

# CISP

## Critical Infrastructure & Security Practice

### ICSJWG Fall 2011 Conference

# Secure Data Transfer from Lower to Higher Security Levels

10/26/2011

Bernie Pella, GIAC GSLC

**i n v e n s y s**<sup>TM</sup>  
Operations Management

Avantis Eurotherm Foxboro IMServ InFusion SimSci-Esscor Skelta Triconex Wonderware

© 2010 Invensys. All Rights Reserved. The names, logos, and taglines identifying the products and services of Invensys are proprietary marks of Invensys or its subsidiaries. All third party trademarks and service marks are the proprietary marks of their respective owners.

# 1

## Agenda

# Agenda

## What will be discussed

- Transfer of data to an Industrial Control System (ICS)
- Current methods of data transfer
- Problems with using current data transfer methods
- Solution to ensure reliable and secure data transfer
- Advantages and Disadvantages of solution
- Review

# 2

## Transfer of Data in an ICS

# Data Transfer to an ICS

- Many Industrial Control Systems (ICS) use external data
  - Laboratory or Sample Results
  - Remote Sensor inputs
  - Vendor or Contractor Supplied (Meteorological, Other Facilities, etc.)
  - Calculation data input
- External source data used as part of ICS operation
- Data must be in specific format for use in ICS
  - Format varies by type of system used
  - Specific limitations to types and frequency of use
- Data pathway requires security implementation and validation

# 3

## Current Methods of Data Transfer

# Currently used Methods

- Data transfer methods to an Industrial Control System (ICS)
  - Ethernet from connected system
  - Manual Data Entry
  - Sneaker Net (CD, DVD, USB drive, Floppy)
  - Serial Connection or Modem
  
- This does not include data from Input/Output Modules or field devices

# 4

## Problems with Current Data Transfer Methods

# Problems with Current Methods

- Ethernet from connected system
  - Firewall rules do not validate data
  - Blocks or permits data which may create problems
  - Data Diodes do not allow for data transfer both directions
  - Most Firewalls not designed to look at actual contents of data packets to ensure correct contents for ICS use
- Manual Data Entry
  - High potential for incorrect data entry, “Fat Finger”
    - Additional personnel needed to review and validate data
    - Data validation process not 100% accurate
    - Humans make errors

# More Problems with Current Methods

- Sneaker Net (CD, DVD, USB drive, Floppy)
  - Stuxnet
  - Contaminated devices
  - Little or no control of media
  - Should not have the ability to connect external media
    - This was discussed in Fall 2010 ICSJWG Presentation, Essential Cyber Security Implementation for Industrial Control Systems
- Serial Connection or Modem
  - War dialers
  - Potential for anyone to get access to system

# 5

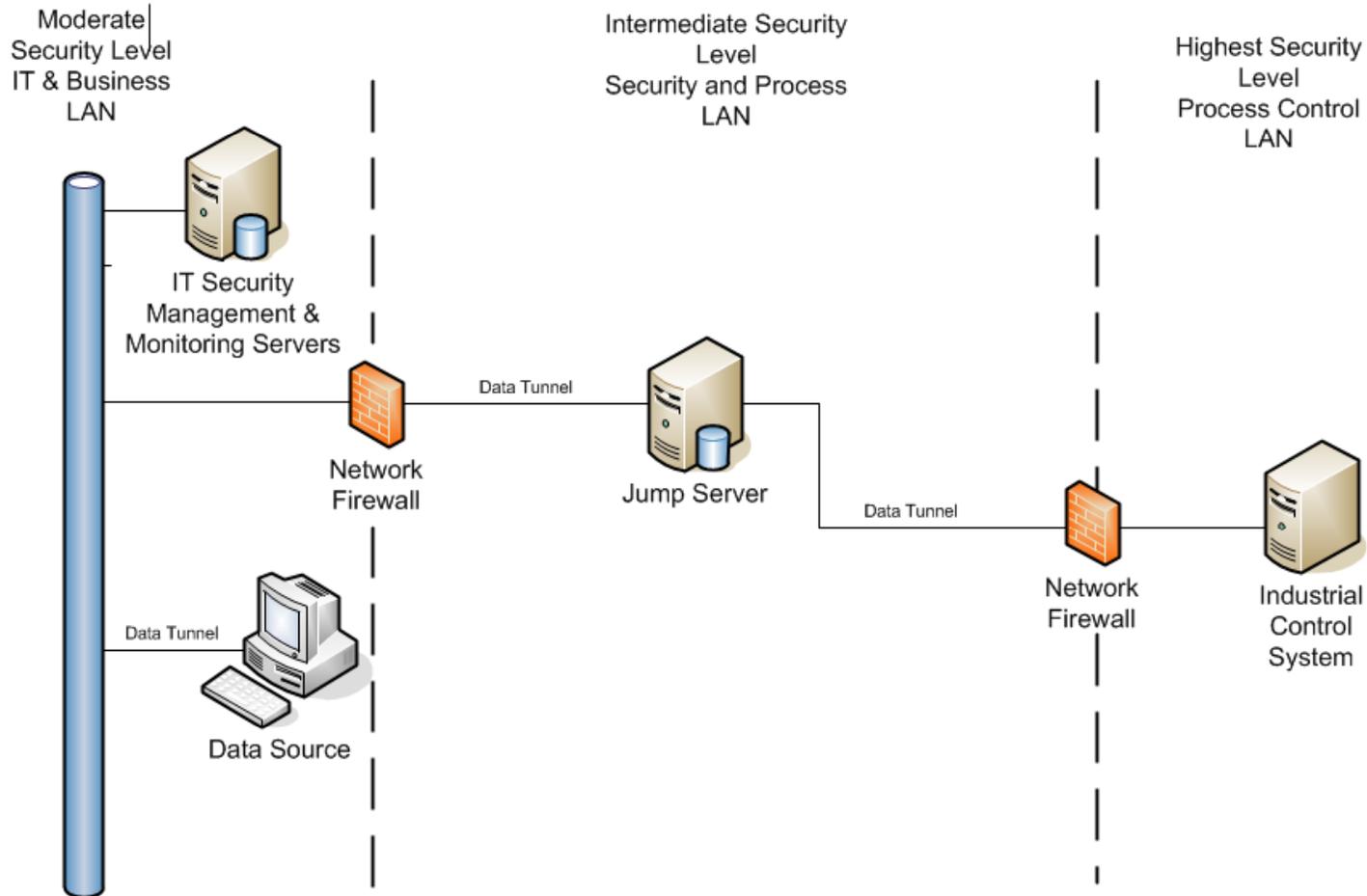
## Solution to Ensure Reliable and Secure Data Transfer

# The Secure Solution

- Use a dedicated server to validate all data for use in an ICS
  - Referred to as a “Jump Server”
- Connect server to ICS and Data source using “VPN” or tunnel
  - IP in IP
  - GRE Tunnel (Supports IPv6)
  - OpenVPN (SSL/TLS)
- Use Separate Network cards for each network connection, no bridging or virtual NIC
- Use firewalls on both sides of Jump Server
- Use Minimum open port rule-set

# The Secure Solution

## ICS Jump Server Network Architecture



# The Secure Solution Software

- Use Linux operating system for the Jump server
  - Linux permits minimum install
  - Linux allows installation of programs necessary to support the MySQL database
  - No need for web browser, e-mail, other potential vulnerabilities
  - Minimizes patching and other support activities
  - Price is very good compared to Microsoft Server
- Use MySQL and Stored Procedures for all data validation
  - Stored procedures provide additional level of validation and security
  - Provides similar schema and capabilities as other databases
  - Price is very good compared to Microsoft SQL Server

# The Secure Solution Hardware

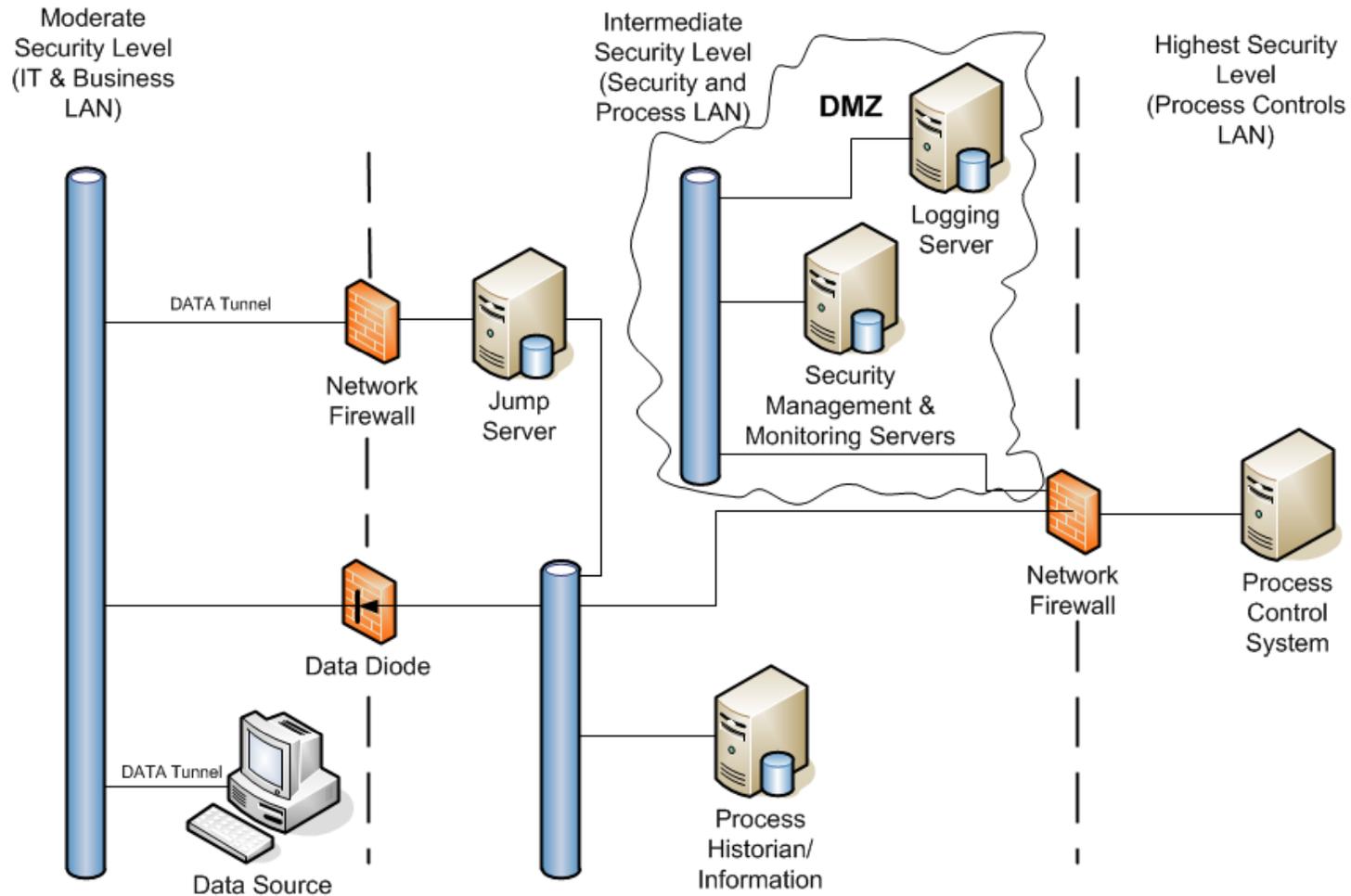
- Using Linux reduces need for high end server
  - Linux has low overhead so server will run fast
  - Spend money on data storage since Linux will run on a slower processor
  - Jump Server will not be a high traffic server so need for high end “enterprise” server not needed
  - Firewalls do not need extreme transport speeds
  - This all reduces Jump Server cost

# The Secure MySQL Solution

- All input Data will be in specific format so data validation is easy
- MySQL schema very specific and limiting to provide additional data validation
- No BLOBS or Binary Fields
- Data from external source should be:
  - Numeric
  - Text
  - Date/Time
- If you don't know the type and details of data, how can you securely put it in your ICS

# Complex Secure Solution Architecture

## Jump Server with Logging and Security Architecture



# More Complex Secure Solution

- Use Separate Jump Server, not virtual machine
- Integrate Jump Server connectivity into security network
- Does not impact Logging and Security Servers
- Firewall rules very limited and specific to tunnel to the Jump Server
- Allows backup to an external device
- Assists in meeting compliance requirements
  - Will require explanation of Firewall and Jump Server settings
  - Justification of need for external data

# 6

## Advantages and Disadvantages of Recommended Solution

# Advantages

- Provides secure ability to transfer data to an ICS
- Hardware and software are reasonably priced
- Easily integrated into the existing network architecture
- Assists in meeting regulatory requirements
- Typical and prominent attack vectors do not apply
- Patching is minimal and can be performed without restart
- Linux was initially developed with security capabilities
- Linux installation does not require unnecessary software installed as part of the OS

# Disadvantages

- Many not experienced with Linux
- Linux is Open Source so licensing must be thoroughly reviewed
- MySQL is Open Source with specific license criteria
- This is not a proprietary solution
- Some training will be required to support long term implementation
- Some Linux versions upgrade kernel annually
- No specific vendor support
  - Invensys CISP does support this solution
- Hardening of components is still required
- Not a “cookie cutter” solution

# 7

## Review and References

# Review

- Transfer of data to an Industrial Control System (ICS)
- Current methods of data transfer
- Problems with using current data transfer methods
- Solution to ensure reliable and secure data transfer
- Advantages and Disadvantages of solution

# Presenter Information

**Bernie Pella, GIAC GSLC**

CISP, Principal Consultant

Critical Infrastructure & Security Practice

M: +1.706.504.7753

O: +1.706.993.2221

i n v e n s y s

Critical Infrastructure & Security Practice

# Questions

