Unidirectional Connectivity as a Security Enabler for SCADA and Remote Monitoring Applications

Toronto, 2010

Lior Frenkel
Co-Founder & CEO
Waterfall Security Solutions Ltd.
Introducing: Waterfall Security Solutions Ltd

- Headquarters in Rosh-Ha’ayin, **Israel.** Local Office in the **USA.**
- Product core developed at 2004 and is evolving since
- Technology and Business Focus:
  - **North American** SCADA Networks, Industrial Control networks, Utilities and Critical Infrastructures
  - Tight and continuous relationships with relevant **regulators and authorities**
- Installed-base:
  - **Nuclear Plants, Fossil Plants, Pipelines, Refineries, Oil & Gas, Petro-Chemicals, Transportation, Airports, Water & Wastewater,** and many other critical infrastructures and industrial organizations.

Confidential and Proprietary
What do we do:

**Unidirectional Security Gateways**, end to end solutions – hardware based security solution enabling a fully unidirectional, real-time information transfer out of Industrial/SCADA/control networks to business networks. Nothing can go “back” and nothing can risk the industrial network.

Why customers buy our solutions:

- Assist achieving compliance to NERC-CIP, NRC, CFATS and other regulations
- Installed base includes Nuclear, Fossil and other power plants, pipelines, refineries and more – all in industrial, critical or operational environments
- Robust, reliable, manageable, unidirectional security gateways
The Quickly Changing Landscape

- Constant Change:
  - Communication and process control networks are evolving
  - Cyber-Threats are evolving
  - Security measures – Better evolve as well...

- The Threat
  - **Critical National Infrastructures** has become a **prime target** for Cyber Terror and Cyber Crime
  - The assaults are backed up by capable entities (**nation-states or terror groups with means**)
  - The perpetrators risks are minimal
  - There are several documented “successful” attacks on utilities and critical infrastructures
The Threats are Real

New threat: Hackers look to take over power plants

Stuxnet

From Wikipedia, the free encyclopedia

Stuxnet is a Windows-specific computer worm first discovered in June 2010 by VirusBlokAda, a security firm based in Belarus. It is notable because it is the first discovered worm that spies on and reprograms industrial systems.[1] It was specifically written to attack SCADA systems which are used to control and monitor industrial processes. Stuxnet includes the capability to reprogram the programmable logic controllers (PLCs) and hide the changes.
Main Threat Scenarios:

- Let’s focus on two main *threat* scenarios:
Scenario I – Linking Critical and Business Networks

- The critical (operational, industrial) network is required to send real-time information to business/administrative networks
  - Plant and production information
  - Operational monitoring and status information
  - Alerts and events

- The business network is commonly connected to other networks, including the Internet

- Via these connections, attackers can gain access to the critical network and carry out remote, online attacks into it
Scenario II – Remote Monitoring of Critical Networks

- A Control Center or Operations Center is remotely monitoring a critical network or an equipment within it
- This can be a 3rd party vendor or service provider monitoring equipment for maintenance and service level
- The Control Center usually monitors many other networks, from other facilities and other countries

- Critical network now exposed to threats originating from each and every network which is monitored by this Control Center
The Traditional Solution Approach – IT Security

- Deploy standard IT security means and techniques:
  - Firewalls, intrusion detection and prevention systems
  - Anti-viruses and content filters
  - Encryption and authentication

- IT Security is not enough here:
  - All IT Security products suffer
    - Software bugs
    - Vulnerabilities and exploits
    - Misconfiguration and human errors
      - thus, can be hacked and circumvented

Is this good enough *when considering the risks?*
“Only one of the firewalls exhibited just a single misconfiguration. All the others could have been easily penetrated by both unsophisticated attackers and mindless automatic worms”

A. Wool, IEEE Computer, June 2004
Software Based Security

“What you must learn is that these rules are no different than the rules of a computer system. Some of them can be bent. Others can be broken. Understand?”

(Morpheus; The Matrix, chapter 15)
Unidirectional Security Gateway – The Solution
Unidirectional “Security”

- Unidirectional data connectivity from the industrial network to a corporate network
- Hardware based security, providing physical segregation
- Software agents installed on both ends to enable seamless connectivity with existing infrastructure
Waterfall’s Security Unidirectional Core

Transmitter

Hardware Based Unidirectional Security Gateway

Receiver

Laser – Transmit Only

Photocell – Receive Only
IP networks and applications are bidirectional, at all levels of communication.

Solution – Mimic behavior of each “side” of the play:

- “Mimic” Tx side as if transmissions reached original destination
- “Mimic” Rx side transmissions as if coming from original sender
- Additional polling, pre-scheduled or trigger based activities and operations
Waterfall Implementation in Industrial Networks

- Used for transmitting data from the critical network
- Hackers on the outside have no path into the network
- The critical network is 100% protected, business needs is 100% fulfilled
Usage Scenarios – Supporting all the needs

- Replicating applications and historian systems
- Transferring SCADA protocols
- Remote View and Remote Assistance
- Support for “standard” IT
Common (Insecure) Topology

- Critical assets are located in the industrial network
- The corporate network is considered as an insecure and is usually connected to the Internet
- Corporate User’s stations are located in the corporate network
- The user’s stations communicate directly with the Historian at the industrial network

- The Industrial Network and critical assets are accessible from the industrial network and thus at risk.
Waterfall Based (Secure) Topology

- The Waterfall Gateway enforces a unidirectional replication of the Historian to a Replica Historian
  - The Replica Historian contains all data and functionalities of the Historian
  - The user’s stations communicate ONLY with the Replica Historian

- The Industrial Network and critical assets are physically inaccessible from the business network and thus 100% secure from any online attack
- Compliance with NERC, NIST and CFATS regulations – easily met
- The corporate users can continue to utilize the Historian data as they used to do before
Remote Monitoring and Remote Assistance

- Enabling secure external display of control rooms and monitoring centers screens
- Enabling simplified and now secure remote assistance and maintenance
- Real-time unidirectional replication of workstation or server display screens, to external networks.

Waterfall keeps the Control network physically inaccessible from external networks.
Waterfall One-Way™ includes connectors for:

**Leading Industrial Applications/Historians**
- OSISoft PI, GE iHistorian, GE iFIX, Scientech
- R*Time, Instep eDNA, GE OSM, Siemens
- WinCC, SINAUT

**Leading IT Monitoring Applications**
- Log Transfer, SNMP, SYSLOG
- CA Unicenter, CA SIM, HP OpenView
- Matrikon Alert Manager

**File/Folder Mirroring**
- Folder, tree mirroring, remote folders (CIFS)
- FTP/FTFP/SFTP/TFPS/RCP

**Remote Screen View™**
- Real Time Screen capture for remote assistance

**Leading Industrial Protocols**
- Modbus, OPC (DA, HDA, A&E)
- DNP3, ICCP

**Other Connectors**
- UDP, TCP/IP
- NTP, Multicast Ethernet
- Video/Audio stream transfer
- Mail server/mail box replication
- IBM Websphere MQ series
- Antivirus updater, patch (WSUS) updater
- Remote Print server
Compliance Made Easy(ier)

Relevant regulations and guidelines

- **NRC** RG5.71
- **NERC**
  - CIP 002 to 009
- **NIST**
  - **800.53** - Security Controls for Federal Information Systems and Organizations
  - **800.82** - Guide to Industrial Control Systems Security
- **10 CFR 73.54**
- And more

“provide high assurance that digital computer and communication systems and networks are **adequately protected against cyber attacks**, up to and including the design basis threat as described in Title 10 of the Code of Federal regulations (**10CFR**) Part 73, Section 73.1.”

“implementation of state-of-the-art defense-in-depth protective strategies” RG 73.54 c (2), whose aim “**to ensure that the functions or tasks required to be performed by the critical assets ... are maintained and carried out**” RG 73.54 c (4) and “to prevent adverse effects from cyber attacks” (**NRC** RG73.54 c (3)).

**Detailed whitepapers**

- **Assessment of Waterfall Unidirectional Security Gateway for NIST Compliance 2010** (800.53 and 800.82)
- **Waterfall NERC Compliance** with regard to NERC-CIP
Waterfall’s Unique advantages

- **Unidirectional Security Gateway™** - provides a full solution, out of the box
- Designed and built to meet **Critical Infrastructure and Utilities needs**
- **Off the shelf** integral support for Historians, SCADA protocols, file transfers, streaming
- Enables compliance with NERC-CIP, NIST 800.53 and 800.82, RG 5.71
- **Host hardware invariance** - server agnostic, hardware independence
- **Host hardware compatibility** – no need to certify hardware with host servers
- Simple hardware **maintenance and replacement**
- **1GB** support – hardware and software
- **High Availability** – Integral in the product, for both hardware and software
- Inherent **buffering** mechanisms
Waterfall in North America

- **Department of Homeland Security** selected Waterfall’s technology for its National Cyber Security Test-bed
- **US Patent** covering SCADA/Control Networks security using Unidirectional Gateways
- Passed a **cyber security assessment** by Idaho National Laboratories
- Pike Research named Waterfall as **key player in the cyber security market**
- **Strategic partnership and cooperation** with: OSIsoft, GE, Siemens, and many other major industrial vendors
- **Large installed base** in the industrial critical infrastructure, in the US and Canada
Waterfall implementations in the US

Over 14 states, more than 25 operational sites
Questions?

THANK YOU!