Practitioner Perspectives

WOLF DEN
ASSOCIATES, LLC

February 2015 *(Vol. 4; Issue 2)*

Top 10 Ways We Earn Our Beads

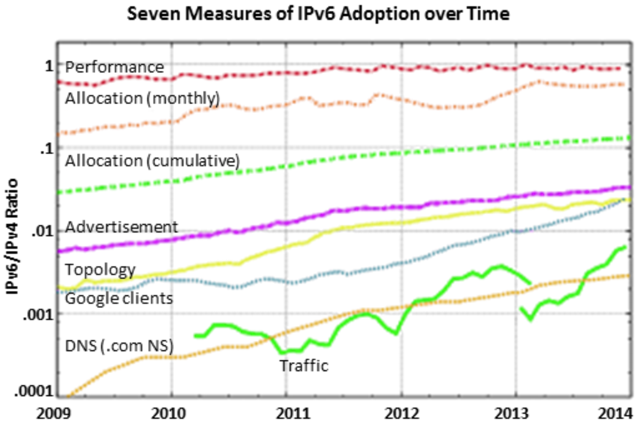
1. ***Deploy enterprise search to help organizations know what they know***
2. ***Develop risk management methodologies for cloud implementations***
3. ***Write meticulous requirements to bridge the gap between stakeholders and developers***
4. ***Analyze TCO and develop recommendations which consider decommission AND data migration costs***
5. ***Develop technology roadmaps defining where to go and how to get there***
6. ***Create BYoD policies that let millennials have their mobile cake with increased productivity and enterprise security too***
7. ***Combat insider threats against languishing user accounts by enforcing account life cycles***
8. ***Rationalize applications to reduce long-term O&M costs***
9. ***Mitigate your SAs and SW developers' pentesting COI issues***
10. ***Transform IT from a back-office function to a business enabler***

Fat Technology Tuesday: A Carnival in Cyberspace

- As the hype cycle cools on cloud and big data, emerging challenges in protocols, authentication, and encryption will take center stage
- With 4.3 billion IPv4 addresses having been allocated, IPv6's time is now
- Clearly a better method for authentication is needed when most users employ the same password across multiple domains, or write them all down without a second thought
- Security best practices dictate intentionally entering wrong information into password recovery systems to avoid exposing accounts to social media trolls and current/ex-spouses
- Zip encryption is one of the most universal forms of securing data, but it is useless if the recipient's email server blocks zip files
- Cringing about transmitting PII over email? Try doing a deep web search; your SSN is out there

Technology Second Line

Cloud computing and big data are the headline acts this season. Federal CIOs and systems integrators alike have planned their spots along the parade route, hoping to grab some beads. While these technologies garner the buzz, the reality is that cloud policies have been codified and customers have either moved to the cloud or are in the process of migrating their back-office applications, while mission applications will remain on bare metal. Similarly, new big data analysis techniques are being developed daily and the pace of commoditization is staggering, especially to new entrants. While many continue to enjoy this parade, there is still action for everyone else in the second line, where issues around IPv6, Identity and Access Management (IdAM), and encryption increasingly create acute pain points.



Despite having been around for 20 years, and the exhaustion of the IPv4 address space, IPv6 is still in its infancy.

Source: Arbor Networks

New Parade Route

For the past seven years IPv4 has limped along fighting retirement. The IPv4 address space has largely been exhausted and is more crowded than Bourbon Street during Mardi Gras. At Shmoocon 2015, the Ghost in the Shellcode CTF tested each team's skills against the forthcoming IPv6. Unfortunately, there was limited success. For an example of the challenge, task your best network engineers to send one IPv6 packet to a server in less than 4 hours from your office network (LTE does not count). It will not be as easy as you think it should be. While new devices and even gaming platforms are IPv6 ready, on the whole it is not consumer ready. As federal customers begin making the transition to IPv6 a reality, they will require infrastructure upgrades and network configurations to make the turn.

Masquerade Ball

Old IdAM solutions are not aging well. Passwords are now written down and cross-pollinated across multiple accounts due to complexity requirements, and recovery questions are easily reverse-engineered via social media profiles. Biometric IdAM is a mixed bag, with fingerprints rendered obsolete by the latest generation of mobile cameras. PKI certs have performed well in the federal space, but have not been widely adopted and they still require a password to unlock. Federated identity management has promise, but lacks a gate-keeper akin to a certificate authority, and the public is unlikely to entrust Google, Facebook, etc. with this much power. Meanwhile, today's cyber criminals can compromise your digital identity as easily as they would don a carnival mask – and with comparable immunity.

Krewe of Konfidentialty

Transmitting PII over email or storing it on a shared drive gives most users pause. As a result, much of this information is transmitted in analog form – via fax machine – which is one of the least secure forms of communication available. From sensitive medical files to passing security clearances, online security concerns have mistakenly resulted in the fax becoming the de facto standard. PGP has been around for a while and a plethora of tools exist that have built-in encryption (pkzip anyone?); all of them, however, require users to insert extra steps in the workflow, forcing a choice between ease of use and security. True end-to-end encryption – complete with email and document-level permissions and revocation functionality – will be the solution that gathers the most doubloons.

1751 Pinnacle Drive
McLean, VA 22102
wolfdenassociates.com

Rick T.
(703) 638-5924
rick@wolfdenassociates.com

John S.
(301) 356-1027
rambo@wolfdenassociates.com

Ian K.
(571) 253-2522
ian@wolfdenassociates.com