Implementing Application Whitelisting – A Case Study

North American SANS SCADA & Process Control System Security Summit
Orlando
January 26, 2012
Introduction

• Case study of the first widespread use of application whitelisting (AWL) in UK North Sea oil & gas industry
• Background
• Project scope
• Motivation & objectives
• What went well
• What didn’t go so well
• Does AWL work?
• Is there a place for traditional anti-virus (AV)?
• Unplanned benefits
UK North Sea Oil & Gas Industry

- Hostile environment
- Ageing assets operating well beyond original design life
- Huge variety process control systems – age & suppliers
- Reliance on vendors for maintenance & support
Client

- Tier 1 international oil & gas company
- Offshore oil & gas production assets
- All North Sea fixed & floating installations
- All control systems machines planned to be running AWL
- First for UK North Sea oil & gas industry

Note: these are not the client’s installations
In-Scope Systems (Examples)

Drilling
Power Generation
Load Management
Gas Compression
Turbine Controls
DCS
SCADA
Data Historian
Utilities
Environmental Monitoring
Vibration Monitoring
Metering
Fire & Gas
ESD
Well Control
Subsea Control
Client Motivation & Objectives

• Company standards require
  – Protective measures from malware infection
  – Controlled change to systems

• Internal audit highlighted shortcomings in these areas

• Standalone systems making traditional AV deployment costly

• Objective to close audit findings by installing whitelisting on all computers running version of Windows supported by the whitelisting product
Selected Product

• CoreTrace Bouncer v6
• Selected because
  – One of few vendors at the time with any track record of use in process control systems
  – Tested at client’s US corporate technology centre
  – Most suitable product for use with networked **AND** standalone systems
The Good, the Bad and the Ugly

The Good
- Relationship with CoreTrace
- Management of change & Installation process
- Vendor testing

The Bad
- Inventory
- Product
- Vendors
- People
Relationship with CoreTrace

• Amor Group is CoreTrace Platinum Partner
• Built up great relationship
  – CoreTrace listen if we hit issues & provide close support
  – Have incorporated enhancement requests
  – NDA with CoreTrace gives us access to information on forthcoming releases
Vendor Testing

- 27 system vendors
  - Set up test system onshore
  - Test system with Bouncer installed
- Exceptions
  - Low risk monitoring systems where agreed with customer & vendor
- Install Bouncer & confirm working
- Test application & confirm working
- Plan live installation
Management of Change & Installation

- Client’s MOC & Permit to Work systems applied
- Rigorous 19 step installation procedure
- Vendor’s field engineer in support unless agreed with client & vendor
- No unplanned outages or shutdowns
Hardware Failures & Virus Infections

• Hardware failures
  – Power supplies
  – CD drives
  – Repair or replace

• Virus infections
  – Previously unknown infections
  – Clean up or rebuild
Inventory

- Inventory supplied by client
- First site visits highlighted inventory not complete or accurate
- Survey carried out on all sites
- Inventory increased >50%
Product

• Some initial glitches with Bouncer installer
  – Good support from CoreTrace to address them quickly

• Very few between Bouncer & applications
  – Named pipes
  – Dynamic discs
  – FAT v NTFS
Control System Vendors

• Vendor support very variable
  – Helpful to obstructive
  – Security awareness good to bemused to none

• Old systems, companies acquired & many people retired…lack of detailed knowledge on the equipment

• Very few permanent test systems on which to test Bouncer
People

• Communication to
  – Customer’s personnel offshore & onshore
  – Vendor sales, support & engineers

• Little knowledge of AWL in general & Bouncer in particular
  – IT
  – C&I Engineers
  – Control System Vendors

• Lack of security culture & awareness
Does AWL Work?

- No known re-infections
- No requirement to re-visit any systems on which AWL installed
- No unplanned interruptions from AWL
- Avoided cost of vendor supplied AV & OS patch updates
- Avoided on-going AV maintenance costs
- Reduced risk from AV maintenance
- Reduced risk of unmanaged changes
Is AWL & AV Needed?

• AV is still needed to check media (especially USB drives) & files before copying to control systems

• If goal is to protect the control system, don’t install AV on the control system
  Frequent updates = Risk

• Can the control system be a vector for viruses?
  – Only if used as a source from which to copy files
Unplanned Benefits

• (More) complete inventory of process control systems
• Revealed previously unknown
  – Hardware issues
  – Virus infections
• Forced other known system issues to be resolved prior to Bouncer installation
• Site staff converted from sceptics to supporters
Summary

• AWL is a better solution than AV for protecting process control systems from malware infection

• There are no short-cuts to implementing AWL
  – Change management
  – Testing
  – Vendor support needed

• Where there are many different, standalone systems, AWL licence cost is trivial compared to effort to implement

• Expect to get some surprises along the way
...and the Ugly

Andrew Wadsworth
Head of Process Control Security
Amor Group
andrew.wadsworth@amorgroup.com

Johnstone House
52-54 Rose Street
Aberdeen
AB10 1UD
United Kingdom
Office  +44 1224 649999
Cell  +44 7914 356962

Bryan Parker
VP Sales (USA)
Amor Group
bryan.parker@amorgroup.com

2500 Citywest Boulevard
Suite 300
Houston
TX 77042
Office  +1 713 267 2207
Cell  +1 832 494 7575