Setting the Standard for Automation™

LOGIIC Project 3: AWL Project Summary

Rick Fell,
Chevron
Brian Peterson,
Business Risk Mgmt Consultants

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Presenter

- Rick Fell….
- Brian Peterson is the principle consultant at Business Risk Management Consulting LLC which provides global consulting services to ensure companies achieve Information Risk Management Compliance. He has worked in the Information Risk field for over 15 years. Brian developed program and implementation tools for Information Security, SCADA Security, Privacy, and BCP. Brian holds a degree in Business Administration from Saint Mary's College in California.

Host Protection
Business case for the project

- Protection of process control data, networks, applications, and host operating systems, particularly in multi-vendor environments, is a critical, ongoing requirement for the Oil & Gas sector.
- The threat to a control system's availability, integrity and access is real, and attack methods and tactics are diverse. These are evidenced by the recent StuxNet attacks.
- A loss of control over a critical process potentially results in production loss, economic cost, environmental impact, facility damage, personnel injury, and loss of life.
- The exponential growth in cyber threats, attempted and successful, malicious or unintentional combined with operational demands for increased system reliability and availability motivate the need for a better approach.
- System maintenance increasingly centers on patching vulnerable automation software and operating systems, many of which have reached manufacture end-of-life, are unsupported by the vendor, and/or lack economic basis for replacement.
- This situation presents a formidable challenge to facility owners demanding process automation and environment reliability.

Host Protection Components
Understanding common solutions

- **Anti-malware** (Virus, Trojans, spyware) solutions scan systems for executables matching known signatures.
- **Host Intrusion Prevention Systems** (HIPS) encompass a broad range of technologies including combination of behavioral monitoring, signature detection, host firewall, and application control.
- **Host Computer Firewalls**: A firewall examines communications between a given computer and the network and permits or blocks network packets based on a pre-defined rule-base.
- **Application Control/Application Whitelisting** (AWL) defines what applications are allowed to run and blocks everything else.
- **Memory Protection** is often offered with AWL solutions to prevent execution of unknown code that may be loaded into memory to bypass normal AWL execution prevention
- **Device Control** is offered with some AWL solutions to disable external devices (like USB)

AWL vs. AV

Comparing Application Whitelisting to AV

- AV is based on maintaining a “blacklist” of known bad file patterns or signatures that represent viruses or other malware (AV proactively removes malware)
  - Exponential growth of the number of entries in the AV blacklists and also the rate at which new entries are added, led to the emergence of whitelisting technology
- AWL maintains a “whitelist” inventory of known files (assumed to be good)
  - AWL does not have the ability to prevent execution of files with malware
    - If you whitelist a file that is bad it will execute
- AWL doesn’t address all forms of program code execution (IE, Word, etc.)
  - Some applications import and run code that does not originate from an executable file

	What is bad (“black”)	**What is good (“white”)**
Policy (default) stance	Default-permit	Default-deny
Facility access example	No-access list (terminated staff, known criminals, etc.)	Access permission previously arranged for staff, others, etc.
Computer security example	Antivirus	Application whitelisting
Main motivation	Easily finds bad things without impacting those not on the bad list	Tighter security because anything not explicitly listed as good is questioned
Main problem	All bad things may not be on the list (leads to “false negatives”) permitting access/execution when it should not occur (e.g. malware executes or bad guys get access)	All good things may not be on the list (leads to “false positives”) preventing access/execution when it should occur (e.g. business disruption)

Project Goals & Objectives
LOGIIC achieved these goals & objectives

- Project Goal : lower complexity, cost, and administrative overhead of host protection, without adversely impacting system reliability or performance
- Project Objectives:
  - Determine how AWL integrates with current AV solutions
  - Understand best combination of host protection security solutions – AWL and AV
  - Assess how AWL solutions impact maintenance effort (e.g. AWL maintenance, OS and application patching, AV signature updates)
  - Develop a single AWL solution that can support multi-vendor automation systems, when possible (which is a goal for some LOGIIC members)
  - Enable deployment of AWL solutions into automation environments by obtaining automation vendor accreditation
  - Verify the effectiveness of AWL solutions particularly to manage StuxNet-type and other zero-day attacks
  - Identify how AWL solutions can support various Legacy components (e.g. OS, process control systems)
- We evaluated technologies reasonably mature and available for testing

Project Scope & Major Activities
Project activities performed by LOGIIC

- Generate a short-list of technology/vendor candidates to participate in project
- Select a test environment consisting of typical assets found in ISA-99’s reference architecture Level 2-3.5 zoned, windows-based test environment, instrumented with solutions representative of best-practice security
- Assemble and develop a test suite of malware and attacks of particular concern in automation environments
- Develop vendor selection criteria and test evaluation criteria
- Evaluate solutions effectiveness by running a test suite against a baseline configuration (with AV and without AV) and candidate AWL solutions
- Ensure AWL solution is secure from attacks
- Document “host protection’ best practices, processes, and procedures with some relative measure of effort, easy of use, etc.
- Evaluate AWL risks that effect automation processes (e.g. change mgmt)
- Publish the base-line recommendations and practices

LOGIIC AWL Evaluation Criteria
How we evaluated AWL test results

- Show Stoppers Evaluation Criteria
  - Excessive Client installation time greater than 5 minutes
  - Significant Air-gap (stand-alone) issues that prevent AWL management
  - Negative performance impact (e.g. CPU) on BPCS (Basic Process Control System - specifically HMI)
- Other Key Evaluation Criteria
  - Effectiveness to prevent malware
  - Operational complexity: Easy of deployment and use of AWL
  - Ability to apply solution into Installed Base and new projects
  - Memory protection to prevent execution of unauthorized files
  - Costs (deployment, operational) of AWL solution
  - Automation vendor Accreditation/support of AWL solution(s)
- An evaluation test template was developed which will be shared

LOGIIC AWL Technical Approach
How we evaluated AWL test results

- Assessment Methodology: $R(f) = TxVxC$
  - Measured performance of technology by defined, realistic scenarios rooted in existence of a plausible (T) threat, existing (V) vulnerability, and observed (C) consequence.
- Assessment Approach
  - Clearly defined AWL, what it is, and what it is not
  - Considered several constants in control system environment: the need for 24/7/365 uptime, operational situational awareness, unobstructed access to system during incidents, and life-safety criticality of data and control decision integrity
- Analysis of Findings included consideration of data sources:
  - Baseline information gathered from technical scans, vendor documentation and discussion, and network reconnaissance
  - Performance during technical red teaming and exploit response
  - Observations during the assessment
  - Usability testing
  - Completion of functional test matrices
  - AWL and automation vendor roadmap discussions were also considered

Project Conclusions

AWL Value Conclusions

Summary of LOGIIC Conclusions

- AWL provides good protection against execution of files on systems, media, etc.
  - AWL prevented Stuxnet in the lab (e.g. like before AV signature was developed)
  - AV is recommended to prevent executables with known virus
  - AWL provides protection when A/V signature and patches updates are infrequent
- AWL addresses threats not addressed by AV or patching
  - AWL may reduce criticality/frequency of AV updates, OS and app patches
- AWL is most effective for systems that repeatedly perform the same functions with minimal changes (e.g. static apps and functions)
- AWL adds more value for older systems and increases in value as newer systems become older
  - AWL is more effective on older OS (e.g. Windows2003/XP) vs. new OS (e.g. 2008/Win7) because new OS has up-to-date built-in security controls
- AWL may be better suited for a subset of BPCS systems, rather than facility-wide deployment (based on criticality of BPCS) – particularly when A/V is not practical
- A single AWL enterprise solution is desirable, BUT
  - AWL vendors don’t support some Install Base
  - AWL may not be cost effective or operational practical in some cases
  - Alternative Host Protection strategies may be appropriate in some cases

AWL Other Benefits and Limitations

Summary of LOGIIC Conclusions

- Other Benefits of AWL
  - AWL creates an accurate inventory of your applications
- Limitation of AWL:
  - AWL doesn’t protect against all attacks
  - Some memory protection solutions require signature updates and/or custom rules
  - Maintenance and end of life for AWL solutions may present challenges in the future
  - AWL will trust all software delivered by a trusted updater
- Benefits with Limitations
  - Change Mgmt and Release Mgmt processes must be improved with AWL
    - BUT if they are not there could be a disruption in automation system availability
  - Device Control can be a valuable tool to prevent introduction of files (e.g. USB)
    - BUT some vendor implementations make solutions difficult to maintain
    - Note: Device Control is not inherently part of AWL but is often offered with the solution

AWL Selection Considerations
Specific to your company BPCS

- Resource load on the system (CPU usage and memory) varies by memory protection product and/or Automation Application
- Effort required to interface AWL with AV
  - AWL/AV suite often works together better than heterogeneous solutions
- Your typical BPCS architectures and support capabilities vs. AWL solution requirements (e.g. AWL server hardware, software distribution, etc.)
  - Comparing your BPCS connectivity, remote sites, and staff skills to AWL Architecture and support complexity
- Your Legacy (OS) requirements vs. supported OS in AWL
  - AWL vendors support for legacy systems varies
- Your functional requirements vs. AWL capabilities
  - Understand your most critical functions vs. AWL product capabilities
- Your typical Asset Life Cycle for BPCS systems
  - Older assets gain greater value from AWL than newer assets
- Your likely AWL overall cost of ownership for each AWL solution
  - Admin costs and number of AWL licenses vary greatly by vendor

AWL Configuration Considerations

AWL configuration and maintenance is critical

- AWL requires careful implementation and AWL policies
  - AWL requires fine tuning for operation of critical functions and for system changes/updates
- AWL must be implemented and maintained correctly which can be resource intensive (varies by product)
- Memory protection has limitations
  - System restart required for some memory protection (and AWL)
  - Memory protection ineffective for some AWL products
- AWL may conflict with AV which may cause systems to become unresponsive)
  - May have to replace AV to be compatible with AWL (e.g. suite)

AWL Testing Attributes

- Server Install
- Client Install
- Time to Whitelist
- Protection against Conficker
- Protection against Stuxnet
- Memory Protection
- File execution protection (zip, USB, etc.)
- Works with common AV solutions
- Reboot Required
- Works in an Airgapped Environment
- Device Control
- Administration
- Ease of Use with Vendor Architecture
- Ease of Tuning with the Vendor Architecture

Appendix B:
Project Background

Project Out-of-Scope items

- Embedded Operating Systems, Non-Wintel, PLC/RTU's, and Field Devices
- Mobile/Portable/Hand-held devices
- Network Security Products (Firewalls, Intrusion Detection/Prevention, logging, Network Access Control (NAC)
- Provisioning, Patch & Configuration management products for OS & Control Apps and Security Compliance monitoring technologies and practices
- Software Assurance tools and techniques (app scanning, code review)
- Network Devices (router/switch/gateways, wireless)
- Encryption technologies, Data-loss prevention (DLP, data leakage)
- Non-commercially available, not-for-public release or research products
- Vendors/Technologies requiring confidentiality/non-disclosure agreements
- Security Vendors/products not reasonable available to Automation/Control systems
- SIS

AWL Vendor Selection Weights

Used to select project participants

AWL Vendor Selection Criteria	Weight
Alignment with project objectives	5
Roadmap going forward: technology and strategic alliances related to AWL	5
Willingness to participate in an evaluation	20
Willingness to provide evaluation copy of software	20
Engineer support for 2 days onsite and stand-by (phone) support at 3 sites	10
Strategic alliances with automation vendors or integrators specializing in integration > Experience with Process Control, e.g. installed product in Automation environments	20
Procedures for signature updates or whitelist modification, as appropriate to technology	10
Interoperability with other standard security solutions	5
Other security capabilities can you provide in the process control environment	5
Candidates POSSIBLE Weighted Score	100

Auto Vendor Selection Weights
Used to select project participants

Automation Vendor Selection Criteria	Weight
Vendor alignment with project objectives	3
Roadmap going forward: technology and strategic alliances related to AWL	2
Willingness to participate in an evaluation	5
Ability to provide a test facility for 2 weeks - Availability of test facility in Sept-Nov 2011	20
Willingness to allow LOGIIC, SME, AWL vendors to test various attacks in test facility	15
Availability of an engineer to support the AWL test	8
Willingness to allow on network a Security Mgmt Console and attack workstation	10
List of the OS and Process Control applications with patch levels in your lab	10
Host security solution(s) in vendor’s standard configuration(s)	5
Alliances with security solution providers	4
Willingness to allow us to install other AWL software on your systems	8
Process for certifying third-party security solutions to run in the vendor’s system - Willingness to accredit successfully demonstrated AWL solutions	10
Candidates POSSIBLE Weighted Score	100