



# Identity Management Ecosystems

Pete Lindstrom, CISSP  
Research Director

Spire Security, LLC  
[www.spiresecurity.com](http://www.spiresecurity.com)  
[petelind@spiresecurity.com](mailto:petelind@spiresecurity.com)

# Identity Management Ecosystems

---

## **Identity Management Ecosystems**

Day: Wednesday, 5/12

Time: 11:30am–12:00pm

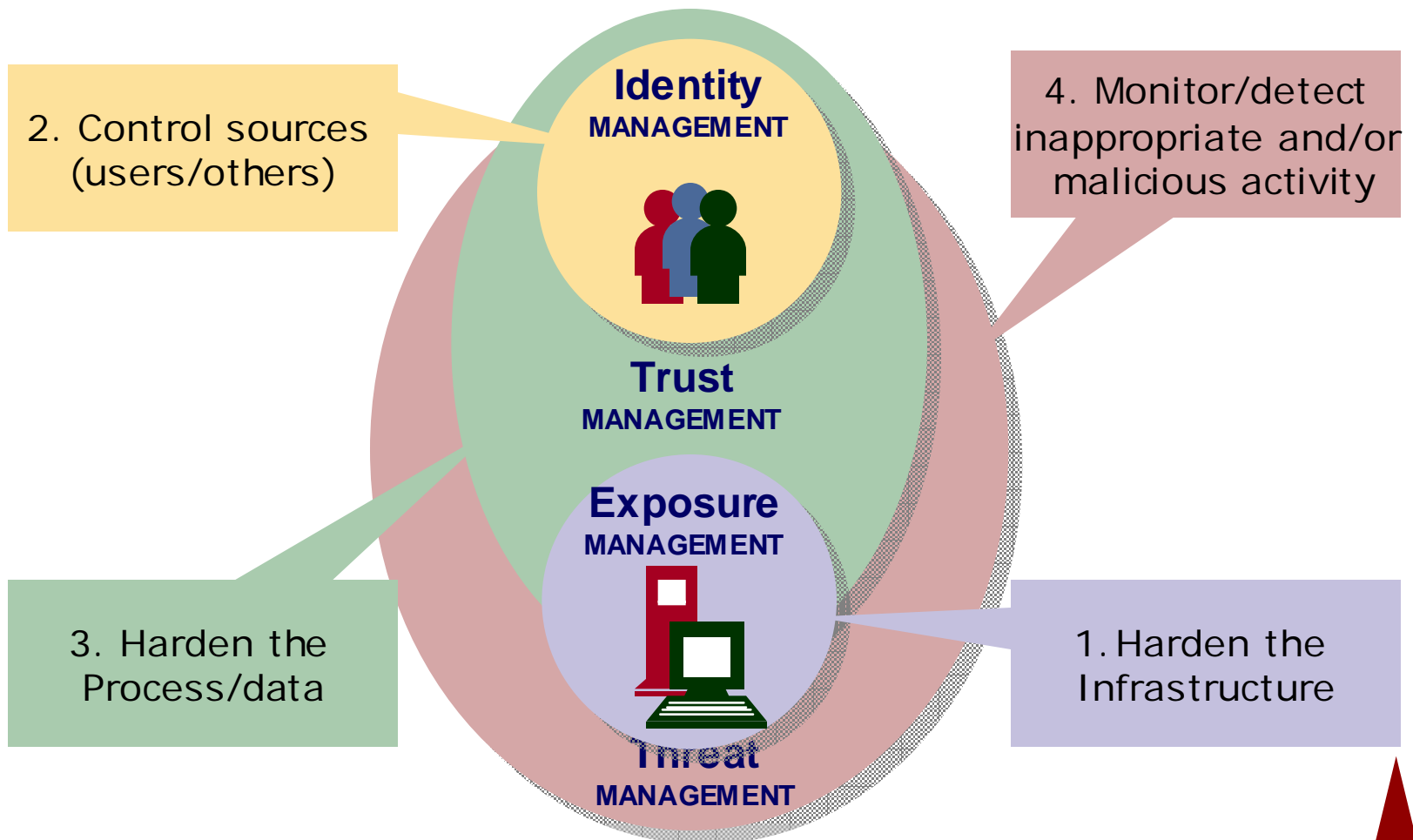
## **Session Speakers**

[Pete Lindstrom, CISSP](#)

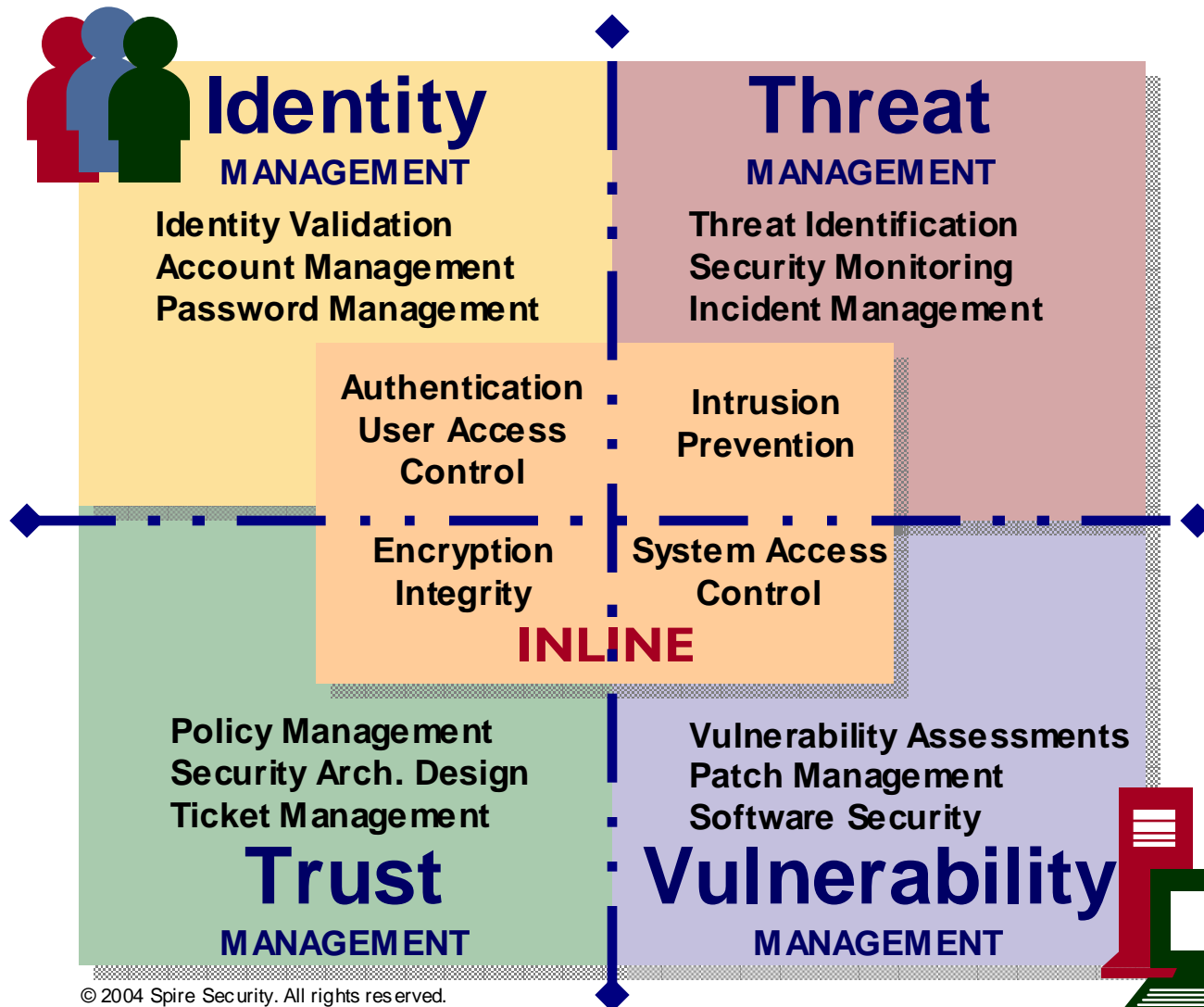
Research Director, Spire Security, LLC

Identity Management is a concept that can be interpreted in many different ways. This leads to confusion in the marketplace and diverts attention from the primary objective of Identity Management: to provide access for the correct people to the correct resources. This session looks at two ecosystems within identity management that strive to address this problem: the user administration ecosystem addresses the request, fulfillment, and management of user accounts; and the in line ecosystem addresses the more traditional authentication and access control process in real-time.

# Security Reference Model



# Four Disciplines of Security Management



# Identity Management Objective

---

*To reduce the amount of activity from unidentified or inappropriate sources\* by associating all activities in a computing environment with known users.*

\* Users as well as sources like devices, applications, and data

# Identity Management Goals

---

- ✦ Validate the identity of users requesting access to system resources.
- ✦ Ensure that user accounts are used only by appropriate personnel (e.g. owners).
- ✦ Ensure that user accounts are only granted access to those resources that have been authorized.
- ✦ Ensure that activities can be traced back to an identifiable source.

# Risks (affects anticipated results)

---

- ★ Non-attributed system access
  - Unknown account ownership
  - Shared accounts
- ★ Misappropriated accounts
  - Social engineering
  - Password guessing
- ★ Regulatory non-compliance
- ★ Increase efficiency of IT, help desk, users, auditors.

# Risk Reduction

---

- ✦ Reduce likelihood of data being stolen/copied by limiting access to authorized users. (confidentiality)
- ✦ Reduce likelihood of data being modified or deleted by limiting access to authorized users. (integrity, availability)
- ✦ Reduce likelihood of systems being misappropriated. (liability)

# Identity Management Ecosystems

---

## User Administration Ecosystem

- ★ Identify users
- ★ Assign accounts/rights
- ★ Maintain identity (passwords)

## In-Line Ecosystem

- ★ Validate sessions (authenticate)
- ★ Authorize access

# Ecosystem: User Administration

---

## Account request and fulfillment

- ✦ Validate user identity
- ✦ Approve access (business side)
- ✦ Assign tasks (IT support side)
- ✦ Create/modify accounts/rights
- ✦ Maintain identity (passwords)

# Solution: Provisioning

---

- ★ Account request and creation process for enterprise applications.
- ★ Efficient (ROI)
  - Verify form validity.
  - Predefined authorizers with automated workflow routing.
  - Institutionalized process.
  - Users quicker to productivity.
  - Online record keeping.
- ★ Effective (ROSI)
  - Difficult to subvert process.
  - Quick disabling of accounts.
  - Stronger accountability
- ★ Business Layers, Thor, IBM, Courion, M-Tech, Waveset...

# Solution: Consolidated Admin

---

- ★ Account creation process for enterprise platforms.
- ★ Efficient (ROI)
  - Single interface for admin.
  - Faster account creation.
- ★ Effective (ROSI)
  - Quick disabling of accounts.
  - Stronger accountability.
- ★ IBM, BMC, NetVision...

# Solution: Password Management

---

- ✦ Password resets and synchronization.
- ✦ Efficient (ROI)
  - Eliminate/reduce help desk interaction.
  - Users more productive.
- ✦ Effective (ROSI)
  - Eliminate/reduce social engineering of help desk.
  - Reduce admin rights required by help desk.
- ✦ Courion, M-Tech...

# Ecosystem: Inline Identity Mgt

---

## Authentication and Access Control

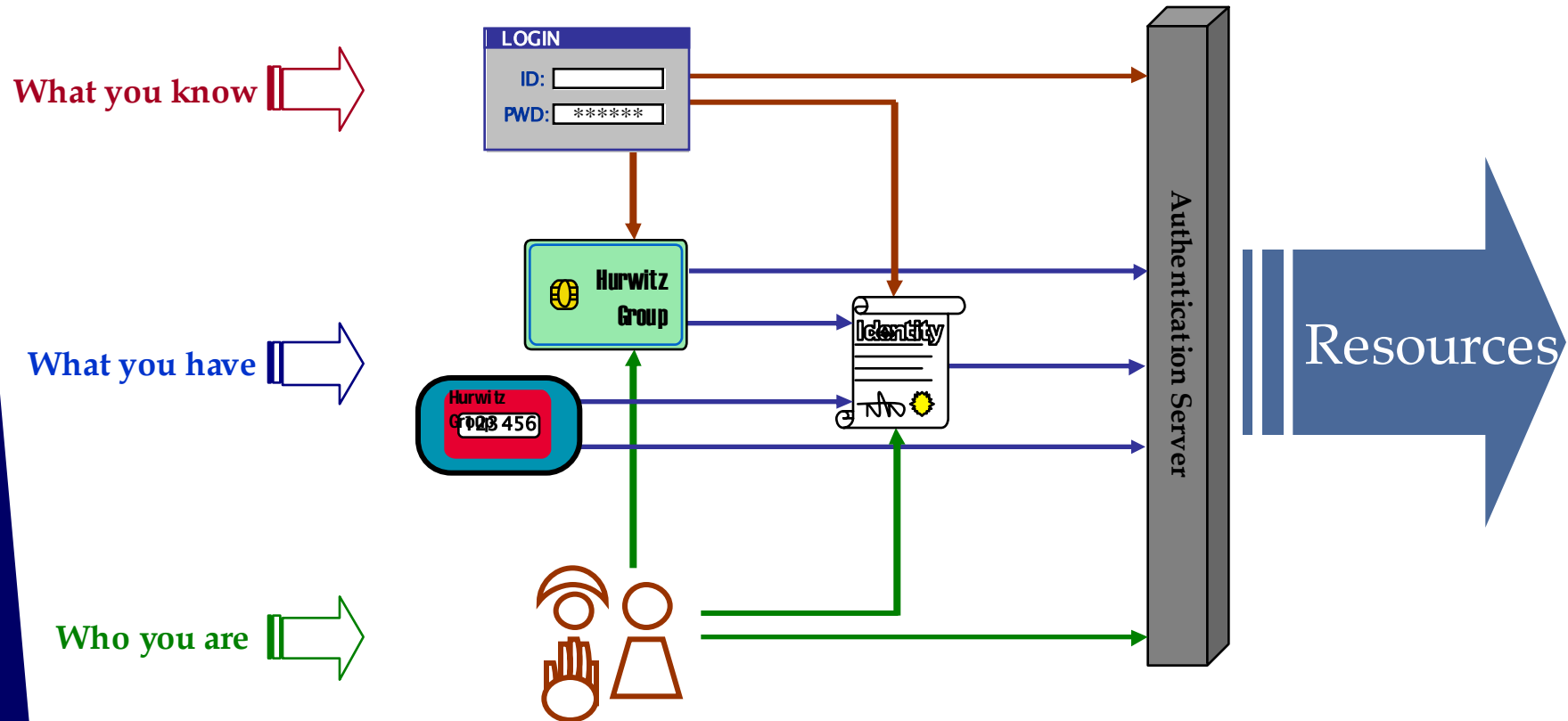
- ★ Present credentials during session initiation (Identify).
- ★ Demonstrate valid ownership of credentials (authenticate).
- ★ Determine access to resources - files, applications, etc. (authorize).

# Solution: Multi-Factor Authentication

---

- ★ Enhanced authentication capabilities.
- ★ Efficient (ROI)
  - Reduces number of incidents...(?)
- ★ Effective (ROSI)
  - Reduces likelihood of identity fraud.
- ★ Biometrics (Identix), Tokens (RSA, PassGo, Secure Computing), Smartcards (GemPlus, Schlumberger, RSA), PKI (RSA, Entrust), etc...

# Authentication Emancipation



# Authentication Solutions

---

<u>Factor</u>	<u>Strengths</u>	<u>Weaknesses</u>	<u>Considerations</u>
What you know (passwords)	Secrecy	Memory ++	Most popular by far. Acceptable for "routine" B2C.
What you have (smartcards, tokens)	Possession	Loss Hardware	Good precedents (credit cards, etc.). High-risk B2C or B2B.
Who you are (biometrics)	Uniqueness	FAR/FRR Hardware	Paranoia. Okay for Intranet use, some B2B.

# Solution: Web Access Control

---

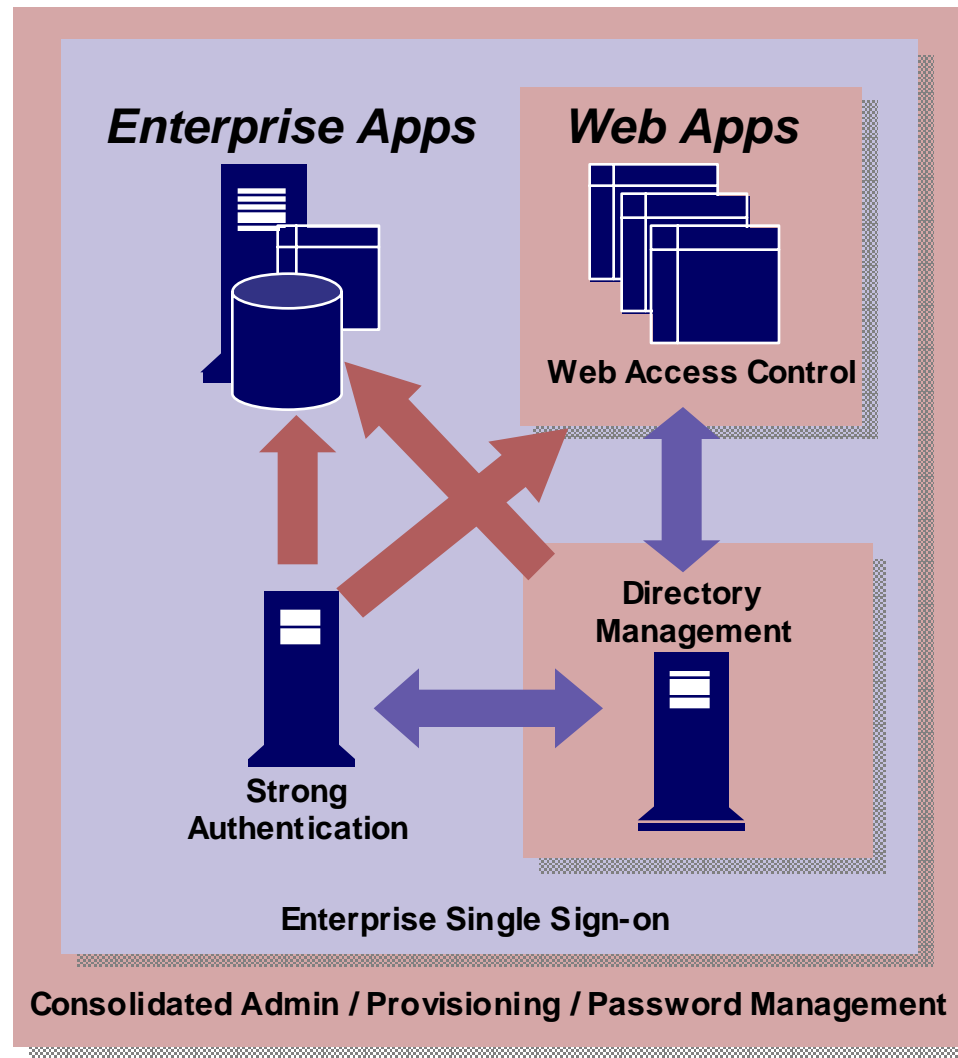
- ★ Provides single sign-on and authorization for web resources.
- ★ Efficient (ROI)
  - Quicker development/integration of apps.
- ★ Effective (ROSI)
  - Reduces complexity.
- ★ Netegrity, Entrust, RSA, IBM, CA, Sun, OpenNetworks, etc...

# Solution: Enterprise SSO

---

- ✦ Single credential used for enterprise apps.
- ✦ Efficient (ROI)
  - Keeps users productive.
  - Reduces help desk interaction.
- ✦ Effective (ROSI)
  - Reduces passwords being written down.
- ✦ Imprivata, Passlogix...

# Identity Management Solutions



# Summary: Benefits

---

- ✦ Provisioning: to reduce acct request lifecycle and provide stronger records.
- ✦ Consolidated Admin: to make administration easier.
- ✦ Password Management: to eliminate help desk interaction.
- ✦ Multi-factor Authentication: to strengthen the authentication process.
- ✦ Web access control: to standardize authentication and access control for web apps.
- ✦ Enterprise SSO: to make users lives easier.



# *Agree? Disagree?*

Pete Lindstrom

[petelind@spiresecurity.com](mailto:petelind@spiresecurity.com)

[www.spiresecurity.com](http://www.spiresecurity.com)