IPv6 Operations
Internet-Draft
Intended status: Informational
Expires: September 7, 2015

E. Vyncke
Cisco

March 6, 2015

HTTP State Management Mechanisms with Multiple Addresses User Agents
draft-vyncke-v6ops-happy-eyeballs-cookie-01

Abstract

HTTP servers usually save session states in their persistent storage indexed by session cookies generated by the HTTP servers. It is up to the HTTP user-agent to send this session cookie on each HTTP request. Some HTTP servers check whether the cookie is associated with the HTTP user-agent by the means of the user-agent IP address. Everything linking a state to an IP address (such as OAuth access code) to an IP address has the same issue.

If the Happy Eyeball mechanism is used to select between IPv6 and IPv4, it may happen that while using the same HTTP server, some HTTP requests are done over IPv6 and the others over IPv4, which leads to two different sets of session states in the HTTP server. This has the consequence of inconsistencies at the HTTP server.

The only purpose of this document is to document this issue in more details than in section 8.2 of RFC 6883 including security considerations and mitigations.

A similar problem arises with the use of non RFC 6888 compliant Carrier-Grade NAT (CGN) devices used to access an IPv4-only HTTP server or HTTP user-agent using multi-homing.

Status of This Memo

This Internet-Draft will expire on September 7, 2015.

Copyright Notice

Table of Contents

1. HTTP Session Management with HTTP Cookie

HTTP requests are basically stateless, therefore if a HTTP server requires to have some states associated to a HTTP user-agent (such as user name, login state, history, shopping basket, ...), there is a need to conserve those states. This is usually done by using a HTTP cookie (see also RFC6265 [RFC6265]) identifying the session; also called "session state cookie".

This session state cookie is generated by the HTTP server at the very first HTTP request from a HTTP user-agent. The cookie is usually opaque (often a random number) and has no semantic except as being an index within the persistent storage of the HTTP server. This index is used to access the complete state of the user-agent. This mechanism is secure if the cookie is transferred with confidentiality

between the server and the user-agent. If the cookie transfer and storage are not secured, then any hostile user-agent can reuse this cookie to access the full original session states (including shopping basket, payment details, ...); this attack is called 'session cookie stealing'. This attack can happen if the HTTP traffic is intercepted by a man-in-the-middle attack but a good use of Transport Level Security RFC5246 [RFC5246] can prevent it. The attack can also happen with some hostile scripting or other pieces of malware running on the user agent, that could copy and send the session cookie to the hostile user-agent; hence, it is not enough to use TLS to secure the session cookies.

Some HTTP applications link the user-agent IP address (whether IPv6 or IPv4) to the session state, probably for additional security checks in order to prevent session cookie stealing. This link leads to some issues in a dual-stack world which are described in this document.

The author knows about at least two large web sites having this problem. It was so severe that those sites which were dual-stack had to move back to being IPv4-only... until the application and its security is updated.

1.1. Other Use of Session Cookies

Beside the use of session cookies by the HTTP server to keep states on the server, the very same cookie is also sometimes used by Server Load Balancing (SLB) mechanism to ensure that all HTTP requests from the same user-agent (even if behind a NAT) are always sent to the same physical HTTP server. This is required if the server persistent storage is local to the server and is not shared by all the physical servers behind the SLB.

1.2. new section

Actually the problem is more generic than the session cookie, everything linking a state to an IP address has the same issue. This includes OAuth [RFC6749] access tokens, bearer tokens, ... but also other mechanisms such as rate limiting per IP address or access control per IP address (for instance a captive portal for a guest net).

2. Issues

Similar issues can be caused by Happy Eyeball RFC6555 [RFC6555], Carrier-Grade NAT (CGN) and having multiple interface or being multi-homed.

2.1. Happy Eyeballs Issue

When a HTTP user-agent uses the Happy Eyeball mechanism to access a HTTP server, then, part of the HTTP requests can happen over IPv6 and another part over IPv4 if the latency between IPv4 and IPv6 varies quickly over time. If there is a link between the session cookie and the user-agent IP address, then upon the first change of IP protocol version, the states associated to the cookie will be invalidated and will be deleted. Here is an example:

1. User-agent with IPv4 address, ADDR4, connect to the server by using IPv4 because IPv6 is slower; the first request does not have any HTTP cookie;

2. Server generates a new cookie C4 and stores in its persistent storage that C4 is associated with address ADDR4;

3. User-agent continues his/her session using IPv4, on each new request the HTTP server receives the cookie C4 and checks that the user-agent address is indeed ADDR4;

4. Latency of IPv6 changes and becomes now faster than IPv4;

5. User-agent now uses its IPv6 address, ADDR6, to connect to the same server and continues to use the same cookie C4 as the server name is unchanged;

6. The server receives the HTTP request with the C4 cookie and checks whether C4 is associated with ADDR6 which is not the case... All session states are deleted and a new cookie, C6, is generated and associated to the IPV6 address ADDR6;

7. The end-user becomes frustrated because he/she has to restart his/her complete session from the beginning.

This cookie invalidation may have some security benefit but it actually prevents a host using Happy Eyeballs to have a persistent session with a dual-stack HTTP server; with painful consequences for the user-experience: disconnection, loss of shopping basket, ...

2.2. Carrier-Grade NAT Issue

RFC6888 [RFC6888] describes the CGN requirements but not all CGN implement them. Some CGN in the real world have a pool of IPv4 addresses and do not always use the same public IPv4 address for all requests from a CGN client. This obviously leads to the same problem as in section Section 2.1. This will happen for IPv4-only HTTP servers.

Whether the CGN is used by IPv4 clients or by IPv6 clients (via NAT64 RFC6146 [RFC6146])does not make any difference to the problem. The use of the address family translation by MAP-T MAP-T [I-D.ietf-softwire-map-t] does not suffer from this issue for IPv4-only HTTP servers since one subscriber is restricted to several layer-4 ports from a single IPv4 address.

2.3. Multiple Interfaces Issue

When the HTTP user-agent has multiple interfaces, for example 3GPP and Wi-Fi, the preferred IP address depends on the WiFi or 3GPP availability. In this case, a similar issue to Section 2.1 also happens as the session cookie can be linked first to the Wi-Fi IP address then when the user-agent looses its Wi-Fi connectivity the session cookie will be overwritten by a new session cookie linked to the 3GPP address.

Whether the user-agent uses IPv4-only, IPv6-only or dual-stack has no impact on the issue.

3. Mitigations

The obvious mitigation for this issue is NOT to link any HTTP state management (including cookies) to any IP address of the HTTP user-agent at the risk of increasing the risk of "session cookie stealing".

The author also believes that:

> Multipath TCP RFC6824 [RFC6824] hides completely the set of addresses of the client to the application. Only the first subflow's IP addresses are exposed to the application, even if a later subflow uses a different address family; so, any session cookie will be permanently linked to the first IP address used by the HTTP user-agent;
>
> HTTP/2 [I-D.ietf-httpbis-http2] multiplexes multiple HTTP sessions over a single TCP connection, therefore, Happy Eyeball (or bad CGN) sees only one TCP connection and a change of IP address will never occur during the lifetime of this TCP connection.

4. IANA Considerations

This document contains no IANA considerations.

5. Security Considerations

The association of the session cookie with the user-agent IP address has some security value as it can help prevent "session cookie stealing" in some limited situations; this benefit should be balanced with the lack of persistent session and the remaining vulnerability if the HTTP session can be intercepted by a man-in-the-middle attack. Moreover with more and more CGN being deployed, linked a session cookie to an IP address shared by hundreds of subscribers is less effective as the cookie could be reused by any subscribers using the same shared public IP address.

6. Acknowledgements

The author would like to thank Brian Carpenter, Ray Hunter, Jeroen Massar, Dan Metzler, Erik Nygren, Mark ZZZ Smith, Joe Touch, Dan Wing and Andrew Yourtchenko for some discussions on this topic. Of course, RFC6883 [RFC6883] has already mentionned this issue without many details.

7. Informative References

[I-D.ietf-httpbis-http2]
Belshe, M., Peon, R., and M. Thomson, "Hypertext Transfer Protocol version 2", draft-ietf-httpbis-http2-17 (work in progress), February 2015.

[I-D.ietf-softwire-map-t]
Li, X., Bao, C., Dec, W., Troan, O., Matsushima, S., and T. Murakami, "Mapping of Address and Port using Translation (MAP-T)", draft-ietf-softwire-map-t-08 (work in progress), December 2014.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6265] Barth, A., "HTTP State Management Mechanism", RFC 6265, April 2011.

[RFC6555] Wing, D. and A. Yourtchenko, "Happy Eyeballs: Success with Dual-Stack Hosts", RFC 6555, April 2012.

[RFC6749] Hardt, D., "The OAuth 2.0 Authorization Framework", RFC 6749, October 2012.

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, January 2013.

[RFC6883] Carpenter, B. and S. Jiang, "IPv6 Guidance for Internet Content Providers and Application Service Providers", RFC 6883, March 2013.

[RFC6888] Perreault, S., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common Requirements for Carrier-Grade NATs (CGNs)", BCP 127, RFC 6888, April 2013.

Author's Address

Eric Vyncke
Cisco
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 2 778 4677
Email: evyncke@cisco.com