I Want to Be Secure: Best Practices for Securing Your PI System

Presented by

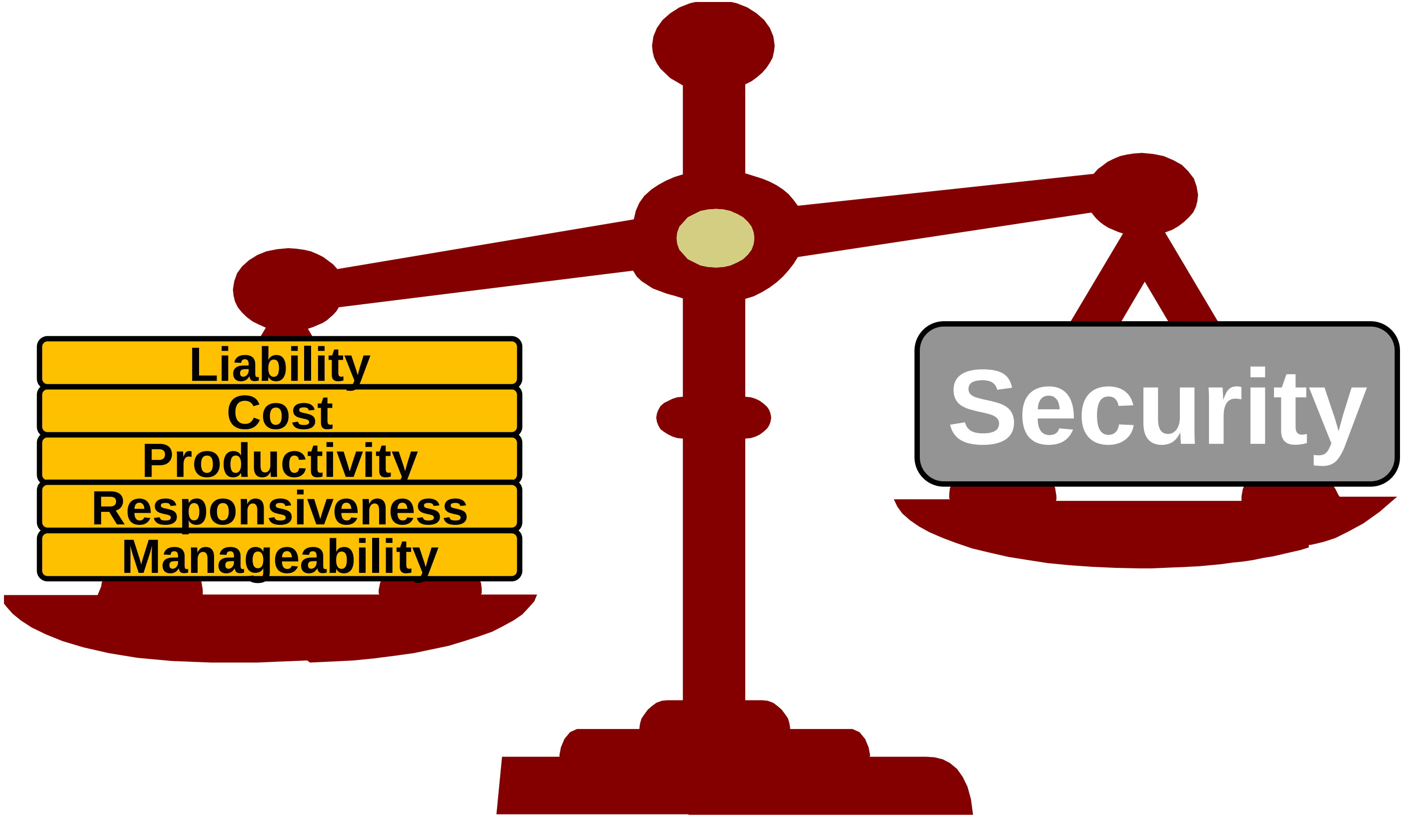
Michael Jakob,

Head of Field Service and Customer Support EMEA

What is a best practice for security?

- Security is all about risk mitigation
- Best practices for security are:
  - Not necessarily about technology, it’s technique and methods
  - Must be practical and effective
  - Not absolutes, but guidelines for application
  - **Everyone is different, must adapt security for your situation**

How much security is "good enough"?



Why is security so hard?

- Implementing security requires effort – cost can be high
- Security needs change – expanding scope, unclear requirements
- **Working with other groups – especially IT!**
- Multiple software tools – different configurations
- Various security architectures – throughout PI System and organization
  - Crossing network boundaries – Process Control Network vs. Business Network
  - External access – across firewalls and Internet
- Manageability effort is high:
  - Adding/removing users and groups
  - Remembering passwords – Single Sign On (SSO)

How does the PI System help?

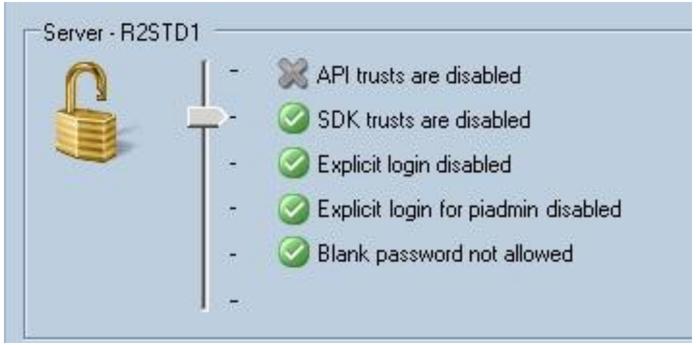
- Acts as secure layer between end users and control systems or critical assets
- No need to reinvent the wheel
  - PI System integrates with Microsoft technologies and your existing IT infrastructure
  - If you’re using Windows security for SQL Server or other data sources, then PI System security is analogous

Where does Windows security apply in PI System?

- Securing access to all nodes in the PI System
  - PI Interfaces, PI Server, PI Data Access, PI Clients
- Securing the PI System through the network
  - Intranet and Internet
- Securing PI System data and metadata
  - PI Tags, PI AF elements, etc.
- Securing files and configuration
  - Archives, displays, spreadsheets, etc.
- Securing applications
  - SQL Server, SharePoint, Terminal Services, etc.

What options are available in PI Server?

- Explicit Login is disabled by default now
  (TS Bulletin 10/1/09 – Security Alert: PI Authentication Weakness)
- PI Trusts are required for most PI Interfaces, PI ACE, PI Notifications
- Windows security is recommended for all interactive user scenarios
  - No more passwords to remember!
  - Stronger and more flexible security
  - Centralize user management in AD



Server - R2STD1

- ✗ API trusts are disabled
- ✓ SDK trusts are disabled
- ✓ Explicit login disabled
- ✓ Explicit login for piadmin disabled
- ✓ Blank password not allowed

What tools and technologies can help?

- PI Server 2010
  - Supports Windows authentication
  - PI MCN Health Monitor can detect security breaches
  - Audit trail in PI Data Archive and PI Asset Framework
- Additional security technologies
  - Client impersonation using Kerberos, Claims-based Identity
  - Protecting network traffic using IPsec, SSL/TLS, or VPN
  - Unidirectional networks using data diodes (Waterfall, Owl)

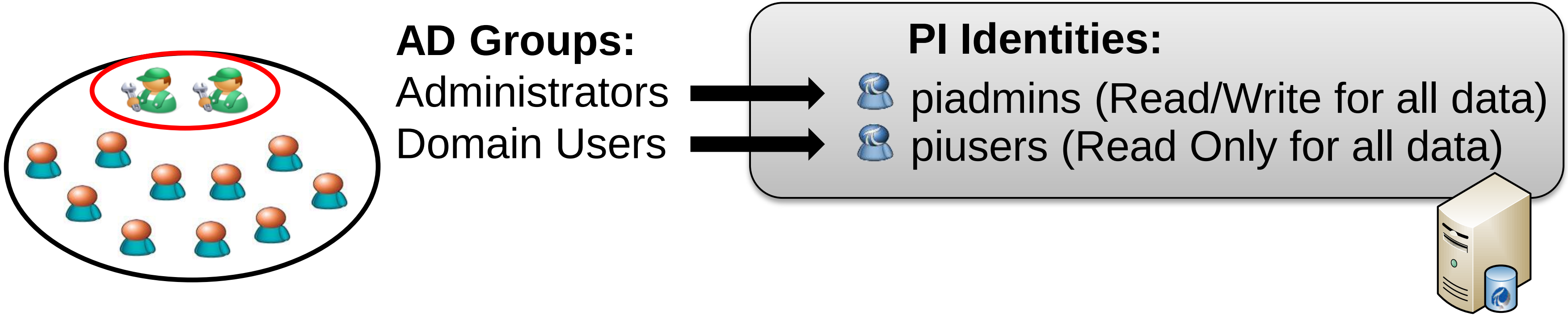
What else should I know about my PI System?

- Any unexpected changes?
- Who is using privileged access?
- Is the operating system healthy?
- Are network connections secure?
- When was the last security review?

What is the right security model for me?

- Role-based security for different groups and access levels
  - Who should access your PI System data
- Determine the right number and type of roles
  - What departments in your organization use the PI System
  - Which PI System products are you using
  - Who manages data vs. configuration vs. applications
  - What data types (tags, elements, displays, etc.) should be secured

What is the easiest way to get started?



AD Groups:

Administrators

Domain Users

PI Identities:

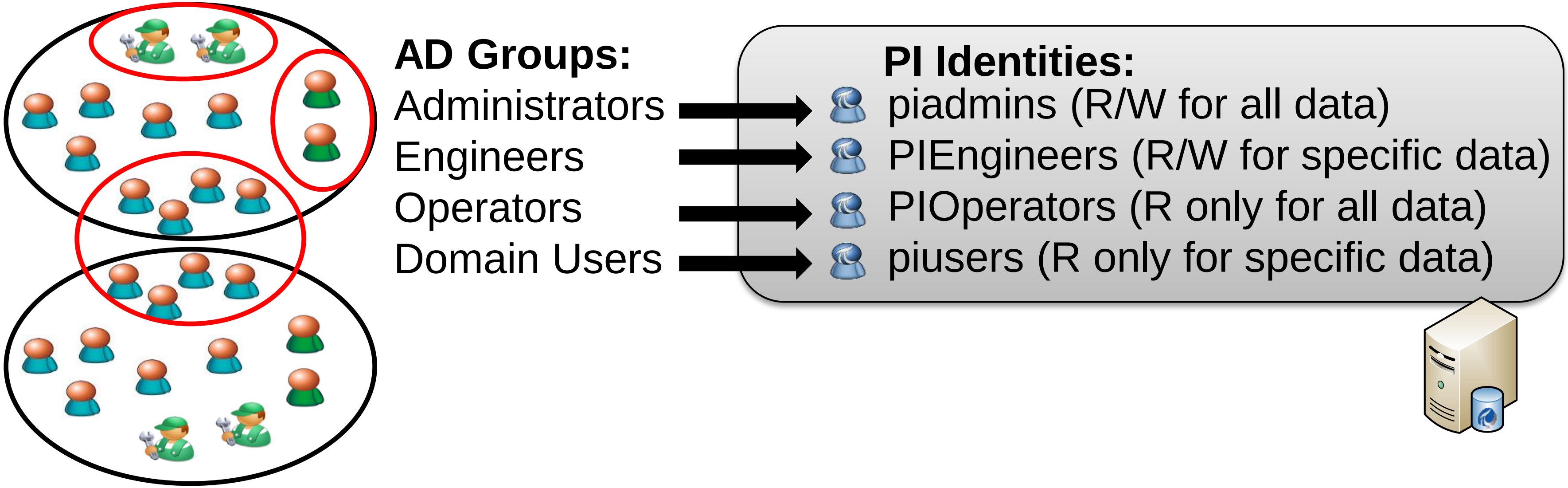
piadmins (Read/Write for all data)

piusers (Read Only for all data)

- First, enable Windows integrated security on the PI System
- Configure mapping between Active Directory Groups and PI Identities
- Only use PI Trusts for PI Interfaces, PI ACE, PI Notifications or other special cases
- Last, disable PI Users and Groups (piadmin/pidemo)

What if I want more control?

- Use the security principle of **least privilege**



AD Groups:

Administrators → piadmins (R/W for all data)

Engineers → PIEngineers (R/W for specific data)

Operators → PIOperators (R only for all data)

Domain Users → piusers (R only for specific data)

PI Identities:

- piadmins (R/W for all data)
- PIEngineers (R/W for specific data)
- PIOperators (R only for all data)
- piusers (R only for specific data)

What should I do next?

- **Review resources on Microsoft and PI System security**
- **Analyze your requirements**
- Plan your architecture
- Acquire/upgrade/install the latest PI System products
- Test/verify your configuration
- Schedule your rollout
- Monitor/audit the PI System
- Watch the Tech Support Site for security info

Where can I learn more?

- Microsoft TechNet Security Process Map
  - Plan and evaluate your IT infrastructure
- OSIsoft Resources on PI System security
  - Tech Support site → Knowledge Center → System Manager Resources → PI Server Security
  - PI System 101 - Security webinar on OSIsoft vCampus
  - Support for Windows Security in PI Server 3.4.380 Training webinar
  - Essentials for PI in a NERC CIP Environment Training webinar
  - KB Article # KB00354: Windows Security Requirements for PI Server 3.4.380.36 and later
  - PI System Manager I Training course

What are the key takeaways?

- There is no “one size fits all” approach to security
- Security is applied across the entire PI System
- Whatever your security policy or requirements, PI System is flexible enough to accommodate it
- OSIsoft (especially Tech Support and Center of Excellence) can help!

Thank you