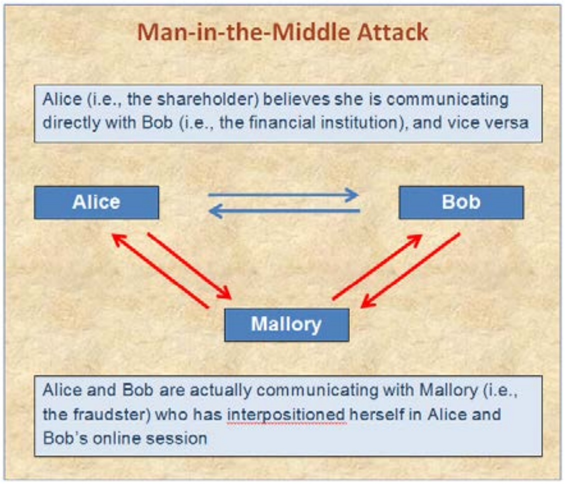
The text below is an excerpt from the ICI Mutual risk management study *Shareholder Authentication: Managing the Risk of Fraudulent Transactions.* The full study may be accessed at www.icimutual.com/ShareholderAuthentication.

Limitations of Authentication Measures Generally

While strong authentication measures may significantly reduce the risk of fraudulent transactions by unauthorized persons, it is important to recognize the limits of authentication. Even the strongest authentication measures cannot completely eliminate the potential for fraudulent transactions.[1]

A fraudster may defeat authentication measures by *compromising* the systems of a financial institution (whether through hacking, social engineering, or otherwise) and causing transactions to be initiated. It was recently reported that dozens of banks and other financial institutions suffered losses estimated to be in excess of $300 million and perhaps as high as $1 billion after their systems were compromised through spear phishing e-mails sent to employees. Once the systems were compromised, the cybercriminals opened fraudulent accounts, transferred money to fraudulent accounts, and caused ATMs to dispense cash at given times and locations.[2]


Man-in-the-Middle Attack
Alice (i.e., the shareholder) believes she is communicating directly with Bob (i.e., the financial institution), and vice versa
Alice
Bob
Mallory
Alice and Bob are actually communicating with Mallory (i.e., the fraudster) who has interpositioned herself in Alice and Bob's online session

A fraudster may also defeat authentication measures by otherwise *circumventing* them. As one cybersecurity expert noted a decade ago, two-factor authentication may be defeated by a man-in-the-middle attack or a Trojan attack.3 In a man-in-the-middle attack, a fraudster “hijacks” an online session in which a user has already been authenticated by an organization. Because the fraudster is impersonating both the user (to the organization) and the organization (to the user), neither party may be aware that the session has been hijacked. In the Trojan attack, the fraudster installs malware on the victim’s computer; once the victim logs in to his or her financial account, the fraudster may either use the properly authenticated session to conduct fraudulent transactions or gather the user’s credentials to conduct fraudulent transactions at a later time.[4]

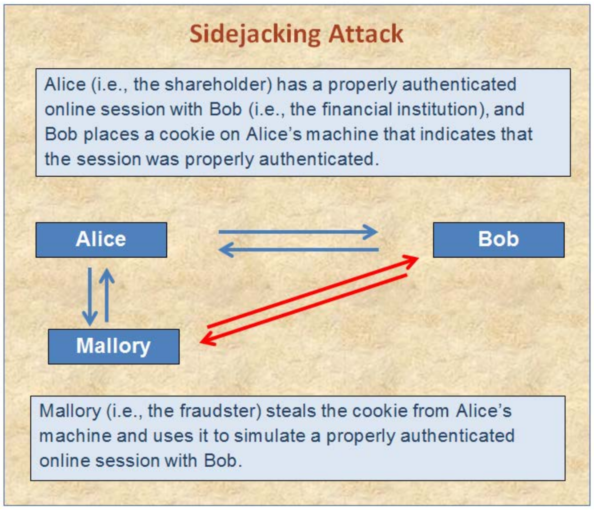
An exposed vulnerability of a commonly used blogging tool illustrates another means of circumventing authentication measures (called a sidejacking attack).5 In this case, the blogging tool provided its users with the option of using two-factor authentication, which should provide a high level of security. Once a session was authenticated, a cookie was placed on the user’s

About ICI Mutual: ICI Mutual is the predominant provider of D&O/E&O liability insurance and fidelity bonding for the U.S. mutual fund industry. Its insureds represent more than 60% of the industry’s managed assets. As the mutual fund industry’s dedicated insurance company, ICI Mutual is owned and operated by and for its insureds.

ICIMutual
The safest decision you can make.

The text below is an excerpt from the ICI Mutual risk management study *Shareholder Authentication: Managing the Risk of Fraudulent Transactions.* The full study may be accessed at www.icimutual.com/ShareholderAuthentication.

machine. However, this cookie was not encrypted and could be copied to another machine. A fraudster with access to the user's computer (e.g., if the user were using an unsecured WiFi "hotspot") could then copy the cookie and impersonate the user.[6] This form of attack has been referred to as "sidejacking" the session.



Sidejacking Attack

Alice (i.e., the shareholder) has a properly authenticated online session with Bob (i.e., the financial institution), and Bob places a cookie on Alice's machine that indicates that the session was properly authenticated.

Mallory (i.e., the fraudster) steals the cookie from Alice's machine and uses it to simulate a properly authenticated online session with Bob.

Endnotes

[1] *See, e.g.,* Paul Ducklin, *Can Strong Authentication Sort Out Phishing and Fraud?*, Virus Bulletin Conference (Oct. 2006), http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/phishingandfraud.pdf?dl=true ("[A]uthentication alone is not enough to protect computer users against the efforts of organized crime to thieve their credentials, their data and even their identity. In fact, strong authentication in only one part of a system may even make things worse if users expect to rely entirely on technology to protect them from phishing and related attacks.")

[2] *See* Carbanak APT: The Great Bank Robbery, Kaspersky Lab (Feb. 2015), https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf; David E. Sanger and Nicole Perlroth, Bank Hackers Steal Millions via Malware, New York Times (Feb. 14, 2015), http://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html.

[3] *See, e.g.,* Bruce Schneier, Two-Factor Authentication: Too Little, Too Late, Schneier on Security (Apr. 2005), https://www.schneier.com/essays/archives/2005/04/two-factor_authentic.html.

[4] *See id. See also* Antone Gonsalves, World of Warcraft attack highlights two-factor authentication weakness (Jan. 7, 2014), CSOnline.com, http://www.csoonline.com/article/2134279/social-engineering/world-of-warcraft-attack-highlights-two-factor-authentication-weakness.html (criminals tricked online gamers into installing malware, which then intercepted the gamers' authentication credentials in a man-in-the-middle attack).

[5] *See generally* Verisign, White Paper, Protecting Users from Firesheep and Other Sidejacking Attacks with SSL (2011), https://www.verisign.com/ssl/ssl-information-center/ssl-resources/whitepaper-protect-sidejacking.pdf (describing Firesheep, a browser extension that uses a packet sniffer to intercept unsecured cookies).

[6] *See* Dan Goodin, *Unsafe cookies leave WordPress accounts open to hijacking, 2-factor bypass*, Ars Technica (May 26, 2014), http://arstechnica.com/security/2014/05/unsafe-cookies-leave-wordpress-accounts-open-to-hijacking-2-factor-bypass/.

About ICI Mutual: ICI Mutual is the predominant provider of D&O/E&O liability insurance and fidelity bonding for the U.S. mutual fund industry. Its insureds represent more than 60% of the industry's managed assets. As the mutual fund industry's dedicated insurance company, ICI Mutual is owned and operated by and for its insureds.

Information current as of September 2015