Internal Security Policies

Proposal for Work Item and Roadmap

Marcel Winandy (Huawei)

Areas of Interest for Int. Sec. Policy

Areas of Interest for Int. Sec. Policy

OPNFV Security Group

Project Work Areas

OPNFV Security Vulnerability Management (OSVM) → Normative Rules ?

Documentation

Internal Security Policies

Secure Coding Guidelines

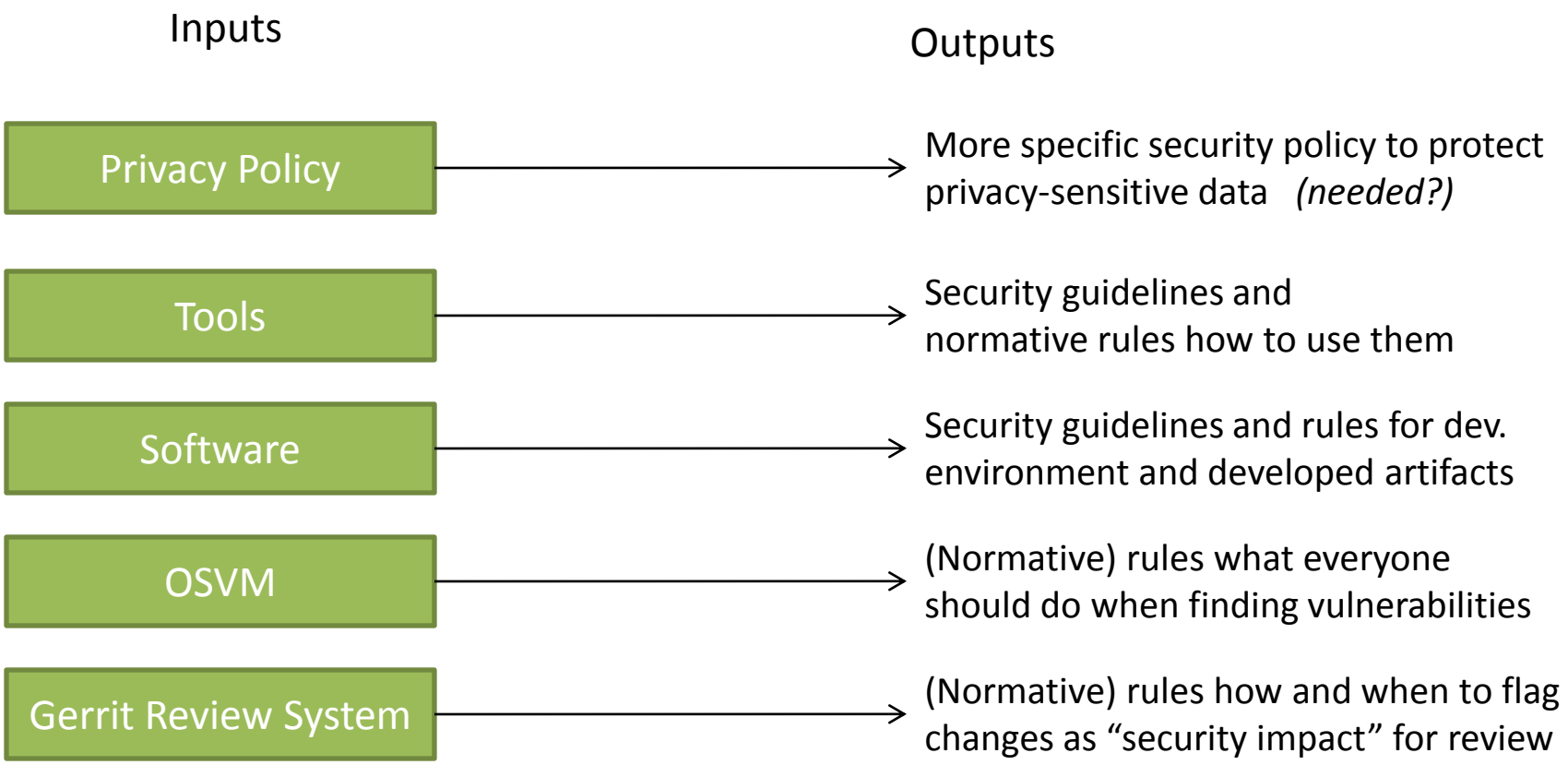
Upstream collaboration

Gerrit Review System → Normative Rules ?

Research Projects

Development Projects

Work Item Breakdown



Example: OPNFV Privacy Policy

What information OPNFV collects

OPNFV may collect two types of information from users of Sites: "personally identifiable information" (such as name, email address, postal address, telephone, birth date) and "aggregate information" (such as frequency of visits to Sites, IP address, Site pages most frequently accessed, browser type).

SECURITY

To prevent unauthorized access or disclosure, maintain data accuracy, and ensure the appropriate use of information, OPNFV implements physical, electronic, and managerial procedures to safeguard and secure the information OPNFV collects. OPNFV uses encryption when collecting or transferring sensitive personally identifiable information. However, OPNFV does not guarantee that unauthorized third parties will never defeat measures taken to prevent improper use of personally identifiable information.

Internal OPNFV access to users' nonpublic personally identifiable information is restricted to OPNFV's administrators and individuals on a need-to-know basis. These individuals are bound by confidentiality agreements.

User passwords are keys to accounts. Use unique numbers, letters, and special characters for passwords and do not disclose passwords to other people in order to prevent loss of account control. Users are responsible for all actions taken in their accounts. Notify OPNFV of any password compromises, and change passwords periodically to maintain account protection.

Structure of Int. Sec. Policy

Two main parts:

- **Defining security rules and guidelines when creating artifacts (development environment)**
  - Development and testing environment of opnfv infrastructure, how developers should take care of their environments, passwords, reporting security issues, etc.
  - Related to: Privacy Policy, Tools, OVSM, Gerrit Review System
  - Examples:
    - WebKit Security Policy https://www.webkit.org/security/
      (defines how to report security bugs, how to join security group, privileges and responsibilities, etc.)
    - Xen Security Policy http://www.xenproject.org/security-policy.html
      (defines how to report vulnerabilities and handle pre-disclosure information)
    - Symfony Security Policy http://symfony.com/doc/current/contributing/code/security.html
      (defines how to report and resolve security issues when contributing code)
- **Defining security rules and guidelines how to create artifacts (developed software)**
  - Best practices to include in the development of modules, configurations, documentation etc., e.g., "use secure default config options“, “avoid dangerous input parsing libraries”
  - Definition of security functionality need in OPNFV (IDS, Certificates/PKI, VMM security, etc.)
  - Related to: Software
  - Examples:
    - https://github.com/openstack-security/Developer-Guidance

Work Item Activities / Roadmap

- Privacy Policy:
  - Check whether we need to define additional security policy rules how to protect privacy-sensitive data
- Tools:
  - Check whether we need to define security policy rules for using these tools, or reference to their security guidelines
- Software:
  - General guidelines, e.g., using secure channels, secure by default
  - Component-specific guidelines
    - Traversing through the architectural components / projects
    - Gather security critical aspects and requirements
    - Define security guidelines (identify general and specific issues)
  - Identify missing and cross-cutting aspects (e.g. security monitoring)
  - Architectural aspects of opnfv security
- OSVM:
  - Take output of this work item and identify aspects to be defined as rules for everyone
- Gerrit Review System:
  - Take output of this work item and identify aspects to be defined as rules for everyone