WebSec

IETF 86

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

- Agenda Bashing, Blue Sheets
- Document status
- Framework Requirements (Hodges)
- Key Pinning
- Session Management
  - Introduction (Yoav)
  - Session-Cont-Prob (Phillip Hallam-Baker)
- Open Mike

Session Management

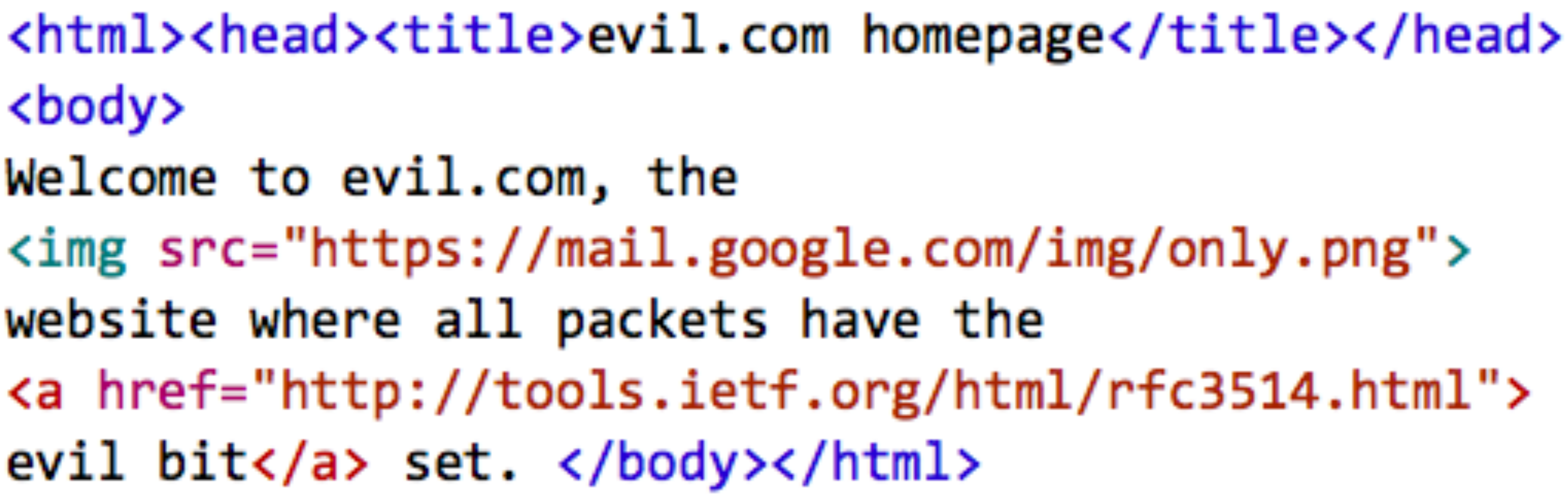
- Issue came up at the httpauth BoF in Atlanta.
- Need to tie together multiple requests from the same client.
  - Give them authorization bound to some authentication from a previous request.
  - Access to stored state.
- Client controls association of requests
- Either side can break a session
  - Not just forget about it.

Session Management

- Today we use session cookies.
- They are bearer tokens, making them attractive targets.
  - BEAST, CRIME, Lucky 13
- Session is fixed from before to after authentication
  - “Weaning the Web off of Session Cookies” describes security issues with cookies.
- Either contain encrypted state, or a key to encrypted state stored on the server.
  - Only one side can “log off”
- The rules were not set for security

Do-Over

- Suppose I get the following HTML page from http://www.evil.com .



```
<html><head><title>evil.com homepage</title></head>
<body>
Welcome to evil.com, the
<img src="https://mail.google.com/img/only.png">
website where all packets have the
<a href="http://tools.ietf.org/html/rfc3514.html">
evil bit</a> set. </body></html>
```

Do-Over

- Rendering the page causes the browser to send a request, controlled by evil.com to Gmail, and that request is authenticated with the user's session cookie for mail.google.com.
- If the user clicks the link, another request goes to tools.ietf.org, also controlled by evil.com, and using the tools cookie.
- These are just examples. There’s Javascript, applets, and other kinds of active content.
- We can never change cookie behavior
- We can change a new mechanism's behavior

Session Management

- We've asked a design team to try to draft a list of requirements for a session management protocol.
- The team included Nicolas Williams, Phillip Hallam-Baker, Yaron Sheffer, and Paul Leach.
- They came up with a requirements document
- They also started working on a solution document, but we'll ignore that for now.

Session-Cont presso goes here

Session Management

- To summarize, what we might get from Session Management is:
  - Session tied to authentication
  - Per-request authentication tied to the session
  - Log-off-ability by both server and client (and user!)
  - Limited re-use of sessions by third party
    - Perhaps with communicable policy
  - Potential to communicate session data and authenticated identity to the user.
  - The chance to create a security-focused mechanism

Session Management

- To be clear, this is not part of our charter. We have seen this presentation as an idea for a future work item. We are trying to see if it's a good fit for WebSec.
- If we can reach rough consensus that it is, then we can ask our AD and the IESG to add this to our charter.
- The plan is:
  - A problem statement document (not sure if must be published)
  - A protocol document
  - A document covering client practices (when should it use the same session, and when not to) – may be combined with protocol.
  - Optionally more documents with more auth binding.

Session Management

- The usual questions:
  - Is this a worthy thing to spend time on?
    - Is this solving a real world problem?
  - Is this group a fitting place?
  - **Can we find people to edit these?**
  - Can we get people to commit to review?
  - Is draft-williams-websec-sess-cont a good starting point?