DRAFT DISCUSSION DOCUMENT

NTIA Vulnerability Handling
Driving Awareness and Adoption

Problem statement:

Today, limited adoption of “best practices” for the way that technology vendors and researchers handle vulnerability disclosure results in uncertainty and distrust. This ultimately hurts consumers, whose interests are best protected when vendors and researchers cooperate to address security vulnerabilities.

Best practices for vulnerability disclosure do exist – researchers, vendors, and coordinators have worked to develop various recommended practices for more than a decade, and there are even internationally ratified ISO standards that offer guidance on vulnerability disclosure and handling. Yet adoption remains limited due to a variety of factors, including lack of awareness, lack of allocated resources, lack of customer pressure, and philosophical disagreements on approach.

To tackle this challenge, we must consider how to increase awareness and education for three primary audiences:

- Vendors, including developers, manufacturers, and service providers
- Security researchers, including professional researchers and accidental discoverers
- Technology or application consumers, particularly those that engage in large-scale procurement

Some useful background:

- ISO 29147 on vulnerability disclosure: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170
- ISO 30111 on vulnerability handling: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231
- Introduction to vulnerability disclosure and handling ISO standards: https://youtu.be/-L3DNZtK8lc
- Vulnerability Coordination Maturity Model: https://hackerone.com/vulnerability-coordination-maturity-model
- Microsoft’s vulnerability handling policy: https://technet.microsoft.com/en-us/security/dn467923.aspx
- Facebook’s vulnerability handling policy: https://www.facebook.com/whitehat/
- GE’s vulnerability handling policy: http://www.ge.com/security
- HP Zero Day Initiative vulnerability disclosure policy: http://www.zerodayinitiative.com/advisories/disclosure_policy/
- Rapid7’s vulnerability disclosure policy: https://www.rapid7.com/disclosure.jsp
- Some links on the history of the vulnerability handling debate:
    - RFPolicy from 2000: https://dl.packetstormsecurity.net/papers/general/rfpolicy-2.0.txt
    - IETF draft on disclosure from 2002: https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00
    - https://www.ee.oulu.fi/research/ouspg/Disclosure_tracking

Approaches to addressing the problem:

1) Getting agreement on and setting expectations around what wanted outcomes of broad adoption of vulnerability handling best practices are (e.g., agreeing that vulnerability research is a valuable part of securing the ecosystem)
2) Identifying the common best practices and standards that we want to see adopted; clarifying and addressing any limitations there may be around those best practices and standards
    a. For example, ISO 29147 and 30111 are quite complex and cost money, and participation in ISO standards development must be through a national body (like NIST) or special liaison (like FIRST), unlike broad multi-stakeholder processes
        i. One way to address the complexity would be to develop a simplified overview of the ISO standards, helping businesses to address the main points of a vulnerability disclosure process and program (i.e. way to receive reports, policy on response, policy on remediation, and policy on notifying affected consumers)
    b. For example, corporate best practices differ, resulting in ambiguity and disagreement
3) Delineating and describing the barriers to adoption for researchers
4) Delineating and describing the barriers to adoption for technology providers, some of which include:
    a. Lack of awareness
        i. Of the need for vulnerability disclosure processes
        ii. Of the best practices for vulnerability disclosure
    b. Lack of consumer demand
        i. Open question: focus on enterprise and government consumers only or also on broader public?
    c. Ambiguity among best practices and standards
    d. Lack of resources (e.g. new players focused on building products or services don’t prioritize maintenance/bug fixing)
    e. Supply chain responsibility confusion (i.e. those that are leveraging third party products and services and receive vuln reports for those products or services don’t know what to do with them)
    f. Cultural barriers (e.g. manufacturers new to vuln disclosure may have a longstanding culture of secrecy)
5) Delineating and describing the barriers to awareness (i.e. productive media coverage)
6) Outlining roles that various actors might play in driving awareness and adoption; some potential actors with a role include:
    a. Government agencies (e.g. NIST, FTC, FDA, DHS, DOT-NHTSA, Treasury, FBI/InfraGard, DOJ)
    b. Industry organizations (e.g. ISACs, US Chamber, standards organizations like IETF/W3C, ICASI)
    c. Civil Society (e.g. EFF, CDT, OTI)
    d. Mature enterprises
        i. Educational programs for new vendors
        ii. Publishing data around the cost proposition/value add of having a mature process to receive vulns, feed learnings back into SDL
        iii. Attracting and motivating security researchers (could tie to bug bounties, gamified leadership boards)
    e. Mature researchers
        i. Need positive examples to flow to new researchers (i.e. how to clearly communicate finding and its severity without seeming threatening to vendors;

how to research without improperly accessing data; how to protect your findings)

      ii. Could promote cooperation, grandstand on defensive capability (i.e. Tesla partner with researcher on a live demo OTA update)

   f. CERT/CC – plays an important role in mediating between vendors and researchers when vendors are unreachable, don't understand researchers, or don't exist anymore; ultimately wants out of role, but currently tries to lead by example in cases that pose novel issues

   g. Managed PSIRT/bounty providers (e.g. HackerOne)

      i. Offers disclosure assistance, including to those not offering bounties (i.e. don't want details of vuln but can help locate appropriate contact)

   h. Academia and educators

7) Assisting researchers and vendors in identifying/understanding each other's perspectives

   a. Vendors should consider their frustration when their customers get compromised through a vulnerability in an upstream component, especially when that upstream component may or may not be responsive in providing timely fixes. To researchers, vendors are that upstream provider creating a vulnerability for their organization or for them personally.

   b. Researchers should consider how difficult it is for vendors to prioritize security fixes over other requirements and over other researchers' findings in their queue. Fixing code that's already been written is rarely the highest priority for programmers or vendors. With that in mind, clearly communicating and demonstrating a vulnerability's risk is helpful to vendors, especially when they're unfamiliar with reporters and regularly receive lots of submissions, creating a lot of noise.

Open questions to resolve re addressing the problem:

- How do we effectively engage those (listed above) that have a role to play in the spreading of awareness and adoption, and how do we encourage them to participate?
- Are there particular sectors on which it might be important or valuable for us to focus?
    - If so, what organizations within those sectors? And what's our outreach plan to engage with those sectors/organizations?
- What impact, if any, does the emergence of "cyber safety" issues have? Does it create an opportunity for broader awareness and adoption? If so, how do we execute on it?
- How do we evaluate the state of vulnerability disclosure and how do we measure progress?

Milestones toward a solution:

1) Discuss with the Economic Incentives WG the possibility of linking our work streams, as incentivizing behaviors that represent agreed-upon best practices is a practical next step
2) Discuss with the Safety Industry WG the possibility of linking our work streams, as companies from and researchers focusing on safety industry verticals are key audiences for increasing awareness and adoption of best practices
3) Issue questionnaire to gain insight into state of vulnerability disclosure program adoption
4) Agreement on problem statement
5) Agreement on the best practices and standards that we want to promote
6) Agreement on audience (i.e., who needs more/different kinds of exposure to existing standards and best practices?)
7) Agreement on and development of materials necessary to provide needed resources (i.e. organizational contacts for disclosure); to document/explain existing standards and best practices; and to support the spreading of awareness and adoption

8) Agreement on approach to and venues/forums for promoting developed resources as well as existing standards and best practices
9) Development of an outreach plan (i.e. what audiences, what venues)
10) Secure engagement and commitment of adoption by third parties
11) Implementation of a process to track and evaluate success of the materials and the impact on the vulnerability disclosure ecosystem