RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Measurement as a Key to Confidence: Providing Assurance

SESSION ID: GRC-R02

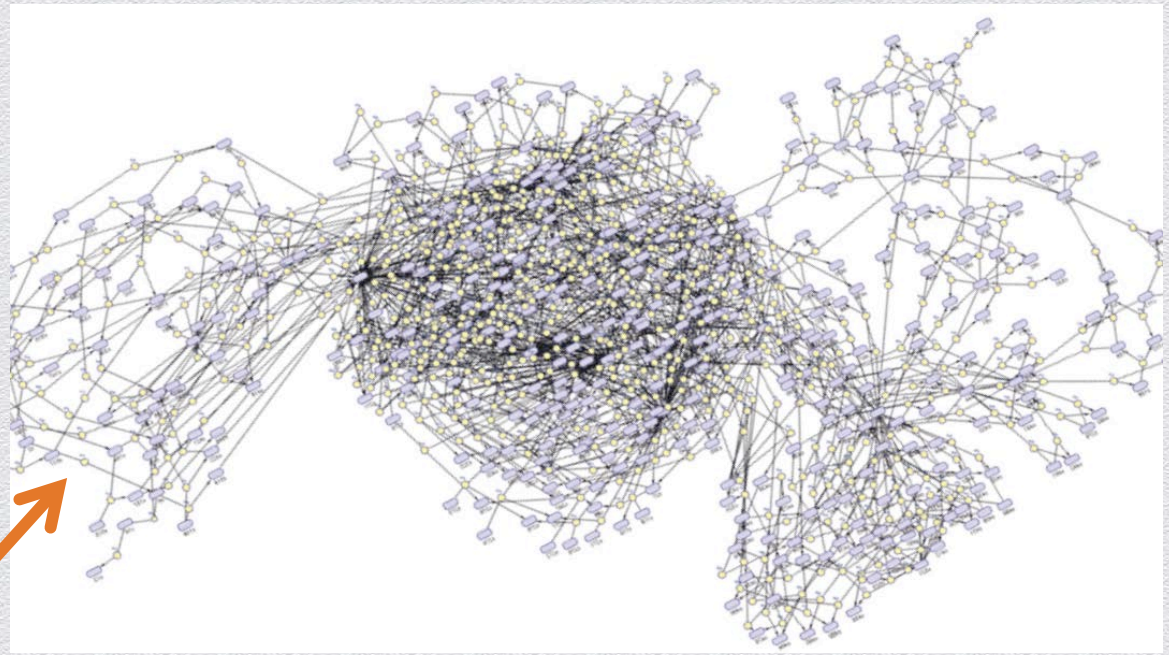
Moderator: Dan Reddy (CISSP, CSSLP)
Sr. Consultant Product Manager, EMC Corp, Product Security Office
@danlj28

Panelists: Sally Long
Director , The Open Group / Trusted Technology Forum

Robert Martin
Senior Principal Engineer, MITRE

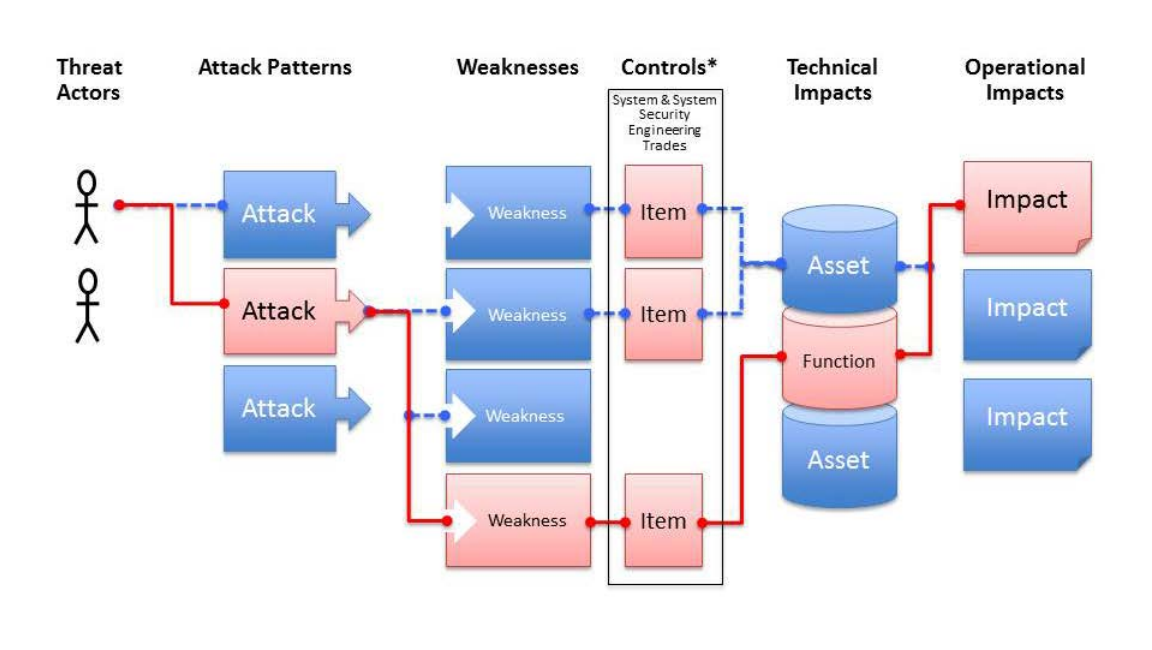
Ron Ross
Fellow at the National Institute of Standards and Technology (NIST)

Helmut Kurth
Chief Scientist & Laboratory Director, atsec



Others Need to Understand Your Assurance Work

When this other system gets subverted through an un-patched vulnerability, a mis-configuration, or an application weakness…



What is the Risk to the Business based on Operation of the System?

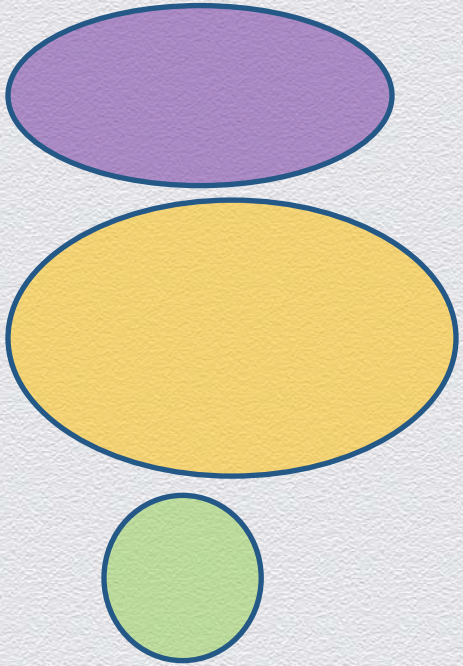
Controls include architecture and design choices, added security functions, activities & processes physical decomposition choices, code assessments, design reviews, dynamic and pen testing

Technical Impact	Automated Analysis	Automated Dynamic Analysis	Automated Static Analysis	Black Box	Fuzzing	Manual Analysis	Manual Dynamic Analysis	Manual Static Analysis	Other	White Box
Execute unauthorized code or commands		78, 120, 129, 131, 476, 805	78, 79, 98, 120, 129, 131, 134, 190, 798, 805	79, 129, 134, 190, 494, 698, 798		98, 120, 131, 190, 494, 805	476, 798	78, 798		
Gain privileges / assume identity			798	259, 798		259	798	798, 807	628	
Read data	209, 311, 327	78, 89, 129, 131, 209, 404, 665	78, 79, 89, 129, 131, 134, 798	14, 79, 129, 134, 319, 798		89, 131, 209, 311, 327	209, 404, 665, 798	78, 798		14
Modify data	311, 327	78, 89, 129, 131	78, 89, 129, 131, 190	129, 190, 319		89, 131, 190, 311, 327		78		
DoS: unreliable execution		78, 120, 129, 131, 400, 476, 665, 805	78, 120, 129, 131, 190, 400, 805	129, 190	400	120, 131, 190, 805	476, 665	78		
DoS: resource consumption		120, 400, 404, 770, 805	120, 190, 400, 770, 805	190	400, 770	120, 190, 805	404	770		412
Bypass protection mechanism		89, 400, 665	79, 89, 190, 400, 798	14, 79, 184, 190, 733, 798	400	89, 190	665, 798	798, 807		14, 733
Hide activities	327	78	78			327		78		
Other		400, 404	400, 798	198, 484, 494, 698, 733, 798	400	494	404, 798	596, 798, 807	628	484, 733

Design Review

Static Analysis

Pen Testing Service



Most Important Weaknesses (CWE's)

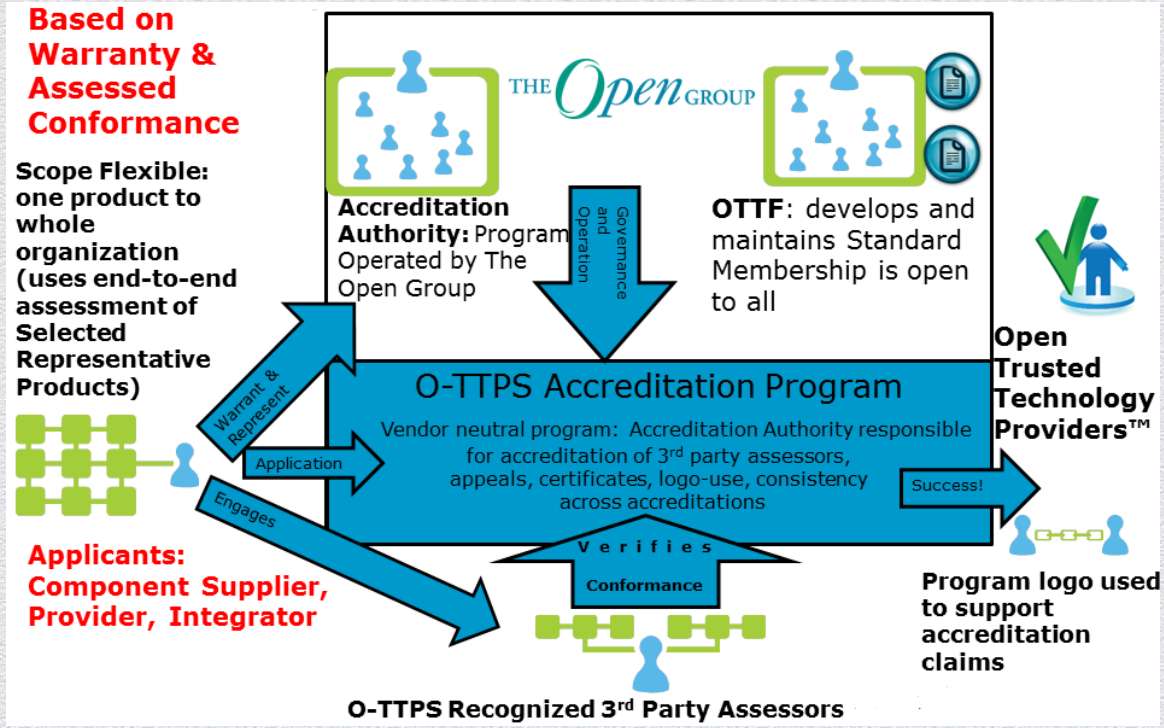
Set of CWE's a detection method can gain insight about

Which Detection Methods can give me assurance about the CWE's I care about?

The Open Group Trusted Technology Forum

A global industry-led initiative defining best practices for product integrity and supply chain security so that you can “Build with Integrity and Buy with Confidence™”

THE Open GROUP



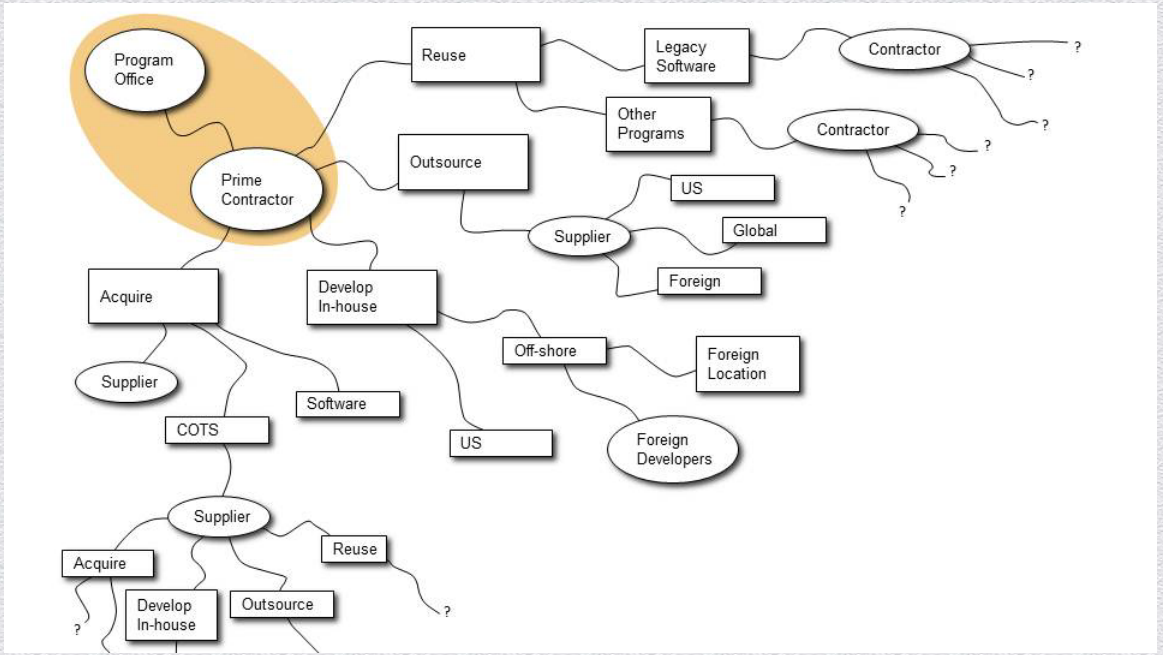
O-TTPS: Accreditation Program

Mitigating Risk of Maliciously Tainted and Counterfeit Products

Assessments by 3rd Party Labs backed by Warranty from Organization

- Publically Available Assessment Procedures
  - Help achieve objectivity, repeatability, and consistency across accreditations
- Two types of requirements/evidence to be assessed: process and implementation
  - Process – Need to provide evidence there are documented processes
  - Implementation – Need to provide evidence that the processes were implemented
- Formal Recognition of O-TTPS 3rd party labs
  - Must meet established criteria and assessors must pass O-TTPS Assessor exam.
  - Receive certificates and listed on public registry

APPENDIX



The Software Supply Chain

* "Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"