Validation of HTTP cookie domains

Yngve N. Pettersen
Opera Software ASA

draft-pettersen-dns-cookie-validate-00.txt

draft-pettersen-subtld-structure-00.txt

HTTP Cookies

HTTP Cookies are named values sent to the client by the server, which the server expects the client to send back to the server with all or some of its HTTP requests

Cookies can be used for varius state management tasks, such as remembering preferences or individual users

Cookies can be set for a given server, or (with some limitations) for a group of servers within the same parent (or grand-parent) domain as the server setting the cookie

Problem with domains in cookies

- The domain rules from the original Netscape cookie specification for non-generic domains (two internal dots) are not practically possible to implement because domain structures vary enormously from TLD to TLD
- Neither is the RFC 2965 "one level up" rule practical, there are too many websites with deep domain-structures
- It is still possible for a server to set a cookie for a Registry-like domain (a subTLD), e.g. co.uk, based on current rules

Registry-like (subTLD) domains

- co.uk
- vgs.no
- kommune.no
- city.state.us

Normal domains

- parliament.uk
- vg.no
- opera.no

How to prevent setting cookies for a subTLD?

- Block some subTLD names. Problem: Won't catch all possible subTLDs.
- Extensive blacklist of subTLDs. Problem: Expensive to research and maintain
- Use more DNS features. Problem: May not be available through general APIs
- Separate lookup webservice: Problem: Must be deployed
- DNS lookup of target domain. Problem: False negatives

Current status

MSIE
: Short black list of second level domains, like co.tld

Mozilla
: Uncertain, but it does have a configurable black list. May also have other policies that can be enabled.

Opera
: DNS lookup of target domains that meet certain criteria, e.g. second level domains (draft-pettersen-dns-cookie-validate)

Solution requirements

- Reliable results
- Must work in an environment that has only HTTP access to the Internet
- Must not require implementation of OS level protocols (e.g. DNS) in the application
- Should require few lookups

Suggested action. Alternative 1

draft-pettersen-subtld-structure-00.txt suggests the following:

- Each TLD registry pusblishes a list of TLD-like subdomains (subTLDs)
- The format will be either a plain textfile, or an XML document
- The specification is general, and not limited to cookies
- Clients download the specification from a well known location at most once a month
- The clients use the specification to evaluate domain names when they need to know the type of the domain, according to profiles for that operation

Suggested action. Alternative 2

draft-pettersen-dns-cookie-validate-00.txt suggest using DNS to validate cookie-domains

Benefits

- Easy to implement
- Does not need deployment of new protocol
- Method is already used by many large websites

Problems

- Not general, will mostly work only for cookies
- Require mandated IP address policies for subTLD-domains. E.g. No directories on the TLD name
- Each Webmaster must add and IP address for their domain.