National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Attn: Cybersecurity RFC 2015
Washington, D.C. 20230
Docket Number: 150312253-5253-01

Submitted May 27th, 2015 via email to securityRFC2015@ntia.doc.gov

CloudFlare comments on
"Stakeholder Engagement on Cybersecurity in the Digital Ecosystem"

Thank you for your interest in improving the security of the Internet. It is a timely topic, given nearly daily news about vulnerabilities and attacks on companies, governments, and individuals.

CloudFlare is a web security and performance company, protecting and accelerating websites that are part of the CloudFlare community. We also block threats and limit abusive bots and crawlers from wasting our customer's bandwidth and server resources. We are invested in building a better Internet - as the Internet continues to become more secure, users' trust also improves.

The Department of Commerce and NTIA can help facilitate progress in online security by engaging a broad set of stakeholders, considering the broader audience of Internet users, and identifying several concrete steps for collective action.

Stakeholders

The security of the Internet impacts every Internet user and every company that is online. While the wide array of companies providing security services and technologies - like CloudFlare - are an important constituency, it is likely more useful to ask other businesses, which purchase such services, what their needs are, and what their roadblocks are. It will be important to engage companies outside the security industry in order to understand the challenges they face, particularly because some industry sectors face unique or unusual security challenges.

Every hosted website today is vulnerable to security threats. Whether that is malware inserted into the site itself, distributed denial of service (DDoS) attacks on the origin server, or direct attempts to access data, at some level all users have a stake in the security of the Internet.

Topics for discussion and action

The most immediate way to improve the overall security of the Internet is to identify a few, concrete issues where progress can be made. In general, these issues will be ones where there has been, in the past, a collective action problem - that is, individual entities are not incentivized to fix it individually, but the entire community could benefit from change.

Our ideas tend to focus on the fundamental infrastructure of the Internet, because that is generally where attacks on our customers originate. We consider it important to promote the development and continuing improvement to these protocols in order to keep the Internet safe. It is also an area in which the NTIA can serve a convening role to allow for stakeholders to make progress on these difficult problems.

Secure open DNS resolvers

The Domain Name System (DNS) serves as a metaphorical phone book for the Internet, translating human-entered names (like the domain name www.cloudflare.com) to numeric Internet addresses (like 198.41.214.163 or 2400:cb00:2048:1::c629:d7a3). Despite being a fundamental component of the modern Internet, DNS is one of many protocols that can be co-opted to attack other network elements. To be clear, DNS works extremely well - but on top of the very functional day-to-day DNS use, there's still plenty of nefarious DNS traffic flowing across the Internet. It is that nefarious traffic that CloudFlare successfully mitigates each-and-every second of the day.

Using open DNS resolvers, attackers can use DNS Amplification Attacks to flood a target with more traffic than any one host is likely to be able to handle. Unfortunately, it is possible to multiply the impact of an attack many times by exploiting what are now seen as flaws in the DNS protocol, as we have explored on our blog. Unfortunately, many people operating these resolvers have not made the configuration changes to avoid becoming part of these attacks, since they do not necessarily directly impact the operator.

Secure NTP servers

Similarly, an amplification attack can be accomplished using unpatched Network Time Protocol (NTP) servers. NTP attacks have been responsible for some of the largest DDoS attacks ever observed. NTP is a protocol that is used to synchronize computer clock times in a network of computers. However, it can also be used to direct a DDoS attack at a third party.

In the past, CloudFlare has published lists of networks from which these kinds of DDoS attacks have originated. On a positive note, many of the vulnerable servers have been patched - but many more remain unpatched. If the multistakeholder process could encourage that NTP servers be updated to patch this vulnerability, it could significantly decrease or eliminate this type of DDoS attack.

Encourage DNSSEC implementation

The multistakeholder process should identify and encourage tools and methodologies that have already been developed to make the Internet more secure. The Domain Name System Security Extensions (DNSSEC) is just such a protocol, and addresses a problem that was recognized, and a solution developed, in a multistakeholder manner. The Internet community came together to develop a more trustworthy DNS using a set of security extensions that provide the means for authenticating DNS records.

The Domain Name System Security Extensions (DNSSEC) were published by the IETF in 2005, but have yet to see broad adoption. You can see the DNSSEC validation rate by country with this APNIC tool. The NTIA has already played at part within the global Internet's adoption of DNSSEC with its stewardship of the IANA functions and the signing of the root zone. Now it's time for NTIA to further that process by supporting additional DNSSEC deployment.

NTIA and the multistakeholder group should also look to other existing and successful multistakeholder groups, such as that within the Communications Security, Reliability and Interoperability Council.

Support the use of strong encryption

Encrypting and authenticating as much web traffic as possible to prevent data theft and other tampering is a critical step toward building a safer, better Internet. We're proud to be the first Internet performance and security company to offer SSL protection at no cost to our customers.

In the past, organizations had to choose between performance and security when encrypting their web server traffic. Even if they were willing to tolerate increased latency for higher security, that tradeoff came with a host of operational difficulties.

This situation has changed. With recent developments in HTTPS technology, such as SPDY, sending requests over HTTPS can be faster than using regular HTTP. Also, the complicated operational issues associated with sending encrypted data can be handled by third parties like CloudFlare. It's time for enterprises to take another look at securing their web traffic.

Industry leaders and other stakeholders can come together to share strategies and develop best practices for HTTPS usage. The multistakeholder process should recommend that all websites use HTTPS and secure their data with encryption or other means to hide it from attackers.

Encourage open source stewardship

Many of the fundamental protocols of the Internet are maintained by the open source community. Open source software is reliable, easy to modify, and easy to maintain. It's also a community effort that helps keep the Internet secure. The more people look at any given piece of code, the better (and hopefully more secure) it gets. That means that for incidents like Heartbleed and Shellshock, all types of contributors work together as a community to implement fixes and patch systems quickly.

In addition, recent vulnerabilities have encouraged vulnerability rewards programs and a community effort to find vulnerabilities before they are exploited. This is a part of the proactive stance that must be taken to security.

NTIA should encourage all software companies to contribute back to the community and work on fundamental protocols, especially in security contexts. We have been encouraged by other agency efforts in this area, and hope that NTIA can collaborate and learn from their efforts, as well.

Conclusion

Thank you for the opportunity to provide input on the upcoming NTIA multistakeholder process. We appreciate the engagement of a broad set of stakeholders, since we all have an interest in making the Internet safe. In particular, it would be immediately productive to focus on those Internet security issues that have a collective action problem; the NTIA is well situated to make an impact by encouraging adoption of better security, encouraging software and firmware updates to Internet infrastructure, and recommending that companies use strong encryption and contribute to the open source code that supports the entire Internet's infrastructure.

For questions or additional information, please contact: Heather West, Public Policy (heather@cloudflare.com)
Michael Nelson, Public Policy (mnelson@cloudflare.com)