Trust in the Cloud

i2Coalition & the M3AAWG Hosting SIG

Introductions by Matt Stith, Rackspace

Speaker 1:

Allan Friedman, PhD

Building trust through collaboration: How the U.S. Government is promoting vulnerability disclosure discussions.

Allan Friedman is the Director of Cybersecurity Initiatives at National Telecommunications and Information Administration in the US Department of Commerce.

Speaker 1:

Allan Friedman, PhD

Prior to joining the Federal government, Friedman was a noted cybersecurity and technology policy researcher. Friedman has over a decade of experience in cybersecurity research, with a particular focus on economic, market, and trade issues. He is the coauthor of Cybersecurity and Cyberwar: What Everyone Needs to Know (Oxford University Press, 2014).

Speaker 2:

M3AAWG
Messaging Malware Mobile
Anti-Abuse Working Group

Ram Mohan, EVP & CTO; Afilias

The case for upgrading the Internet by focusing on IPv6, DNSSec and Universal Acceptance

Ram Mohan is the Executive Vice President of Business Operations and Chief Technology Officer at Afilias Limited. He has worked extensively and led developments on Internet security and internationalization.

Focusing on three technical areas

- **OUR FOCUS: Making a case for IPv6, DNSSec and Universal Acceptance**
  - **There are other areas worthy of technical discussion including:**
    - **Securing BGP**
    - **Wide deployment of TLS**
    - **DANE**
    - **DDoS mitigation**
      - **…many more**

IPv6

- It's been four years since World IPv6 Launch Day, June 6th, 2012
  - As of the 11th of June, 2016, 12.15% IPv6 adoption
  - U.S. is at 27.1% which puts it ahead of most countries
- IPv4 is exhausted as of September 24, 2015
  - Secondary market is increasingly expensive and often shady
- Without broad IPv6 adoption, it stymies growth for a lot of the smaller players
- The growth of IoT and other Internet connected devices will push requirements for IPv6 in order for it to maintain a secure network
- A carrier-grade NAT is not a solution, it doesn't scale well. All alternatives are temporary fixes.

DNSSec

- **Few technologies are more critical to the operation of the Internet than the Domain Name System (DNS). DNS Security (DNSSEC) is designed to authenticate DNS response data. It verifies responses to ensure a DNS server's response is what the zone administrator intended. It does not address all threats (nothing does), but it provides a building block for providing additional data security, and not just within the DNS but also within the applications and services that are built on it.**

- **When TCP/IP was designed, security was not at the forefront of the design. As the importance of the network of networks has grown, the importance for security has increased.**

- **After a burst of well publicized activity from 2009-2011 — .org, .com, .net, and .gov adopting DNSSEC, roots signed, other Top-Level Domains (TLDs) signed — the pace of adoption appears to have slowed in recent years.**

Universal Acceptance

- **The Internet Name Space has Changed**
  2010 Top Level Domain in 'foreign' scripts introduced
  2013 Hundreds of new Top Level Domains Introduced
    ua-test.**link**
    ua-test.**technology**
    ua-test.**世界**
    普遍接受-测试.**世界**
    اختبار-القبول العالمي.**شبكة**
- **Application Software has NOT kept Up**
- **Accept, Validate, Process, Store, Display**
- **Universal Acceptance Steering Group**
- **Email Address Internationalisation**
  Supporting non-English Characters in Local and domain parts
- **For more information, see www.uasg.tech**