OSIsoft.

vCampus Live! 2011

Network Architecture & Active Directory Considerations for the PI System

By: Bryan Owen - OSIsoft
Joel Langill - SCADAhacker

Agenda

- Moore's Law
- Network Architecture
- Domain Services in a DMZ

HD Moore's Law

"Casual Attacker power grows at the rate of Metasploit"

Corollary:

Metasploit won't tell you you've done "enough" but it just might prove if you haven't.

Anatomy of an Attack

Information Gathering

Scanning
Enumeration
Fingerprinting

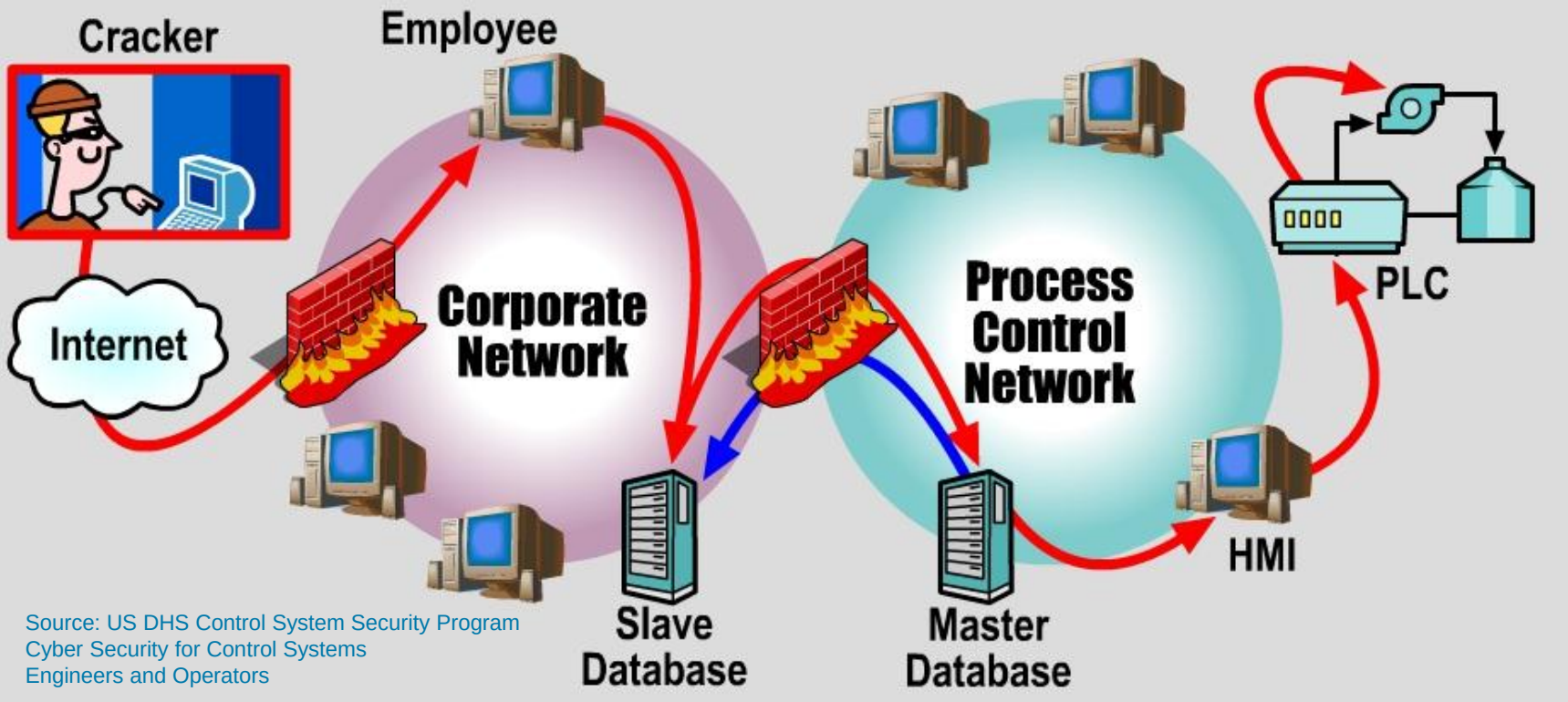
Turning point … When a threat becomes an attack!

Gaining Access

Maintaining Access

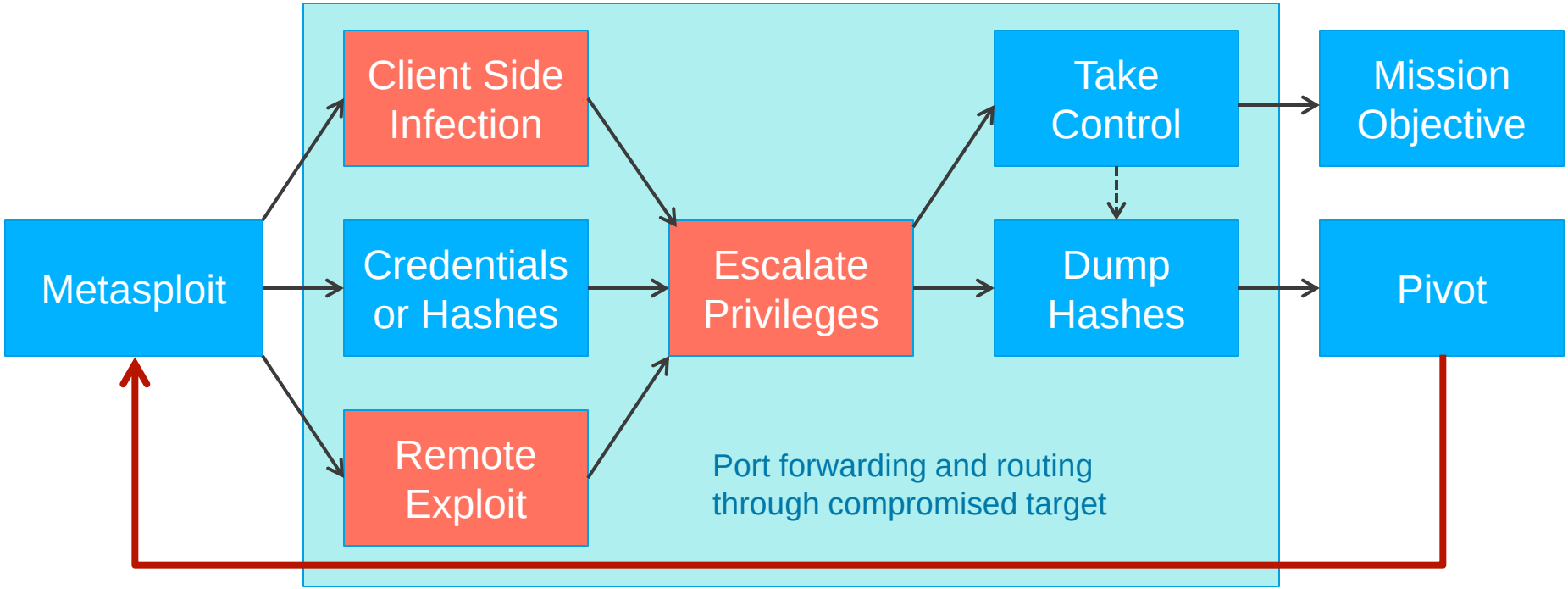
Covering Tracks

Attack Process



Source: US DHS Control System Security Program
Cyber Security for Control Systems
Engineers and Operators

Pivot Attacks



Pass the Hash

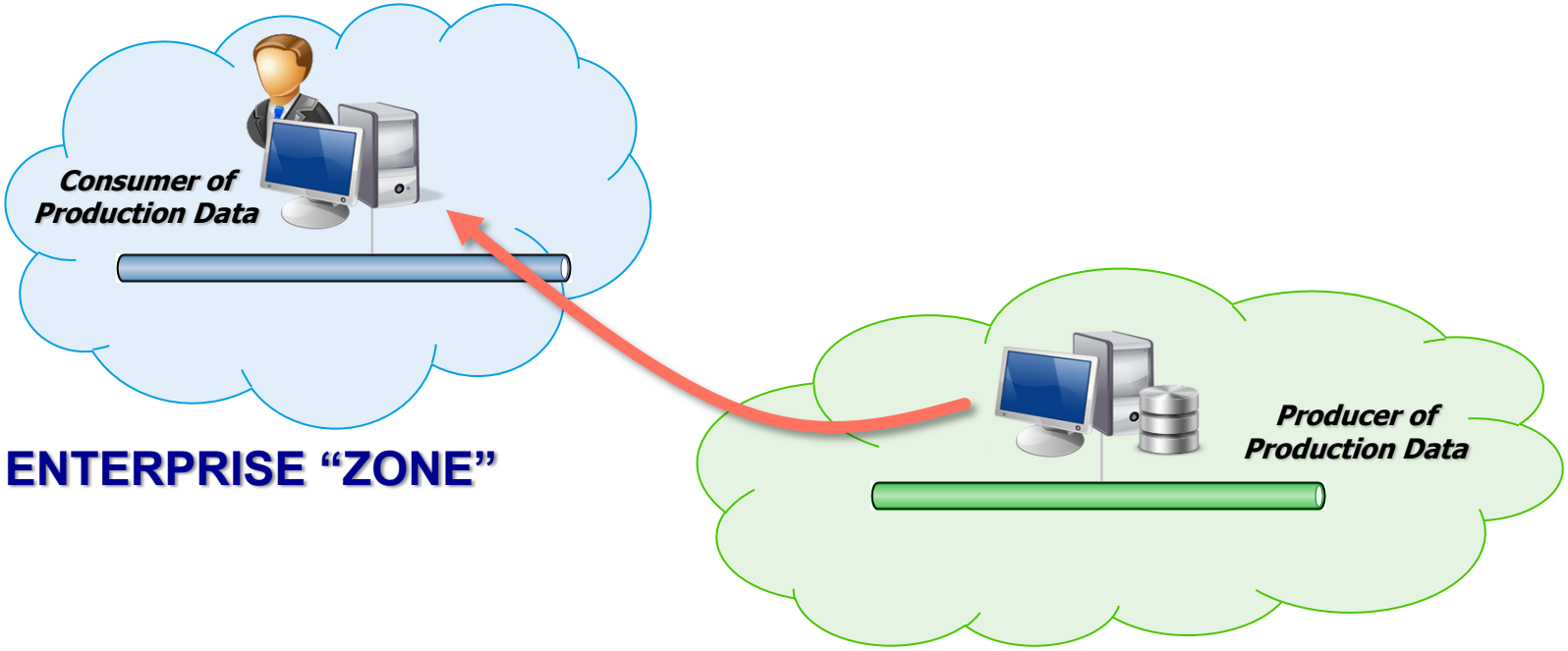
- Well known pivot technique (1)
  - Many tools to crack or “pass” password hashes
  - Even NTLM passwords susceptible
  - As good as clear text password
- Password hashes are well protected except:
  - Administrators and users with ‘Debug programs’ rights
  - Processes with ‘Act as part of the operating system’ rights

(1) SANS reading room: “Why Crack When You Can Pass the Hash?”

Finding the ‘Right’ Balance

- Access to Information, Ease of Administration, Scope of Accountability, Security
  - Many companies are moving the direction of a “single sign-on” or SSO approach
  - Authentication and Credential Management remain as a top vulnerability within manufacturing systems
- Network segmentation, Domain services
  - Complex firewall rules and “dynamic ports”

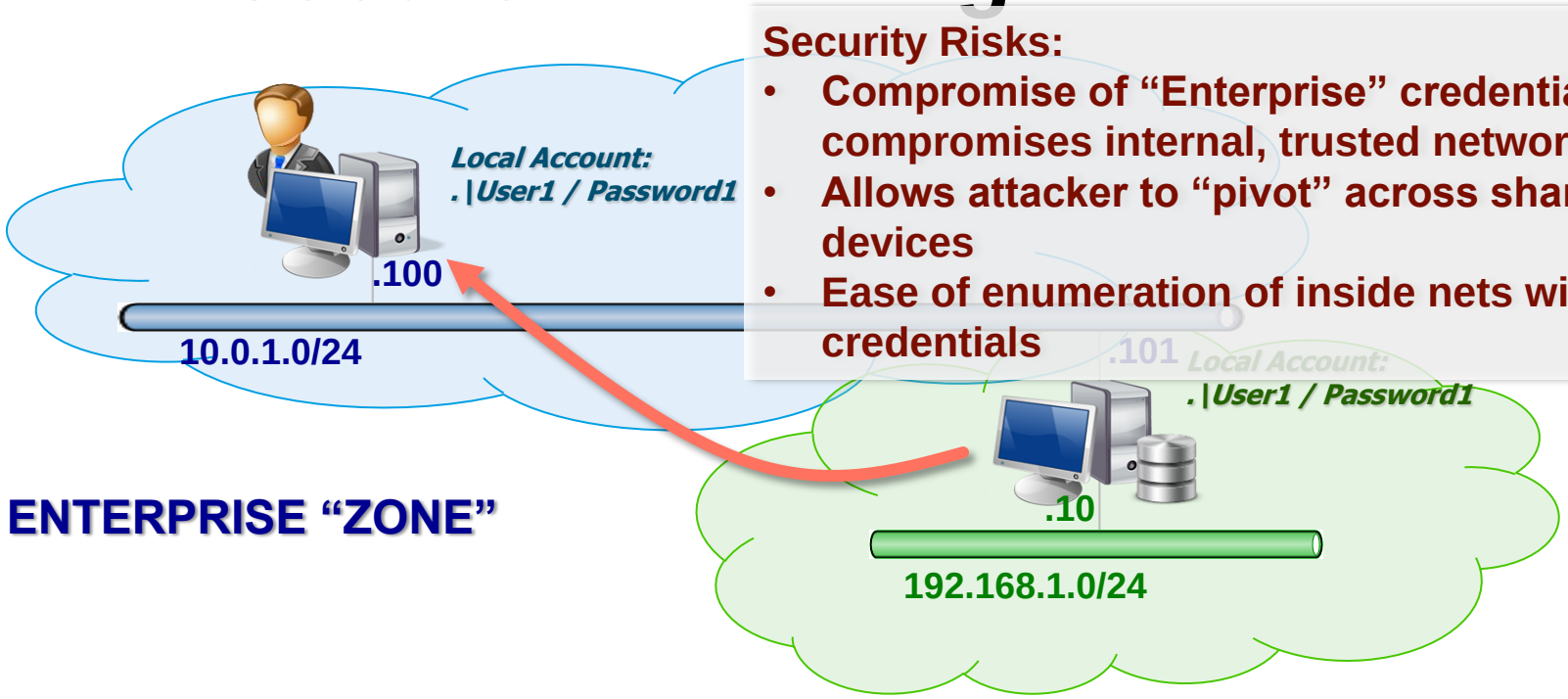
Simplified Manufacturing Info Data Flow



ENTERPRISE "ZONE"

PRODUCTION "ZONE"

“In”secure Data Integration



Security Risks:

- Compromise of “Enterprise” credentials compromises internal, trusted networks
- Allows attacker to “pivot” across shared devices
- Ease of enumeration of inside nets with valid credentials

Network Segmentation Standards

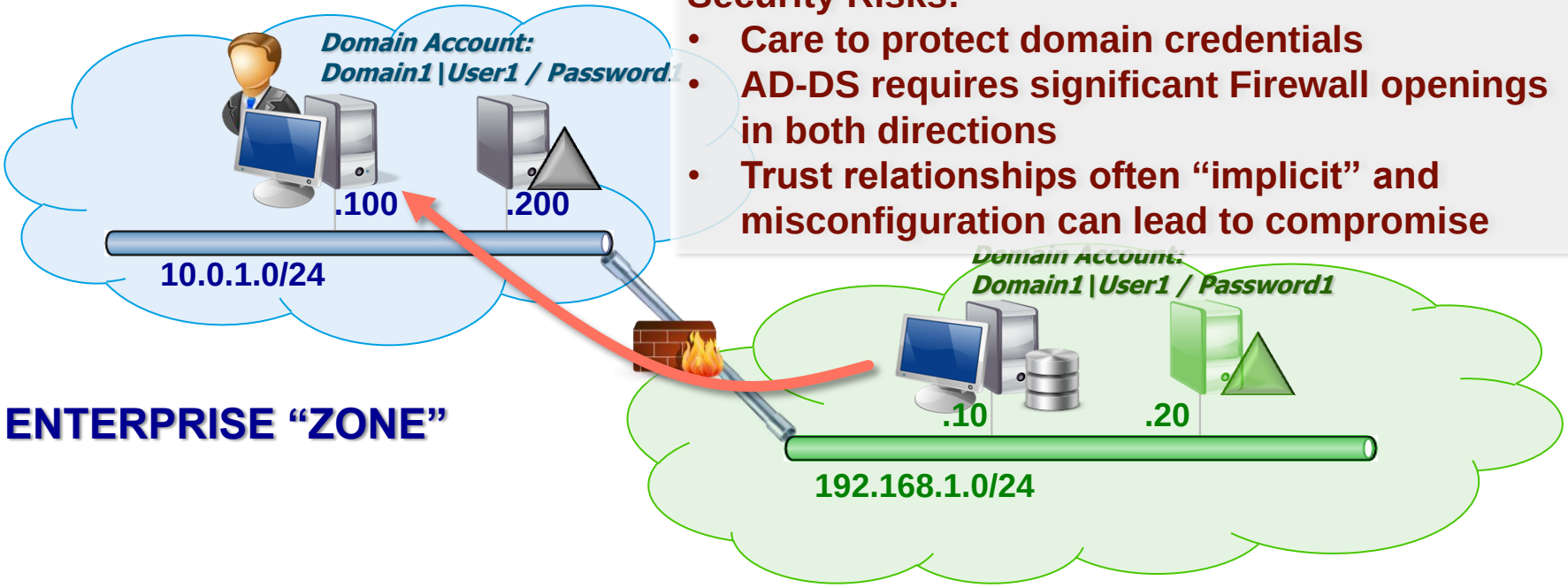
- DHS CSSP, ISA 99, NERC CIP, NIST 800-82

> *... no systems other than firewalls should be configured as dual-homed ... [to span security zones]*

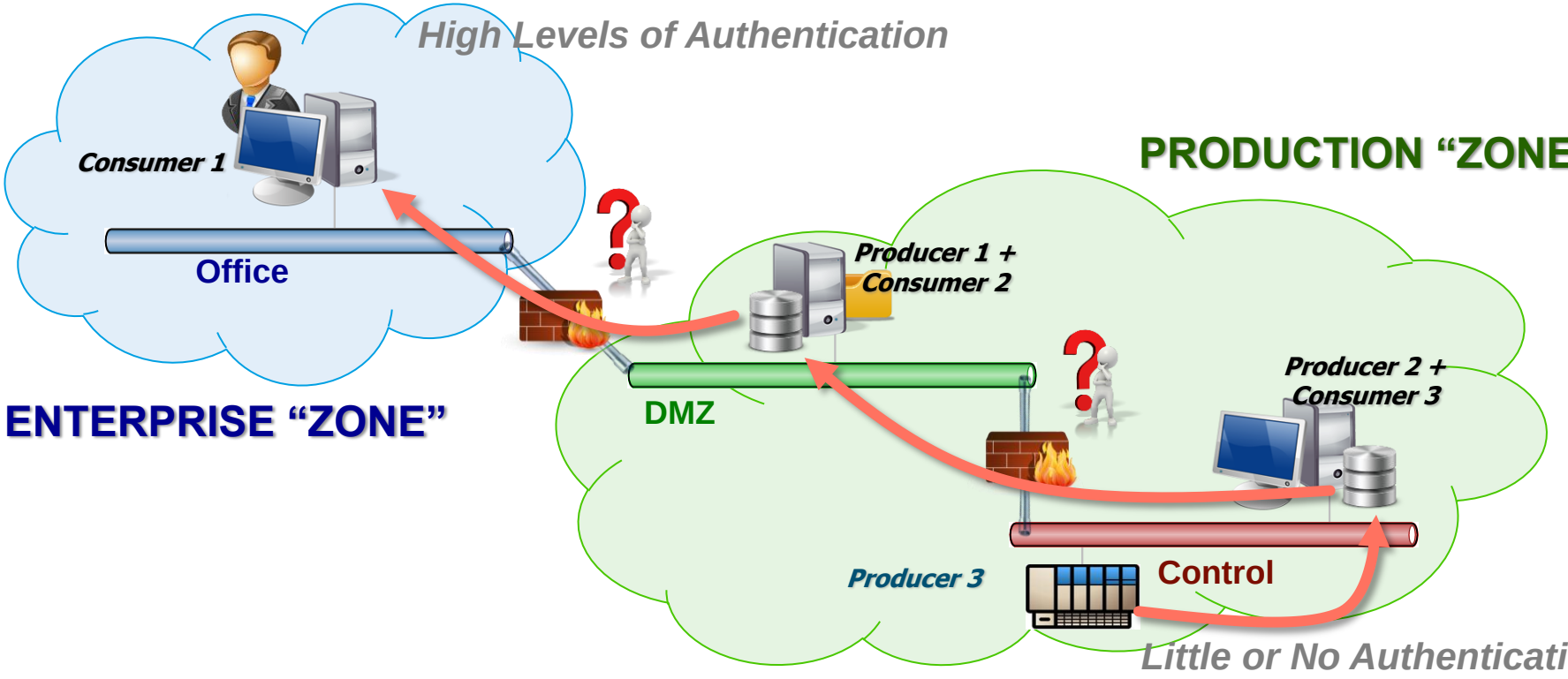
“Less” Secure Data Integration

Security Risks:

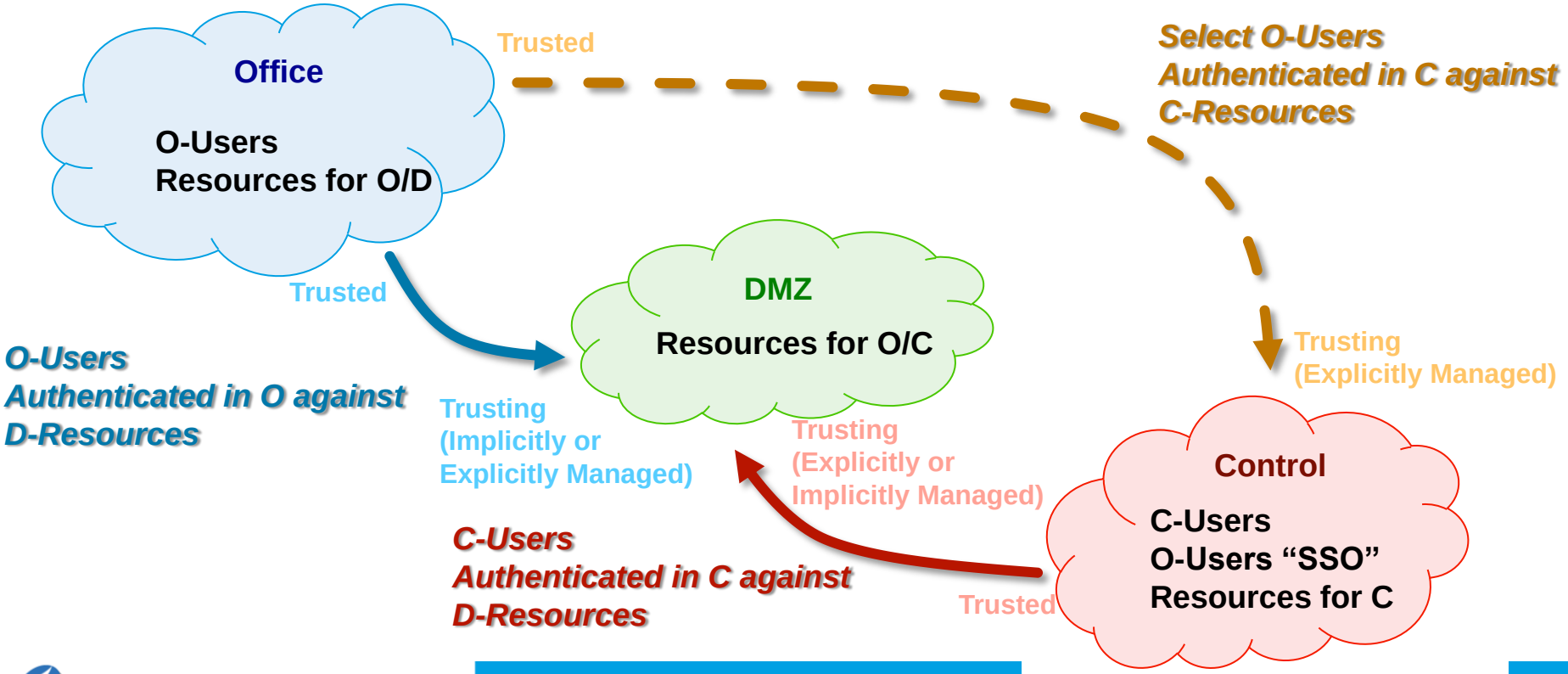
- Care to protect domain credentials
- AD-DS requires significant Firewall openings in both directions
- Trust relationships often “implicit” and misconfiguration can lead to compromise



Manufacturing Info Data Flow

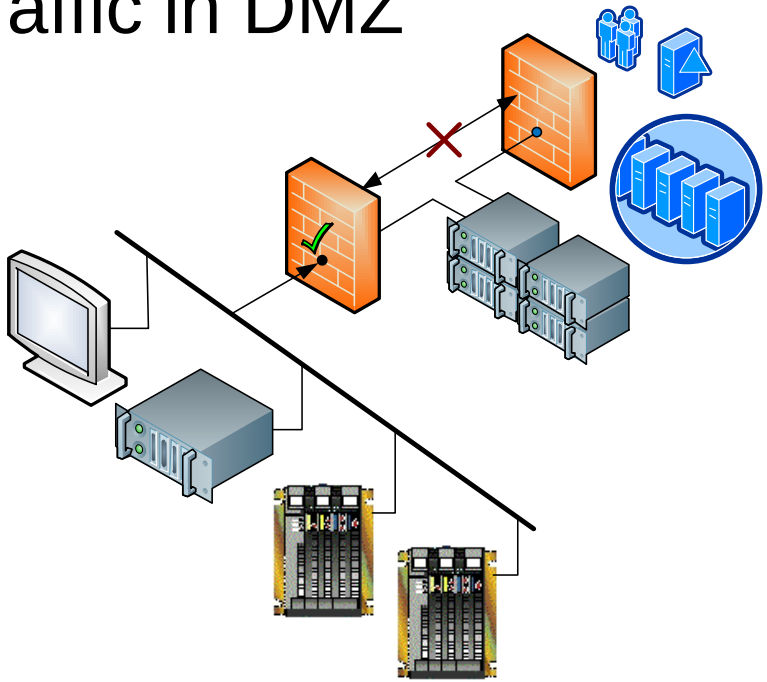


Trust and the 3-Zone Model



PI System DMZ Practices

- Terminate cross boundary traffic in DMZ
  - No thru traffic bypass exceptions
  - Block DMZ to internet
  - Restrict local logons and RDP
- Control network
  - PI Interface node with buffering
  - Minimize office and web protocols
  - Monitor DMZ traffic
  - Separate logon authority



Considerations for Authentication

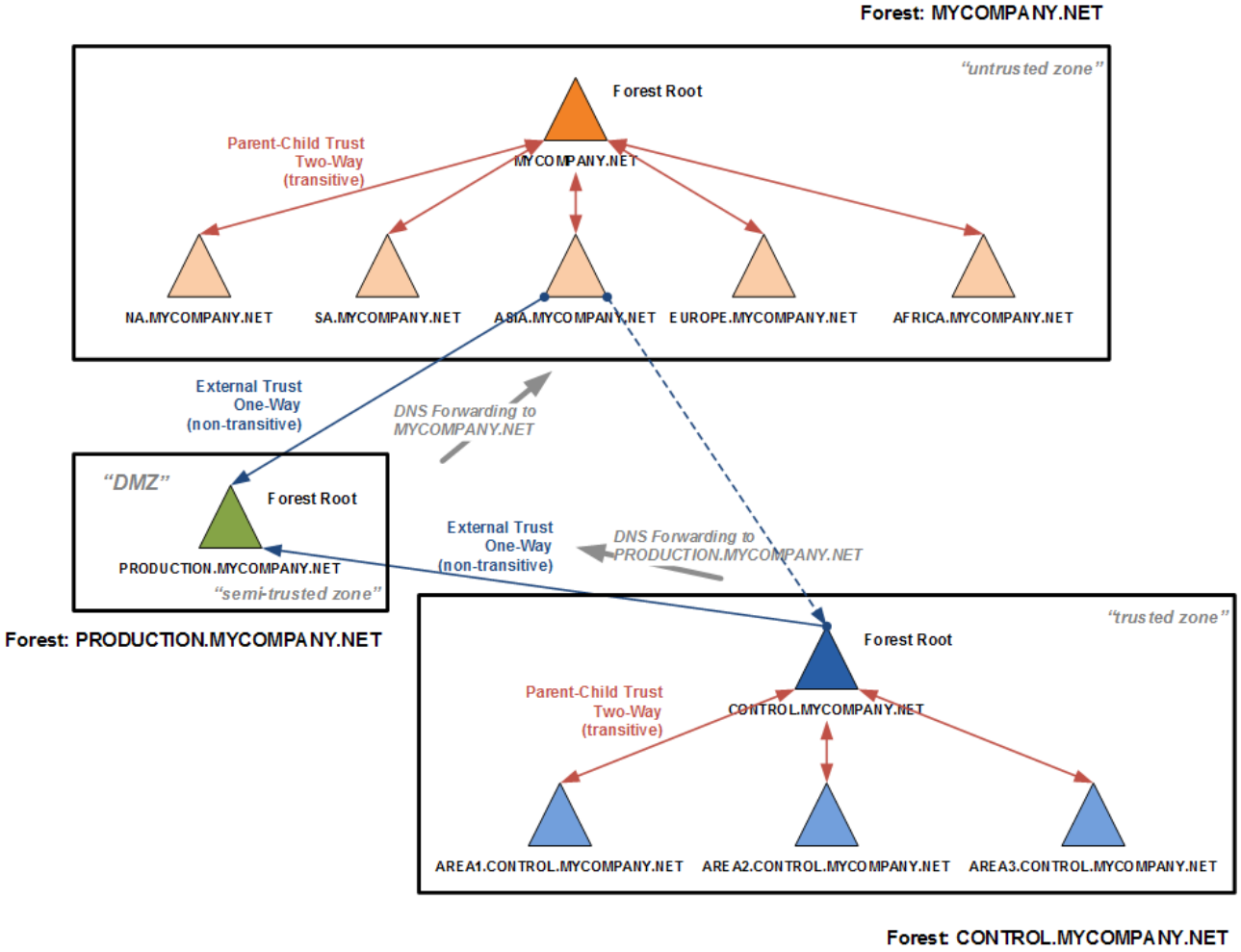
- Level of Autonomy or Isolation
- Differences in Group Policies
- Separation of “General” & “Administrative” Rights
- Active Directory Replication
- Integrity of Global Catalog and Schema
- Kerberos or NTLM

Options to Authentication

1. Integrated Windows Authentication using NTLMSSP or mirrored “local” accounts
2. ~~Integrated Forest – Single Domain~~
3. Integrated Forest – Unique Domains
4. Unique Forests

Comparison between Options

FEATURE	IWA (NTLM)	SINGLE FOREST	MULITPLE FORESTS
Single Account to Manage	No	Yes	Yes
Password Hashes Shared between Office/Production	2	1	n/a – Tickets
Segregation of Administrative Rights	Yes	No	Yes
Trust Transitivity between Office/Production Domains	n/a	Transitive	Non-Transitive
Trust Definition between Office/Production	n/a	Implicit Explicit	None
Trust Direction	n/a	2-way	1-way
Scope of Authentication	Local	Any Domain in Forest	Any Domain in Forest
Global Catalog / Schema	n/a	1	2
Replication across Firewall	n/a	Yes	No
Replication Requirements (DC to DC)	2 tcp / 2 udp	9 tcp / 3 udp (2003) 10 tcp / 6 udp (2008)	1 tcp / 1 udp



Summary

- Restrict access in and out of control networks
  - Enforce with a network DMZ and domain based services
- Caution on use of administrator accounts
  - Includes debug rights and highly privileged service accounts
- Decide on an approach you can sustain
  - Involve subject matter experts in your process

Additional References

- Active Directory Replication Over Firewalls
  http://social.technet.microsoft.com/wiki/contents/articles/active-directory-replication-over-firewalls.aspx
- How to Configure a Firewall for Domains and Trusts
  http://social.technet.microsoft.com/wiki/contents/articles/active-directory-replication-over-firewalls.aspx
- Active Directory Domain Services in the Perimeter
  http://technet.microsoft.com/en-us/library/dd728034(WS.10).aspx
- Windows Server 2008 Security Resource Kit

Bryan Owen

bowen@osisoft.com
Cyber Security Manager
OSIsoft, LLC

@bryansowen 

Joel Langill

joel@scadahacker.com
ICS Security Specialist
SCADAhacker

@SCADAhacker 

Thank you