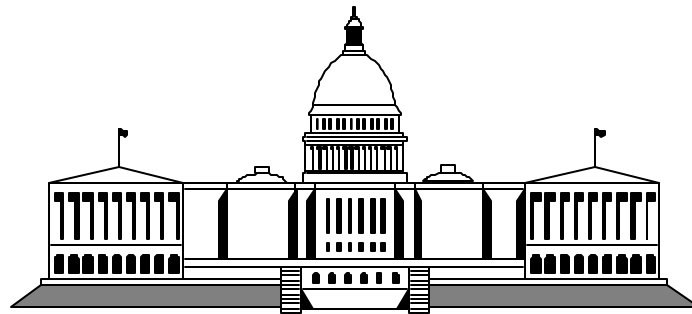


S/390 Security and the Web

Mike Kearney, CISSP
kearney@us.ibm.com

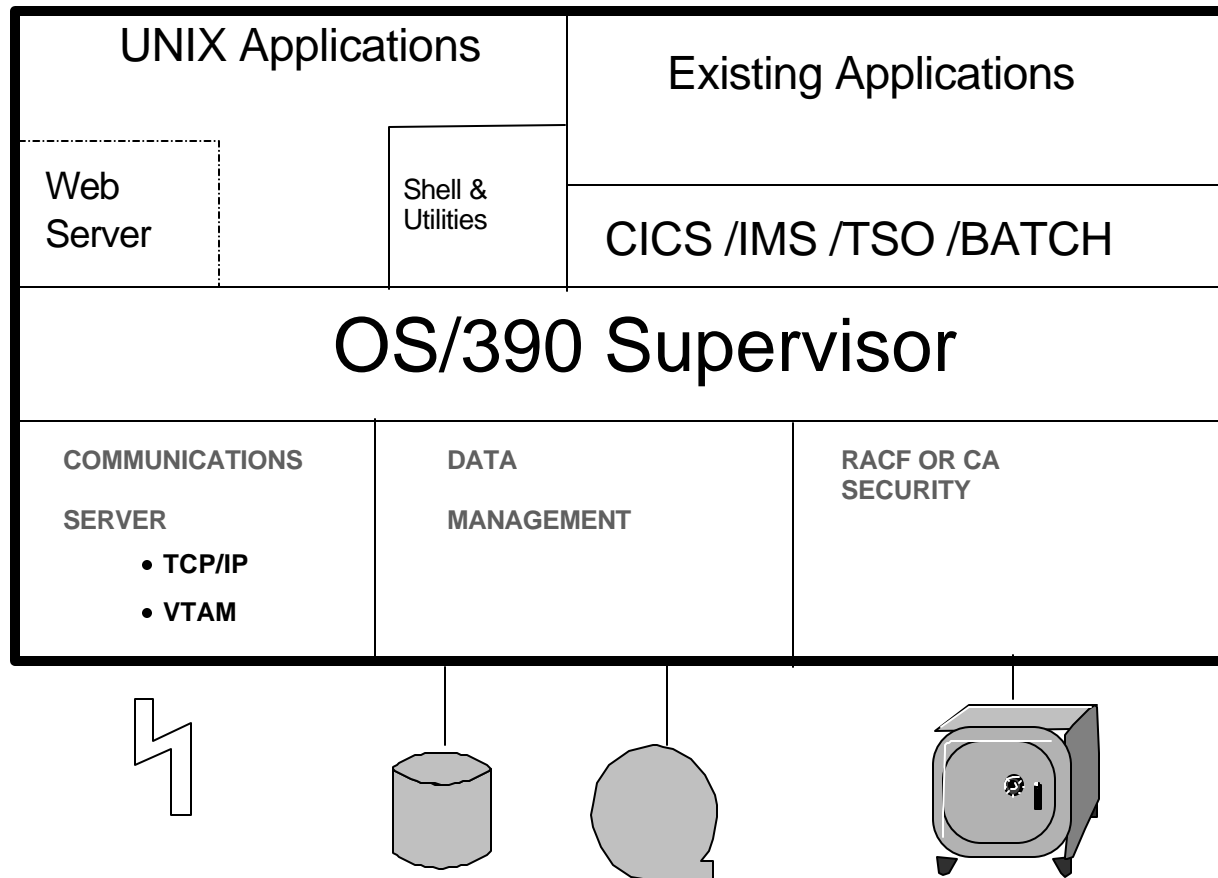


Washington System Center

S/390 Security and the Web

S/390 support for legacy applications has earned it a reputation as a secure system. This presentation describes the architecture and features that make S/390, including UNIX System Services, the most secure server platform for Internet applications as well.

OS/390 UNIX System Services



OS/390 Design: System Integrity

System Integrity means there is **no way** for any unauthorized program, using any system interface, defined or undefined, **to:**

- Bypass store or fetch protection
- Bypass OS password, VSAM password, or RACF security checking
- Obtain control in an authorized state

System Integrity is not limited to conventional OS/390 workloads, it applies to UNIX System Services as well.

OS/390 Design: UNIX System Services



- User Authentication by RACF. No /etc/passwd file.
 - No brute force password guessing attacks
- No trusted hosts, (hosts.equiv) or trusted remote hosts (.rhosts) support
 - No rlogin without authentication
- No remote execution /etc/rexecd file.
 - No command execution without authentication
- These are 'features' found in other UNIX systems that have resulted in breakins. USS doesn't have them.

OS/390 Design: UNIX System Services and RACF



- UNIX Superusers (uid=0) Have Complete Authority Over UNIX Systems. In OS/390 Their Use Is Minimized and Controlled.
- OS/390 UNIX Superuser Authority
 - Assigned Via uid=0 or READ Access to BPX.SUPERUSER
 - Superuser Authority Confers No RACF Administrative Authority
 - Superuser Authority Confers No MVS Resource Access Authority
 - Superusers Are 'Super' In USS Only
- BPX.SUPERUSERS Require SU Command To Enable Authority
 - Increasing Awareness

- Superuser Granularity through RACF Profiles
 - Grant Selected Superuser Capabilities To Non-Superusers
 - Minimizes Superusers
 - See List Next Page
- Exceed System Resource Limits through RACF Profiles
 - Set Higher Limits by Userid
 - Max. CPU Time
 - Max. Address Space Size
 - Max. Number of Files/Process
 - Max. Number of Processes/UID
 - Max. Number of Threads/Process
 - Max. Memory Map Size
 - Minimizes Superusers

Profiles Defined in RACF Class UNIXPRIV

- SUPERUSER.FILESYS
- SUPERUSER.FILESYS.MOUNT
- SUPERUSER.FILESYS.QUIESCE
- SUPERUSER.FILESYS.CHOWN
- SUPERUSER.FILESYS.PFSCTL
- SUPERUSER.FILESYS.VREGISTER
- SUPERUSER.PROCESS.GETPSENT
- SUPERUSER.PROCESS.KILL
- SUPERUSER.PROCESS.PTRACE
- SUPERUSER.IPC.RMID
- SUPERUSER.SETPRIORITY

OS/390 Design: UNIX System Services and RACF

- 'Protected' Userids for Started Procedures and Daemons
 - No Logon, No SU, No Revoked Userid from Password Guessing
- 'Restricted' Userids for 'guest' Users
 - Access Authorities Must be Explicitly Granted to User or Group in RACF Profiles
 - No 'default' Access Authority Surprises
- A Userid Can be Both Restricted and Protected

OS/390 Design: Program Control

- Any Program Run By a Superuser Can Be a Threat to USS Security
- Programs in APF-Authorized Libraries are Assumed to Be 'Well-Behaved' (i.e. a 'Clean' Environment)
- Programs in Unauthorized Libraries:
 - Might Be Safe If They Are Protected from User Update (System Controlled)
 - Are Not Safe If Users Can Update (not System Controlled)
- OS/390 Will Not Allow A 'Clean' Environment to Become 'Dirty'
- The Entire HFS is Treated As An Unauthorized Library
- Individual HFS Programs Can Be Marked APF-Authorized

OS/390 Design: Thread Level Security

- Process: A program using USS kernel services.
 - Three types of Processes
 - User processes - associated with a program or shell user
 - Daemon processes - perform systemwide services, for example a Web Server or Print Spooler
 - Kernel processes - perform system-wide functions for the kernel
 - Processes run in their own address spaces.
- Thread: A single flow of control within a Process. For example, a Web Server daemon responding to your request will start a thread for you. A thread runs within the address space of the Process.

OS/390 Design: Thread Level Security

- Thread Level Security: The ability of a process to start a thread which runs under the authority of a separate userid.
 - Examples:
 - A Web Server that serves data based on the user's authority to access it.
 - An LDAP Server that provides information based upon the user's authority to access it.
 - A 'multi-user' address space (sound a little like CICS TS?)

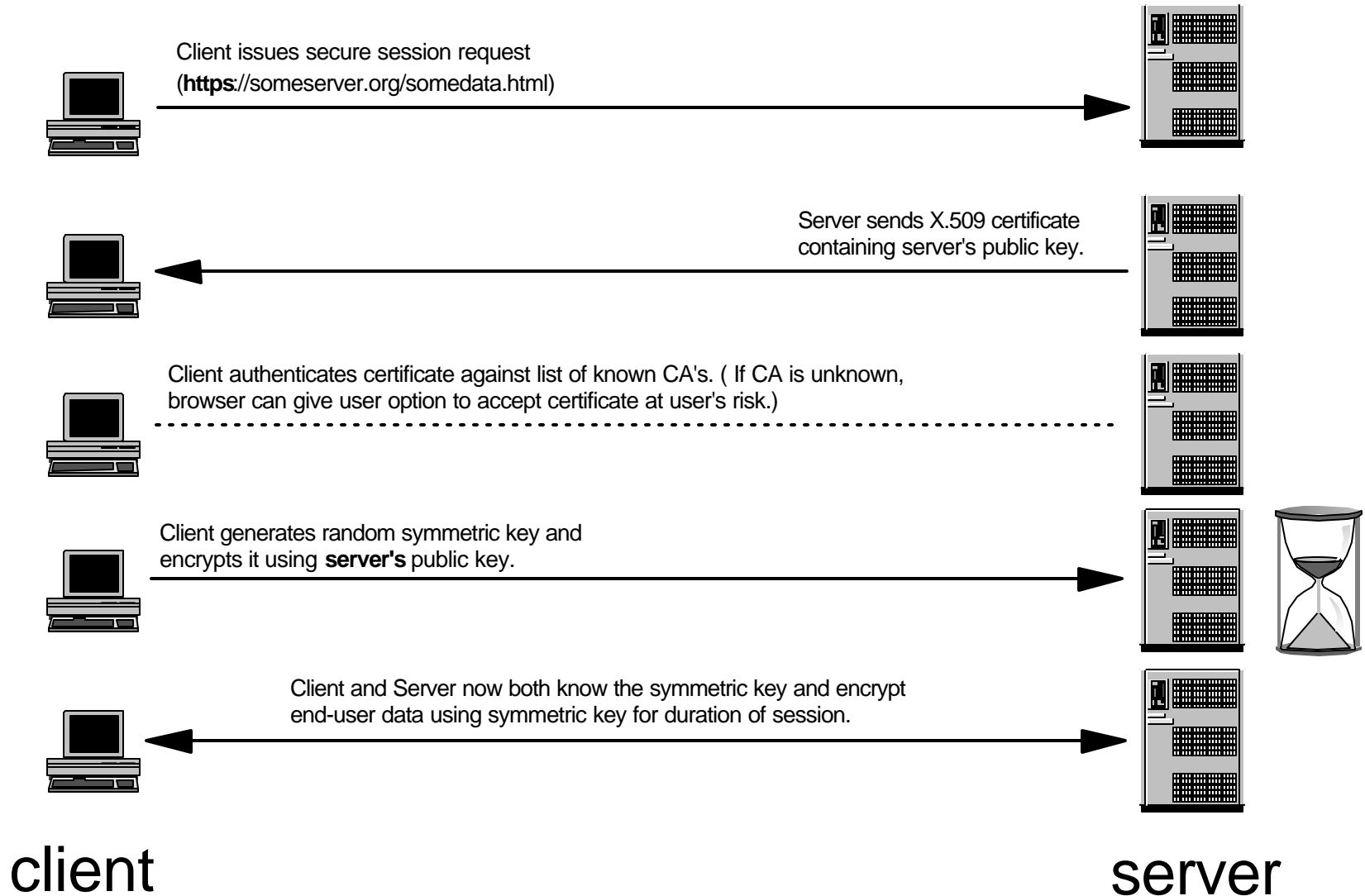
OS/390 Design: HTTP Server for OS/390

- The HTTP Server has Thread Level Security
- Each Web User's Request Runs With the Authority of a RACF Defined Userid
 - HTTP Configuration Options Allow that Userid to be:
 - The Server's Userid
 - A Guest Userid, Like PUBLIC
 - A Userid/Password provided by the User, Authenticated by RACF
 - A Userid/Password provided by the User, Authenticated by RACF, protected by SSL
 - A Userid Associated with a Digital Certificate, Authenticated with a SSL Handshake

S/390 Design: Integrated Hardware Cryptographic Support

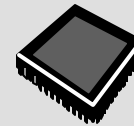
- Cryptographic Operations Use CPU Cycles
- Public Key Cryptography is ***Especially*** CPU Intensive
- The Pre-Master Secret decrypt is the single most expensive part of the SSL protocol
- S/390 Cryptographic Hardware provides a significant performance benefit over software encryption

SSL Simplified



S/390 Design: Integrated Hardware Cryptographic Support

- **Standard feature on Generation 4 and later Parallel Enterprise Servers and Application StarterPak**
- **Integrated support in OS/390 V2**



- Highly secure storage of cryptographic keys
- Validated by US Gov't NIST at FIPS 140-1 Level 4
 - IBM has the first two products to reach this level of assurance
- Reduces MIPS usage for crypto intensive operations (e.g., SSL)
- Offloads crypto operations onto integrated high performance engine



- **S/390 Cryptographic Coprocessors**
 - ◆ specialized hardware accessible from OS/390
- **PCI Cryptographic Coprocessors**
 - ◆ Optional, Additional Features for Capacity and Function
- **OS/390 Integrated Cryptographic Services Facility (ICSF)**
 - ◆ Software Interface to Crypto Hardware
- **Trusted Key Entry Workstation**
 - ◆ Optional S/390 feature for More Secure Key Entry

9672 G6 SSL Performance

- 9672-X77, 2 crypto coprocessors, 8 PCICC
 - ▶ 1000 SSL trans/sec, 70% busy
 - 80% symmetric, 20% public key
 - ▶ 950 SSL trans/sec, 90% busy
 - 100% public key
 - ▶ 2500 SSL trans/sec, 100% busy
 - 100% symmetric

Crypto and the HTTP Server for OS/390



- If the Cryptographic Hardware and ICSF are implemented, the HTTP Server will use them for SSL support.
- No Options Need to be Specified in the HTTP Server config.
- The HTTP Server Benefits From Crypto Hardware Support for:
 - ◆ Decryption of Pre-Master Secret using the Server's private key
 - ◆ Message Encrypts and Decrypts using Triple-DES or DES
- The HTTP Server Message Log will Indicate if Hardware is/is not being used if `GSK_SSL_HW_DETECT_MESSAGE=1` is present in the `httpd.envvars` file.
- SMF Type 30 Record (SMF30CSC) Will Indicate ICSF requests Executed in HTTP Server address space.

OS/390 Design: TCP/IP Security



- Multiple IP Stacks, Each in its Own Address Space
 - System Integrity Separates Trusted and Untrusted Networks
- Firewall Services in Each IP Stack
 - IP Packet Filtering
 - Network Address Translation
 - Virtual Private Networking with IPSec and IKE

OS/390 System Testing

- We Hack OS/390
 - Using IBM's Hawthorn Research Lab Experts
 - Research Keeps Current with Hacker Sites, CERT, etc.
 - Test With and Without the Firewall Technologies
 - Test at Component Test time
 - Test Again Under Load at Integration Test time
 - Fix Exposures and Test Again
- To Date, We Have Not Been Notified By Any Customer of a Successful Hacking Incident on S/390
 - But We Won't Rest, and Neither Should You!

S/390 Design: Logical Partitioning (LPAR)

- LPAR Provides up to 15 Isolated System Images on a Single CEC
- Organizations Have Relied for Years On LPARs to Provide Multiple Security Environments
- Received ITSEC E4 Security Certification in 1999
 - Identification and Authentication
 - Access Control
 - Audit and Accountability
 - Object Reuse
 - Availability of Service

■ S/390 Web Security Workshop (WSW01)

◆ Objective

This hands-on, *no-charge* workshop is designed to demonstrate the security capabilities of the HTTP Server for OS/390, along with an overview of LDAP and the Firewall Technologies for OS/390.

◆ Lectures and Labs Include

- ▶ HTTP Server Authentication with RACF Userids, Passwords
- ▶ HTTP Server and SSL
- ▶ HTTP Server, SSL and Client Authentication with Digital Certificates
- ▶ LDAP Access to RACF Information

◆ Upcoming Classes in Gaithersburg, MD

- ▶ October 24-26, November 14-16, December 12-14
- ▶ Contact your IBM rep. to enroll, or
- ▶ Contact kearney@us.ibm.com for more information

Summary

- Security Has Always Been an Important Component of S/390 Design
- UNIX System Services Builds on This Legacy
- S/390 Provides Thread Level Security
- S/390 Minimizes the Number of Superusers
- Emerging Security Standards are Supported Today
- S/390 Cryptographic Hardware On Most Models Provides Performance Over Software
- Extensive Testing for Security Vulnerabilities

References

- MVS Planning: Security, SG28-1439
- OS/390 UNIX System Services Planning, SC28-1890
- OS/390 UNIX System Services User's Guide, SC28-1891
- Security Server (RACF) Security Administrator's Guide, SC28-1915
- HTTP Server Planning, Installing and Using, SC31-8690
- ICSF Overview, GC23-3972
- S/390 PR/SM Planning Guide, GA22-7236
- Security In OS/390-based TCP/IP Networks, SG24-5383