



# Addressing Embedded Security in LabVIEW RIO Systems

Carlos Pazos

Product Marketing Manager








Embedded Software

# Why Care About Security?

## ATTACK ORIGINS

#	COUNTRY
557	 China
347	 United States
183	 Russia
182	 France
57	 Taiwan
42	 Singapore
39	 Hong Kong

## ATTACK TYPES

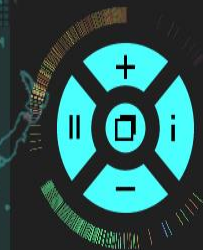
#	PORT	SERVICE TYPE
175	23	 telnet
102	10881	 unknown
101	5902	 vnc-2
75	80	 http
60	8080	 http-proxy
50	137	 unknown
46	6379	 unknown

## ATTACK TARGETS

#	COUNTRY
1116	 United States
330	 Russia
75	 Philippines
61	 Taiwan
53	 Saudi Arabia
51	 France
14	 Hong Kong

## LIVE ATTACKS

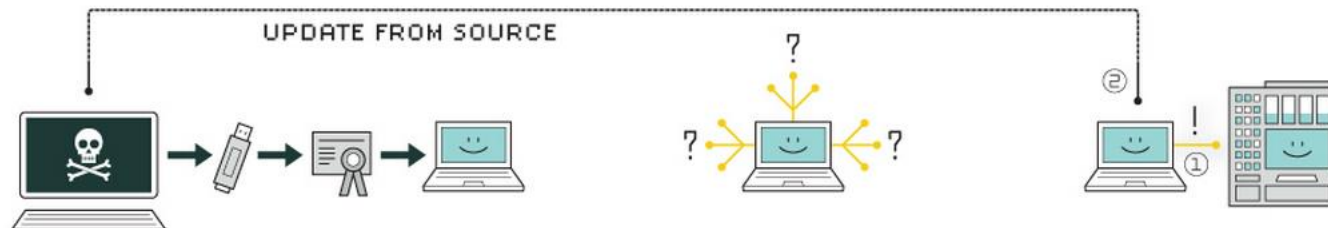
TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER ...	TARGET GEO	ATTACK TYPE	PORT
16.06.2015 16:2...	Chinanet Jiangsu Province Net...	222.186.2...	Nanjing, CN	Saint Loui...	vnc-1	59...
16.06.2015 16:2...	Chinanet Jiangsu Province Net...	222.186.2...	Nanjing, CN	Saint Loui...	vnc-1	59...
16.06.2015 16:2...	Chinanet Jiangsu Province Net...	222.186.2...	Nanjing, CN	Saint Loui...	vnc-1	59...
16.06.2015 16:2...	Chinanet Jiangsu Province Net...	222.186.2...	Nanjing, CN	Saint Loui...	vnc-1	59...
16.06.2015 16:2...	Chinanet Jiangsu Province Net...	222.186.2...	Nanjing, CN	Saint Loui...	vnc-1	59...
16.06.2015 16:2...	Chinanet Jiangsu Province Net...	222.186.2...	Nanjing, CN	Saint Loui...	vnc-1	59...
16.06.2015 16:2...	Chinanet Jiangsu Province Net...	222.186.2...	Nanjing, CN	Saint Loui...	vnc-1	59...
16.06.2015 16:2...	Chinanet Jiangsu Province Net...	222.186.2...	Nanjing, CN	Saint Loui...	vnc-1	59...



# Why Care About Industrial Security?



# Stuxnet Explained



## 1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

## 2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

## 3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



## 4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

## 5. control

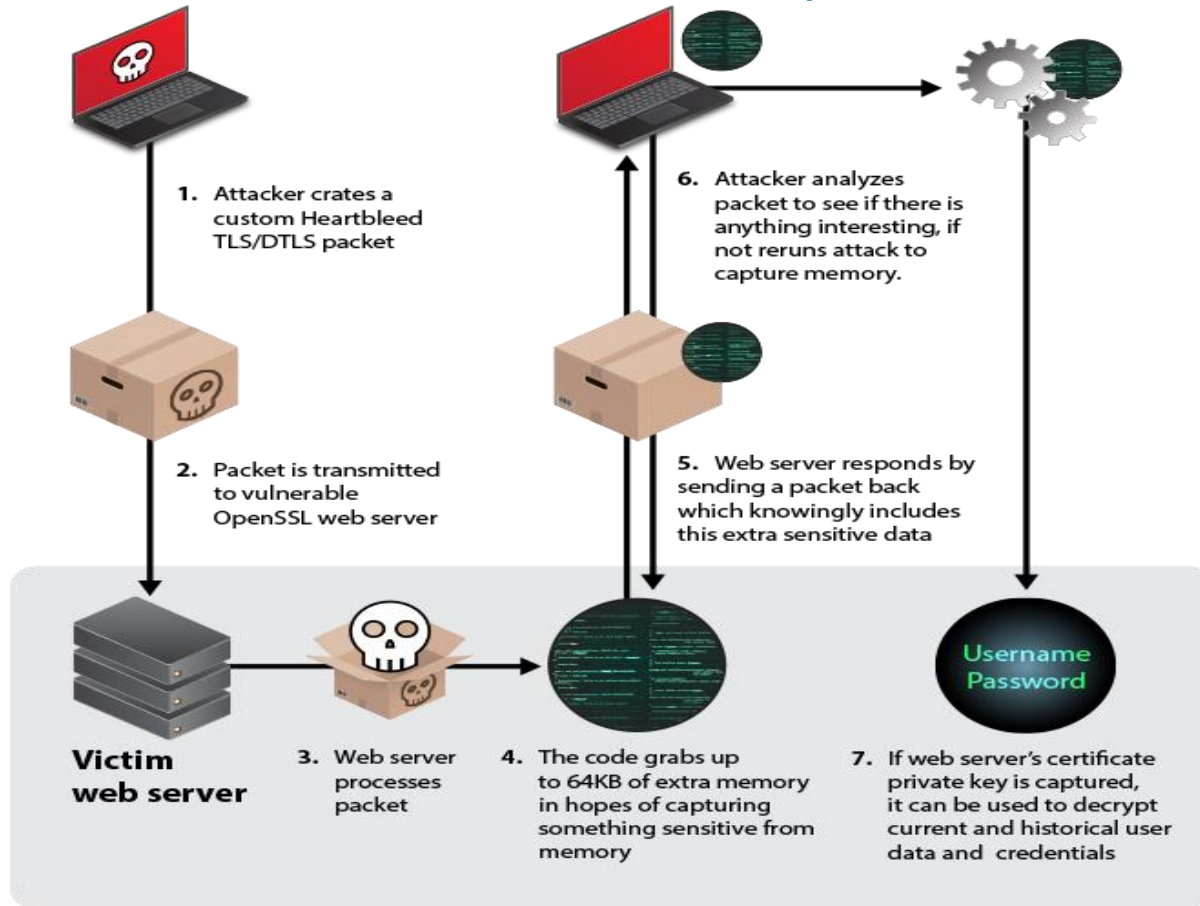
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

## 6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.



# OpenSSL Heartbleed Vulnerability



# Security is a Shared Responsibility

- **Customers:** Define security objectives, assess application-specific risks, evaluate and implement security steps
- **NI:** Provide best practices, provide security features that enable deployment in your threat environment, listen to customer's feedback for the future

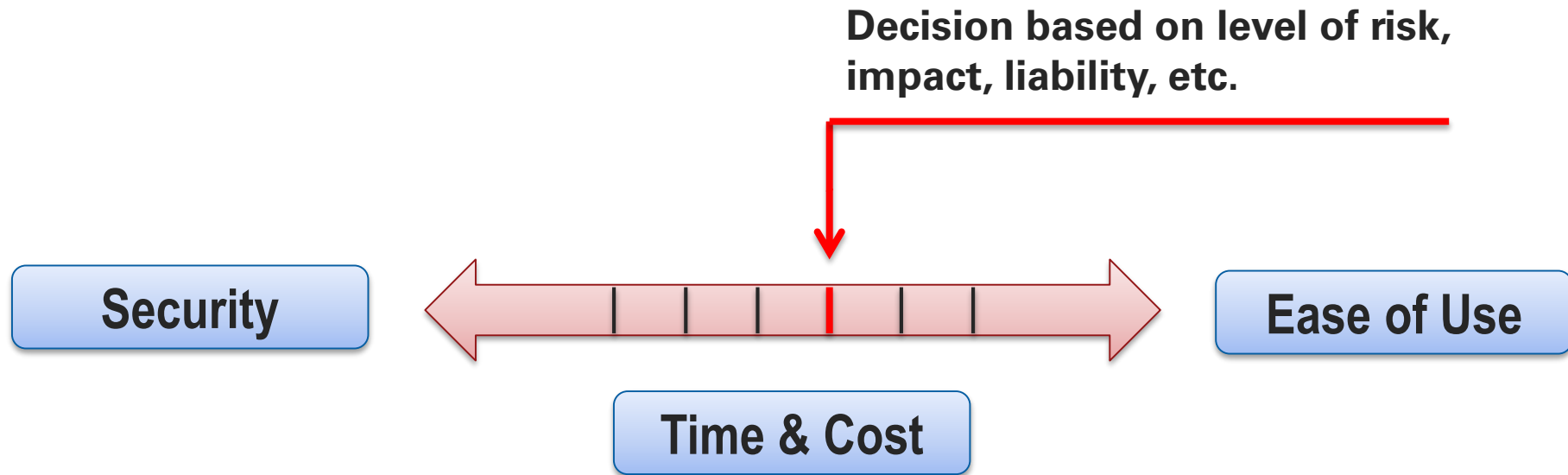
**We want to work with our customers to tackle this complex challenge.**



How much time should be invested in security?



# Balancing Security with Other Constraints



# The Challenge

## **Development is hard:**

Build a system that functions as designed

## **Security is really hard:**

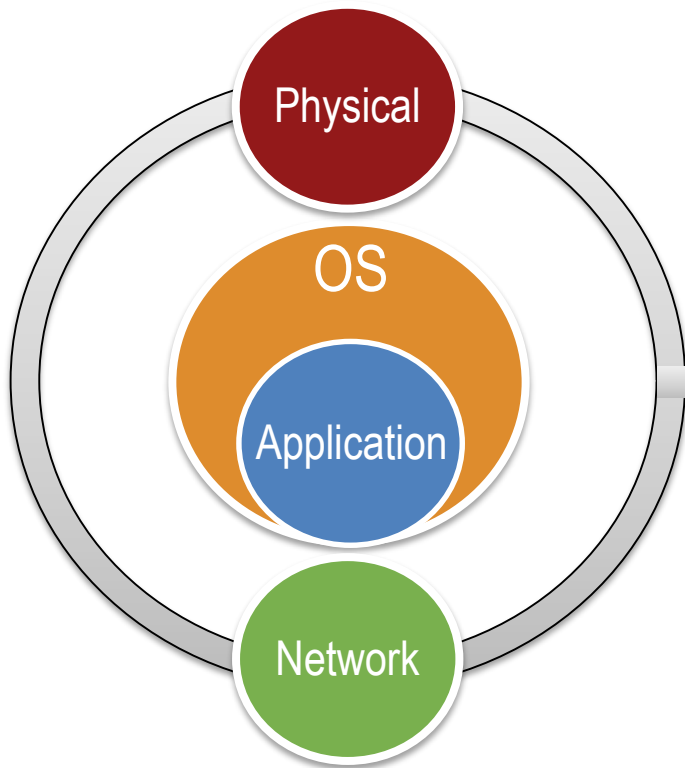
Build a system that *can't be used any other way*

*Examples: Surveillance, theft, impersonation, base of operations*

"A system's security is a function of its weakest link."

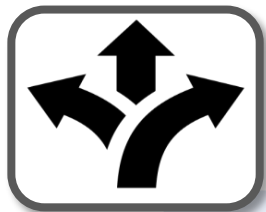
# Layered Model of Security

- Security can be defined at many layers
- A breach at any layer can compromise other layers
- “Don’t invest in a retinal scanner for your house if you are going to leave your window open”
- “Defense in Depth”

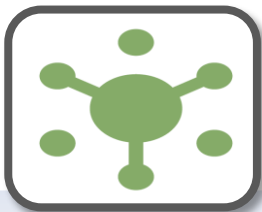


# CompactRIO Development Stages

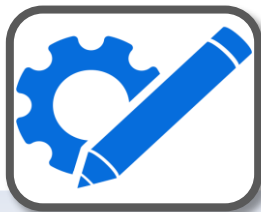
Platform  
Selection



System  
Configuration



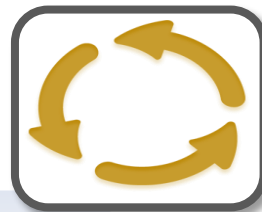
Application  
Development



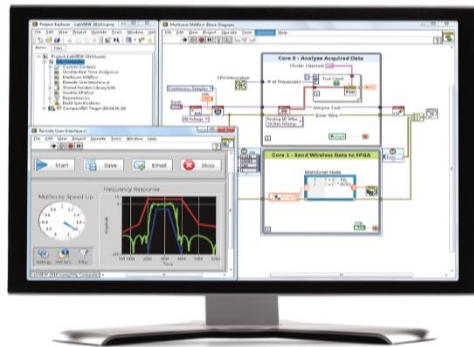
Application  
Deployment



Application  
Maintenance



# CompactRIO Development Stages



**Development and/or  
Deployment PC**

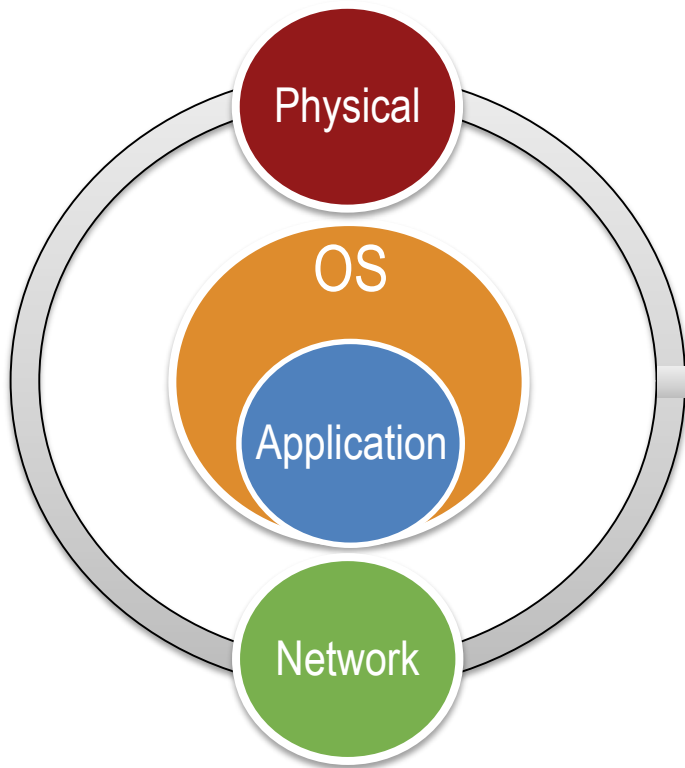
**Ethernet**

A red dashed double-headed arrow pointing from the PC to the CompactRIO system.

**CompactRIO Embedded  
System**

# Agenda: Security Best Practices

1. Physical Security
2. Network Security
3. Application & OS Security
  - NI Linux Real-Time





# Physical Security

# Physical Security



- Limit environmental/physical access to Host PC and physically enclose the real-time target
- Disable or require encryption on I/O (USB, CD Drive, etc.)
- Implement hardware checking
  - USB dongle for IP Protection
  - Digital I/O to validate that enclosure is properly secured

# Network Security

# General Network Security

- **Secure network**

- Isolated network if possible; firewall if you connect to public infrastructure

- **Use web services for network communication**

- HTTPS provides integrity and confidentiality
- SSL certificate-based authentication between devices
- Password-based user authentication between services

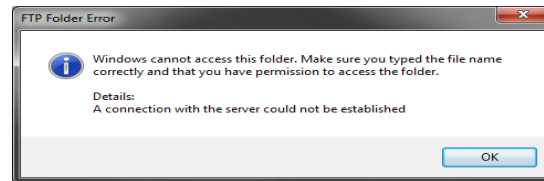
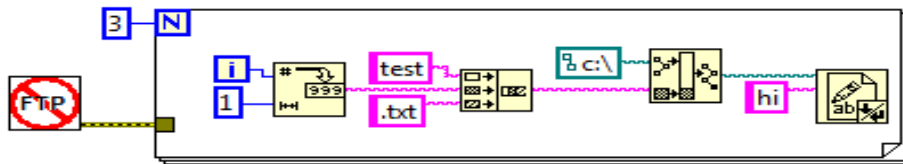
- **Understand the security risk of network protocols.**

No authentication nor confidentiality for:

- Remote Front Panel, Remote VI Server, Network shared variables
- Mitigation:
  - **Good:** Use IP address access control, blacklist Exported VIs
  - **Better:** Use lower-layer tunnel (e.g. VPN or SSL)

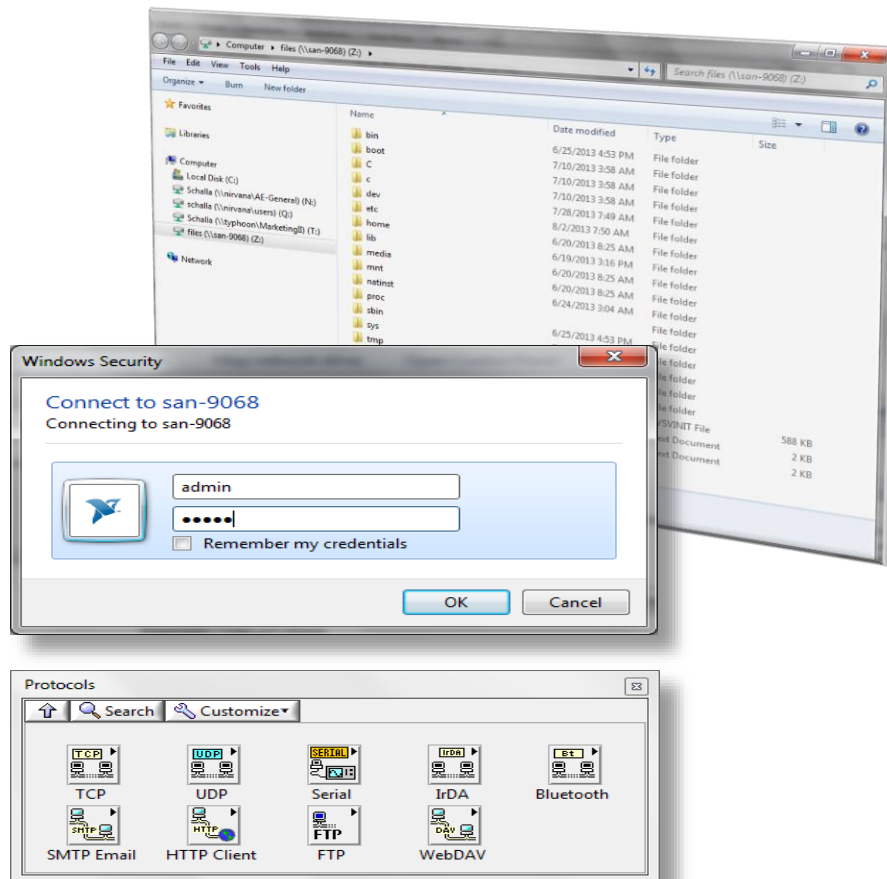
# Disabling the FTP Server

- Only on **VxWorks & Phar Lap**
  - There is no unsecured FTP by default on NI Linux RT
- Use Shutdown RT FTP Server VI in your RT application
- Must reboot to enable FTP server
  - Disable RT Startup App to enable FTP



# File Transfer: WebDAV

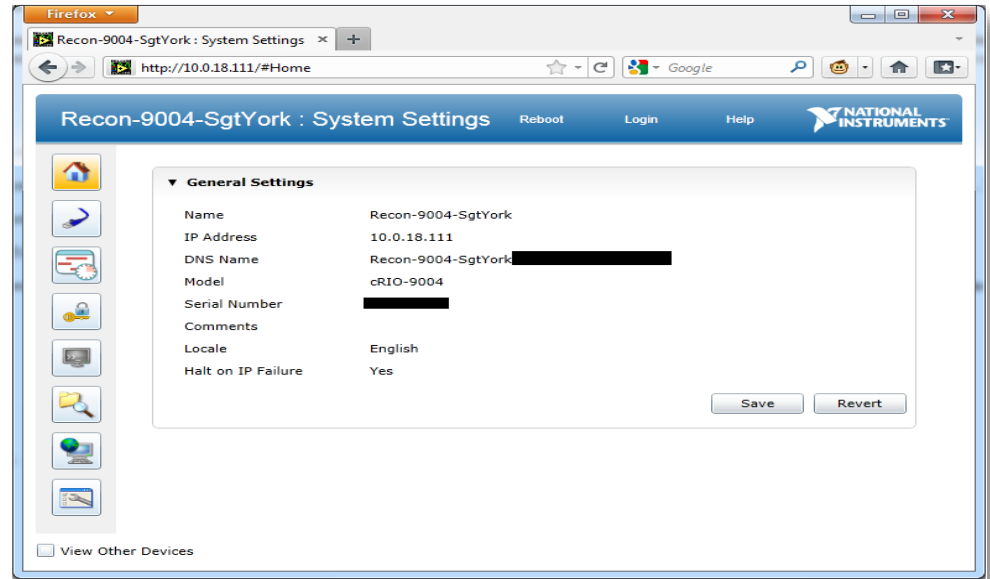
- Industry Standard Protocol
- Manage files on targets remotely over HTTP(S)
- Secure File Access
  - Authentication & Encryption
- Supported by all modern OSes and Web Browsers
- LabVIEW API for programmatic access
- WebDAV File Browser





# Web Based Configuration and Monitoring

- Use to access NI Auth settings
- cRIO:
  - [http://<cRIO\\_ip.addr>](http://<cRIO_ip.addr>)
- Host PC
  - [http://<host\\_ip.addr>:3582](http://<host_ip.addr>:3582)



# NI-Auth Users & Permissions

The screenshot shows the 'Recon-9004-SgtYork : Security Configuration' window. The 'Users' tab is selected, showing a list of users with 'admin' selected. The right pane shows the configuration for the 'admin' user.

**User Name:** admin

**Built In:** ☒

**ID:** 0

**New Password:** [Empty field]

**Password Last Changed:** Thursday, July 28, 2011 1:31:14 PM

**Comments:** [Empty text area]

**Group(s):**

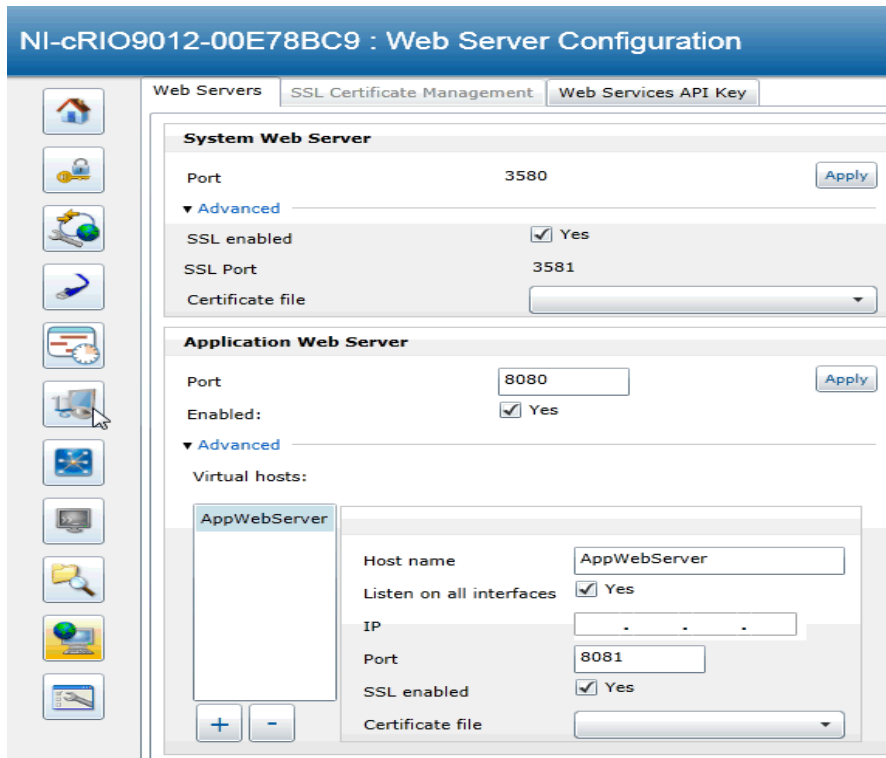
Name	Is Part of Group?
administrators	<input checked="" type="checkbox"/>
everyone	<input checked="" type="checkbox"/>
powerusers	<input type="checkbox"/>
users	<input type="checkbox"/>

**Permission(s):**

Name	Has Permission?
FSDelete	<input checked="" type="checkbox"/>
FSRead	<input checked="" type="checkbox"/>
FSWrite	<input checked="" type="checkbox"/>
GetDB	<input checked="" type="checkbox"/>
ManageExtensions	<input checked="" type="checkbox"/>
Reboot	<input checked="" type="checkbox"/>
RemoteShell	<input checked="" type="checkbox"/>
SetDB	<input checked="" type="checkbox"/>
SetDeviceInfo	<input checked="" type="checkbox"/>
SetLocale	<input checked="" type="checkbox"/>
SetRTLockPassword	<input checked="" type="checkbox"/>
SetSystemConfiguration	<input checked="" type="checkbox"/>
ViewConsoleOutput	<input checked="" type="checkbox"/>
WiFiConfigureAppServer	<input checked="" type="checkbox"/>

- **Change password on 'admin' account**
- Set permissions on users and groups to restrict users & groups to only activities they are responsible for
- Currently applicable only to web services and web management

# Enable SSL



- Enable SSL for both System and Application Web Servers
- Turn off HTTP version and rely only on the HTTPS version
- Select and setup self signed certificates or go through a CA
- System Web Server available at
  - `https://<cRIO_ip.addr>`
  - `https://<host_ip.addr>:3581`

# Web Services Security palette

- Allows web service to retrieve NI-Auth attributes

- User name
- Group
- Permissions
- Session key (320 bits)

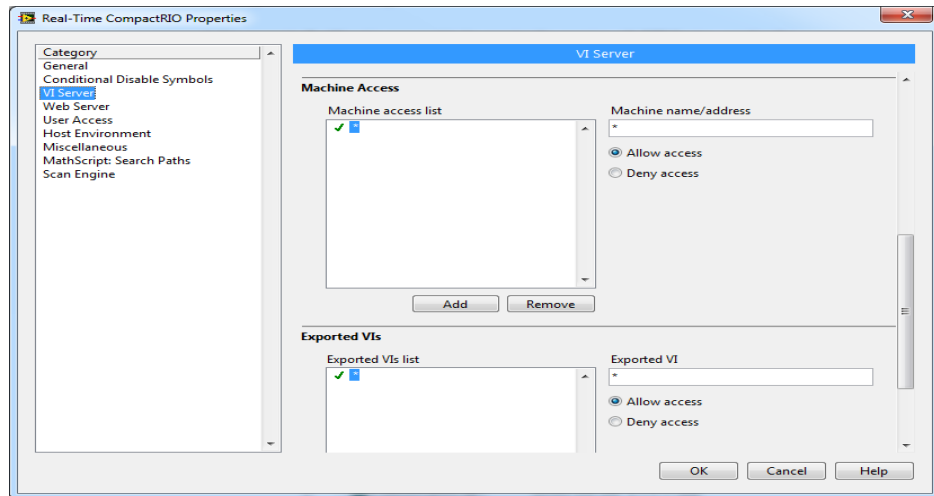
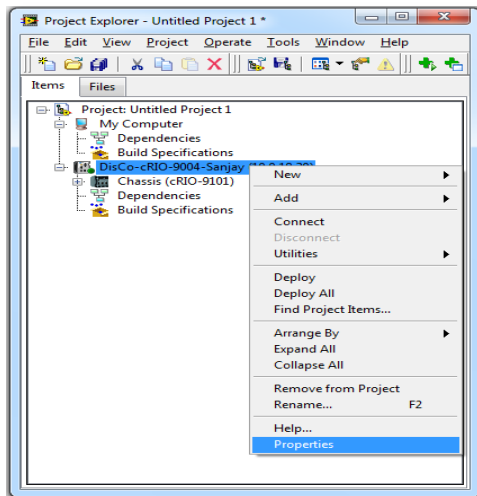


- Encryption functions that use the session key
  - Secure Remote Password (RFC 2945) using SRP\_SHA1
  - Message confidentiality
  - Message authentication/integrity using third-party HMAC



# Managing VI Server Access

- Manage VI Server (TCP) Access to prevent 'LabVIEW' viruses
  - Prevent remote access & execution of code on your PC or RT target
- For Host PC: Tools » Options » VI Server
- For cRIO: use Project Explorer as shown here

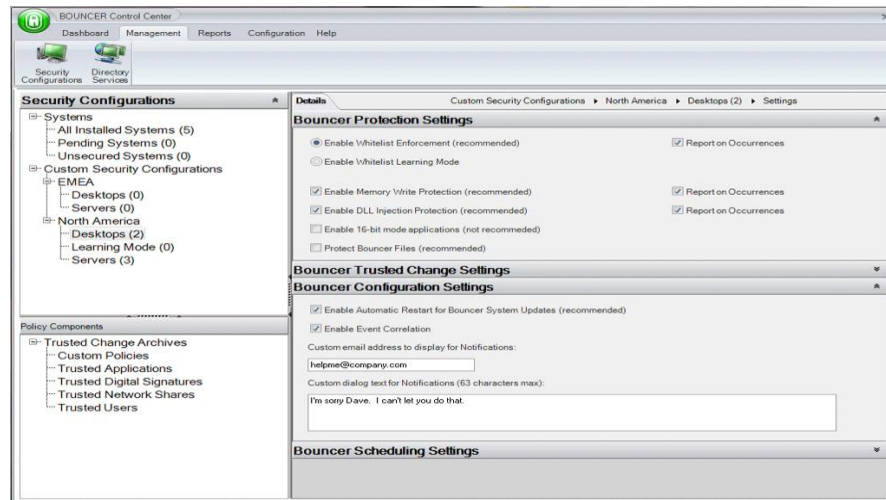


# Application & OS Security



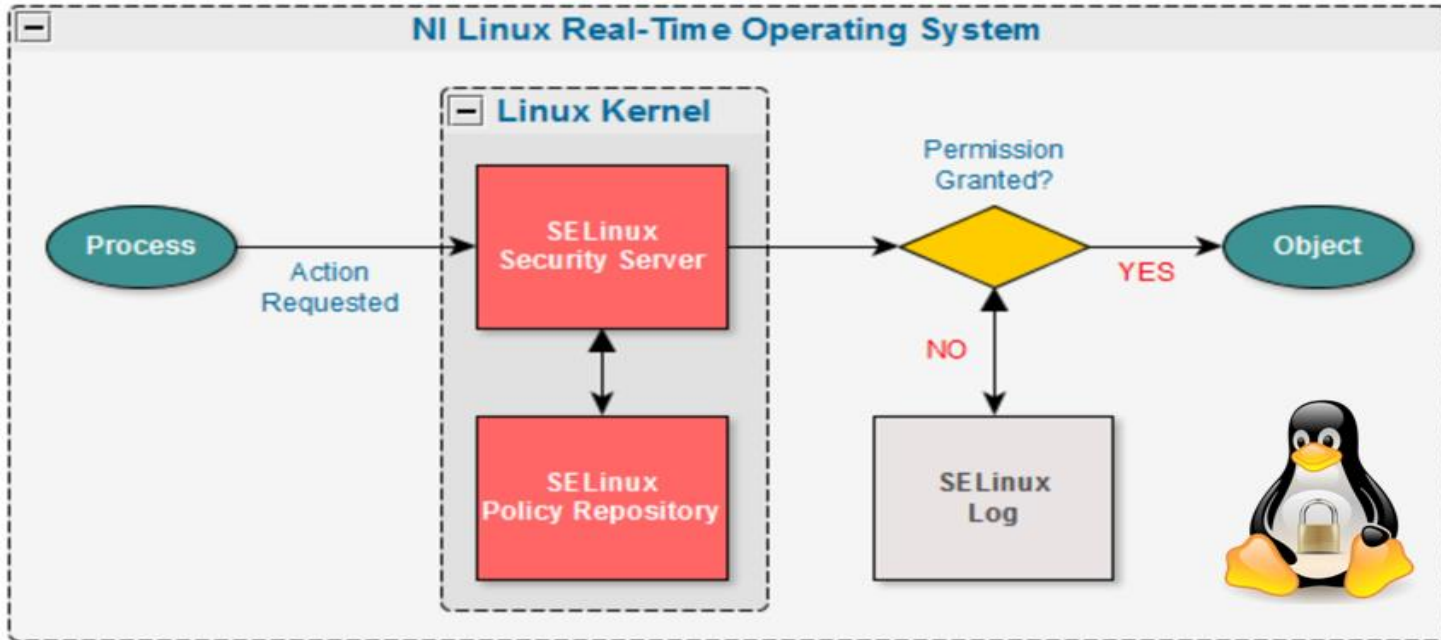
# Application Whitelisting

- Use to regulate code execution on host computer
- Compute and store checksum in a known good state
- Compare checksum against table
- Solutions:
  - CoreTrace Bouncer
  - McAfee Application Control
  - Bit9 Parity Suite
  - Microsoft AppLocker



# Malicious Code Prevention

## Security Enhanced Linux (SELinux)



# GitHub Reference Policy

The screenshot shows the GitHub interface for the repository 'ni / ni-refpolicy'. At the top, the GitHub logo is on the left, followed by a search bar with 'This repository' selected. Navigation links for 'Explore', 'Features', 'Enterprise', and 'Blog' are on the right. Below the repository name, there is a 'Watch' button with a count of 5. The description reads 'NI's SELinux reference policy.' A statistics bar shows 3,834 commits, 3 branches, 0 releases, and 20 contributors. Below this, a green 'fork' button is next to a 'Branch: master' dropdown and the repository name 'ni-refpolicy / +'. A commit history section shows a commit titled 'README.md: add blurb for udev-cache issues' by 'harisokanovic' on Apr 28, with a sub-commit by 'beshelto' on Apr 29. The latest commit hash is 'e49ecf0c95'. Below the commit history, a file named 'config' is listed with a commit message 'natinst: Added admin user to have same permissions as root' from 7 months ago. The bottom of the image has a torn paper effect.

**GitHub** This repository Search Explore Features Enterprise Blog

**ni / ni-refpolicy** Watch 5

NI's SELinux reference policy.

3,834 commits 3 branches 0 releases 20 contributors

Branch: master **ni-refpolicy / +**

README.md: add blurb for udev-cache issues ...

**harisokanovic** authored on Apr 28 latest commit e49ecf0c95

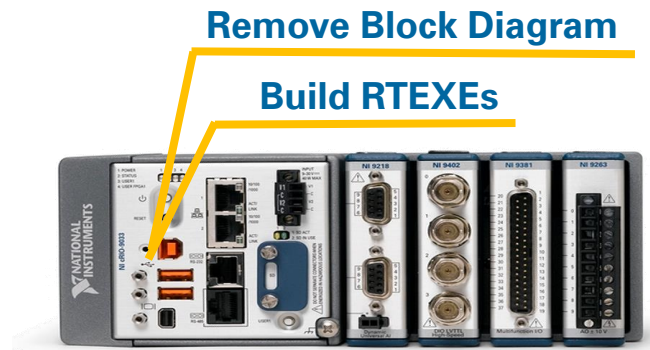
→ **beshelto** committed on Apr 29

**config** natinst: Added admin user to have same permissions as root 7 months ago

# Sensitive Data Protection

- Options for encrypting data in storage
  1. Several individuals offer LabVIEW VIs
    - Caution: Much slower than C/C++ implementations
  2. Use .NET library in LabVIEW
    - system.security.cryptography library
    - Add reference to mscorlib.dll
  3. Use DLL calls to the host OpenSSL/CAPI library
- General principle: "*Ensure the confidentiality of sensitive data through its entire lifecycle.*"

# LabVIEW and LabVIEW Real-Time Application Security



- Remove the block diagram: [LabVIEW Help: Removing Block Diagrams from VIs](#)
- Use Build Specifications such as EXEs & RTEXEs
- Remove the source code and the development environment from host computers on the deployed network

# LabVIEW FPGA

## Application Security



**FPGA Bounds**



**FPGA Safe States**

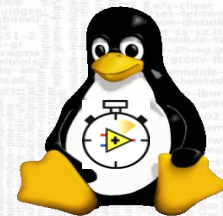
- Implement bounds checking on FPGA I/O to prevent damage
- Use an FPGA Watchdog over RT and default to FPGA 'safe states' if something is erroneous on RT



# NI Linux Real-Time

# NI Linux Real-Time

- Owned and maintained by NI
  - Custom built and optimized for NI embedded hardware
    - Supports ARM and x64, with cross-compilers provided
  - Easier integration of third-party peripherals and applications as most have Linux drivers or packages available
  - NI Package Repository: [download.ni.com/ni-linux-rt/](http://download.ni.com/ni-linux-rt/)
    - Over 3,000 packages
  - OS source: [github.com/ni](https://github.com/ni)
- PREEMPT\_RT
  - Enables real-time reliability through pre-emption, priority inheritance, and scheduling
  - Standard approach to real-time performance on Linux



# Linux Ecosystem



## Database

Raima  
MySQL  
SQLite  
MongoDB  
CouchDB



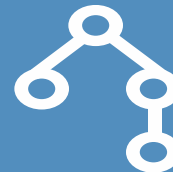
## Security

**SELinux**  
OpenVPN  
IP Tables  
System Logging  
fail2ban  
denyhost



## Code Re-use

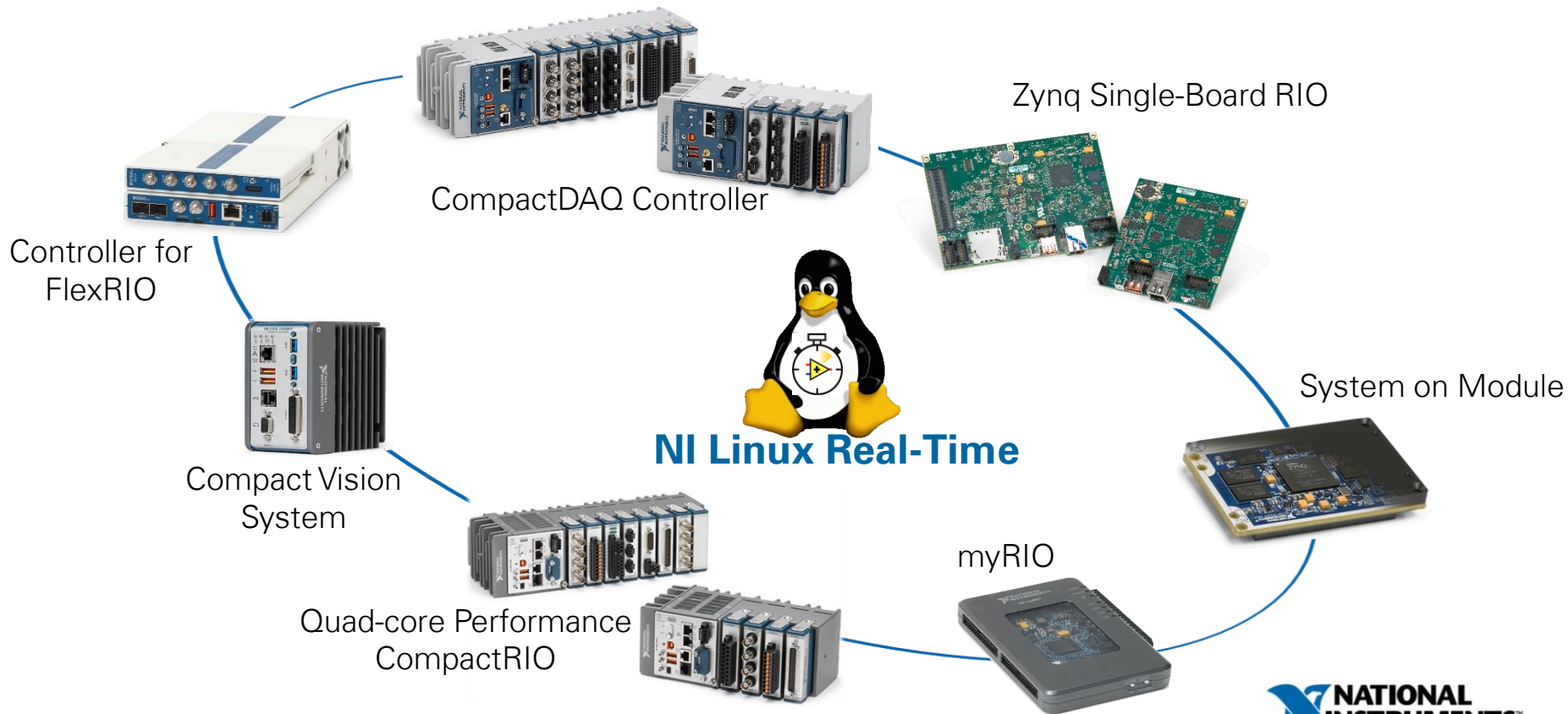
C/C++  
Shell scripting  
Python  
Ruby  
Perl



## Connectivity

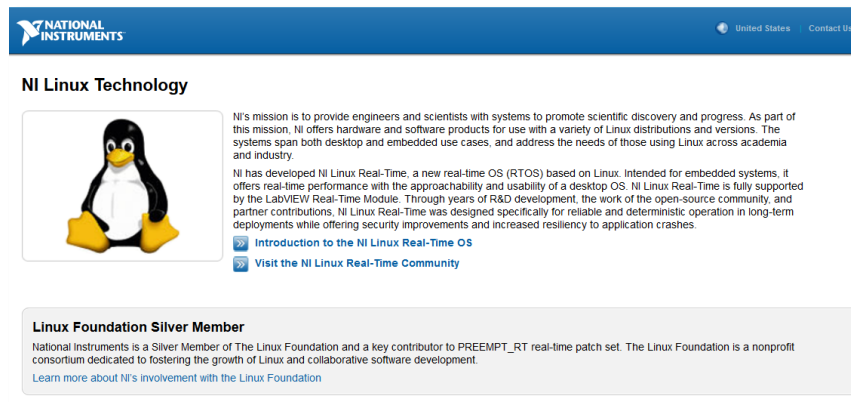
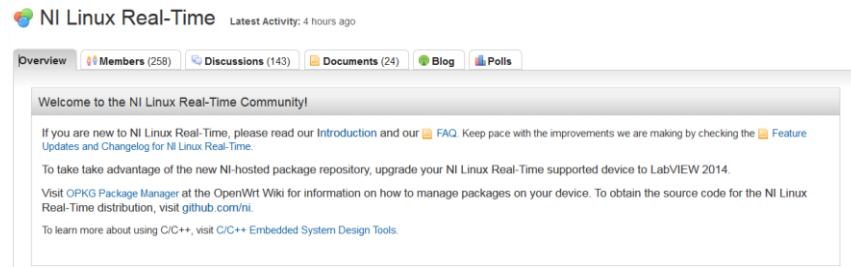
Isshd  
IPv6  
SNMP  
NTP  
netstat

# Integration with the Latest Hardware Products



# Key Resources

- [ni.com/linuxrtforum](https://ni.com/linuxrtforum)
  - Tutorials
  - Documentation
  - Forum for discussions
- [ni.com/linux](https://ni.com/linux)
  - Links to whitepapers
  - Embedded and Desktop uses
- [download.ni.com/ni-linux-rt/](https://download.ni.com/ni-linux-rt/)
  - Package Repository
- [github.com/ni](https://github.com/ni)
  - OS Source



# Next Steps

- Sign up at [ni.com/security](https://ni.com/security)
- Leverage online resources: [Overview of Best Practices for Security on NI RIO Systems](#)
- Engage NI with security needs such as security certifications (NERC CIP, IEC 62351, etc.)
- Use the Best Practices Checklist to evaluate and secure your system

## RIO Security Checklist

### Recommended:

Host	RIO Device
<input type="checkbox"/> Network Firewall	<input type="checkbox"/> VI Server Access
<input type="checkbox"/> Anti Virus	<input type="checkbox"/> NI Auth Settings
<input type="checkbox"/> OS Updates	<input type="checkbox"/> SSL System Web Server
<input type="checkbox"/> OS 'Limited User Accounts'	<input type="checkbox"/> SSL App Web Server with Web Service
<input type="checkbox"/> VI Passwords	<input type="checkbox"/> Disable FTP
<input type="checkbox"/> Build EXEs, remove source code	<input type="checkbox"/> RIO on internal network
<input type="checkbox"/> VI Server Access	<input type="checkbox"/> FPGA Bounds
<input type="checkbox"/> NI Auth Settings	<input type="checkbox"/> FPGA Safe States
	<input type="checkbox"/> RTEXE, not interactive mode <input type="checkbox"/>

### Optional:

Host	RIO Device
<input type="checkbox"/> Limit Physical access	<input type="checkbox"/> Limit Physical access
<input type="checkbox"/> Disable/Encrypt I/O (USB hub, CD Drive, etc.)	<input type="checkbox"/> VPN Hardware Firewall/Router
<input type="checkbox"/> Status signal to RT	<input type="checkbox"/> Status signal to host
<input type="checkbox"/> Change default ports	<input type="checkbox"/> Change default ports

### Extreme:

Host	RIO Device
<input type="checkbox"/> Application <del>Whitelisting</del>	<input type="checkbox"/> Software Checking
<input type="checkbox"/> Change default ports	<input type="checkbox"/> Hardware Checking
	<input type="checkbox"/> Encrypt Communication between FPGA and RT

### Resources:

[DevZone Article: Overview of Best Practices for Security on NI RIO Systems](#)  
Contact your local rep and/or support

# Questions?



## **Carlos Pazos**

Product Marketing Manager  
Embedded Software  
[carlos.pazos@ni.com](mailto:carlos.pazos@ni.com)