wurldtech
security technologies

Achilles Assurance Platform

Dr. Nate Kube
Founder / CTO Wurldtech

Presentation Outline

- Statement of the Problem
- 3rd Generation Achilles Assurance Platform
- Questions and Answers
- Achilles Certification Program
- Questions and Answers
- Demonstration

wurldtech
security technologies

The Problem

- Adoption of COTS technologies in control networks has resulted in less isolation from the outside world
- Ease of connectivity facilitates misuse
- Merger of technologies has dramatically reduced the robustness and safety of control networks
- Minimal visibility into the real degree of the affect

wurldtech
security technologies

What do we know about protocol vulnerabilities?

- Communication protocols are complex and their specifications may contain areas of ambiguity
- Incorrect assumptions or carelessness of the implementer are common sources of vulnerabilities
- Integration of 3rd party protocol stacks commonly have unpredicted consequences
- Segmentation faults, stack, heap or buffer overflows, etc.,

What are the limitations of today's vulnerability assessment tools?

- Signature centric assessment tools are based on CERT and BugTraq vulnerability lists which are IT focused
- Control devices are not the usual Unix or Windows based platforms
- Minimal abilities to find unknown vulnerabilities
- Quantifiable coverage is not possible without the employment of formal test methodologies

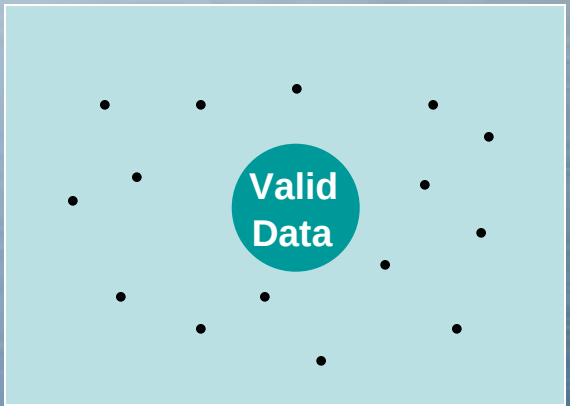
The Result

- Few thorough stack testing tools are available to vendors and asset owners
- Invalid protocol packets are often neglected in QA cycles
- Control systems are being deployed with numerous network vulnerabilities
- Lack of robustness has impacted communications availability and hence plant operations

Test Data Generation

- Construction of test data comprises a large part of a software project

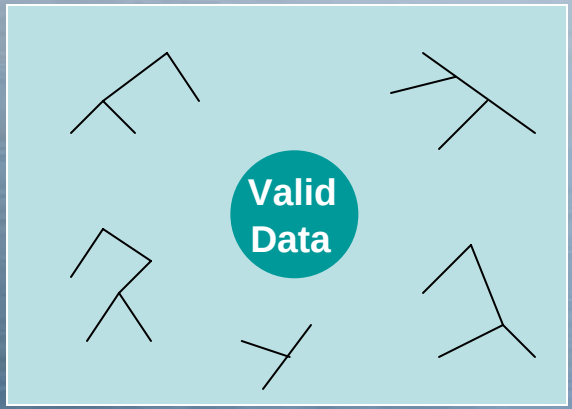
- Path-oriented methods, data flow methods, random testing, adaptive testing, and syntax-based testing are a few of the methods employed

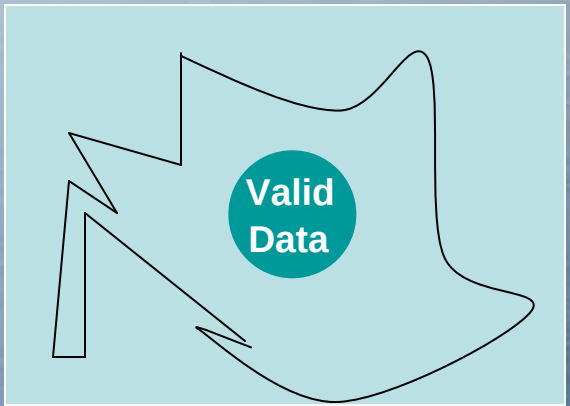


Test Data Generation

- Essential characteristic of syntax-based testing is that a syntactic description, such as a grammar, is used to define the test domain

- The syntax is then used to generate elements in the test domain





Grammars and Formal Languages

- A grammar is a precise description of a formal language
- 2 main categories

  generative: sets of rules for generating strings in the language

  analytic: sets of rules for recognizing if a string is in the language
- Example

  rule: S::=aSb | ε derivations: S->aSb->ab

  S->aSb->aaSbb->aabb
- **The grammar "type" dictates the allowable complexity of the test domain it encodes**

wurldtech
security technologies

The Chomsky Hierarchy

Type 3 (no memory)

S::=aS | ε

Type 2 (stack memory)

S::=aSb | ε

Type 1 (Linear bound)

S::=abc | aSBc

cB::=Bc

bB::=bb

Language Class	Grammar	Automaton
3	Regular	NFA or DFA
2	Context-Free	Push-Down Automata
1	Context-Sensitive	Linear-Bound Automata
0	Unrestricted (Free)	Turing Machine

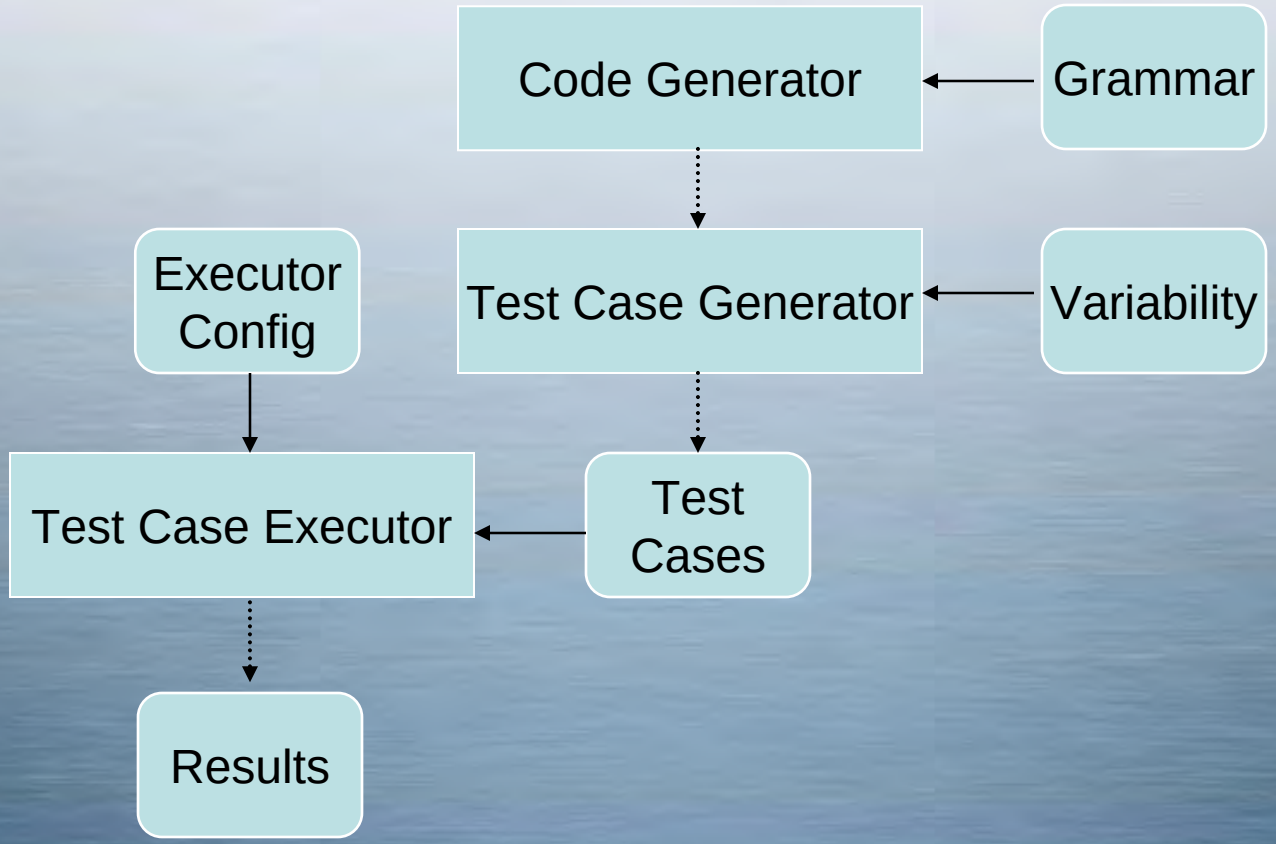
The Chomsky Hierarchy

wurldtech
security technologies

Achilles Attribute Grammars

- Can encode Type 0 - unrestricted (free) languages
- Achilles Attributes provide Turing Power
- Achilles Attributes are used to build contextual information
- Enables production of test sequences - test data and the expected output which solves the test oracle problem
- Enables quantifiable coverage of the test domain

Achilles Attribute Grammars



wurldtech
security technologies

Achilles Attribute Grammars

- Modularity is a powerful characteristic of the framework
- Supports multiple roles
  - plant operator given test cases and an appropriate executor
  - network engineer given the test case generator
- Easy transition to new protocols
  - procure a description of the protocol
  - produce a new grammar file
  - one grammar file may make use of any other

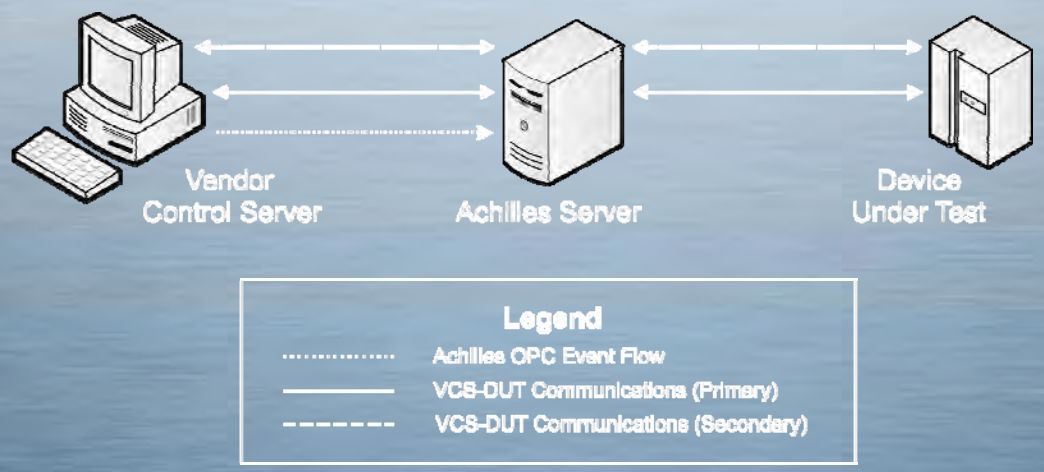
What is Achilles?

- Automated, comprehensive network assurance platform
- Multi-pronged approach:
  - **Profiling Tools:** Fingerprinting to determine vulnerable services
  - **Known Flaw Testing:** Check for well-known flaws (CERT list)
  - **Resource Starvation Testing:** Investigate performance when bombarded with traffic or requests
  - **Grammar Testing:** Formally created, quantifiable data sets crafted to exercise a protocol's implementation

wurldtech
security technologies

How is Achilles used?

- Sample test bench



wurldtech
security technologies

Field Experience

- Commonly detected vulnerabilities loosely categorized into one of three classes:
  - **Critical**: the DUT exhibited an internal fault and power cycled
  - **Loss-of-view**: the communication between the vendor control software (HMI for example) and the DUT was eliminated
  - **Non-critical**: the controller exhibited an error in expected functionality but did not experience a reset (e.g. protocol non-conformance)

Field Experience

- Common triggers of critical vulnerabilities:
  - Derivatives of unicast, broadcast and multicast Ethernet storms
  - Derivatives of multicast and unicast IP storms
  - Variations on TCP handshakes
  - Minor attacks on proprietary application services
  - Attacks on control protocol implementations (MODBUS/TCP, DNP3/IP, etc)

Field Experience

- Common triggers of loss-of-view vulnerabilities:
  - Low rate Ethernet or IP DoS's
  - ARP floods
  - Unsolicited ARP replies
  - Invalid IP fragments
  - Derivatives of TCP SYN floods
  - Derivatives of unicast, broadcast and multicast IP storms
  - Minor attacks on proprietary application services

What can Achilles do for you?

- Achilles enables the user to:

– accurately identify new vulnerabilities in control systems
– gain acute knowledge of the robustness of deployed network stacks
– demonstrate compliance to emerging industrial and gov't regulations
– maintain network stability and increase overall quality assurance
– prevent security breaches and stay ahead of cyber security threats
– promote reputation as a leader in security preparedness
– strengthen system availability ergo increase worker safety

wurldtech
security technologies

Questions?

- For more information on the Achilles Assurance Platform please contact:

Dr. Nate Kube

nkube@wurldtech.com

604 669 6674

wurldtech
security technologies

wurldtech
security technologies

Achilles Controller Certification Program

Dale Peterson
Digital Bond

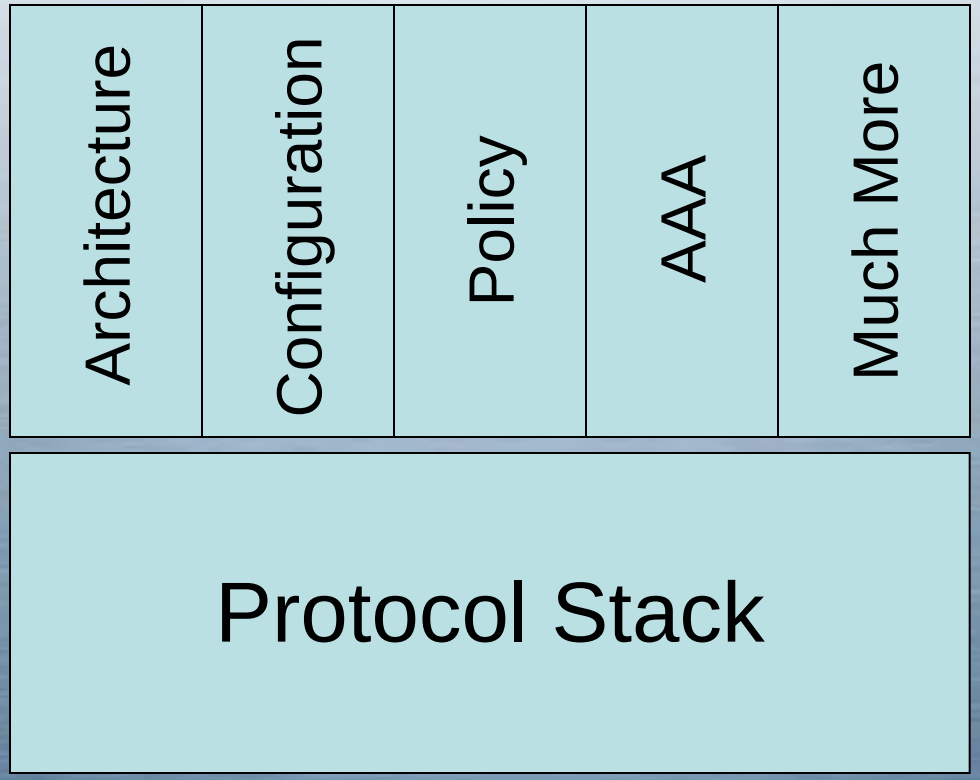
What is Digital Bond doing?

- Helping to structure the Achilles Certification
  - Define the initial certification levels
  - Determining the content and format of certification information made available to the public
  - Gather feedback from the community
  - Raise Achilles Certification awareness
- Digital Bond is not involved in testing nor do we see any non-public test results

Achilles Certification

- You asked for it!
  - Asset owners involved with Achilles wanted to purchase products that were Achilles ‘tested’
  - Vendors involved with Achilles wanted recognition that their products had a higher level of security assurance
  - Need it now, delay is unacceptable

Achilles Certification $\neq$ Security



wurldtech
security technologies

Foundation: Protocol Stack

- A vulnerable stack can negate all security controls
  - Bypass authentication, authorization …
- Each end user shouldn't need to test the stack
  - Very inefficient use of time and money
  - How would they test the stack?
    - Vendors have difficulty testing their own stacks
  - How does a vendor prove their stack is robust and secure?
- Achilles Certification lets asset owners focus on aspects of a cyber security program under their control

wurldtech
security technologies

Achilles Controller Certifications

- Controller Level 1
  - Available today
- Controller Level 1 + Control Protocol
  - Modbus/TCP, DNP3/IP and Vnet/IP available today
  - Future + certifications planned
- Controller Level 2
  - Criteria announced on September 2007

wurldtech
security technologies

Controller Level 1

- Controller Level 1 Certification
  - Tests controllers with Ethernet interface
    - Over 30 million individual tests
  - Test layer 2 to 4 protocols
    - Ethernet, ARP, IP, ICMP, TCP and UDP
    - Tests for proper implementation
    - Tests resilience to structured fuzzing of the protocol
  - Subject controller to Nessus and nmap
    - Verify controller will withstand common scans
    - Set of Nessus plugins that will be updated annually

Controller Level 1+

- Control protocol support varies by vendor & controller
  - Would not be a level playing field if included in Level 1
- + Certifications are protocol attribute grammars
  - Standard Modbus/TCP and DNP3/IP
  - Proprietary Vnet/IP
  - Other standard protocols planned
  - Proprietary protocol grammars can be developed
- Asset owners should require Level 1 + control protocol(s) they will use

wurldtech
security technologies

Controller Level 2

- All Level 1 test case families plus
  - Storms for layers 2 to 4
  - Application layer protocols
    - Commonly used management protocols
    - http, ftp, snmp, telnet, ssh
  - Additional common scanning tools

We want your suggestions for Level 2

wurldtech
security technologies

Failed Certification Test?

- Wurldtech can help
- Failed Test Software
  - Software utility that allows vendor to rerun the failed test in the lab prior to submitting for retesting
- Professional Services
  - The team can help pinpoint the root cause
- Controller + Firewall Certification

wurldtech
security technologies

Publishing Certifications

- Achilles Certification & testing value increases for vendor, asset owners and community if published
  - Controller Certification and test results
    - Only passing results will be posted
  - Broad information about test case families
    - Asset owners need to understand the assurance level of Achilles Certification
- Published on Wurldtech Security website

wurldtech
security technologies

Wurldtech | Achilles Certification Program

http://www.wurldtech.com/ACP/

Contact Us

wurldtech security technologies

RAISING THE BAR FOR CONTROL SYSTEMS SECURITY

HOME | CORPORATE PROFILE | SECURITY SERVICES | OUR PRODUCTS | SUPPORT | WURLDTECH LABS | I Am Looking For?

Certification Results

Vendor
Category
Model
Firmware Version

TEST CASE FAMILY	COMPONENT	# OF TESTS (APRX)	RESULT
Ethernet	Grammar	5,700,000	Pass
ARP	Flood	5,000,000	Pass
ARP	Grammar	900,000	Pass
IP	Fragmentation	1,700,000	Pass
IP	Grammar	3,000,000	Pass
ICMP	Grammar	2,700,000	Pass
ICMP	Type/Code	6,500,000	Pass
TCP	Syn Floods	500,000	Pass
TCP	Land Attacks	6,00,000	Pass

TEST CASE DETAILS : ICMP GRAMMAR

The ICMP Grammar tests for improper handling of packets with malformed standard ICMP header fields and proper handling for values at the upper and lower limit for the fields. The ICMP Grammar also tests the device's processing of rogue ICMP packets including destination unreachable, redirect, time exceeded and source quench directives.

wurldtech security technologies

Achilles Certification Awareness

- Achilles Certified logo program for vendors
- Achilles Certified awareness campaign
  - Highlight certified controllers
  - Stress the benefits of a secure stack
  - Advertising and articles in industry publications
  - Participation in industry conferences and user group events

Benefits For Asset Owners

- Level of security assurance prior to purchase
  - Provable testing coverage of protocols
  - Independent, third party security testing
- No need to develop in house expertise
  - Almost impossible without a tool like Achilles
  - Requires expertise not needed to install and manage a secure control systems
- Reduced number of security patches
- Add Achilles Certified as an RFP requirement

wurldtech
security technologies

Benefits For Vendors

- Easy answer to the security question
  - Independent testing and certification
  - Vendor now has documentation
  - Saves time and money in RFP process
  - Eliminates a time delay in procurement cycle
- Significantly reduce future vulnerabilities
  - Identify and fix implementation bugs prior to release
- Satisfy a RFP requirement
- Private, detailed Achilles Controller Certification Test Report can be provided to prospects

wurldtech
security technologies

How You Can Help

- Asset Owners
  - Add Achilles Certified to controller RFP's
  - Push vendors to get installed products tested
  - Talk to other asset owners
- Vendors
  - Submit controllers for Achilles Certification
  - Place Achilles Certified on materials, website
  - Have an Achilles Certified presentation at your next major Users Group event

wurldtech
security technologies

Questions?

- For more information on the Achilles Certification Program or to schedule a product for Certification testing contact

Dr. Nate Kube
nkube@wurldtech.com
604 669 6674
or
Mr. Dale Peterson
peterson@digitalbond.com
954 303 7560

wurldtech
security technologies