Risks of the Passport single Signon Protocol

David P. Kormann and Aviel D. Rubin
Presented by Vembar and Chiu
Attacks to Passport

- Bogus merchant-- example: setup a phony merchant server, obtains a certificate for a domain.
- Use the fake domain like pasport.com to simulate the passport.com.

User might not be aware without checking misspelled URL or the certificate content. They tend to inherently trust the web Passport.
Active attack

- Attacker waits between the client and merchant site for HTTP direct to Passport server.
- If the redirection is not protected by SSL, the attacker intercepts the packet and rewrites the URL to redirect to bogus Passport server.
- The server acts as a proxy between the client and Passport server and between the client and merchant site.
Active attack

1. Request page
2a. Redirect to passport.com
2b. Redirect to psport.com

Browser

www.psport.com

IBM.com

Passport Server

All requests from browser proxied, URLs/redirects rewritten

3. Redirect HTTPS GET Rewritten replies

All requests from browser proxied, URLs/redirects rewritten
Active attack

- Protection?

Checking the site who invoked a redirect is legitimate by inspecting HTTP Referer (header) might not help because this can also be rewritten.

Using challenge response scheme, needs to be considered about the interoperability (eg. if IE function with HTTP Digest)
DNS attacks

- Attacker inserts bogus record in the local DNS server
- When the client is redirected by the merchant service by DNS name, it connects to the bogus server because of modified IP address mapping to the attacker’s fake service
- Or, append bogus DNS to valid DNS replies.
- May require other mechanisms like DNSSEC to provide digitally signed DNS information to protect this attack.
Conclusion

- Passport, ambitious tool, requires no changes to existing browsers and servers.
- Passport flaws arise from reliance on untrustworthy systems (HTTP referrals, DNS), lacking of user awareness (SSL), or interface at Netscape.
- Rotating keys, SSL for all transaction, using challenge response-to avoid an attacker to do forged redirect and reuse passwords.
- Passport should be viewed with suspicion without fundamental changes protocols (adopting DNSSEC and IPSec), because its risks may be inevitable for a system with its requirements.