COMMENTS ON REQUEST FOR COMMENT
"Cybersecurity, Innovation, and the Internet Economy" Green Paper
76 FR 34695
DOCUMENT NUMBER 2011-14710
U.S. DEPARTMENT OF COMMERCE
INTERNET POLICY TASK FORCE

RESPONSE FILED BY:
U.S. PUBLIC POLICY COUNCIL OF THE ASSOCIATION FOR COMPUTING MACHINERY

On behalf of the U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM) we are submitting the following comments in response to the Request for Comment by the Department of Commerce Green Paper "Cybersecurity, Innovation, and the Internet Economy" issued by the Department's Internet Policy Task Force.

With over 100,000 members, the Association for Computing Machinery (ACM) is the world's oldest and largest educational and scientific computing society. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. Our comments are informed by the comments USACM submitted[1] on the previous Department of Commerce Green Paper[2]. Should you have any questions or need additional information, please contact Cameron Wilson, our Director of Public Policy, at 202-659-9711 or at cameron.wilson@acm.org

We appreciate and welcome the attention the Department of Commerce and the Internet Policy Task Force have placed on cybersecurity, especially as part of a larger policy effort that includes online privacy. All too often these two concepts are placed in opposition to each other. Security and privacy need not be considered as tradeoffs, but should be seen as complementary concerns that can support each other. We believe that effective security policies and practices can provide benefits to consumers and commercial interests alike. Many of our comments address the issue of trust in cybersecurity, and how forming an effective trust relationship will be important to ensuring the effective operation of the Internet and Information Innovation Sector (I3S). Effective privacy practices and policies can assist in fostering the trust that will help address cybersecurity threats, and we recommend that the Department's actions going forward on security and privacy work together rather than separately.

Specific Questions

Our responses to the questions listed in the "Cybersecurity, Innovation, and the Internet Economy" Green Paper are premised on the Green Paper's definition of the "Internet and Information Innovation Sector (I3S)" (page 2).

3. What are the most serious cybersecurity threats facing the I3S as currently defined?

As the Green Paper notes, trust issues are an important principle (p. iv) when examining the potential impact of I3S cybersecurity threats. The trust negotiation, built up over time and transactions, between the consumer and the organization can be quickly shattered as a result of instances of consumer personal information loss, site defacement, malware infestation, or failure to properly manage transaction security via SSL. At the same time, though, organizations must reconcile management of these issues with operational exigencies.

For example, an organization that routinely updates customers with customized e-mail messages may provide a basis for a phishing attack and, as a result, its customers could disclose authentication information (e.g., login and password) to a fake web site. The organization's willingness to communicate with customers provided information to attackers (e.g., e-mail design and approach) that enabled attackers to exploit this attack vector. Balancing operational goals and initiatives against such potential risks is, and will be, an ongoing challenge for some time.

---

[1] http://usacm.acm.org/PDF/Commerce_Department_Online_Privacy_Comments_USACM.pdf

[2] http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf

By their very nature, I3S organizations must maintain a public presence on the Internet. Protecting public web sites against malicious software (i.e., malware) infestation is critical to maintaining the trust relationship. Although no I3S participant would willingly deliver malware to its users, various exploits allow attackers to convince users to download malware delivered through an embedded link in a legitimate web site via a cross-site scripting (XSS) attack. I3S organizations must keep server software updated, develop code that prevents such attacks, and educate both themselves and their users regarding these issues. This is no small task.

Maintaining current security patches also runs into the tension between operational and security needs. As a result of patches, server configurations may change and break other processes. However, servers with out-of-date software enable many web site and web application attacks. Dealing with patch management so as to address both operational and security issues is challenging, especially for small- and medium-sized organizations that do not have sufficient trained staff (or any at all) to maintain systems. Many smaller I3S organizations will depend on outsourced services and may have no indication whether these services are current in their security patches.

No matter how diligently an I3S organization works to keep its security technology current, there remain challenges: zero-day exploits and third-party application vulnerabilities. Addressing zero-day exploits requires a major shift in the software and services industry. One such technique would be to make software developers more accountable for the software they produce and market. If an I3S organization develops its web site using Flash, for example, it cannot account for the various attacks that occur because of shortcomings in the Flash software. An I3S business might need to choose between innovation and market share versus security. This is a difficult choice to make.

Finally, one of the initial trust negotiations is the establishment of a secure connection between the I3S organization and the customer. Here, we see a challenge in that organizations must not only purchase a site certificate to correctly identify themselves, but they must also choose from an increasing number of certificate authorities. Although competition is needed to ensure that prices for certificates remain affordable for small- and medium-sized I3S organizations, the proliferation of certificate authorities presents a number of problems. Cost competition can lower the level of scrutiny that some honest certificate authorities apply to applicants for certificates. At the same time, as the number of certificate authorities grows, it becomes progressively more difficult for users to discriminate among them. Lower levels of scrutiny in general, moreover, make it easier for fraudulent certificate authorities to operate.

Most web browsers do not yet have usable options for revoking fake or compromised certificates. An SSL connection works just as well to encrypt data during transmission regardless of whether the data is delivered to a legitimate or a fake site. What happens to the data at the receiving end may result in identity theft or other fraud.

Ultimately, in order to remain operational and maintain the trust relationship through viable security measures, I3S organizations must be provided with better tools, techniques, and training so they can continue to innovate while minimizing risk.

11. Are the standards, practices, and guidelines indicated in section III.A.2 and detailed in Appendix B of the Green Paper appropriate to consider as keystone efforts? Are there others not listed here that should be included?

We agree that although the private sector as well as academia and professional organizations should be the main drivers behind standards development, it might be useful for certain standards to be adopted/adapted to promote cybersecurity within the I3S.

Many of the frameworks noted in the Green Paper such as PCI and NIST SP 800-53 are well developed. PCI is industry driven, has a large degree of private sector buy-in, and should help address the needs of various I3S participants. On the other hand, NIST SP 800-53, while certainly useful, is not as widely or comprehensively employed in the private sector. It could serve as a starting point for guidelines and practices more amenable, in particular, to use by small- to mid-sized I3S participants. Appendix B of the Green Paper speaks to this need in the "Challenges" section (p. 56).

The National Strategy for Trusted Identities in Cyberspace (NSTIC) shows promise and, with time, may be a standard for identity management on which we might rely. However, it is far too soon to make this determination.

Most of the technical standards noted in section III.A.2 and Appendix B work well and will continue to develop to meet the targeted needs. These are largely driven by both academic and industry researchers and supported by professional organizations, such as the Internet Engineering Task Force.

More attention should be devoted to increasing trust within I3S transactions, as well as working toward more comprehensive web security and web application standards. This will be vital as more businesses place data within cloud computing environments, including Software as a Service (SaaS), not only to quickly implement innovative business processes, but also to minimize infrastructure and security costs. In addition to secure transaction implementations (e.g., SSL and valid certificates), reasonably constrained data retention policies and practices can help foster a sense of trust in each transaction.

The Organization for the Advancement of Structured Information Standards (OASIS) is currently working on establishing technical standards for Web services such as the Web Services Security specification (http://www.oasis-open.org/committees/wss/). Many practical web security standards and processes are being developed and tested by the Open Web Application Security Project (https://www.owasp.org/). OWASP focuses specifically on improving web application security and services through various projects, such as the Enterprise Security Application Programming Interface (API) that enables developers to incorporate security into existing and new web applications.

Processes and tools such as these will enable I3S participants to achieve appropriate security standards, thereby increasing trust in transactions.

41. What are the specific areas on which education and research should focus?

To strengthen cybersecurity within the I3S it is critical to stress security education not only for the businesses working to innovate within this realm, but also for their customers. Without the ability to create secure web offerings resistant to known attack vectors (we cannot yet account for zero-day attacks), sustaining trust relationships among organizations and individuals will prove difficult. Providing practical resources and processes to secure web applications and services, as well as usable guidance for consumers, will help minimize the impact of current attacks.

Addressing the cybersecurity threat also requires developing stronger technical computer science skills in both the technical workforce and the rest of the population. This foundation must start with K-12 computer science education. Both the Computer Science Teachers Association[3] and the College Board[4] have released new frameworks for K-12 computer science education incorporating cybersecurity into the curriculum. Examples of how these frameworks are being experienced by students include: fifth graders being exposed to how technology impacts their lives (e.g., social networking, cyber-bullying, mobile computing); an introductory computer science course in high school teaching students the principles of security by examining encryption, cryptography, security threats and authentication techniques; an advanced course such as AP Computer Science; or a specialized vendor-based course on cybersecurity.

Courses built on these frameworks will not only provide students with the foundational concepts of computing but will also introduce students to potential careers in this field – including cybersecurity. These courses will have value for anyone who takes them, regardless of their future in cybersecurity. Without computer science courses, cybersecurity education will have no home within K-12 education. The pervasive and still growing presence of computing in our lives makes it unacceptable to wait until the latter stages of schooling to address these issues.

We must also increase research in the areas of web application and services security. As cloud computing initiatives grow, we must be able to rely on these services not only to run our applications but also to secure our data and ensure redundancy in case of system failure. Standard approaches to access controls can be used as starting points, but we must look to new approaches that take into account, among other things, wireless access via mobile systems.

---

[3] http://csta.acm.org/Curriculum/sub/ACMK12CSModel.html
[4] http://www.collegeboard.com/html/computerscience/index.html

Research into wireless security needs to continue as well. As more consumers move from wired to wireless access for all of their computing needs, we need to ensure that transmissions and transactions that occur over the air are indeed secure. Simply forcing use of SSL would be a good start and can help guard against session hijacking, but stronger protocols need to be developed and incorporated into mobile devices, including phones, laptops and tablet computers.

Education and security advances notwithstanding, though, it is not realistic to think that we can ever prevent any and all attacks. Therefore, we also see a need for greater research into forensic methods, especially forensics that do not degrade privacy. The methods we currently use to pursue cyber criminals are clearly insufficient, particularly as their sophistication grows.

1828 L Street Northwest, Suite 800
Washington, D.C. 20036
http://usacm.acm.org/usacm
202-659-9711 *tel*
202-667-1066 *fax*