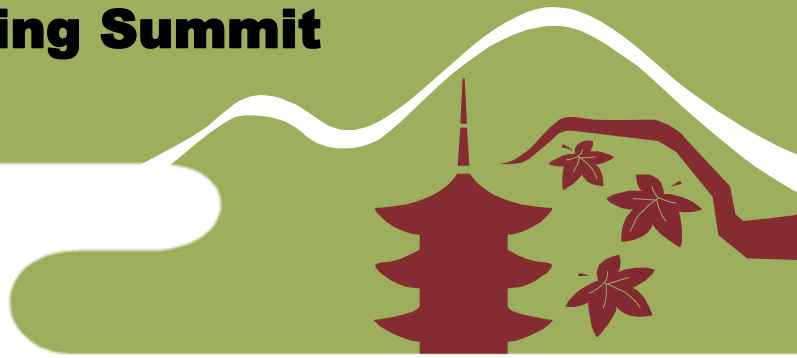


Summit Days

Proposal of FIRST SIG planning "Vulnerability Reporting and Data eXchange"

November 15, 2012

Masato Terada

first sig(special interest groups).

Special Interest Groups (SIGs)

Special Interest Groups exist to provide a forum where FIRST Members can discuss topics of common interest to the Incident Response community. A SIG is a group of individuals composed of FIRST Members and invited parties, typically coming together to explore an area of interest or specific technology area, with a goal of collaborating and sharing expertise and experiences to address common challenges.

Special Interest Groups define their own missions and goals, and serve as a forum of the FIRST Members to discuss technologies, challenges and solutions in specific areas of mutual interest, including hearing relevant presentations from SIG participants and Invited Guests. SIG meetings are free to build their own meeting schedule but are also encouraged to co-locate meetings with FIRST Conferences, Technical Colloquia or other events.

SIGs can generate papers and publications for the industry covering their area of interest. While these papers and publications shall be distributed by the FIRST, they do not represent the official position of the FIRST members, or the FIRST itself.

FIRST Members who are interested in forming a new SIG should fill out the form and submit to the FIRST Secretariat at first-sec@first.org

first sig(special interest groups).

- **Framework for FIRST Special Interest Groups**
  http://www.first.org/global/sigs/framework
- **Charter process**

  A Motion to Charter a Special Interest Group is only in order at a FIRST SC meeting if all supporting background information and Proposed Charter are on the agenda and published to all SC members two or more weeks before the SC meeting. A SIG is chartered by a 2/3 majority vote of the FIRST SC in accordance with the FIRST Operational Framework.
  [In order to allow the charter process to move along smoothly, SB(SIG Board) members are allocated to liaison roles with the active SIGs and FIRST SC. This is a relationship to ensure that there's a SB member to whom members of the group can turn for SIG Charter related advice.]

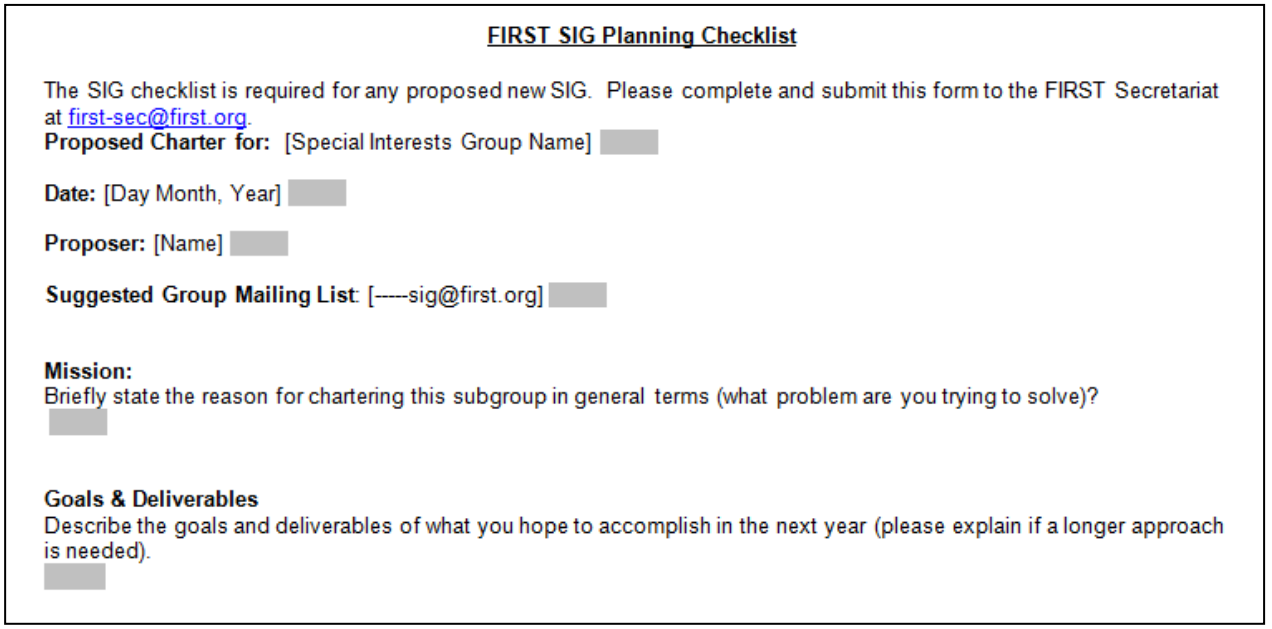
first sig(special interest groups).

- FIRST SIG Startup process
  http://www.first.org/global/sigs

  - Make a FIRST SIG Planning Checklist
  - Initial members fixed
  - Send first-sec@first.org

first sig(special interest groups).

- FIRST Members who are interested in forming a new SIG should fill out the form and submit to the FIRST Secretariat at first-sec@first.org



FIRST SIG Planning Checklist

The SIG checklist is required for any proposed new SIG. Please complete and submit this form to the FIRST Secretariat at first-sec@first.org.

Proposed Charter for: [Special Interests Group Name]

Date: [Day Month, Year]

Proposer: [Name]

Suggested Group Mailing List: [-----sig@first.org]

Mission:
Briefly state the reason for chartering this subgroup in general terms (what problem are you trying to solve)?

Goals & Deliverables
Describe the goals and deliverables of what you hope to accomplish in the next year (please explain if a longer approach is needed).

vrdx-sig; first sig planning checklist(draft) proposer.

sig-checklist-ccveR2d
(16:35 2012/11/13)

FIRST SIG Planning Checklist

The SIG checklist is required for any proposed new SIG. Please complete and submit this form to the FIRST Secretariat at first-sec@first.org.

Proposed Charter for: Vulnerability Reporting and Data eXchange SIG (VRDX-SIG)

Date: [Day Month, Year]

---

xx May 2013

Proposer: [Name]

Masato Terada, Sugurau Yamaguchi, Art Manion

vrdx-sig; first sig planning checklist(draft) group mailing list, mission.

Suggested Group Mailing List: [-----sig@first.org]

---

vrdx-sig@first.org

Mission:

Briefly state the reason for chartering this subgroup in general terms (what problem are you trying to solve)?

VRDX-SIG is primarily chartered to research and recommend ways to identify and exchange vulnerability information across disparate vulnerability databases.

Vulnerability databases have different scopes, identification, data schemes, data feeds and supporting languages. These differences lead to difficulty responding to vulnerability reports. By studying existing practices, the SIG seeks to develop recommendations on how to better identify, track, and exchange vulnerability information across disparate vulnerability databases.

vrdx-sig; first sig planning checklist(draft) goals & deliverables.

Goals & Deliverables

Describe the goals and deliverables of what you hope to accomplish in the next year (please explain if a longer approach is needed).

In the initial two year charter, the SIG plans to accomplish three overall tasks.

1. Review of existing vulnerability identification schemes and exchange/feed formats, including features and issues
   - Regional/national vulnerability databases/reporting frameworks
   - Non-government vulnerability databases
   - Product vendor vulnerability databases (include vendor advisories)
   - Emerging vulnerability reporting domains such as mobile devices, industrial control systems, and vehicles

2. Report covering identified issues in existing work

vrdx-sig; first sig planning checklist(draft) goals & deliverables(cont.).

3. Document of best practice/requirements for a vulnerability identification and exchange scheme

- Requirements for a global ID system?
- Requirements for a best practice system, could be regional/local?
- for a global ID system
- best practice for vulnerability ID, regional/local vulnerability DB
- best practice for vulnerability handling framework
- Reference list of related works such as vxref, SCAP, CYBEX, JVN, continuous monitoring, and draft-booth-sacm-vuln-model-00

This work supports more comprehensive vulnerability reporting, coordination, and disclosure frameworks, however the initial scope of the SIG is limited to identification, tracking, and exchange of vulnerability information.

vxref: Specification for how to relate one vulnerability repository to another (federation)
SCAP: Interoperable specifications which include CVE, CVSS and others
CYBEX: ITU-T standard specifications
Continuous monitoring: Process and technology to detect compliance and risk issues
draft-booth-sacm-vuln-model-00: NIST Software Vulnerability Data Model and Data Exchange Format

vrdx-sig; first sig planning checklist(draft) chairperson, initial members.

Initial Chairperson(s):

Chairperson and Team Affiliation (needs to be a FIRST member or liaison)

Art Manion, CERT Coordination Center

Initial Members:

Please list anyone that has shown interest in participating and their email

---

vrdx-sig; first sig planning checklist(draft) member expectations, budget.

Member Expectations:

Briefly state the expectation for the SIG participants including requirements for participation, deliveries or activity

---

Participate in a reasonable number of meetings, contribute to offered/assigned tasks, perhaps 1 hour/week. Mailing list discussion, document drafting/editing, moderate research into existing vulnerability identification systems, conference/video calls (perhaps monthly).

Budget

Please list anything that may require funding and the Secretariat will help estimate the budget prior to submitting to the CFO. Consider needs such as: meeting space at the conference, travel, and any infrastructure (see below).

Infrastructure (see below), meeting space at annual conference (estimate half-day room with projector, 20 people), possible meeting space at TCs.

vrdx-sig; first sig planning checklist(draft) infrastructure, meeting detail.

Infrastructure

In addition to a mail list, will you use the Wiki, Yammer, phone bridge/WebEx, etc.? If a SIG member can sponsor the phone bridge that is preferred.

Possibly email list, definitely Wiki. CERT/CC can probably sponsor conference calls. Does FIRST have a task tracking service (like JIRA or Trac?)

Meetings Detail

Please provide tentative schedule or frequency (monthly, quarterly etc) of in person meeting or conference calls.

Possibly monthly conference calls.

vrdx-sig; first sig planning checklist(draft) estimated milestones/schedule.

Other comments:

Estimated Milestones/Schedule

- Jun 2013
  - In-person meeting at FIRST annual conference in Bangkok

vrdx-sig; first sig planning checklist(draft) estimated milestones/schedule(cont.).

- Jul 2013- (4months)
  - Review of existing vulnerability identification schemes
  - Regional/national vulnerability databases/reporting frameworks

    ex.
    - Japan: JVN/JVN iPedia, Information Security Early Warning Partnership
    - USA: CVE/NVD (US) Ecosystem
    - China: CNVD
  - Review of vulnerability identification activities in new domains

vrdx-sig; first sig planning checklist(draft) estimated milestones/schedule(cont.).

- Nov 2013- (4months)
  - Review of existing vulnerability identification schemes
  - Non-government vulnerability databases
    ex.
    - SecurityFocus, IBM ISS X-Force, OSVDB, Secunia, Cisco

- Feb 2014- (3months)
  - Review of existing vulnerability identification schemes
  - Product vendor vulnerability databases (include vendor advisories)
    ex.
    - Microsoft, Oracle, Cisco, Adobe etc.

vrdx-sig; first sig planning checklist(draft) estimated milestones/schedule(cont.).

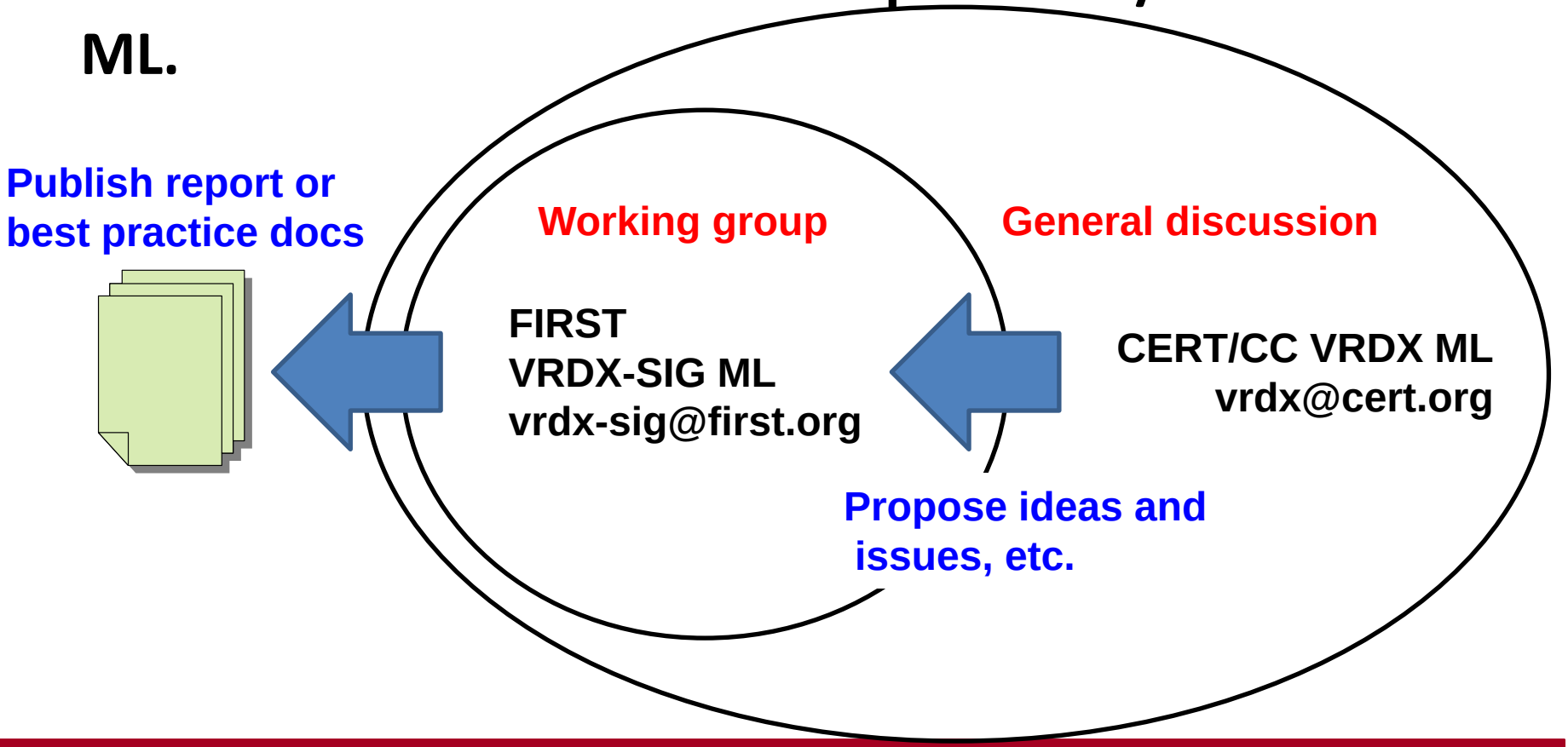
- Jun 2014
  - 2nd meeting at FIRST annual conference
- Jul 2014- (5 months)
  - Report covering identified issues in existing work
  - Review of vulnerability identification activities in new domains

vrdx-sig; first sig planning checklist(draft) estimated milestones/schedule(cont.).

- Dec 2014- (6 months)
  - Document of best practice/requirements for a vulnerability identification and exchange scheme
- Jun 2015
  - 3rd meeting at FIRST annual conference (The initial charter is closed.)

vrdx-sig; first sig planning checklist(draft) relationship to existing work.

- VRDX-SIG will have relationship to CERT/CC VRDX ML.



vrdx-sig activities startup plan.

- Nov 2012
  - Announcement of VRDX ML@CERT/CC for general discussion (art)
- Nov 2012
  - Fixed Initial members of VRDX-SIG (masato & art)
  - Fixed FIRST SIG Planning Checklist (masato & art)
- Nov or Dec 2012 (deadline Dec 20)
  - Submit FIRST SIG Planning Checklist to FIRST sec (masato)
- Jan 2013
  - FIRST SC (face to face meeting)
- Jun 2013
  - Next summit Days (FIRST SIG VRDX-SIG members + CERT/CC VRDX members) at FIRST annual conference in Bangkok

About FIRST TC @ Kyoto Summit Days

Future of Global Vulnerability Reporting Summit

Future of Global Vulnerability Reporting Summit focuses on Current challenges & issues (coverage, scale, numbering and etc.) and proposed solutions of vulnerability tracking, especially "Global Vulnerability Identification Scheme".

Currently one of the most well known vulnerability identification schemes is Common Vulnerabilities and Exposures (CVE). CVE is used by many organizations throughout the world for cross-referencing vulnerabilities across various databases. However, the current process governing CVE has its limitations and has not been able to keep up with the ever increasing number of vulnerabilities being discovered and made public each year. At first, we would like to discuss the limitations of the current process, and how organizations currently use CVE to link their databases across the globe to for cross-referencing vulnerabilities. Second, we would like to discuss the next steps for challenge of "Global Vulnerability Identification Scheme" on the final day.