become available to stay one step ahead.

VIDEO CASE QUESTIONS

1. What are some common types of malicious software, or malware? What best describes the “man-in-the-middle” type of attack?
2. Provide some examples of each type of authentication factor. What are your personal experiences with each?
3. Can you think of any drawbacks of the ZTIC device?

continued

4. How might malicious attackers try to get around devices like the ZTIC?
5. Do you foresee a future where malware is completely eliminated, or protections are so good that malware is no longer a threat? Explain your answer.