IBM

SERVICE MANAGEMENT
WORLD TOUR 2008

THE RIGHT ANSWER, IS RIGHT HERE.

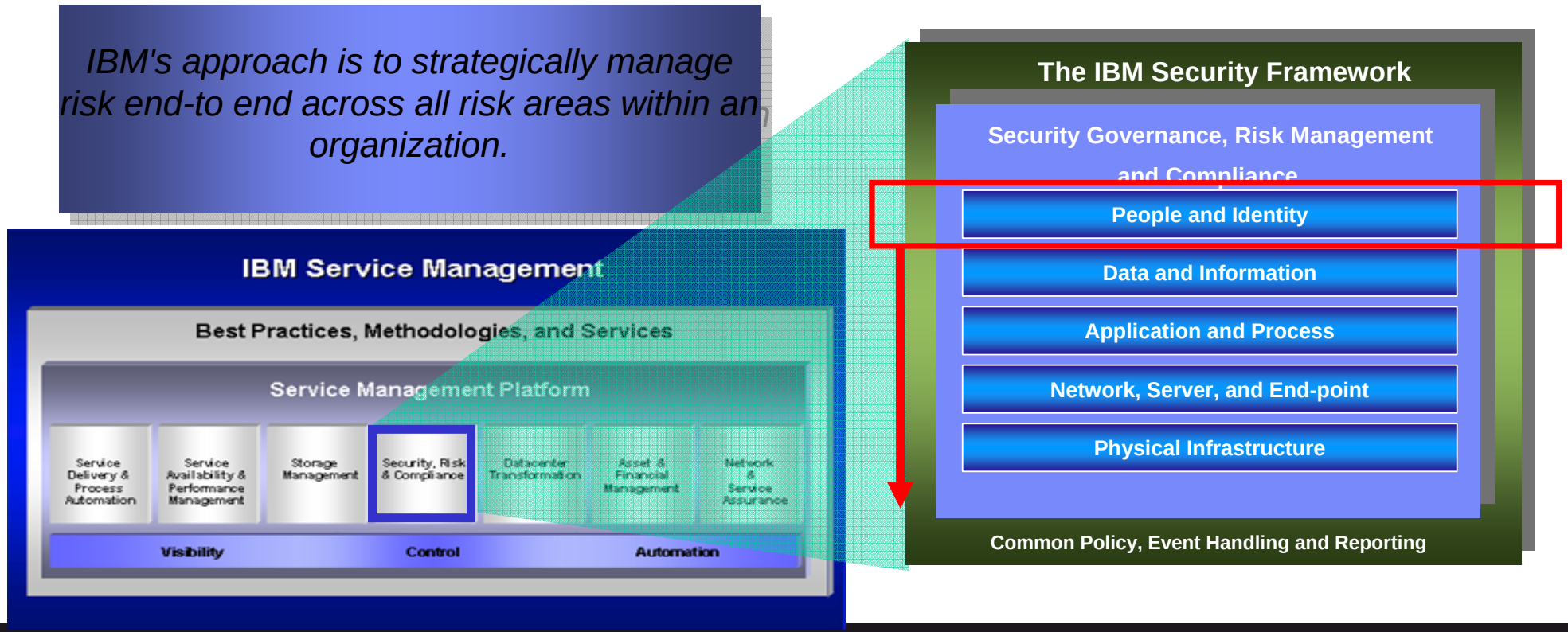
Privileged user management, monitoring and control

Nick Briers

Product Manager, Tivoli Security Information and Event Manager

Privileged user challenge spans the security framework

IBM's approach is to strategically manage risk end-to end across all risk areas within an organization.



What is a ‘privileged user’?

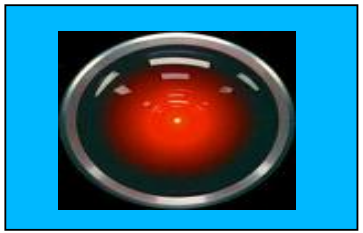
Someone with IT permissions to:

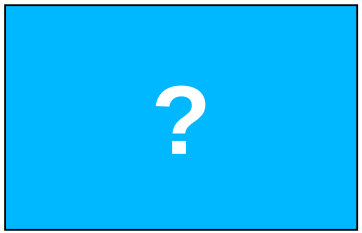
- Access highly sensitive data
- Change critical IT systems
- Conduct high value transactions
- Cover their tracks in the audit trail

As viewed by Analysts:

- Forrester: PUPM (Privileged User and Password Management)
- Burton: “The seedy underbelly” – PAM (Privileged Account Management)

Who is a privileged user?





Who cares about privileged users?

Malicious insiders care…

THE WALL STREET JOURNAL.

The Online Journal GET 2 WEEKS FREE SUBSCRIBE NOW | The Print Journ GET 2 WEEKS FRE SUBSCRIBE NO

As of Friday, January 25, 2008

News | Today's Newspaper | My Online Journal | Multimedia & Online Extras | Mark

OTHER FREE CONTENT FROM THE WALL STREET JOURNAL

EDITORS' PICKS

Retiring Abroad
Texting for Votes
If You Knew Sushi
Tree Hugger
Airline Champs of 2007
Beautiful Country
MORE EDITORS' PICKS

BLOGS

Most Popular Posts

1. Giants Win Super Bowl, Leaving Pats at 18-1
2. Motorola: Death of an American Icon?
3. Clinton Aims Barbs at Obama, McCain
4. On Eve of Super Tuesday, Obama Lowers Expectations

SEE ALL BLOGS

MORE FREE CONTENT

-- Personal Journal
-- Personal Finance
-- Leisure
-- Markets Data Center
-- Video
-- Blogs
-- Forums
-- Interactives
-- Autos

THE WALL STREET JOURNAL. GET FULL ACCESS TO ALL ONLINE JOU

PAGE ONE

French Bank Rocked by Rogue Trader

Société Générale Blames
$7.2 Billion in Losses
On a Quiet 31-Year-Old

By DAVID GAUTHIER-VILLARS, CARRICK MOLLENKAMP and ALISTAIR MACDONALD
January 25, 2008; Page A1

PARIS -- The rogues' gallery of banking has a new candidate for membership: 31-year-old trader Jérôme Kerviel.

In one of the banking world's most unsettling recent disclosures, France's Société Générale SA said Mr. Kerviel had cost the bank €4.9 billion, equal to $7.2 billion, by making huge unauthorized trades that he hid for months by hacking into computers. The combined trading positions he built up over recent months, say people close to the situation, totaled some €50 billion, or $73 billion.

The loss -- dwarfing the $1.3 billion Nick Leeson cost British bank Barings in 1995 -- has forced Société Générale to seek a capital infusion. It is expected to try to raise €5.5 billion, chiefly from its existing shareholders.

The problem:

3 of the Top 10 Threats to Enterprise Security are insider related:

- Employee error
- Data stolen by partner/employee
- Insider Sabotage

Insider driven fraud costs US enterprises over $600 Billion annually

Who cares about privileged users?

Sophisticated outsiders care…

CSO
cso online.com

Threatwatch | Whaling Gets Real

Powered by social-networking sites and compromised corporate databases, super-targeted phishing attacks are moving from theory to practice. Here's how to understand this evolving information-security threat and protect your company and its

By Rick Cook

For the last couple of years, security researchers have been sounding warnings that phishers could turn their attention to **super-personalized attacks targeted at high-level corporate employees--so-called "whaling" attacks**. Now, however, there's growing evidence that this type of attack is moving from theory to practice. The reasons? The bad guys are getting better access to the information they need to bait these e-mails--both because they are getting better at mining databases on compromised corporate sites, and because employees are providing more useful information at networking sites such as LinkedIn and MySpace.

Once launched, the results of a whaling attack can be devastating. "It's really effective," says Joe Stewart, senior security researcher for SecureWorks Inc., a managed security service provider based in Atlanta. "They're hitting the high-level executives and getting access to these people's entire workstations."

Like all "spearphishing" or targeted phishing attacks, whaling involves personal information, but in this case **the targets are high-level, high-value individuals whose credentials, if compromised, can endanger an entire organization**. The targets are carefully chosen, and the number of e-mails distributed is small. Where a massive phishing attack might involve billions of e-mails sent from botnets with a million zombies, whaling usually involves anywhere from a few dozen to a few thousand e-mails, which are sent from a botnet with perhaps 20,000 compromised computers. Conventional methods for identifying phishing attacks depend on spotting a lot of identical messages, so the small scale of whaling attacks makes them essentially invisible to Internet scanners.

"What allows them to fly under the radar is that they are so targeted," says Allan Paller, director of research at the SANS Institute. "If you only go after 20 companies, or 200 companies, nothing will pick up the attack."

Because the targets have such high value, whalers can afford to go to very elaborate lengths to make their e-mails appear legitimate. The basis of a successful whaling attack is information about the intended victims--the more specific the better. At the very least, most whaling attacks involve the name and job of each potential victim, and the whalers will try to have more information than that.

Who cares about privileged users?

Your auditors care…

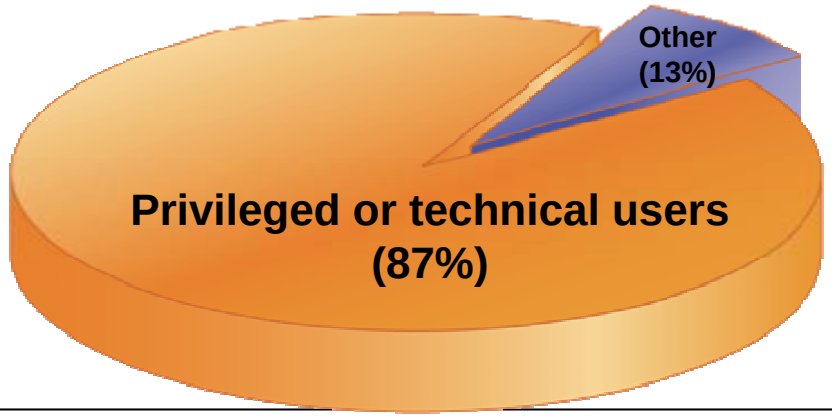
Regulatory Compliance Initiative	Relation to Privileged Account Controls
Payment Card Industry (PCI) Data Security Standard (DSS)	Protect stored cardholder data (#3) Develop and maintain secure systems and applications (#6) Restrict access to cardholder data by business need-to-know (#7) Insufficient internal controls over privileged accounts would negatively impact an organization's capability to meet all of these requirements.
California Senate Bill 1386 (now California Civil Code 1798)	SB 1386 requires organizations that lose private information of California residents to report the loss to affected individuals. Unauthorized users of privileged accounts can bypass the access control mechanisms and audit controls of most systems to access private information without the organization knowing about it.
Sarbanes-Oxley Act (SOX) Section 404	Requires corporate management to take responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting Requires management to assess and report the effectiveness of the internal control structure and procedures for financial reporting. Insufficient internal controls over privileged accounts negatively impact an organization's capability to meet these requirements.

Who cares about privileged users?

YOU care!

- **87% of insider incidents are caused by privileged or technical users**
- **Many are inadvertent violations of:**
  - Change management process
  - Acceptable use policy
- **Others are deliberate, due to:**
  - Revenge (84%)
  - “Negative events” (92%)
- **Regardless, too costly to ignore:**
  - Internal attacks cost 6% of gross annual revenue
  - Costing $400 billion in the US alone

Who Causes Internal Incidents?



abc NEWS

Passport Security Breach on McCain, Clinton & Obama

State Department Contract Employees Fired, Another Disciplined for Looking at Passport File

By JAKE TAPPER and KIRIT RADIA
WASHINGTON, March 21, 2008 —

An embarrassed State Department admitted today that the passport files of all three presidential candidates -- Sens. John McCain, Barack Obama and Hillary Clinton -- have been breached by its employees.

Privileged User Accounts: A closer look

Definition – A user definition on a system, in a directory, or in a database which enjoys extra privileges for operating on that system, within that directory, or against that database

Examples

- Root user or any userid with uid '0' on a Unix(R) system
- RACF userid with “SPECIAL” attribute or “AUDITOR” attribute or “GROUP SPECIAL” privileges
- User in a LDAP directory designated as “adminDN”
- User definition under which multiple operations, at the request of other users, are performed (sometimes called a “service userid”)
- User in the “Administrators” group on a Windows system
- DBAdmin userids
- Financial and ERP accounts of your CEO, CFO, etc.

“With great power comes great responsibility”

What damage can be done?

Privileged users may define new user definitions

- to perform work as a userid which is un-noticed by identity management policy enforcement

Privileged users may change other user's capabilities

- inadvertent escalation of privilege to other users
- create other privileged users
- deny access to services required by a user

Privileged users may access sensitive information

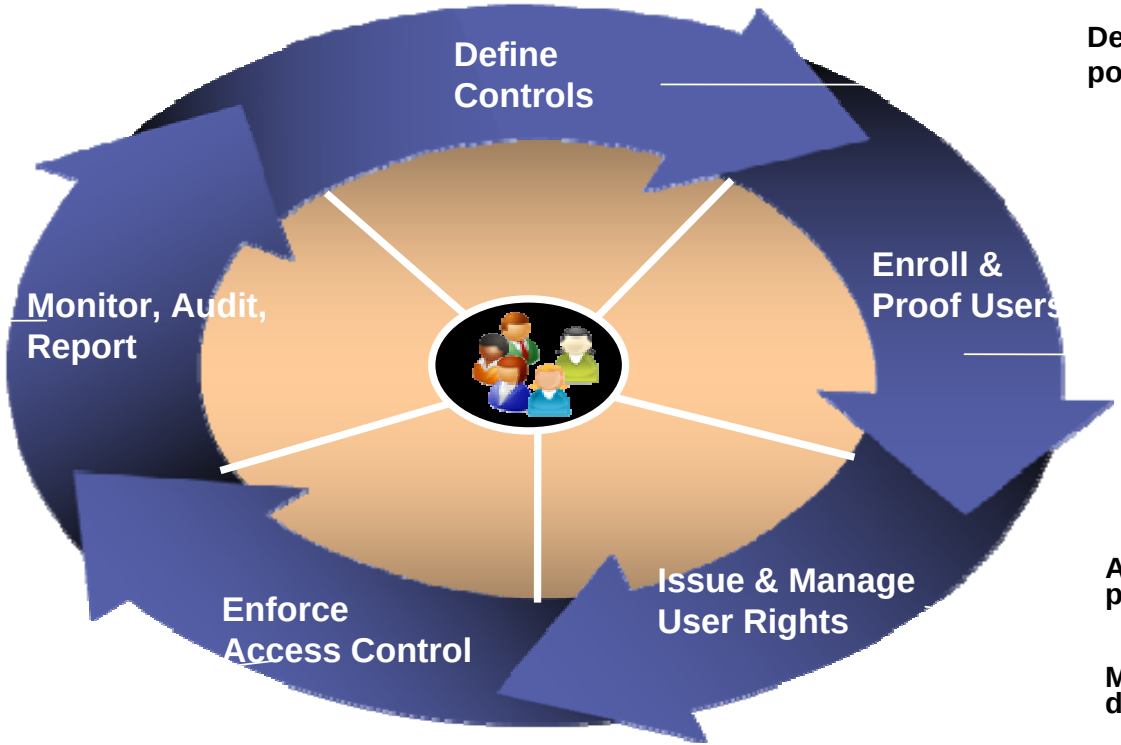
- copy, modify, or destroy

Privileged users may change audit logs

- remove or modify file-based audit logs
- modify audit log records

Privileged users, by their intent, can “own” a system

How do I manage the risk of privileged accounts?



Define security requirements and policies

Verify user information and detect potential risky relationships

Enroll users and provide user self service

Automate access rights provisioning and de-provisioning

Manage shared accounts and delegation of privileges

Monitor user activity and audit events via dashboard pre-built compliance reports

Identity governance, role and user rights recertification and reporting

Control user access to resources and provide stronger authentication

Define Security Requirements and Policies

Goal: Mitigate Risk to the organization

Solution:

- Seek to eliminate the usage of singly all-powerful userids
- Spread the capabilities for administration across a set of roles
- Require user-specific login and interaction with all systems, a user may take on several roles
- Require and enforce separation of duties between roles
- Define policies for exception handling, including human approval processes for emergency user of all-powerful userids
- Require strong authentication for privileged users

Enroll Users and Provide Self Service

Goal: Enable administration within defined policies

Solution:

- Enforce a set of checks and balances in identity administration
- Employ an approval process for users to act in sensitive roles and capabilities
- Ensure that “service” userids are never used for interactive use
- Verify that ALL users defined on systems are accounted for!
- Have a “emergency” procedure for exceptional situations and recovery processing

Automate Access Rights Provisioning

Goal: Eliminate manual and ad-hoc administration of access control settings

Solution:

- Create a roles-based access control model
- Reduce access control administration and increase role membership administration
- Employ the fine-grained access control enforcement capabilities of the systems and applications which privileged users use
- Utilize tools including 'sudo', 'setuid' programs, and similar capabilities for systems administration tasks

Control User Access to Resources

Goal: Guarantee that the right accounts are used for the right tasks

Solution:

- Centralize authentication and credential transform services
- Require user-specific credentials be used as deep as possible in the computing environment
- Ensure that various system-level user/account defintions are not usable in interactive modes (e.g. NOLOGIN settings)

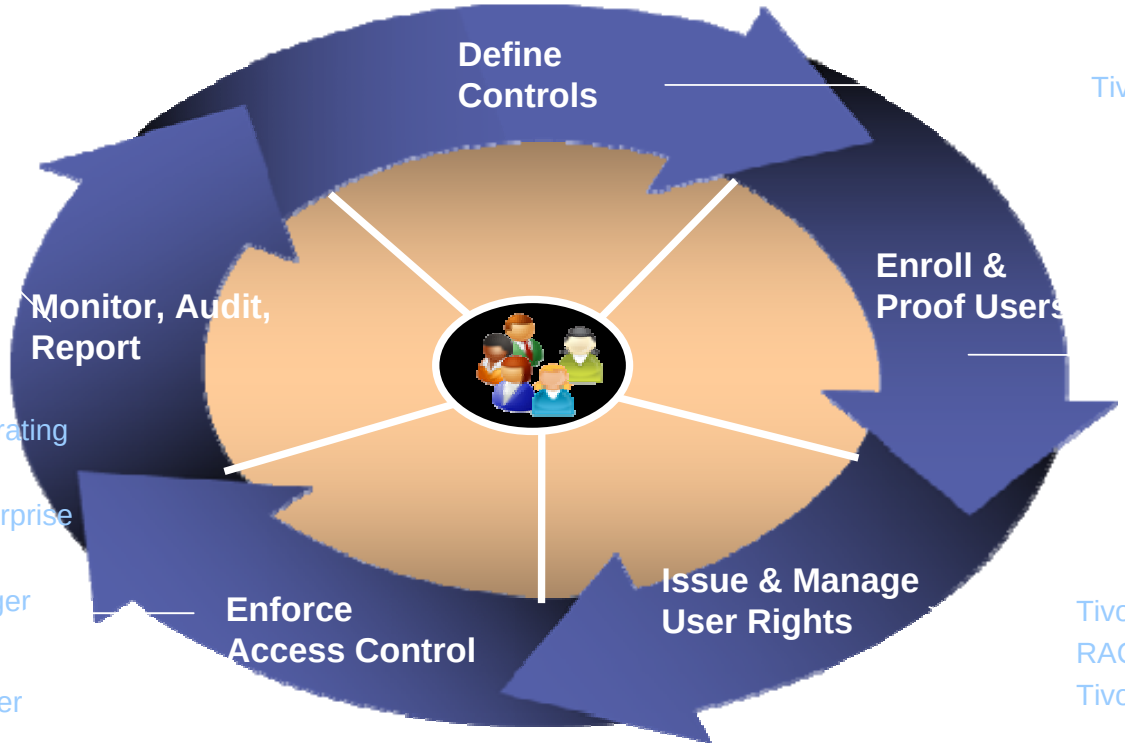
Monitor User Activity

Goal: Validate that no un-expected behavior occurs ... and when it does you know when, where, and by whom

Solution:

- Actively monitor and report on user capabilities and role relationships
- Monitor systems and activities of all users which may act in sensitive roles
- Ensure separation of duties between monitoring and operations
- Remind privileged users of the infrastructure in place

Solutions from IBM today that can help



Tivoli Security Policy Manager

Tivoli Identity Manager

Tivoli Identity Manager
RACF
Tivoli zSecure

Tivoli Access Manager for Operating Systems
Tivoli Access Manager for Enterprise Single Sign On
Tivoli Federated Identity Manager
RACF
Tivoli zSecure Command Verifier

Tivoli Security Information and Event Manager

Account Administration

- Privileged users can often define and/or update other user definitions.
  - Seek to extinguish such capabilities except in emergency situations
  - Employ a process for approving the definition or modification of sensitive userids
- Privileged userids are often defined for emergency administrative use
  - Require human approval for emergency usage
  - Monitor any actions performed by privileged userids and actively review the reports
  - Require reset of the account upon completion of the task/situation
- Service IDs
  - Password changes for service IDs must often be coordinated with application server configuration changes
  - Employ a process for accomplishing this – do not simply mark these userids as having non-expiring passwords
  - Ensure that these userids cannot be used for interactive use

Tivoli Identity Manager 5.0
People & Identity

What's new!

Intuitive User Experience Adaptable to Corporate Branding Needs

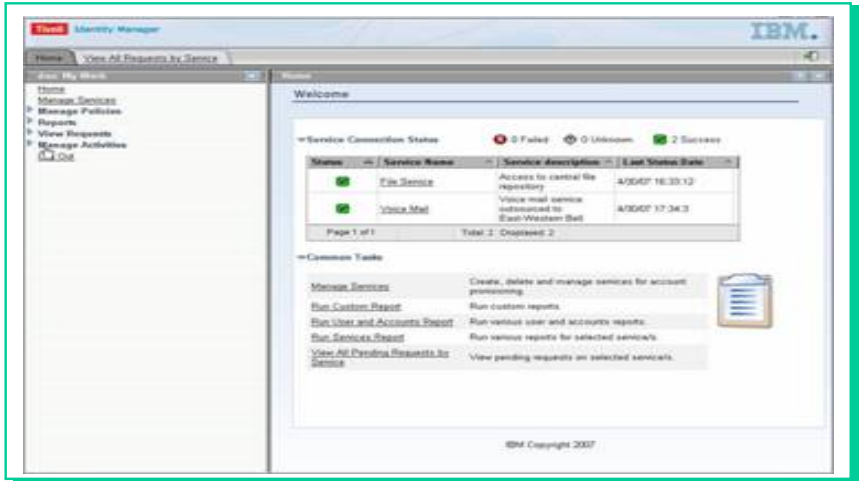
- **Business-friendly provisioning requests & approvals via group management**
- **Request & approve role membership**
- Tailored, configurable user interface views
- Look and feel customizable via style sheets and custom text
- Task oriented wizards & smart searches

Automated Compliance Lifecycle

- **Business-friendly revalidation of granular user access rights**
- Auditor-centric UI view and reports
- Additional compliance related reports
- TCIM integration

Simplified Deployment Options

- **Upgrade from TIM Express to TIM**
- **Single server launch pad installer**, simplified middleware and fixpack application



Business Benefits

Visibility: Bridges gap between business & IT on the meaning of user entitlements & access rights

Control: Identity governance, role management and audit capabilities

Automation. Accelerated deployment and policy management learning curve

Account Authentication

- Privileged user accounts are often used for direct interaction with the system or device for emergency purposes
  - Utilize a set of defined roles and granular access control checking and 'sudo' or command verifier applications to enforce a separation of duties
  - Consider requiring stronger authentication for users which are allowed to perform administrative tasks in interactive mode
- Privileged user accounts that are used for “service IDs” or for systems management functions are often also used for interactive administration on the system
  - Utilize all means to constrain the capabilities of “service IDs”
  - Ensure that “service IDs” cannot be used for user interactive work (e.g. NOLOGIN)

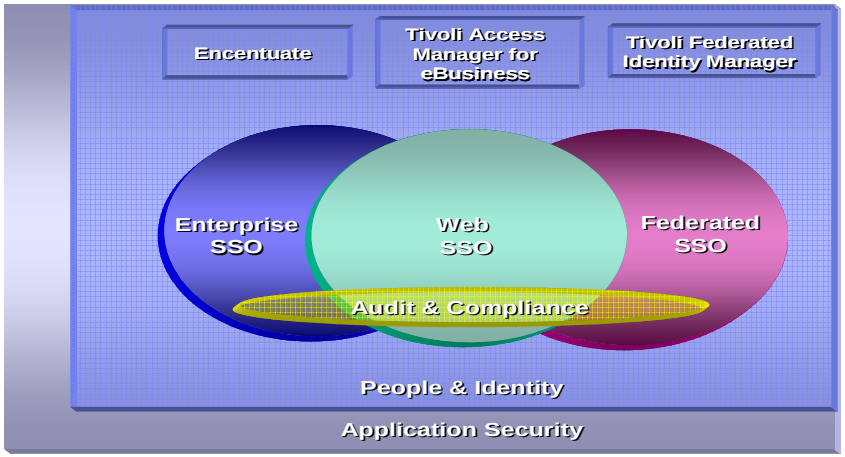
NEW: Encentuate acquisition
People & Identity

What's new!

IBM acquired Encentuate
March 12, 2008

Encentuate offers:

- Automated ESSO to help enhance user productivity, improve security, implement and document compliance efforts, and reduce support costs
- Broad support for common applications and flexible toolkit to extend to applications across the enterprise
- Extensive integration with strong authentication form factors
- Centralized auditing and reporting for visibility into user access
- Controlled session management for shared desktops



Business Benefits

Enables the automation of the sign-on process, control over access to business assets, and visibility into user activity in order to help drive value for our clients.

Account Authorization

Even privileged users often have access control settings which can be used to limit their behavior

- Utilize granular access control rules and separate roles to limit the scope of capabilities of individual users
- On Unix systems employ tools such as 'sudo' to limit users' behavior
- Seek to establish a complete set of 'sudo' rules and granular access controls based on role such that permissions updates are rarely required

Employ a process which includes human oversight for any access control rule changes

- Allow users to perform operations based on the roles they are allowed to act in rather than granting the user explicit permissions to sensitive operations

Some systems allow for a distinct separation of duties to be employed

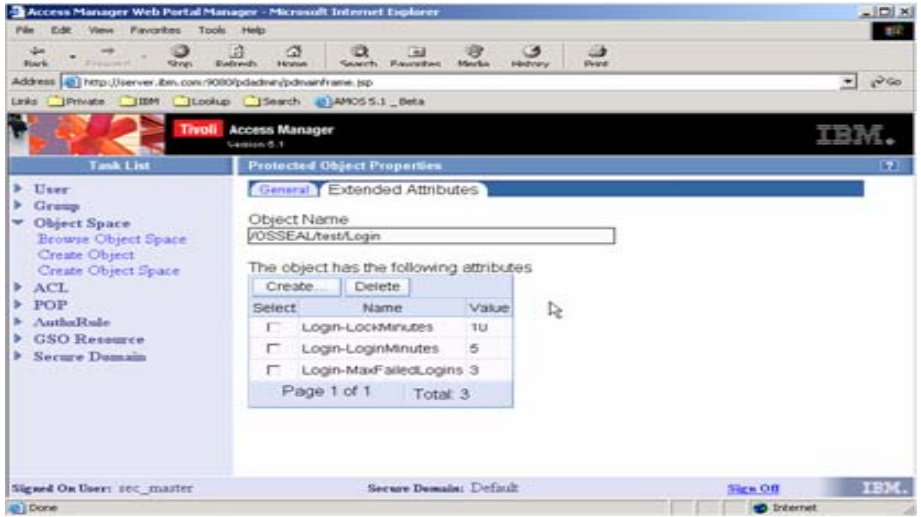
- In RACF, a userid should not have both “SPECIAL” and “AUDITOR”.
- Verify that expected separation of duties is maintained and that user definitions are set up as expected per the policies defined

IBM Tivoli Access Manager for Operating Systems

Tivoli Access Manager for Operating Systems protects individual application and operating system resources by addressing system vulnerabilities surrounding privileged user access (e.g. super user or root accounts)

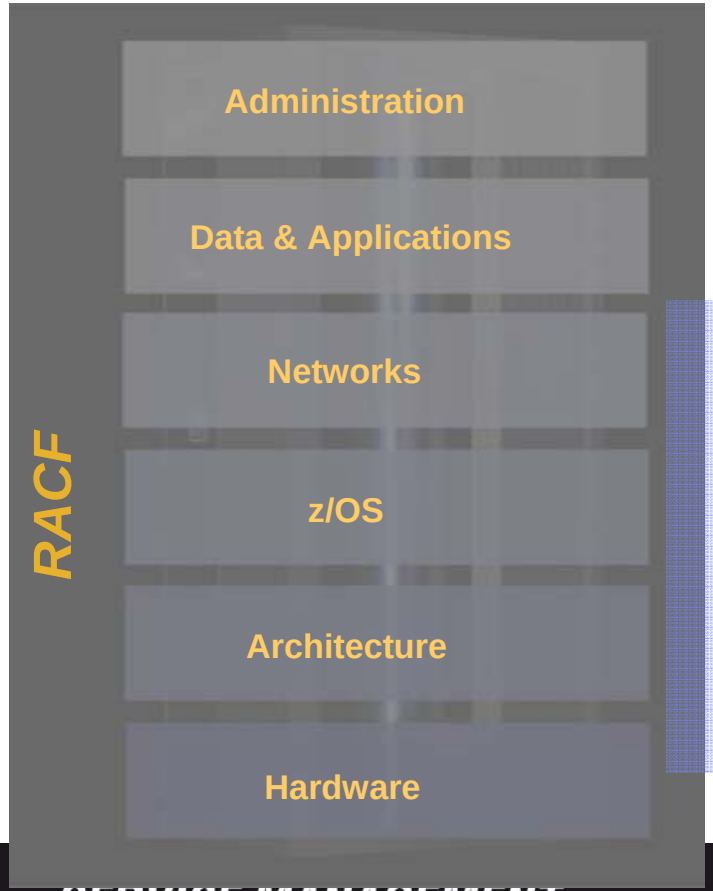
Key Features

- Defends against the top security threat that enterprises face: misuse by internal users and employees
- Centralized, policy-based user access management, tracking and control in a heterogeneous OS environment
- Delivers mainframe-class security and auditing in a lightweight, easy-to-use product
- Provides Persistent Universal Auditing to document compliance with government regulations, corporate policy and other security mandates
- Common Criteria certified



Resource Access Control Facility (RACF)

The backbone of mainframe security



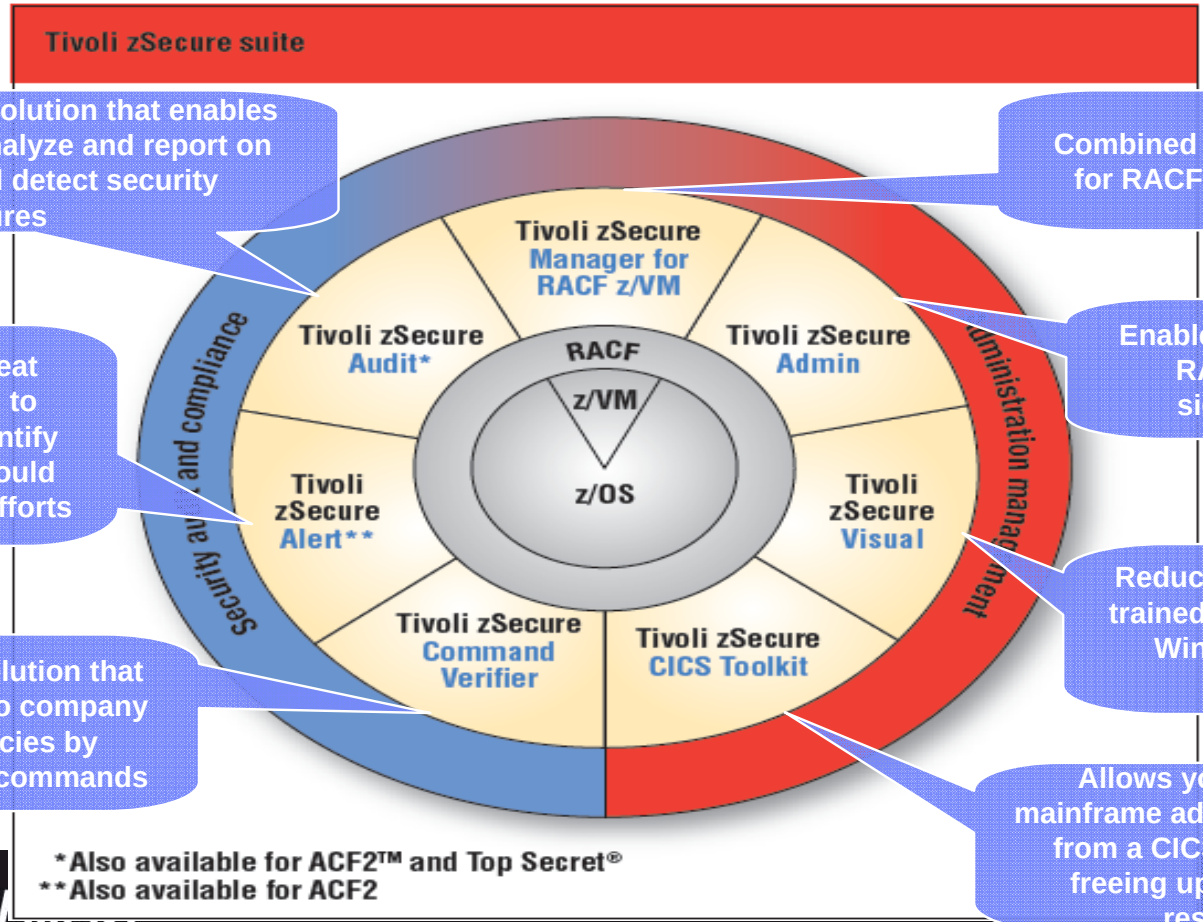
- ✓ Authentication
- ✓ Authorization
- ✓ Administration
- ✓ Auditing

Enables application and database security without modifying applications

Can reduce security complexity and expense:

- Central security process that is easy to apply to new workloads or as user base increases
- Tracks activity to address audit and compliance requirements

IBM Tivoli zSecure Suite



Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

Combined audit and administration for RACF in the VM environment

Real-time mainframe threat monitoring allowing you to monitor intruders and identify mis-configurations that could hamper your compliance efforts

Enables more efficient and effective RACF administration, using significantly less resources

Policy enforcement solution that enforces compliance to company and regulatory policies by preventing erroneous commands

Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

Account Auditing

- Privileged users often have access (read and write) to any logs of what operations they (or others) may perform.
  - Utilize granular access controls to protect logs from modification
  - Eliminate usage of all-powerful userids except for emergency situations and only after human approval at the time of use
- Passive logging of operations performed by privileged users is often used as a means of being able to do forensic analysis.
  - Log successful and unsuccessful operations of privileged users
  - Protect and gather the logs
  - Review reports on the activities of privileged users – look for anomolies

Tivoli Security Information and Event Manager
Security Governance, Risk Management & Compliance

What's new!

New soft-bundle offering of Tivoli Security Operations Manager and Tivoli Compliance Insight Manager products with additional product integration to provide the broadest set IBM SIEM capabilities

Single part number, reduced, consistent pricing

Two-way SIM – SEM event integration

- Standardized taxonomy mappings
- Targeted Operations to User Monitoring scenarios

Enables unified SIM module compliance reporting

- Leverages critical SEM correlated events, or audit-centric original events in unified reports

Business Benefits

- Improves security posture through timely visibility to vulnerabilities
- Facilitates compliance management through comprehensive log management and auditor centric views/reports
- Helps reduce costs and drive efficiency for compliance and security operations management efforts

Recommendations

Define strict policies for privileged user definition and use

Verify that ALL users defined on systems are accounted for!

Closely track and recertify a user's need to access privileged accounts

Eliminate usage of singly all-powerful userids

- Employ usage only for emergency/exceptional purposes

Ensure that "service IDs" are not used for interactive work

Enable centralized and strong authentication mechanisms for privileged users

Employ granular access control mechanisms to limit privileged user behavior

Monitor all privileged user operations ... read and act on the reports!

- Look for anomolies

Questions?

For More Information

Tivoli User Community
An active and lively community for Customers, Business Partners, and IT professionals. **Free membership** provides you with valuable resources, tools and networking capability. Log on to www.tivoli-ug.org or visit the ped in the PULSE EXPO

Tivoli Training
IBM offers technical training and education services to help you acquire, maintain and optimize your IT skills. For a complete Tivoli Course Catalog and Certification Exams visit www.ibm.com/software/tivoli/education

Tivoli Services
With IBM Software Services for Tivoli, you get the most knowledgeable experts on Tivoli technology to accelerate your implementation. For a complete list of Services Offerings visit www.ibm.com/software/tivoli/services

Tivoli Support
IBM Software Premium Support provides an extra layer of proactive support, skills sharing and problem management, personalized to your environment.
Visit www.ibm.com/software/support/premium/ps_enterprise.html