Strategic Identity Management for Industrial Control Systems

Justin Harvey
Encari

ICSJWG 2010 Spring Conference

Ground Rules

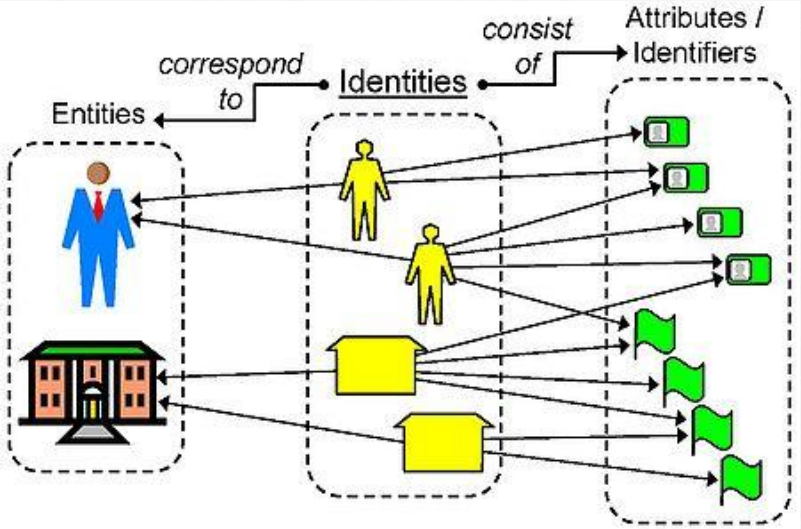
Sticking to vendor neutral

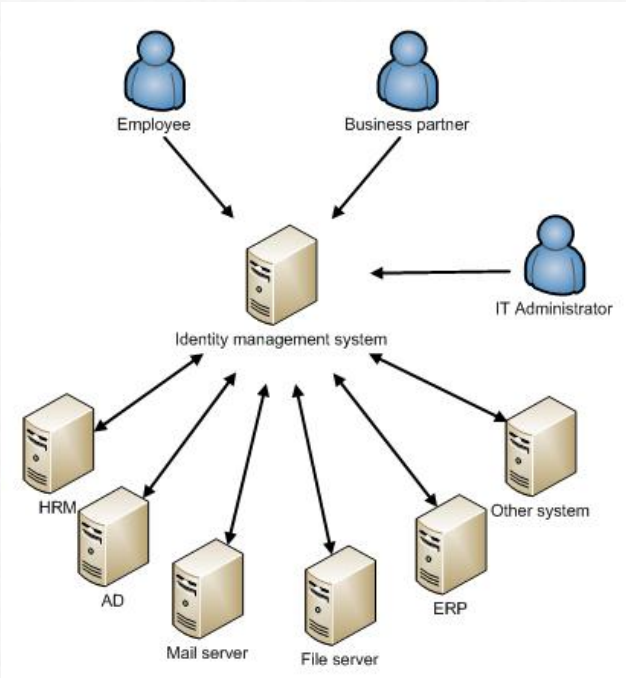
Questions Welcome

Email me for a copy of the deck: jharvey@encari.com

What is an Identity?

“Identity management or IDM is a term related to how humans are identified and authorized across computer networks. It covers issues such as how users are given an identity, the protection of that identity and the technologies supporting that protection such as network protocols, digital certificates, passwords and so on.” -- Wikipedia





What is “Identity Management”?

Known by many acronyms and names

The industry associates the following concepts as being apart of “Identity Management”:

- Access Management
- User Provisioning & De-provisioning
- Password Management and Synchronization
- Self Service
- Delegated Administration
- Workflow Based Services
- Role Based Access Control

- The industry has settled on IAM to denote Identity and Access Management.
- You may also still hear SIM, IDM, metadirectory, user synchronization terms.
- Identity Management is a *concept and process*, not just a technology.

Identity Linking & Centralization

- Most modern day OS provide a unique identifier (UID or GUID)
- Identity Linking is keeping a central repository for dissemination of user data across disparate platforms
- IDM systems may use AD, an LDAP or RDBMS for storage of UID’s

Access Management

It’s not just about cookies

Single Sign-on “The Holy Grail”

Simplified Sign-on - Not always a secure route to take

Does not always have to entail “single password” methods of authentication

Why Associate Identity & Access Management?

These concepts go hand-in-hand. They are Yin & Yang.

Nearly impossible to implement or address one in an environment while not directly or indirectly implementing the other.

Isn’t managing an identity controlling it’s access?

Advanced Identity Management
Role Based Access Control (RBAC)

Provides a mean of assigning roles and privileges in systems subject to attribute conditions, organizational hierarchy, and workflow

RBAC is a “loose” term in the industry these days.

Where’s the ROI? The jury is still out.

Advanced Identity Management Federation

Allow someone else to authenticate your users while exposing very little to the outside world.

Various industry standard protocols exist: SAML, WS-Security, Liberty Alliance Standards, WS Federation etc.

Typically won't be found in an ICS.

Zero Day Start
Zero Day Stop

"Borrowed Term" from our friends at Novell

Traditionally, on-boarding processes typically require one or more steps:

- One or more emails to managers
- Endless HR forms to fill out
- One or more tickets submitted in various systems
- Phone calls without the ability to track status
- Manual workflow approvals

- IDM systems can provide a means of instantly provisioning or ***deprovisioning*** personnel based upon HRMS system events.

Industrial Control Systems

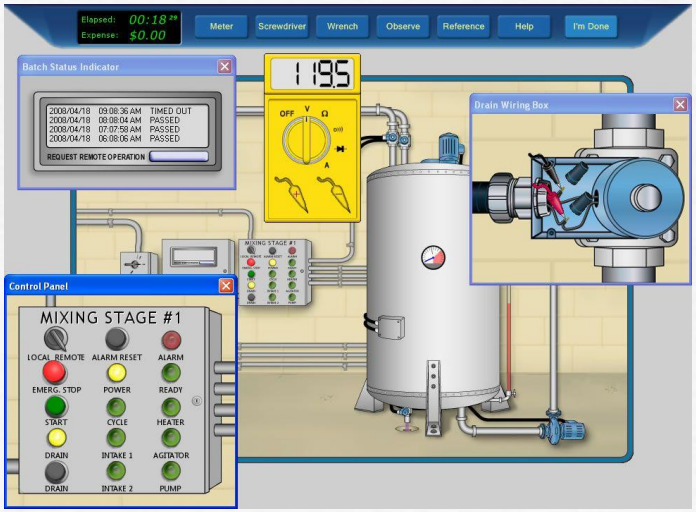
In many cases, systems have been in place 5-20+ years without routine maintenance or security checks.

Cumbersome and difficult to patch due to vendor constraints

Antiquated user and password controls & checks

Newer platforms utilizing Windows for management workstations

Active Directory is becoming more and more prevalent



NERC CIP

Does NERC CIP require an IDM System?

Short answer: No….BUT…..

What reliability standards apply?

- **CIP-004 R4.2:**
  - R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.
- **CIP-005 R2:**
  - R2.4 - Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
  - R2.5. The required documentation shall, at least, identify and describe:
  - R2.5.1. The processes for access request and authorization.
  - R2.5.2. The authentication methods.
  - R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.
- **CIP-007 R5.2 & R5.3:**
  - **R5.2.** The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
    - **R5.2.1.** The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
    - **R5.2.2.** The Responsible Entity shall identify those individuals with access to shared accounts.
    - **R5.2.3.** Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
  - **R5.3.** At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:
    - **R5.3.1.** Each password shall be a minimum of six characters.
    - **R5.3.2.** Each password shall consist of a combination of alpha, numeric, and “special” characters.
    - **R5.3.3.** Each password shall be changed at least annually, or more frequently based on risk.

How does CIP-006 fall under Identity Management?

- **CIP-006 R2:**
  - **R2.** Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
  - **R2.1.** Be protected from unauthorized physical access.
  - **R2.2** Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP- 004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP- 006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

Upon termination, IDM can revoke system privileges as well as physical badge access!

Why the minimum for NERC CIP won't do.

How many Security Managers can stand up and provide an accurate accounting of their user data?

How long does it take for a user to be deactivated and removed from key control systems in the event of a termination? How about non critical cyber assets?

If an unauthorized login attempt is detected, how will you track down that user?

Are your user deprovisioning processes fully documented? With backup procedures?

What about employees who transfer out? They're not terminated……

STOP DOING THE MINIMUM!

Secure for Confidentiality, Integrity, Availability: not compliance.

Logging & Reporting

Provides key information on users, groups and activities:

- User Provisioning
- User Deprovisioned
- User (successful & attempted) login / logout
- Password Reset, Change & Expiration
- Workflow Approval of granting group access
- Advanced IDM integration with SIEM platforms can lead to “joined” reports and increase SSM efficiencies.
- Tie-ins with physical access

NERC CIP IDM Misconceptions

"I don't need password controls on my control center workstations"

"It's OK to use one login on a workstation we keep unlocked 24/7"

"I don't need to terminate and lock old accounts since the personnel can't get into the building"

"Active Directory provides all the security I need."

"I have an identity management system, I don't need password standards!"

Are you covered?

Among our various service offerings is our 5-day NERC CIP Identity Roadmap.

Includes:

- Review and recommendations on user and password controls.
- Review and recommendations on identity related NERC CIP documentation, policies, procedures and processes.
- Technology review and recommendations for securing your cyber asset's access control.
- Provide a NERC CIP perspective into access controls

Contact Information

Encari, LLC

866-943-9901

www.encari.com

Justin Harvey, Sr. CIP Consultant

925.890.7118; jharvey@encari.com