Scoping Draft Proposed Content from Economic Incentives Working Group
Prepared for the NTIA Multistakeholder Process on Cybersecurity Vulnerabilities

Problem Statement

Vulnerability disclosure must balance a set of potentially perverse incentives.

1. For the vendor, the incentive is to ship early, with least reasonable testing. Once a vulnerability is discovered the most cost-effective response is to fail to disclose or act to prevent disclosure. With a trusted third party, vendors have both an incentive and a historical pattern of failing to remediate disclosed vulnerabilities. The easiest short-term solution is to try to suppress vulnerability discovery, and instead use the engineering and PR cycles they have to work on improving or creating new products. This leads, however, to long-term technical debt and reputational damage.
2. For those discoverer, the most profitable choice is to sell the information. This sale may be made to malicious users.
3. Consumers have no consistent way of discerning the different risks presented by different vulnerabilities. At best they can take advantage of signaling, at worst consumers not only fail to patch but also attackers use the desire to patch as a vector for infection (e.g., fake AV).
4. Law enforcement and national security interests can leverage vulnerabilities. Subversion of target assets is a powerful investigation tool.

Approaches

There is a corresponding set of possible incentives that can be leveraged with disclosure.

1. For the vendor, reliable code and a level playing field can allow organizations to distinguish themselves and the quality of their products. A more sustainable solution is to have a process to address vulnerabilities with that includes triage, management, and fixing of vulnerabilities. This solution takes ongoing engineering and PR cycles, but keeps technical debt down and protects the vendor reputation.
2. For those discoverer, an open marketplace can enable purchasing and bidding with no fear of vendor pursuit or prosecution for simple discovery.
3. Consumers can be empowered to make secure choices.
4. Law enforcement and national security, beyond the immediate investigation, defend information assets. Advanced persistent threats and the reality of a asymmetric playing field can only be addressed by a combination of enforcement and a more secure infrastructure.

But disclosure is not uniform, simple, or easy. For #2, in a marketplace, perhaps customers could commit to paying for remediation as well as for the vulnerability itself.

Sub-Components

1. Detail: What level of information is provided to different parties?
2. Duration: When is information shared?
3. Who? Scope of the sharing

4. How to keep the near term incentives from overwhelming the larger ones?
5. Dissemination of mitigation — Who is best positioned? Mobile phones a good example - perhaps the carrier?, IoT - who is providing/managing the software platform?

Reference Material

Andy Ozment, "The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting", Fourth Workshop on the Economics of Information Security, 2005, Cambridge, MA

Ashish Arora and Christopher M. Forman and Anand Nandkumar and Rahul Telang, "Competitive and Strategic Effects in the Timing of Patch Release", Fifth Workshop on the Economics of Information Security, 2006, Cambridge, UK.

Ashish Arora and Ramayya Krishnan and Anand Nandkumar and Rahul Telang and Yubao Yang, "Impact of Vulnerability Disclosure and Patch Availability – An Empirical Analysis", Third Workshop on the Economics of Information Security, 2004, Minneapolis, MN.

Ashish Arora and Ramayya Krishnan Rahul Telang and Yubao Yang, "An Empirical Analysis of Vendor Response to Disclosure Policy", Fourth Workshop on the Economics of Information Security, 2005, Cambridge, MA

Rahul Telang and Sunil Wattal, "Impact of Software Vulnerability Announcements on the Market Value of Software Vendors – an Empirical Investigation", Fourth Workshop on the Economics of Information Security, 2005, Cambridge, MA

Jay Pil Choi, Chaim Fershtman, Neil Gandal Network Security: Vulnerabilities and Disclosure Policy, WEIS 2007 - Sixth Workshop on Economics of Information Security, Pittsburgh PA, 7-8 June 2007.

Cavusoglu, H., H. Cavusoglu, S. Raghunathan (2007), "Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge," IEEE Transactions on Software Engineering, 33(3), March, pp. 171-185