

Mashups Legitimize Man-in-the-Middle Attacks: A Position Paper for the 2007 IEEE Web 2.0 Security and Privacy Workshop

Paul A. Karger
IBM Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
karger@watson.ibm.com

Abstract

This position paper examines the inherent contradictions between mashups and end-to-end cryptography. It points out that unless these contradictions can be resolved, the level of internet-related crime is likely to increase even faster than it is already.

1 What is a Mashup?

Mashups have become a major part of the Web 2.0 culture. A *mashup* is defined in Wikipedia as “a website or application that combines content from more than one source into an integrated experience.” [2] The mashup may run on a separate server, or it may run in code that is downloaded onto the client’s machine. Mashups can be created by a web site, because another web site, such as Google Maps, provides an application programming interface (API) so that other web sites can interact with it, sending requests and receiving responses. The intent is to create new and innovative web sites that can do things like locate a product you wish to buy at the lowest price, allow you to place the order at the store, provide routing information to drive to the store to pick it up, display the weather and traffic information along the route, etc., all on a single web page as seen by the user.

To make all of this work, the mashup server has to be between the user’s web browser and all of the various web sites that will provide information and services to make the complete experience. The mashup server has to see what the user is typing, decide where to send that request, then look at the response, combine that response with material from other servers and display the total result on the user’s screen.

2 Man-in-the-Middle Attacks

A cryptographic *man-in-the-middle attack* is defined in Wikipedia as “an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.” [1] The important thing to see from this definition is that the man-in-the-middle attacker and the mashup server have almost exactly the same properties! The mashup user may (or may not) understand that there is an intermediary that is reading and modifying the traffic, but the user will have no way to tell if the mashup server is doing good modifications or if the mashup server is actually an evil man-in-the-middle attacker. Unfortunately, computers do not do a very good job of distinguishing good and evil. For that matter, neither to human beings!

3 End-to-End Cryptography

In pre-computer days, cryptographic devices were developed to encrypt messages sent over teletype lines. My teletype encrypts the message and sends it to your teletype which decrypts the message. As computers began to need cryptographic protection, the teletype cryptographic devices were modified to interface to computer dial-up modems to perform what was called *link encryption*. In a switched network, link encryption has a serious disadvantage, because the messages must be decrypted at each routing switch and then re-encrypted to be sent to the next destination. This meant that anyone who had access to the switches could read the messages in unencrypted form and potentially modify them, thereby carrying out a man-in-the-middle attack.

To solve the man-in-the-middle problem, *end-to-end encryption* was developed in which the message is encrypted before entering the network and is only

decrypted at the final destination. End-to-end encryption was initially thought to be impractical, because each node would have to have different cryptographic keys for each other node, resulting in an order N^2 problem. However, Branstad [4, 5] introduced the notion of a key distribution center (KDC) that would establish session keys between any two pairs of nodes in the network. Any given node would only need to know a key for communicating with the KDC, and the KDC would only need N keys, one for each node, rather than the order N^2 keys required before. Diffie and Hellman [7] introduced public-key cryptography as a major improvement of KDCs as a way of making end-to-end cryptography practical. (Public key cryptography was actually first developed in 1970 by Ellis [9] at the UK Communications Electronics Security Group (CESG), but was kept classified for many years.) Public key cryptography is the basis of the Internet Key Exchange (IKE) [10, 11], Secure Sockets Layer (SSL), and the Transport Layer Security (TLS) protocols [6].

4 Phishing Attacks and Mashups

Phishing is defined in Wikipedia as “a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.” [3]

Phishing attackers are essentially a form of man-in-the-middle attack, and much effort is being spent to try to teach ordinary users to only enter their sensitive information into trustworthy web sites to which they have a secure, end-to-end encrypted connection. We have not done very well at such user education, as has been shown in many studies, of which these are only two examples [8, 12].

The problem with mashups is that they essentially make the secure, end-to-end encrypted connection impossible. Where before, we at least could try to educate users about Phishing, and we could try to improve browsers to make such attacks more difficult. However, with mashups, the presence of a man-in-the-middle is totally legitimized. The operator of the mashup might be trustworthy, or the operator might be an evil attacker, and the end user has no way of knowing the difference. Without end-to-end encryption, we not only have to educate the users better and improve the browsers. We also have to come up with a totally new way of ensuring cryptographic protection for the sensitive information. That level of cryptographic breakthrough might take decades, if it can be done at all.

5 Conclusions

At first glance, mashups appear to be in fundamental conflict with end-to-end cryptographic protection, yet end-to-end cryptography is our fundamental tool for protecting personal privacy and electronic commerce on the web. Unless we can develop new ways of constructing mashups that are compatible with end-to-end cryptography, the level of criminal activity on the web is likely to grow at rates much faster than the already extremely high rates that we are seeing on the Internet now.

The existence of these mashup problems is *not* intended to suggest that the current state of security for electronic commerce on the web is in any way good. Quite the contrary, it is already in a very bad state. The point of this position paper is to argue that mashups make the state of security even worse, because they institutionalize the man-in-the-middle as a legitimate feature, rather than a problem to be solved.

6 Acknowledgements

I must thank Mike McIntosh, Michael Steiner, and Sam Weber for their useful comments on this position paper.

7 References

1. *Man-in-the-middle attack*, 21 March 2007, Wikipedia: The Free Encyclopedia. URL: http://en.wikipedia.org/wiki/Man_in_the_middle_attack
2. *Mashup (web application hybrid)*, 21 March 2007, Wikipedia: The Free Encyclopedia. URL: [http://en.wikipedia.org/wiki/Mashup_\(web_application_hybrid\)](http://en.wikipedia.org/wiki/Mashup_(web_application_hybrid))
3. *Phishing*, 23 March 2007, Wikipedia: The Free Encyclopedia. URL: <http://en.wikipedia.org/wiki/Phishing>
4. Branstad, D. *Encryption Protection in Computer Data Communications*. in **Fourth Data Communications Symposium**. 7-9 October 1975, Quebec City, QC, Canada: p. 8-1 - 8-7.
5. Branstad, D. *Security Aspects of Computer Networks*. in **Proceedings of the AIAA Computer Network Systems Conference**. April 1973, Huntsville, AL: Paper No. 73-427.

6. Dierks, T. and C. Allen, *The TLS Protocol*, RFC 2246, January 1999, Network Working Group. URL: <http://www.ietf.org/rfc/rfc2246.txt>
7. Diffie, W. and M.E. Hellman, *New Directions in Cryptography*. **IEEE Transactions on Information Theory**, November 1976. **IT-22**(6): p. 644-654.
8. Downs, J.S., M. Holbrook, and L.F. Cranor. *Decisions Strategies and Susceptability to Phishing*. in **Proceedings of the 2nd Symposium on Usable Privacy and Security**. 12-14 July 2006, Pittsburgh, PA: ACM Press. p. 79-90. URL: http://cups.cs.cmu.edu/soups/2006/proceedings/p79_downs.pdf
9. Ellis, J.H., *The Possibility of Secure Non-Secret Digital Encryption*, January 1970, Communications Electronics Security Group (CESG): Cheltenham, England. URL: http://www.cesg.gov.uk/site/publications/media/possns_e.pdf
10. Harkins, D. and D. Carrel, *The Internet Key Exchange (IKE)*, RFC2409, November 1998. URL: <ftp://ftp.rfc-editor.org/in-notes/rfc2409.txt>
11. Kaufman, C., *Internet Key Exchange (IKEv2) Protocol*, October 2002, Internet Engineering Task Force. URL: <http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-03.txt>
12. Yee, K.-P. and K. Sitaker. *Passpet: Convenient Password Management and Phishing Protection*. in **Proceedings of the 2nd Symposium on Usable Privacy and Security**. 12-14 July 2006, Pittsburgh, PA: ACM Press. p. 32-43. URL: http://cups.cs.cmu.edu/soups/2006/proceedings/p32_yee.pdf