Proposed ARC 20 questions

Oct. 21, 2008
Rick Matthews

The 20 questions outline serves several purposes. One is to present to the ARC in a uniform manner pertinent information about any case. Many of the answers to these questions can be direct and specific references to other case materials (although care must be taken to keep the references current). A second purpose is to allow an ARC member to get a concise overview of the case in an efficient manner. Another purpose is that the 20 questions should provoke thought and questions for project teams unfamiliar with the ARC process, by asking questions about aspects of the project that need be considered. Lastly, the 20 questions serves as a vehicle between the case owner and the project team as an indicator of preparedness. The 20 questions, as do other ARC materials, remain as documentation of the case plan of record.

1. What is the proposal being presented for review?
   - Give an overview of the project and its phase(s).
   - Describe the exposure (OpenSolaris), scope and type of review desired (overview, full case, etc.)
   - Indicate the release binding requested by the project team.
     See: http://www.opensolaris.org/os/community/arc/policies/release-taxonomy/
   - What are the project's deliverables?
   - How does this project align with existing or proposed ARC cases?

2. Describe user interactions.
   - Are new user interfaces being proposed, or existing interfaces being changed?
   - Explain the similarities in proposed interfaces with existing OS user interfaces (Solaris, Linux, Windows, etc.).
   - Are there any install time changes?

3. What are the imported (consumed by the project) and exported (exposed by the project) interfaces or protocols and their respective stability levels?
   - Is there a versioning scheme in place?
   - Has the team secured interface contracts where necessary?
   - Use an ARC prescribed interface table format.

   See: http://www.opensolaris.org/os/community/arc/policies/interface-taxonomy/

4. Describe any dependencies on hardware (e.g. SPARC exclusive), and on other projects within Solaris.

5. Projects need to be aware of the overall security of the system and how their components affect it. Which parts of this project are critical to the security of the system to avoid such unintended consequences such as unauthorized system entry, unauthorized access to or modification of data, elevation of privilege, denial of service, ...? Does this project require elevated privilege?

   A number of specific policies and practices address various aspects of the security of the system. They are found in appendix 1. Which of these are applicable to this project, and how are they addressed?

6. Describe means of observing project functionality and performance, by an end user or by a system administrator.

7. How does the project deal with faults and interruptions? Initialization and restarting?

8. How does the project interact with Solaris virtualization technologies (xVM, LDOMs, zones, SunCluster, etc.)?

9. Does this project require administration (i.e., configuration or management)? If so,
    - How is the project administered, and what sort of review process has this user interface undergone?
    - Is there a means of aggregating management and/or configuration with other related projects?
    - Does this project deliver its own administration along with the other components, or is this project an administration interface for other projects?
    - Are there any external (to Solaris) management interfaces to consider, or being consumed?

    Projects that require or deliver administrative interfaces are often by their nature security components of the system and should likely address the security question (#5 above, with attention to RBAC and Audit). (See also appendix 2).

10. Have you reviewed the Policies and Best Practices? Are there any exceptions this project needs? (See appendix 3).

Appendix 1. Security references

Plugable Authentication Modules
http://opensolaris.org/os/community/arc/policies/PAM/
Audit Policy
http://opensolaris.org/os/community/arc/policies/audit-policy/
Service Management Facility (SMF) usage
http://opensolaris.org/os/community/arc/policies/SMF-policy/
Install-Time Security
http://opensolaris.org/os/community/arc/policies/ITS/
Network Install-Time Security
http://opensolaris.org/os/community/arc/policies/NITS-policy/
Secure - by - Default
http://opensolaris.org/os/community/arc/policies/secure-by-default/
When to use setuid -vs - RBAC roles and profiles
http://opensolaris.org/os/community/arc/bestpractices/rbac-intro/
Building RBAC Rights Profiles
http://opensolaris.org/os/community/arc/bestpractices/rbac-profiles/
Adding RBAC Authorizations
http://opensolaris.org/os/community/arc/bestpractices/rbac-auths/
Reusable Passwords in Command Line Arguments and Environment Variables
http://opensolaris.org/os/community/arc/bestpractices/passwords-cli/
Storing Reusable Passwords on a FileSystem
http://opensolaris.org/os/community/arc/bestpractices/passwords-files/
Administrative and Security Precedents and Policies
http://opensolaris.org/os/community/arc/bestpractices/overview-admin-security/
Security Questions

http://opensolaris.org/os/community/arc/bestpractices/security-questions/

Appendix 2. Administrative access and control

RBAC (Role Based Access Control):

See PSARC/1997/332 Execution Profiles for Restricted Environments

http://opensolaris.org/os/community/arc/caselog/1997/332

Privilege:

See PSARC/2002/188 Least Privilege for Solaris

http://opensolaris.org/os/community/arc/caselog/2002/188

Appendix 3. Policies and Best Practices references

http://www.opensolaris.org/os/community/arc/policies/

http://www.opensolaris.org/os/community/arc/bestpractices/