Vulnerability Assessment

Elisa Heymann

Computer Architecture and
Operating Systems Department
Universitat Autònoma de Barcelona

Elisa.Heymann@uab.es

Key Issues for Security

- Need independent assessment
- Need an assessment process that is NOT based solely on known vulnerabilities
  - Such approaches will not find new types and variations of attacks

Key Issues for Security

- Automated Analysis Tools have Serious Limitations
  - While they help find some local errors, they
    - MISS significant vulnerabilities (false negatives)
    - Produce voluminous reports (false positives)
- Programmers must be security-aware
  - Designing for security and the use of secure practices and standards does not guarantee security

Addressing these Issues

- First Principles Vulnerability Assessment (FPVA)
  - A strategy that focuses on critical resources
  - A strategy that is not based solely on known vulnerabilities
  - Understand a software system to focus search for security problems
  - Find vulnerabilities
  - Make the software more secure

First Principles Vulnerability Assessment

Step 1: Architectural Analysis
Step 2: Resource Identification
Step 3: Trust & Privilege Analysis
Step 4: Component Evaluation
Step 5: Dissemination of Results

Our Experience

Condor, University of Wisconsin
Batch queuing workload management system

SRB, SDSC
Storage Resource Broker - data grid

MyProxy, NCSA
Credential Management System

glExec, Nikhef
Identity mapping service

CrossBroker, Universitat Autònoma de Barcelona
Resource Manager for Parallel and Interactive Applications

Gratia Condor Probe, NCSA
Feeds Condor Usage into Gratia Accounting System

Condor Quill, University of Wisconsin

Our Experience

Wireshark (in progress)

Network Protocol Analyzer

Condor Privilege Separation, University of Wisconsin (in progress)

Restricted Identity Switching Module

VOMS Admin, Instituto Nazionale di Fisica Nucleare (in progress)

Virtual Organization Management Service

Vulnerability Assessment@EMI

Apply FPVA to relevant EMI Middleware

- Determine which pieces of SW to assess (we need input)
- Assess the SW
- Generate vulnerability reports

  A vulnerability is considered only when we produce an exploit for it.

Vulnerability Report

- One report per vulnerability
- Provide enough information for developers to reproduce and suggest mitigations
- Written so that a few sections can be removed and the abstracted report is still useful to users without revealing too much information to easily create an attack.