Orientatie Informatica
Paper Review

Matthijs Dorst
#1380982

February 11, 2009

1 Summary

Online banking, e-commerce and other privacy-sensitive webapplications rely on a secure channel between servers and users. Using Man-in-the-Middle attacks those channels can be compromised, leading to identity theft, creditcard fraud, etc. It is crucial for these applications that MitM attacks can be prevented.

A technique proposed by Oppliger, Hauser and Basin [4] uses session aware user authentication to prevent MitM attacks. While this is not completely secure, it does provide an additional layer of security which greatly hinders attackers in their attempts to obtain sensitive information.

While promising, more research is required as well as active campaining to increase user awareness of the risks involved in online applications.

2 Introduction

Many online banking and e-commerce applications use SSL / TLS encryption to ensure a third party cannot read the data send forth between a server and client. However, since a potential third party could position himself between the server and client and relay the information, a Man in the Middle (MitM) attack, this attacker is still capable of reading any and all information and additionally alter that information.

The implication of this is that an unknown third party could for example alter the destination for a money transfer, sending the money instead to an account controlled by the attacker [1]. To counter this, various methods have been employed such as trusted devices to identify the user [2], yet these are not always succesfull [3].

Oppliger, Hauer and Basin propose a system of Session-Aware user authentication where an impersonal device authenticates the user to validate an encrypted session [4].

3 Methodology

3.1 Man in the Middle Attacks

Though there are many variations and techniques in use today [5] most are based on the same concept: a user is send to the server controlled by the MitM, assuming it to be the server he intended to reach. This fraudulent server then forwards requests and information from the user to the real intended server and responses from the real server back to the user to make both the user and the real server think they are talking directly to eachother. The man in the middle then either proceeds to alter the information to suit his needs (by for example altering the destination bank account of a money transfer [1]) or simply reads

out the datastream to obtain sensitive information on the user such as SSN's, creditcard numbers or PIN's [6].

3.2 Client Redirection

Though there are few exceptions, almost all MitM attacks are performed by sending a user to the fraudulent server before a secure connection has been made. Various techniques for this are commonly used, such as DNS spoofing which generally relies on DNS ID spoofing or DNS Cache Poisoning [7] or what is commonly known as a Phishing e-mail, where mass send e-mail messages inform users that they need to login on the provided URL (which links to the fraudulent server). Less common are trojans or virii that alter a clients host file and which are relatively easy to thwart by employing an up-to-date virus scanner.

3.3 SSL/TLS Session Aware User Authentication

As established, almost all attacks are based on sending the client to the attackers server from the start and making the client establish a secure connection to the fraudulent server, thus giving him a false sense of security - enough to make the user give out personal information that can be used by the attacker.

Thus, focal point of research should be obtaining methods to ensure only trusted connections can be established between the client and the server. A viable way to achieve this is to bind the *user authentication code* (UAC) to both the user credentials as well as the secure session. The recieving server must be able to verify that this code, send by either the user or the attacker, confirms to both the session as well as the credentials.

If a MitM resends the UAC recieved from the client, this will not be the case: the session between the MitM and the real server must differ from the one between the MitM and the client, thus when a hash of that session is combined with user credentials (unknown to the MitM) simply resending the UAC will invalidate that UAC and the real server can drop the connection since it is most likely compromised.

Oppliger, Hauser and Basin propose a system where impersonal key devices can be used to generate a valid UAC depending on the session and user credentials given [4], effectively rendering many of the common MitM attack methods obsolete.

4 Discussion

4.1 Alternatives To TLS-SA

Though effective, the proposed method still relies on one channel for information transfer. With TLS-SA the channel between the users system and the intended server is secure, yet security fails when either of those is compromised, either by installing a virus or trojan on the clients computer or by hacking the server. While hacking a banking server is usually extremely difficult, getting people to install a trojan has been proven to be a reasonably viable option [1].

To prevent this from occuring, some banks have implemented a system where authentication codes are released on a transactional basis, along with transaction details in an *Short Messaging System* (SMS) message. As long as either of the two channels (internet and SMS) remain uncompromised the information exchange is secure. Thus, unlike other methods, a succesfull MitM attack against SMS TAN codes also require the attacker to physically obtain either the phone or SIM card of the intended victim. Though difficult, it is not impossible as shown by succesfull attacks already made against such a system [8].

4.2 Implementation viability

Using impersonal devices to prevent MitM attacks can be a viable option, as proven by the actual useage of such devices by many banks already. Though implementation varies as well as user friendlyness, overall they serve their purpose - at least, up till a point. Even systems such as these can be succesfully attacked [1] when the clients system is compromised. Though installing a trojan or virus on a targets computer is harder than getting people to click a fraudulent link in an e-mail message, reality is that it is not impossible.

An alternative that uses two communication channels is harder to attack, yet it is also more expensive to implement and not completely secure either [8]. Thus reality is that though MitM attacks can be hindered severely, they cannot completely be prevented. Increasing user-awareness of their vulnerability and the sensitivity of their data is crucial in fighting these attacks, yet also the most difficult.

5 Conclusion

5.1 Fields of Interest

Data security is a vast field, implementing techniques from cryptography, user interfacing, e-commerce, networking and even telecommunication. Communication between servers and clients relies on the security of each and every single component used - when one falls, security can be compromised and attackers can gain entry to the system. Thus, such systems need to be tested on all comprised

components if they are to offer the security required for such applications.

5.2 Non-ICT related Fields

While software engineers and cryptographic experts are vital in securing a system, user education plays at least as big a part. The banking sector has successfully convinced people not to share their PIN, yet effords are still being made to increase user awareness of the dangers of online banking [9][10].

References

[1] "ABN Amro compensates victims of 'man-in-the-middle' attack", *http://www.finextra.com/fullstory.asp?id=16750*, finextra, 2007.

[2] B. Parno, C. Kuo and A. Perrig, "Phoolproof Phising Prevention", *Proc. Financial Cryptography and Data Security*, Springer-Verslag, 2006, pp. 1-19.

[3] B. Krebs, "Citibank Phish Spoofs 2-Factor Authenticatin", *Washingtonpost.com ¿ Technology*, Washington Post, 07/2006.

[4] R. Oppliger, R. Hauser and D. Basin, "SSL/TLS Session-Aware User Authentication", *IEEE Computer 41 (3)*, IEEE Computer Society, 2008, pp. 59-65.

[5] A. Bhatia et all, "Man-in-the-Middle Attack", *IT Toolbox.com Wiki*, http://it.toolbox.com/wiki/, 2008, "Scenarios".

[6] L. Rosencrance, "DiscoverCard users hit with e-mail scam", *ComputerWorld SecurityTopics*, Computerworld.com, 03/2007.

[7] Spacefox, "DNS Spoofing techniques", *http://www.securesphere.net/download/papers/dnsspoof.htm*, SecureSphere, 01/2002.

[8] "Victim's SIM swop fraud nightmare", *www.iol.co.za*, Saturday Star, 01/2008, pp. 8-9.

[9] "Member Awareness", *http://www.alamedacu.org/ASP/links.asp*, Alameda Credit Union.

[10] "Internet Banking - Security Awareness", *http://www.nzba.org.nz/pdfs/Internet Banking.pdf*, New Zealand Bankers' Association