Thomas J. Watson Research Center

Mashups Legitimize Man-in-the Middle Attacks

IEEE Web 2.0 Security and Privacy Workshop

24 May 2007
Paul A. Karger
karger@watson.ibm.com

What is a Mashup?

- **A website or application that combines content from more than one source into an integrated experience**
  - Definition from Wikipedia
- **Mashup might be implemented in the client web browser or in an intermediate web server**
  - Frequently implemented with AJAX, but not necessarily
  - Portal servers have many of the same characteristics
- **Major growing trend**
  - Billions of venture capital dollars going into them

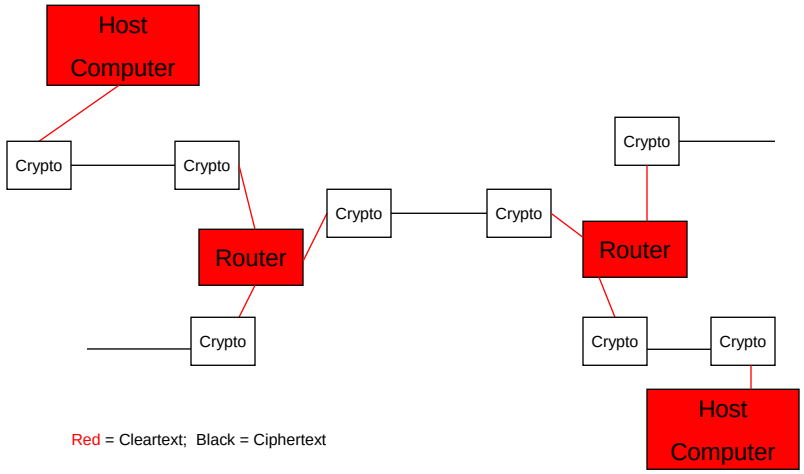
How do you implement a Mashup?

- **Mashup service must intermingle requests and responses to/from multiple sources**
  - Will see requests going to servers to potentially modify or copy those requests
  - Will see responses coming back so as to properly format them together with responses from other servers
- **May be implemented**
  - With code downloaded into local browser
  - Or on an intermediate mashup server that intercepts the requests and responses
  - Or a combination of both

Brief History of Cryptographic Protocols

- **Link Encryption**
- **End-to-End Encryption**
- **Branstad's Network Security Center**
- **Basis for Modern Internet Cryptography**

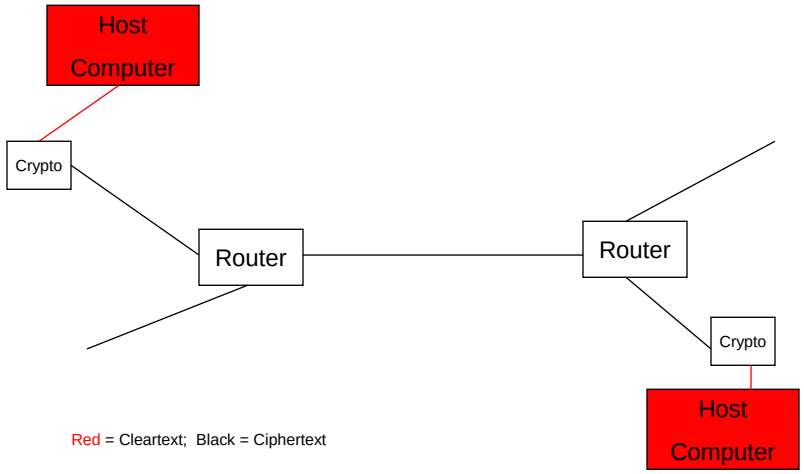
Link Encryption



Man-in-the-Middle Attack

- **Link encryption made man-in-the-middle attacks possible**
- **All routers had to be fully trusted**
- **Attack any router and you get unencrypted access to all traffic**

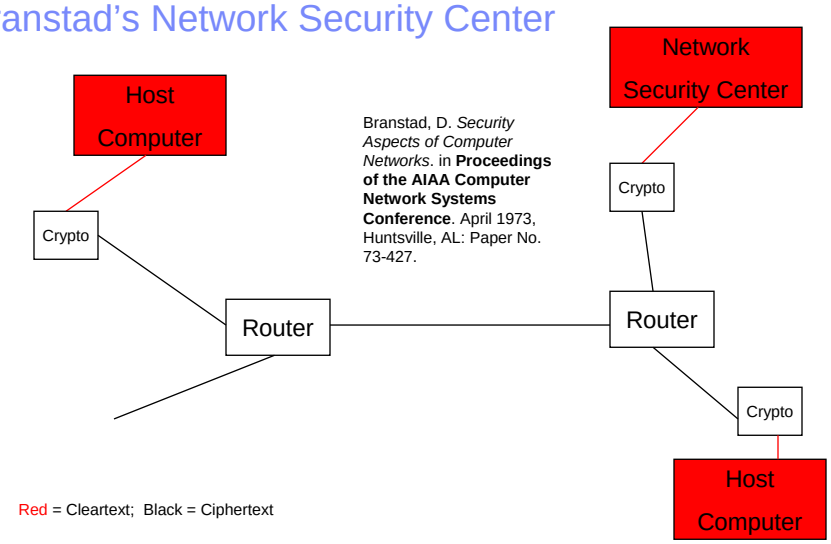
End-to-End Encryption



End-to-Encryption Solves Man-in-the-Middle

- **The introduction of End-to-End Encryption solves the man-in-the-middle attack**
- **The intermediates only see encrypted traffic**
- **But how do you distribute the keys?**

Branstad's Network Security Center

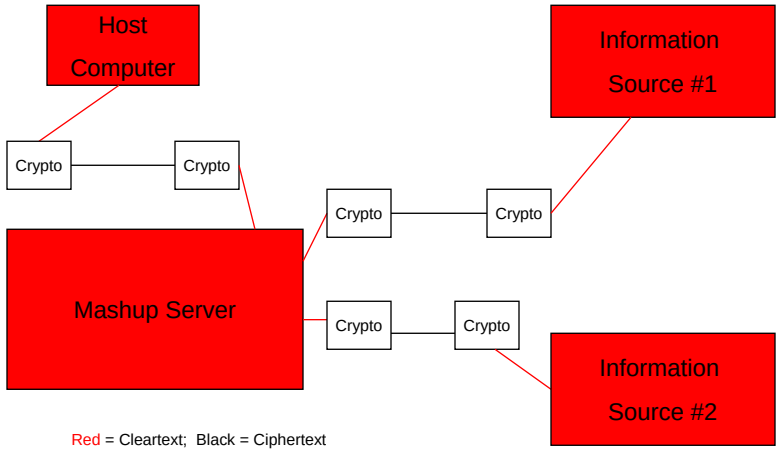


Branstad, D. *Security Aspects of Computer Networks*. in **Proceedings of the AIAA Computer Network Systems Conference**. April 1973, Huntsville, AL: Paper No. 73-427.

Basis for Modern Internet Cryptography

- **Network Security Center was first Key Distribution Center (KDC)**
- **From Branstad's Network Security Center evolved**
  - Needham-Schroeder protocol
  - Kerberos
  - SSL
  - IPSec
  - And all our current end-to-end encryption protocols for the Internet
  - Both secret-key and public-key protocols

Mashup Server Looks Like Link Encryption



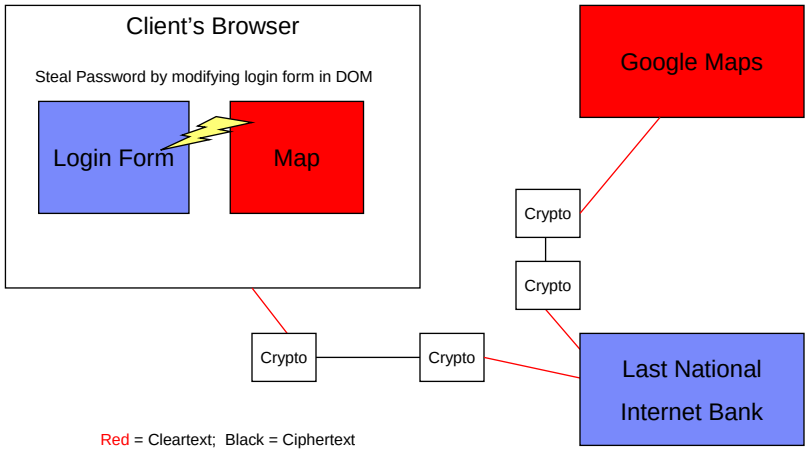
Mashup Server Look Like Link Encryption

- **The mashup server has to see and modify the traffic going to and from the information sources**
- **Perfect opportunity for man-in-the-middle attack**
- **Doesn't matter where the mashup server is located**
  - On a separate machine on the network
  - Integrated into the client's browser
    - Depends on downloaded third party code
    - That might be evil or buggy
    - Inherently cross-site scripting which is a common attack technique

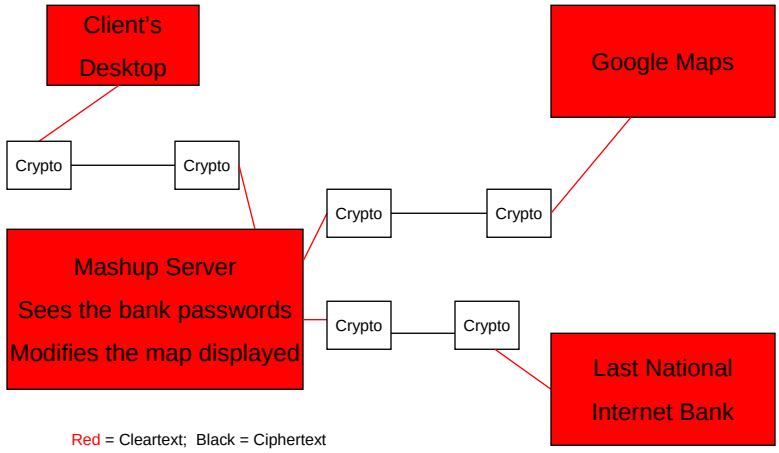
Mashup Attack Scenario

- **Company CEO connects to mashup of Google Maps and his bank**
- **Requests a foreign currency conversion**
- **Wants a map to the bank branch to pick up the foreign currency**
- **Mashup is run by the terrorists who are targetting the company CEO**
  - Two scenarios
  - Cross-site scripting bug
  - Evil intermediate server

Mashup Attack



Mashup Attack



Mission Impossible Scenario

- **Grab the CEO's password and transfer all his money to a secret Swiss bank account to fund terrorism**
- **Modify the map to the bank branch to trick the CEO's chauffeur into driving into an ambush in which the CEO is kidnapped and held for ransom (to be paid from a different bank account than the one they just cleaned out)**

Phishing, Pharming, etc.

- **Most of our current internet commerce crimes are based on man-in-the-middle attacks**
  - Phishing
  - Pharming
  - Etc.
- **We are doing a very bad job of preventing these attacks**
- **Desperately trying to teach clueless users how to recognize their bank from a fake bank**

Mashups Make this Much Harder

- **If mashups become widely prevalent**
  - Then most connections will not be to the real end-point
  - Clueless user will NOT normally connect to the bank, but rather to some intermediate mashup
  - Already very hard problem of teaching the clueless user becomes essentially impossible

Web 2.0 Ignoring Security

- **Most Web 2.0 Developments are ignoring security**
- **One mashup presenter said that security won't be considered until much later – the security experts, of course, can solve all problems later**
  - –Except that end-to-end encryption will have been prevented by then
- **Reviewed several recent books on Web 2.0 and AJAX**
  - –ALL of them treated security as an annoyance
  - –Only advice was on how to supress web browser warnings about insecure transactions!
- **Not everyone is ignoring the problem**
  - –Or this workshop wouldn't be happening

Conclusions

- **No solutions proposed in this talk**
- **Intended as a wake-up call that we need to look at Web 2.0 security very seriously**
- **If we delay, we will institutionalize the man-in-the-middle attack and cross-site scripting**
  - –Analogous to man-in-the-middle problems in cell phone WAP protocols
- **Worst case, we will have to invent totally new encryption paradigms**