SOFTWARE SECURITY WORKING TEAM
PROGRESS & NEXT STEPS

ESGF F2F Workshop,
San Francisco, December 2017

<< George Rumney - Working Team Lead >>

2016 F2F – SSWT Findings

- Software Security is currently reactive and not built into the fundamental design process.
- The highest priority is to perform a risk assessment of the existing code base.
- Form a software engineering/security team that has physical/technical/security insight into the core ESGF components.
- Document the core ESGF modules - generate a current software manifest, architecture, and concept of operations. Freeze if at all possible all work other than patching on these core modules.
- Create a risk assessment of these modules, their use, their interactions, interfaces, etc. and submit to the XC.
- The XC should have the resources of an experienced Risk Executive available to assist in evaluation of the risk assessment report - as required by the ESGF-SSWT security plan. The XC with Risk Executive input shall then direct the ESGF Software Development Team to allocate resources to address the identified risks. ESGF sites shall have access to the risk assessment and XC Risk Executive review in order to perform their own risk mitigations, as necessary.

2016-2017 Progress & Accomplishments

- Current Software security plan was approved by the XC, April 2016
- Software release process was established, with emphasis on scanning - code and live services
- Process includes: Source code scans, Live web scans, & Configuration reviews
- JAR file “scanner” was created by Zed but is manually intensive (due to false positives)
- Risk-based process, the intention of which is to avoid issuing a release with elevated risk (to avoid a repeat of something similar to the June 2015 “Apache Struts” incident)
- We are better able to detect such issues in advance, but risks remain (e.g., Solr), both in the Code base and in the procedures
- Membership in SSWT was established (esgf-sswt@llnl.gov)

2017 Missed Milestones (if any)

Software Security Plan requirements:

- ESGF Risk Executive not yet identified (ref: NIST SP 800-39)
- Software Development Team and Security Team not yet integrated to coordinate ESGF software design
- Manifest of software remains incomplete for third-party software
- *Security is not yet fully a part of the software engineering process.*

Shortfalls

- Installation is still cumbersome and fragile (monolithic and prone to failure)
- The large ESG software footprint is challenging efforts for risk reduction
- Included software (e.g. Tomcat…) makes patching challenging
- The lack of a modular build process (modularity would increase maintainability and enhance local site control)

2017-2018 Roadmap

SSWT plans to:

- Support integration of Software Development Team with Software Security Team efforts (requirements baseline, alternatives analysis, requirements for future releases, etc.)
- Maintain and enhance the software manifest of installed components
- Implement Federal requirements: SSL & IPV6
- Implement SELinux (enforcing mode is being required by NASA)
- Support establishment of the ESGF Risk Executive
- Perform vulnerability determination and risk assessment for future releases
- Support software engineering efforts to reduce risk, increase maintainability
- Define best practices for site installations (e.g., local firewall rules)

Additional Resources Needed

- SSWT supports the allocation of resources for the re-design and re-implementation of the install process;
- Other sites contribution (e.g., JPL, NOAA) will be required to aid scanning efforts, both source code base and live web scans;
- ESGF Risk Executive reviews (most resources will come from the ESGF-SSWT), as needed;
- SSWT team members' contribution to define best practices, as needed.
- Licenses for source code scanning ($$$).

Collaborations Needed

- SSWT collaboration with other ESGF working teams
  - Software Development Team
  - Risk Executive
  - Executive Committee
  - Regular team meetings
- Collaboration with ESGF sites (perform scans, risk assessments, best practices)
- Collaboration with outside entities
  - None