generate a pseudo random number and execute a hash calculation for each DUID. For clients without resource constraints, the effect of these calculations is negligible. For resource constrained devices, the system overhead of DHCPv6 can be significant.

By default, the server stores each DUID until the address timeout period is reached. Since each client is frequently leasing new addresses before their previous address expires, the server often maintains large state tables when clients implement a dynamic DUID. The effect on DHCPv6 server performance was noticeable. After approximately 20,000 new DUIDs, the server began to exhibit a large amount of latency in its operation, specifically, leasing addresses. This decrease in performance can be seen in Figure 4. Since the DHCPv6 server only had to track the state of a single client, the non-changing DUID was trivial for it to maintain. For a single client, lease delays are not apparent when static DUIDs are used. Since the tables of DUIDs and leased addressed remain small, the server does not have to process large files. Yet, the dynamic DUID caused a dramatic increase in lease time after 20,000 DUIDs. The lease delays seen in dynamic DUIDs could be mitigated by changing the type of storage the DHCPv6 servers uses for DUID state tables. If a database or other type of fast lookup is used, lookup performance and lease time could be improved. Since the storage techniques currently used by DHCPv6 are simple file and memory allocations, any improvements to handle the volume of DUIDs generated in a dynamic DUID scheme would lead to large performance gains.

The most effective trigger for DUID regeneration that balanced privacy, security, and system overhead was a combination of DUID regeneration on valid lifetime and network prefix changes. Each interrupt protected against a situation which caused a DUID to remain static. The valid lifetime trigger prevented systems with no movement and long period of uptime, such as desktops or servers, from having the same DUID. The network prefix trigger protected systems which move frequently without rebooting, such as mobile devices, from being geotemporally tracked. DUID regeneration on system state changes was effective for most systems. Adjustments to the valid lifetime regeneration trigger caused similar DUID regeneration and, therefore, similar privacy and security protections.

Due to the system overhead and frequent DUID regeneration and release, mobile systems may want to consider using SLAAC with privacy extensions instead of DHCPv6. The calculations and overhead required for SLAAC and privacy extensions are minimally less than those for DHCPv6 using dynamic DUIDs. This small difference, however, may lead to large differences in battery life.

6. Conclusion

IPv6 is a definite improvement over IPv4, allowing more devices to connect to the Internet using globally unique addresses. However, the privacy implications of static DUIDs should be addressed before the protocol is globally deployed. The ability to track users' DHCPv6 issued addresses combined with the ability to track stateless addresses with static IIDs compromises privacy in all known addressing methods in IPv6. While DUID correlation and analysis is limited in scope, the possibility of relay networks or compromised relays extends an attacker's reach beyond local networks. With both methods of IPv6 addressing compromised, changes must be made to assure users' privacy.

A number of different methods can be used to obscure users' DUIDs from monitoring. While DHCPv6 servers can be configured to increase the randomness of addresses issued, a dynamic DUID configured by the OS appears to be the best privacy option. By changing the DUID at each network connection, all DHCPv6 servers in any configuration will issue randomly available addresses to each client. The lack of client and network support for DHCPv6, however, will likely mean the issue will be ignored until subnets begin to crowd and DHCPv6 is required for efficient operation. Regardless of the solution implemented, some method of DUID obscuration should be deployed as part of operating systems and embedded devices to protect the privacy of users.

7. Future Work

There are many ways that systems using stateful addresses can be exploited, both negatively and positively. In future research, we will explore in detail some fields that could be impacted. Static DUIDs allow for cyber stalkers to gather local information and read targets' traffic. Also, static DUIDs permit terrorists to gather information about targets without alerting authorities. On the other hand, similar types of static identifiers can be captured for legitimate analysis by marketers or gathered by law enforcement officials for forensic analysis. Regardless of intent, users' location and Internet activity should be protected from passive monitoring.

The next phase of the research will focus on designing and implementing a dynamic, nondeterministic method of leasing addresses for DHCPv6 clients. Currently, a client is forced to use a DHCPv6 leased address minimally for of a complete session. With the address being the same for that session, traffic can be correlated within the session. Any unencrypted traffic may expose a user's identity, allowing traffic over multiple sessions to be correlated. By using multiple addresses per session, it becomes statistically infeasible for an attacker to correlate traffic over multiple sessions,

even if the traffic is unencrypted. Also, implementing authentication in lease query requests, either through source addresses or other methods, would help to prevent some of these attacks.

8. Acknowledgements

The authors would like the thank Communications and Network Services at Virginia Tech for their support of this research. Specifically, the knowledge, advice and support of Phil Benchoff and Carl Harris have been invaluable. Their IPv6 expertise allowed this research to be conducted on a production IPv6 network and properly tested and evaluated.

9. References

[1] J. Arkko, J. Kempf, B. Zill, and P. Nikander. SEcure Neighbor Discovery (SEND). RFC 3971 (Proposed Standard), Mar. 2005.

[2] T. Chown, S. Venaas, and C. Strauf. Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues. RFC 4477 (Informational), May 2006.

[3] R. Droms. Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6. RFC 3736 (Proposed Standard), Apr. 2004.

[4] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315 (Proposed Standard), July 2003. Updated by RFCs 4361, 5494.

[5] R. Droms. DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3646 (Proposed Standard). Dec. 2003.

[6] S. Groat, M. Dunlop, R. Marchany, and J. Tront. The privacy implications of stateless IPv6 addressing. In Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, CSIIRW '10, pages 52:1-52:4, New York, NY, USA, 2010 ACM.

[7] W. Haddad. Privacy for mobile and multi-homed nodes: MoMiPriv problem statement, 2005.

[8] S. Kent and K. Seo. Security Architecture for the Internet Protocol. RFC 4301 (Proposed Standard), Dec. 2005.

[9] V. Kalusivalingam. Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3898 (Draft Standard), Oct. 2004.

[10]V. Kalusivalingam. Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6. RFC 4075 (Draft Standard), May 2005.

[11] T. Mrugalski and M. Senderski. DHCPv6: Dibbler - a portable DHCPv6. Available at: http://klub.com.pl/dhcpv6/, (accessed Aug 2010).

[12] L. Morand, A. Yegin, S. Kumar, and S. Madanapalli. DHCP Options for Protocol for Carrying Authentication for Network Access (PANA) Authentication Agents. RFC 5192 (Draft Standard), May 2008.

[13] T. Narten, R. Draves, and S. Krishnan. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 4941 (Draft Standard), Sept. 2007.

[14] T. Narten, E. Nordmark, W. Simpson, and H. Soliman. Neighbor Discovery for IP version 6 (IPv6). RFC 4861 (Draft Standard), Sept. 2007.

[15] Remaining IPv4 address space. Available at: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml, Feb. 2011.

[16] D. Plummer. Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. RFC 826 (Standard), November 1982. Updated by RFCs 5227, 5494.

[17] J. Postel. Internet Protocol. RFC 791 (Standard), Sept. 1981. Updated by RFC 1349.

[18] H. Schulzrinne, Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers. RFC 3319. Proposed Standard. Jul. 2003.

[19] J. G. G. Tams, R. Brown, D. J. Maxwell, and M. A. Pearce. Tracking dynamic addresses on a network. Patent, Mar. 2005. US 686228

