Building a Case for Mainframe Security

Dr. Paul Rohmeyer, Ph.D.
Stevens Institute of Technology
Hoboken, New Jersey
AGENDA

- Problem Statement
- Defining Security
- Understanding Mainframe Security Requirements
- Stevens Institute of Technology Research Project
- Business Case for Mainframe Security
- Conclusions
Problem Statement

- Mainframe security is often missing from the Enterprise Security Program
- This appears to be due to a lack of awareness, and a substantial knowledge gap on mainframe concepts
- The problem is evident in organizations of all sizes
- Government and policy efforts have largely ignored the problem
- …but our most critical and sensitive data is processed on mainframe, including much (most?) critical infrastructure providers
Problem Statement

The following industries are considered part of the US Critical Infrastructure:

- Banking and Finance
- Transportation
- Power
- Information and Communications
- Government Services
- Emergency Services
- Law Enforcement
- Public Works

Hmmmm. . . . do you think any of these industries are STILL using mainframes?
Defining Security

- Confidentiality
- Integrity
- Availability
Defining Security - The Security Dilemma

- Changing Threat Scenarios
- Dynamic Risk Profiles
- Regulatory Requirements
- Auditing and Monitoring
Understanding Mainframe Security Requirements

- Mainframes provide a powerful computing platform for many of the world’s largest transaction oriented applications.
  - CMS (Centers for Medicaid and Medicare Services) utilizes mainframes for Medicare related transactions and statistical analysis
  - Bank of America utilizes mainframes for processing all its credit card transactions
  - Kaiser Permanente and many other healthcare enterprises for processing patient claims transactions
- Industry sources estimate that 30 billion Cobol transactions occur daily; that's more than the number of Web page hits in the same time period.
- Do you think security is a relevant subject for mainframes?
Understanding Mainframe Security

- While mainframes have the reputation of being secure, i.e. less open and less accessible, there are many areas of the mainframe infrastructure that require special treatment to ensure the security of the data and the applications it stores & processes.

- In order to understand these security requirements, one must have a good understanding of the various mainframe components and their own individual security requirements.
Understanding Mainframe Security: Mainframe Components

• Operating System
  – Z/OS, MVS
  – RACF, ACF2, TopSecret

• Operational Environment
  – Web Architectures
  – Storage
  – Communications and Networking
  – System Software

• Applications
  – Databases
  – Middleware
  – Enterprise Applications
Critical Observations

- Each Mainframe Component has its own security requirements
- Mainframe components support various computing architectures such as web-based, J2EE, and Service-Oriented. In order to securely configure mainframe components, it is important to understand these architectures.
Critical Observations (cont.)
Emerging SOA Architecture

Source: SOA Community of Practice, SOA Solution Stack Project
Critical Observations (cont.)

With apologies to any IS Auditors in attendance:

An audit of RACF is not the same thing as an assessment of mainframe security!
Building a Case
Building a Case: SUMMARY

Information and System Importance

Criticality

Sensitivity

Threats & Vulnerabilities

Malicious Data Access

Self-Inflicted Mistakes

June 13 - 15, 2010
Mainframes provide a powerful computing platform for many of the world’s largest transaction oriented applications.

While mainframes have proven themselves over years, changes in the computing paradigm require that mainframe security be considered as part of the overall security management effort within an enterprise.
Building a Case: CRITICALITY

• Large organizations (including critical infrastructure companies) are shifting applications from Wintel to Linux on the mainframe to save costs and increase performance and reliability.

• With today’s applications shifting to more open platforms such as Linux, and the increasing accessibility of mainframe data via IP networks, multiple computing platforms and the Internet, hundreds of thousands of users can now potentially access mainframe data from anywhere.
Building a Case: SENSITIVITY

• Sensitive data is captured via OLTP and stored on the mainframe.
• Privacy Concerns
• Reputational Risk Dimensions
• Organizations need to meet regulatory requirements such as PCI compliance, Sarbanes-Oxley Compliance, GLBA, FISMA, etc.
Building a Case:

THREATS & VULNERABILITIES

• Data Leaks
  – Mainframes process sensitive data, this data needs protection in transit as well as in storage.
  – Data stored on Mainframes is routinely accessed for end user computing or even for the purposes of downloads to the mid-tier applications.
  – Mainframes are just as vulnerable to poor user access controls and user errors as mid-tier or desktop computers are.
Building a Case: 

THREATS & VULNERABILITIES

• **Weak Coding Practices**
  – If Mainframe applications are not coded well, they could be subject to SQL Injection type attacks. Additionally, many of the Mainframe components are lenient on their password policies.

• **Malicious Code**
  – While many web applications today have built-in security protocols, writing secure web application code is difficult and often not the priority of the developer. Malicious code could be imbedded in a XML message.
Building a Case:

THREATS & VULNERABILITIES

• Insider Threats
  – Mainframes are just as vulnerable to insider threats as other computers. As Mainframe administrators are often a close-knit group whose activities are rarely monitored, this alone is a serious threat to consider.

• Hackers
  – As Mainframes are becoming more and more web facing, particularly with their support of protocols such as FTP and HTTPs, Hacker threats have become real. Additionally, many Mainframe databases are directly accessible from the Internet, making Mainframes very vulnerable to Hacking attempts.

• Network Threats
  – Denial of Service
  – Network-based Attacks
Building a Case:

THREATS & VULNERABILITIES

Malicious data access: Hackers and trusted users have increased potential to access the mainframe's core data repository just like any other platform. The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and other standards all point to the need to protect data accountability and integrity. The mainframe can't be an exception.
Building a Case:

THREATS & VULNERABILITIES

• **Self-inflicted mistakes**: A generation of mainframe masters is quickly retiring, and less qualified or less experienced technical staffers (often rushed and overworked) can inadvertently change code or settings to open up holes or deliver too much authorization to the system. A strength of the mainframe is that you can continue to run the old reliable software without too much maintenance. But even mainframe software needs checks, patches and updates to close gaps or simply improve security.
Building a Case: SUMMARY

Information and System Importance

Criticality

Sensitivity

Threats & Vulnerabilities

Malicious Data Access

Self-Inflicted Mistakes
Conclusions
Why Mainframe Security?

- Disclosure of privileged information
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements
- Disruption of the computer infrastructure resulting in the inability to perform critical business functions
- Use of the computer system as a launch pad for malicious activity against other entities (and the potential to be held liable for damaging them)
Why Mainframe Security?

• Next research step: Updating the mainframe security roadmap…
  – Risk assessment framework
  – Evaluating design of controls
  – Creating adequate tests of controls
  – Emphasis on integration points
Questions
Dr. Paul Rohmeyer
908.531.2551
paul.rohmeyer@stevens.edu

Meenu Gupta,
CISA,CISM,CISSP,CIPP,CBP
meenu.gupta@mittal-tech.com