



Who Are you?

Identity and Access Management

Speaker:
Jay Ranade
CISSP, CISA, CISM, CBCP
Director, Educational Services
Technodyne University
jayranade@TechnodyneUniversity.com



technodyne
technology ■ consulting ■ insight

Security: Who are You - Identity and Access Management

The opening line from the song of the same title by The Who describes the ever-growing challenge faced by governments today. The balancing act is how to provide access to a growing number of citizens and other users, while at the same time keeping confidential information private and secure. With the ever-increasing pressure to share information among a wide range of systems, reliable authentication methods are critical. **This session discusses some of the approaches and solutions that are being successfully implemented in the public and private sectors.**

Jay Ranade, Director of Educational Services, Technodyne University

About the Speaker

Jay, a certified CISA, CISM, CISSP, and CBCP, is an internationally renowned expert on computers, communications, disaster recovery, IT Security, and IT controls. He has written and published more than 35 IT-related books on various subjects ranging from networks, security, operating systems, languages, and systems. He also has an imprint with McGraw-Hill with more than 300 books called “Jay Ranade Series”. He has written and published articles for various computer magazines such as Byte, LAN Magazine, and Enterprise Systems Journal. The New York Times critically acclaimed his book called the “Best of Byte”. He is currently working on a number of books on various subjects such as IT Audit, IT Security, Business Continuity, and IT Risk Management.

Jay has consulted and worked for Global and Fortune 500 companies in the US and abroad including American International Group, Time Life, Merrill Lynch, Dreyfus/Mellon Bank, Johnson and Johnson, Unisys, McGraw-Hill, Mobiltel Bulgaria, and Credit Suisse. He was a member of the ISACA International's Publications Committee (2005-2007).

He also teaches graduate-level classes on Information Security Management and Ethical Risk Management at New York University and IT Auditing and Internal Auditing for St. John's University.

Currently, he is the Director of Educational Services for TechnoDyne University at Wayne, NJ, USA.

Taste of (Current) Future

- You file income tax return
 - e-Return
- You cast your vote from your computer
 - e-Vote
- You renew your license from home
 - e-license
- You express your opinion for your congressman from your computer
 - e-pinion
- So, **how does the government agency know that you are who you say you are?**

What is Identity Management

- Ensure that **you are who you say you are**
- Different techniques used in the public sector vs. the private sector
- Private sector usually performs the authentication itself
- Public sector depends upon a third trusted party called CSP
 - Credentials Service Provider
- How do you **maintain privacy** while doing this?

Private Sector vs. Public Sector

- Public Sector has to be more careful
- In private sector, if bank asks verifiable personal information, it is called **authentication**
- In public sector, if agency asks verifiable personal information, it is called **invasion of privacy**
- **How do you maintain balance between the two?**

And what is Involved?

- **Identification**
 - Identify who you are
- **Authentication**
 - Prove it that you are who you say you are
- **Authorization**
 - After you prove it, you are allowed access only to what you are authorized to access
 - e-government is less concerned with this since each agency limits access to information provided

Why we need Identity Management (IdM)?

- Lack of authentication affects CIA
 - And that is a **security/risk** issue
 - Authentication is **more material** than authorization
 - If authentication is weak, authorization has no value
- IdM in Private Sector vs. Public Sector
 - Public sector is equally concerned about privacy risk as confidentiality risk
 - **Confidentiality vs. Privacy**

Why do we need Authorization?

- Lack of Authorization affects CIA as well
 - Authorization can be at various levels
 - Operating system level- mostly authorization is at OS level- based on subject-object model- subjects have clearance and objects have labels
 - Database level
 - Application level

Criteria for Identity Management

- Technical
 - Manage to provide or deny or restrict access
- Law Enforcement
 - **Identity theft issue**
- Social Issues
 - Privacy
 - OECD issues and safe harbor
 - HIPAA and GLBA
- Legal
 - Data protection
- Security
 - Access controls

Control Permutations

- Preventive Administrative
 - e.g. Policies, procedures, employee background check, termination policy
- Preventive Technical (or Logical)
 - e.g. encryption, smart cards, biometrics, call back system, views, virus scanning
- Preventive Physical
 - e.g. fences, dead man's door, biometrics, dogs, environmental, badges

Control Permutations continued

- **Detective Administrative**
 - Policy, background check during job, mandatory vacation, job rotation, auditing, responsibility sharing
- **Detective Technical**
 - e.g. clipping levels, audit trail auto report generation, IDS, NIDS, HIDS
- **Detective Physical**
 - e.g. video cameras, motion detectors, IR detectors, sensors

Access Control Attacks Continued

- Man-in-the-middle
- Replay
 - Use nonce or timestamp
- Session Hijacking
 - Attacker substitutes own IP address

Access Control Attacks continued

- Dictionary attack
- Software exploitation
 - Weaknesses in certain software's
- Trojans
- System scanning
 - Port scanning precedes attack
 - Process: recon, gain system access, clear logs, replace system file with root kit tools, keep backdoors open e.g. NetBus or SubSeven

Access Control Attacks continued

- Brute force attack
 - Serious for which role?
- Social engineering
- Dumpster diving
 - Not illegal
- Password guessing
 - On monitor or under the keyboard 😊

Identification and Authentication

- Identification for accountability
- Three Factors of Authentication
 - Type 1-Knowledge
 - Type 2-Possession
 - Type 3-Self Characteristic
 - Type 4-Action (sometimes)
- Two factor authentication

Passwords- what you know

- Ideally used only once
- Types
 - Static
 - Dynamic
- Financial institutions
 - Add personally known information
 - Still it is not two-factor authentication

Smartcards- what you have

- Four Types
 - Static Password Tokens
 - **Synchronous dynamic tokens**
 - Asynchronous dynamic tokens
 - Challenge-Response tokens
- Two elements of authentication
 - Front end authentication device
 - Back end authentication server

Biometrics- what you are

- Technical or logical access control
- Type 3- who you are
- Sensitivity of the equipment
- Types of errors
 - FRR or type 1 error
 - FAR or type 2 error
- CER or EER

Biometrics Continued

- Fingerprints
- Retina scans
- Iris scan
- Facial scan
- Palm scans
- Hand geometry
- FVID
- Knee scan

Biometrics Continued

- Voice print
- Signature Dynamics
- Keyboard dynamics
- Hand topology

Now the e-government

- Types of e-government
 - **G2C- government to customer**
 - **G2B- government to business**
 - G2G- government to government
 - G2E- government to employee

Potential for e-authentication

- 6500 G2B and G2C applications
- Supports government paperwork elimination act
- It is mandated by powerful OMB
 - Office of Management and Budget

Business-Focused Applications

Type of Transaction	Sample Application	Potential Users
Registration	Employer Identification Number	22.9M small businesses
Taxes	80 forms	22.9M small businesses
Licensing/Permits/ Accreditation	Nat'l Park Service Research Permits	3500 researchers, 10,000 permits requested each year
Compliance	EPA Central Data Exchange	15,000 industries and laboratories
Grants/Loans/ Subsidies	FHA Connection	90,000 mortgage lenders – 1.4M loans approved in FY04
Gov't Contracting	E-Offer	8,000 primary business contracts; 100,000 projected business users
Business Support	NASA Integrated Information	50,000 contractors, industry participants (350M transaction per year)
Int'l Trade	Export.gov	3 million businesses

Citizen-Focused Applications

Type of Transaction	Sample Application	Potential Users
Taxes	IRS: 87 forms	118M returns in 2003 – 52M e-filed, 42M direct deposit
Healthcare	Health & Human Services' Transplant Donor	35M potential donors
Social Security	Statement on Line	47M citizens receiving benefits
Assistance	USA Jobs	Over 15,000 job postings
Recreation	Recreation One Stop	5.7M campers in 2003
Loans	Health & Human Services' National Student Loan	35M student users
Public Safety	Dept. of Justice's Victim Internet System	13M victims and their attorneys
Benefits	Veterans Affairs Medical and Education Benefits	70M veterans, family members or survivors

Four Types of Communications

- Informative
 - Regulatory services, holidays, public hearing schedules, notifications
- Two-way communication
 - User engages in dialogue and posts problems and issues requests
- Conducting Transactions
 - Filing tax return, applying for grants etc
- Governance
 - E-voting, online polling

Is anybody doing it?

- Indiana is the first state to allow government records to be digitally signed
 - Authenticity and Non-repudiation
- Alabama, Wal-Mart, and NIC developed online hunting license services issuance
 - 140,000 licenses issued

Who is Involved?

- Claimant- wants to prove his/her identity
- Electronic credentials- bind claimant to an attribute or token
- Token- secret used for authentication
- Verifier- verifies claimant's identity
- Relying party- the agency
- Assertion- passing of information from claimant to agency
- Credential Service Provider (CSP)- issues credentials, registers, issues tokens
 - Government wants to focus on applications, not get in the business of e-authentication
- Registration Authority (RA)- Identity and proofs subscriber who later becomes claimant

So, what is it then?

- **The E-Authentication service enables you to get access to government services online using log-in IDs (identity credentials) you already have from Web sites that you - and the government - trust.**
- **E-Authentication is a government-wide partnership that is supported by the agencies that comprise the Federal CIO Council. The United States General Services Administration (GSA) is the lead agency partner.**

So, how does it work?

- E-Authentication works through an association with a **trusted credential issuer**, making it necessary for the user to login into the issuer's site to obtain the authentication credentials. Those credentials or **E-Authentication ID** are then transferred to the **supporting government web site causing authentication.**

How did it all start?

- E-Authentication was created in response of an inter-governmental memorandum to the heads of all government departments and agencies on **December 16, 2003**. That memorandum was issued through the **Executive Office of the President, Office of Management and Budget**. Memorandum M04-04

Standards and Recommendations

- NIST e-authentication Guidance SP 800-63
- Four assurance levels
 - Level 1- little or no confidence in identity
 - Level 2- Some confidence in assertion
 - Level 3- High confidence in assertion
 - Level 4- Very high confidence in assertion
- Basis for assessing CSP on behalf of federal agencies

Two Types of Authentications

- Identity Authentication
 - Confirming individual's identity
- Attribute authentication
 - Confirming individual belongs to a group
 - E.g. veteran, military, US citizen
- Attribute establishes level of confidence
 - If there is no established attribute, it is called **anonymous credential**

How Assurance Level is Determined?

- Depends upon type of transaction
- Depends upon risk consequences of false authentication
 - Inconvenience
 - Financial loss
 - Reputation damage (to agency)
 - Civil violation, criminal violation
 - Personal safety

OMB Guidance

- **Only about authentication**
- **Not about** attributes, authorization, or access controls
- Only the agency application makes decisions on access controls

FPKI Architecture

- Federal PKI architecture
- Encompasses multiple CAs
- Each CA supports different FPKI policy and function
- Federal Policy CAs are
 - FBCA (federal bridge certification authority)
 - FCPF (federal PKI common policy framework) root CA
 - C4 (citizen and commerce class common root CA)

E-Governance

- Incorporates e-governance CAs issuing SSL/TLS certificates
 - Assertion-based credentialing for SAML (security assertion markup language) data exchanges

Who calls the shots?

- GSA (general services administration) OGP (office of government wide policy) is the federal PKI management authority (FPKI MA)
- FBCA (federal bridge certification authority) is an IS that facilitates acceptance of certifications for transactions
- FBCA has evolved into FPKIA that supports CA from many vendors supporting different functions

Few Updates

- User certificates generated after 1-1-9 must have 2048 RSA keys
- Certificates and CRLs after 1-1-9 must be signed with SHA-256 hashing algorithm

What does e-authentication involve?

- Initial enrollment
- Visits to agency application
- Identity credentials verification
- Transactions management- audit trail
- Long term records management
- System tests (periodic)
- Suspension, revocation, re-issuance
- Audit

Top 10 countries ...as per UNO- Readiness Index

- | | |
|----------------|---------------|
| 1. Sweden | 13. Estonia |
| 2. Denmark | 23. Singapore |
| 3. Norway | 32. UAE |
| 4. USA | 37. Mexico |
| 5. Netherlands | 42. Bahrain |
| 6. South Korea | 43. Bulgaria |
| 7. Canada | 50. Jordan |
| 8. Australia | |
| 9. France | |
| 10. UK | |

Important Links and Reading Material

- OMB Guidance to agencies on E-Authentication
 - OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, Dec. 16, 2003
 - <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
 - About identity authentication, not authorization or access control---
- NIST SP800-63: *Recommendation for Electronic Authentication*
 - Companion to OMB e-Authentication guidance
 - Draft for comment at: <http://csrc.nist.gov/eauth>
 - Covers conventional token based remote authentication
 - Does not cover Knowledge Based Authentication
- Info about e-gov from Whitehouse
 - <http://www.whitehouse.gov/omb/e-gov/>
- Identity Management website for government
<http://www.idmanagement.gov/drilldown.cfm?action=fpki>

Questions?

- Questions
- Feel free to write any questions to:
 - jayranade@technodyneuniversity.com
 - jayranade@technodyne.net