

Kevin Staggs, CISSP  
June 6, 2006

# Security Testing Methodology

**Honeywell**

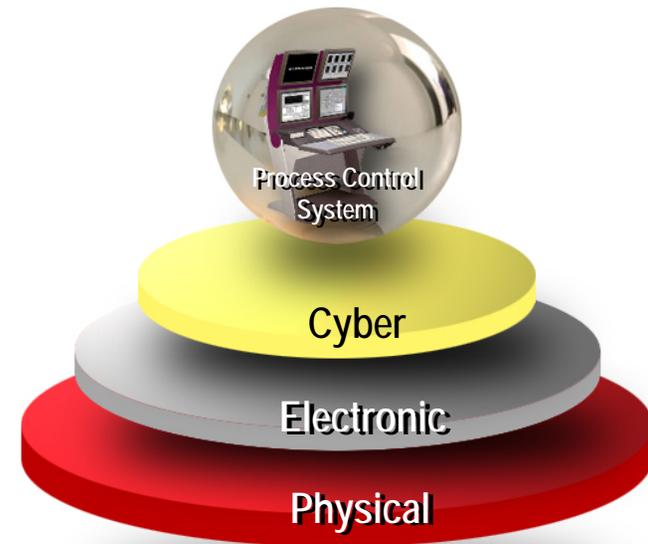


# Topics

- Our Philosophy
- Security Testing Process and Procedures
- Security Testing Needs
- Summary

# Our Philosophy

- Security and safety
  - Without security you cannot have safety
- Key Honeywell initiative
- Defense in depth
  - Security at more than just the perimeter
  - Built-in at every layer of the system
- Security is a journey not a destination
  - Policies and practices are key
  - Continuous security testing and improvements



# Security Testing Process & Procedures

- Controller Testing for IP-based controllers
  - IP protocol testing as part of development
    - Includes protocol fuzzing
  - External verification
    - Achilles Test Harness
    - Honeywell advanced lab testing
- System Security Testing Procedures
  - Security testing part of process
  - Internal security testing
    - Personnel trained on hacking tools and techniques
  - Internal Honeywell security organization
  - External testing
    - Customers
    - Other organizations

# Controller Security Test Methodology

## Unmitigated controller testing

- Utilized Achilles Test Harness
- Controller with no network mitigations
  - Identify raw controller vulnerabilities
    - Denial of service
    - Buffer flooding
- Add network mitigations
  - Honeywell Control Firewall
  - Cisco switch QoS configurations
- Update test scenarios
  - Eg – mitigations required Achilles updates

# System Security Test Methodology

## Utilize inside-out approach

- Use attack tools at level 1 and 2 first
- Evaluate results
  - Create additional attack scenarios
- Rerun attack tools at level 3
  - Evaluate results
  - Measure effectiveness of L2/L3 mitigations
- Rerun attack tools on DMZ
  - Evaluation results
  - Validate firewall mitigations
- Rerun attack tools from Level 4
  - New attacks for L4 applications and capabilities
    - Email
- Evaluate mitigations at each level and improve

# Security Testing Needs

- Common methodology across industry
  - For vendors/OEMs
  - For system integrators
  - For end-users
- Suite of specialized tooling for SCADA and Control Systems
  - Achilles for controller testing
  - System level testing such as CoreImpact