Autonomic Security Compliance Framework
Cihan Tunc, Salim Hariri, and Fabian De La Peña Montero

Background and Problem
- DFARS – Defense Federal Acquisition Regulation Supplement
  - DoD-specific acquisition regulations
  - Contractors to implement NIST SP 800-171 standards no later than December 31, 2017.

Objectives
- Security compliance techniques are
  - Manual and labor intensive
  - Not flexible for complexity, dynamism, and heterogeneity
  - Infeasible to create an organization boundary (defendable perimeter)
  - Malicious attacks (both insider and outsiders)
- NIST SP-800-171: “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”
- Goal: Autonomic security compliance
  - Continuously monitor computers, systems, devices, applications, etc. of each supplier
  - Check if compliance requirements are met based on NIST-SP-800-171
  - Create a compliance report and report the critical issues
  - Provide a suggestion list to fix the problems and/or automated/semi-automated actions to fix

Overall Approach
- Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- NIST SP 800-171

Supply Chain Management
- Autonomic Security Compliance Engine

Development Approach
- NIST SP 800-171
- Company Policy
- Compliance Report
- Critical Issues

Reporting
- Company Compliance Configuration Report
- Compliance Report
- Critical Issues

NIST SP 800-171 Requirements and Solutions
3.1.6 – Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
  - Script name: check_open_ports_SP800_171_3.1.6
  - It uses a given authorized port list to check and compare open ports
  - If any unauthorized ports exist, it gives a critical error to the admin.

3.1.8 – Limit unsuccessful logon attempts.
  - Script name: check_login_attempts_SP800_171_3.1.8
  - Checks the auth.log for number of unsuccessful attempts

3.1.8 – Limit unsuccessful logon attempts.
  - Script name: check_ssh_login_attempt_limit_SP800_171_3.1.8
  - Checks the SSH configuration for the limitation of login attempts
  - Also checks if the found login attempts is below the threshold or not.

3.1.11 – Terminate (automatically) a user session after a defined cond.
  - Script name: check_created_accounts_SP800_171_3.1.11
  - Checks the created accounts
  - Uses a given argument to detect if there is any unauthorized created accounts; if yes, gives critical warning (error)
  - It can also include a list of service accounts

For each system, it checks the individual security control and provides overall information

Detailed information for each security control is reported

For each system, it checks the individual security control and provides overall information

Detailed information for each security control is reported

For each system, it checks the individual security control and provides overall information

Detailed information for each security control is reported