Toward the development of industry standards for security vulnerability handling

Background

- Industry convergence around the need to develop and institutionalize a code of conduct for responsible handling of security vulnerabilities
  - SafeNet 2000: working group to develop guiding principles for security professionals
  - Other influentials throughout the industry have noted the need for standardized, broadly-embraced processes.
- Several conference participants have taken the initiative to begin the process of developing standards
  - @stake
  - Bindview
  - Foundstone
  - Guardent
  - Internet Security Systems
  - Microsoft
  - More to follow
- Will form an organization to drive this effort forward

Long-term Objectives

- Develop industry standards for handling security vulnerabilities
  - Comprehensive
    - Encompass all parties and activities in the vulnerability handling process
  - Collaborative
    - Define a framework through which all parties can work effectively and collegially to protect users from harm
  - Broadly accepted
    - Embraced by a critical mass within the industry
- Plan:
  - Proposed standard to be developed by members
  - Submitted for ratification by associate members
  - Made available for review by the general public as part of RFC process

Near-term Objectives

- Adopt several specific practices even as we pursue our long-term goals
  - Immediately bolster security
  - Demonstrate the feasibility of these practices
- Members commit themselves to:
  - Report and address security vulnerabilities thoroughly and expeditiously
  - Observe a grace period before disclosing details of exploiting newly-announced security vulnerabilities.
  - Exercise due diligence when developing security tools, to limit their use to only lawful purposes

Reporting and Addressing Vulnerabilities

- Purpose: To assure that vulnerability reports are given appropriate weight and proper steps are taken to protect customers as quickly as possible.
  - Members who discover vulnerabilities will inform the vendor in a timely and thorough manner
  - Members whose products are the subject of a report will immediately acknowledge receipt, investigate it thoroughly and expeditiously, and provide timely status updates to the discoverer.
  - Members' security advisories will provide detailed information that lets users understand the vulnerability, the risk it poses and whether it affects them, and how to defend against it. Members will use best efforts not to disclose details that can be directly used to exploit the vulnerability.

Grace Period

- Purpose: Give users a reasonable interval during which to protect their systems against newly reported vulnerabilities
  - Begins with public notice of vulnerability, and lasts for 30 days
  - Is immediately curtailed if vulnerability becomes actively exploited
- During grace period, members will exercise best efforts to avoid disclosing details that can be directly used to exploit the vulnerability
- Does not apply to sharing information with responsible parties such as:
  - Law enforcement authorities
  - Recognized infrastructure protection organizations
  - Other communities in which enforceable frameworks exist to deter onward uncontrolled distribution
- After expiration of the grace period, members may release additional details of the vulnerability.

Security Tools

- Purpose: Take reasonable steps to ensure that vulnerability demonstration and security assessment tools can only be used for lawful purposes.
- Members will limit tools' use via one or more of the following measures:
  - Non-invasive assessment techniques
    - E.g., scan for vulnerability using techniques that do not involve exploiting it.
  - Run-time restrictions
    - E.g., require the user to have administrative privileges on the target system before running or scan only limited IP addresses.
  - Limited distribution channels
    - E.g., distribute tools only within communities in which enforceable frameworks exist to deter onward uncontrolled distribution

Proposed Organizational Framework

- Members
  - Industry-leading companies who are actively engaged in security research and network defense, and leading software vendors.
  - Will draft proposed standards and commit people and resources to driving the effort forward
- Associate Members
  - Influential vendors and organizations within the security community who support the goals of the organization
  - Will ratify Members' proposed standard before it is submitted to the formal process
- Advisory Board
  - Influential customers of the security community who support the goals of the organization
  - Will provide guidance and feedback to Members and Associate Members

Next Steps

- Solicit additional participation
- Draft bylaws and establish procedures
- Develop a web presence to provide information about our status and progress
- Select topics for initial standards work and develop timelines for deliverables