IBM Software Group

TPF Users Group Spring 2005

Hardware Cryptography Support The Details

Mark Gambino

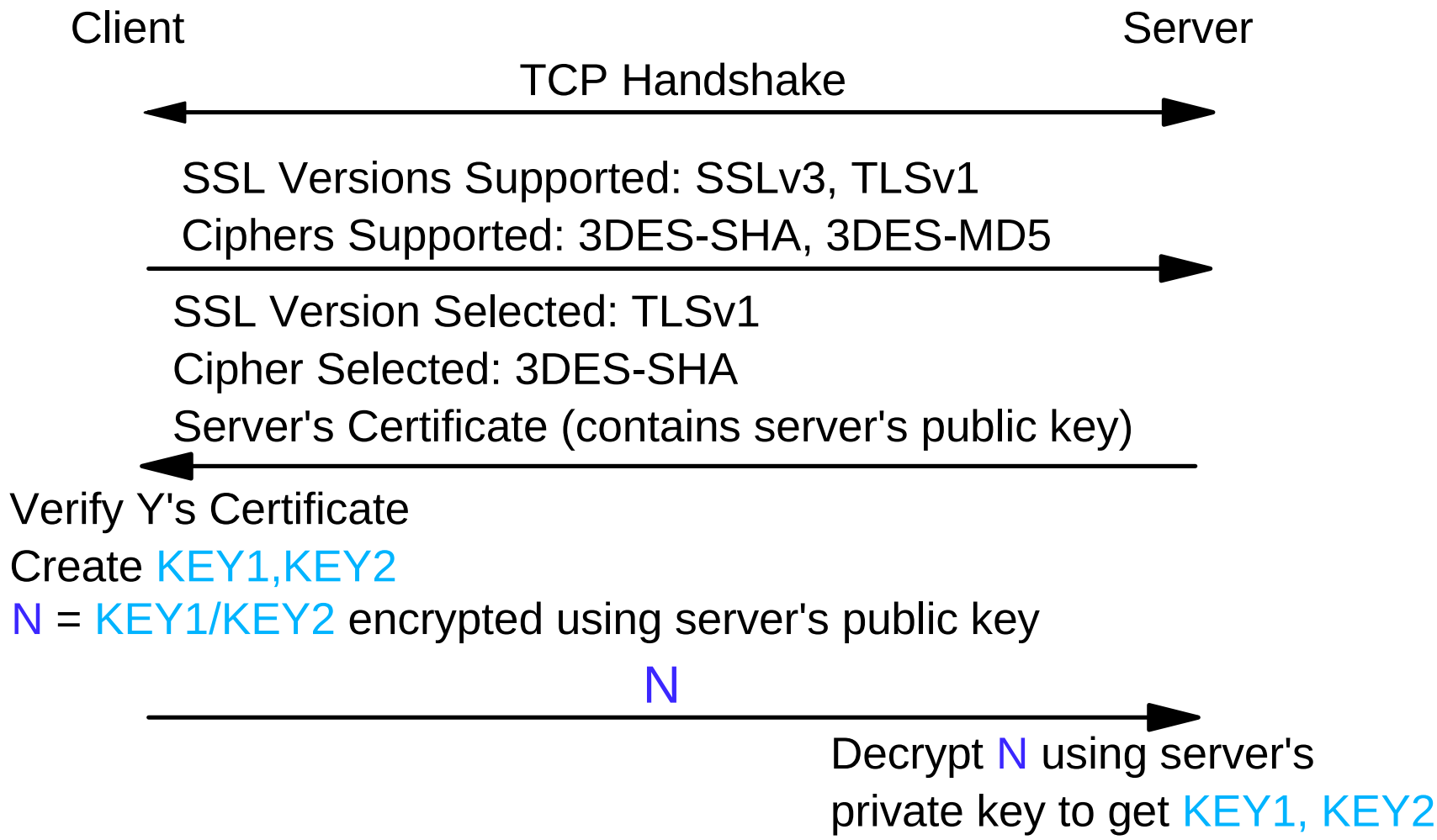
AIM Enterprise Platform Software

IBM z/Transaction Processing Facility Enterprise Edition 1.1.0

Steps for Starting an SSL Session

- Starting an SSL session uses RSA public key cryptography to exchange secret keys (KEY1, KEY2) between the client and server nodes
- RSA uses a public/private key pair
- Data encrypted using the public key can only be decrypted using the corresponding private key
- During the SSL handshake, the server sends its certificate to the client
  - The certificate contains the server's public key
- Client creates the secret keys, encrypts them using the server's RSA public key, then sends them to the server
- Server decrypts the data using the server's RSA private key to get the secret keys created by the client

Sample SSL Handshake Flows



RSA Math

- RSA public key operations are CPU intensive
- RSA private key operations are much more CPU intensive
  - Can be 10x higher than public key operations
- Encrypting or decrypting data using an RSA key involves modular exponentiation (ME)
  - Modulus (M) is typically 1024 bits
  - 2048-bit modulus is also supported
- Processing can be reduced for private key operations if you use the Chinese Remainder Theorem (CRT) rather than ME
  - CRT is roughly 50% savings over using ME
- To use CRT, certain intermediate variables used when the RSA key pair was created must be saved and available in the private key structure loaded to TPF

RSA Key Generation Math

- p, q = large random prime numbers
- n = p*q
- d, e = exponent values
  - Very complicated math to come up with these values!
- dmp1 = d MOD (p-1)
- dmq1 = d MOD (q-1)
- iqmp = q-1 MOD p
- RSA structures:
  - Always have d, e, and n filled in
  - p and q (and derivitives dmp1, dmq1, iqmp) may or may not be filled in depending on how the RSA keys were generated
- CRT can be used if p, q, dmp1, dmq1, and iqmp are available

Hardware Acceleration for RSA Operations

- PCI Cryptographic Accelerator (PCICA)
- Hardware cryptographic accelerator card introduced on the IBM z900 server (supported on z900, z800, z990, and z890)
- PCICA was designed specifically to improve SSL performance
- PCICA only does RSA operations and does them very quickly
  - Each PCICA can do several hundred to over 1000 operations per second (varies based on key type, key size, and whether ME or CRT is used)
- Using PCICA cards enables TPF to start thousands of SSL sessions per second
- APAR PJ30133 (in test phase) adds this support to TPF 4.1.

PCICA Operations

- PCICA can do the following:
  - RSA public key operations:
    - Using ME with a 1024-bit key
    - Using ME with a 2048-bit key
  - RSA private key operations:
    - Using ME with a 1024-bit key
    - Using ME with a 2048-bit key
    - Using CRT with a 1024-bit key
    - Using CRT with a 2048-bit key
- TPF SSL code uses PCICA (if installed) for all RSA operations

Crypto Card Terminology

- Hardware cryptographic accelerator cards such as PCICA are called *adjunct processors (APs)*
- Current processors support up to 16 APs
- Each AP supports up to 16 domains
  - An AP can be shared by up to 16 LPARs
  - You define which LPARs use which APs
- At IPL time, TPF automatically determines which APs are defined to this system and displays that information to the TPF operator console
  - PCICA is the only AP type currently supported by TPF
- TPF automatically detects when new APs are added to the configuration (no IPL necessary)
- Messages are displayed on TPF operator console if a PCICA card fails and if the last PCICA card fails

PCICA Load Balancing

- TPF running native
  - TPF balances the load across all of the PCICA adapters available on this LPAR
- TPF running as a VM guest
  - VM presents one virtual AP (PCICA) to the guest
  - TPF will see only 1 (virtual) PCICA in this enviornment, even if multiple real PCICA adapters are defined
  - VM balances the load across the physical PCICA adapters available on this LPAR

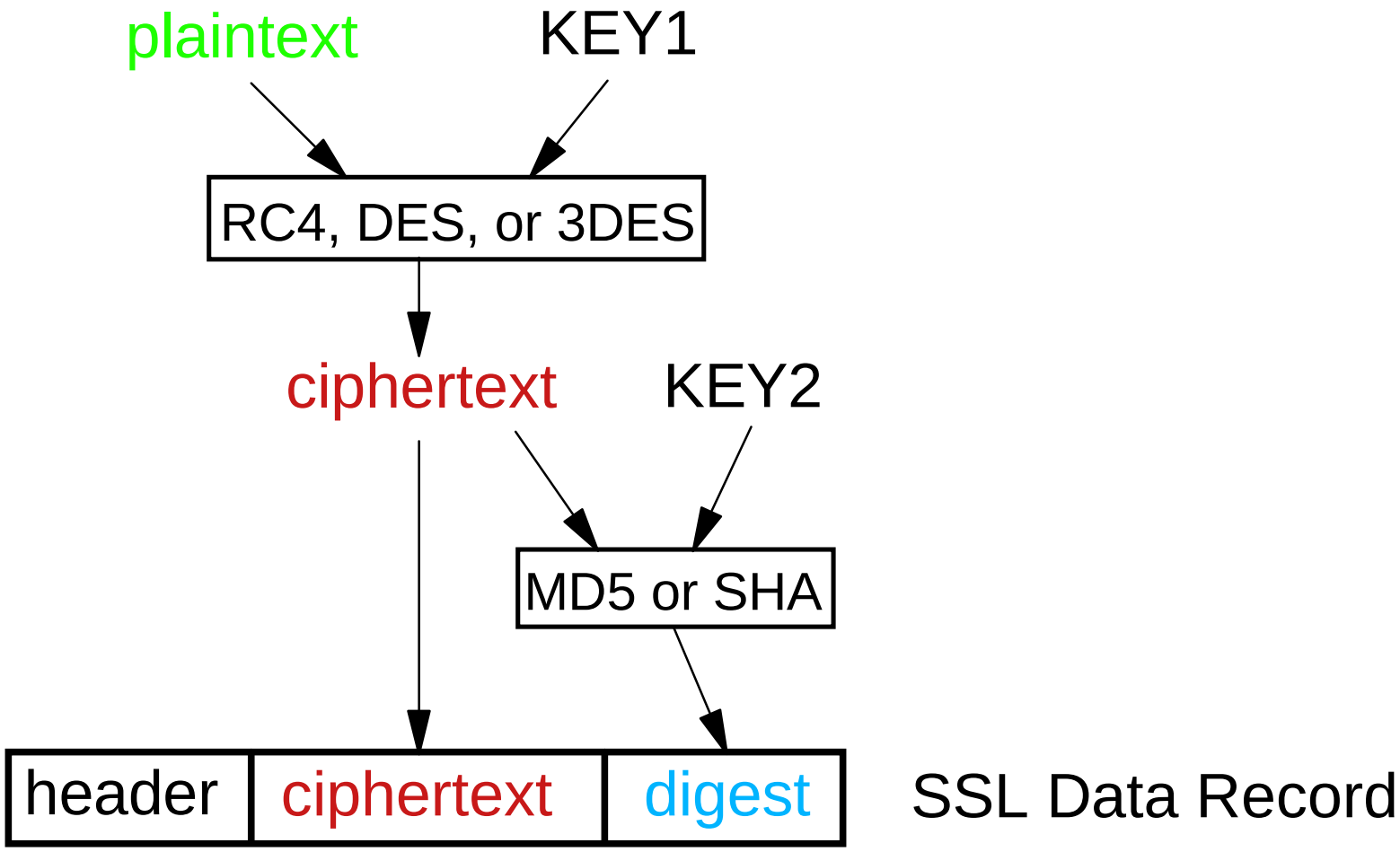
Encrypting SSL Data Messages

- Each SSL data message is encrypted by the sender using one of the following symmetric cryptography algorithms:
  - RC4
    - 128-bit, most commonly used in Web browsing
    - Just as efficient in software as hardware
  - DES
    - 56-bit, block cipher
    - Operates in cipher block chaining (CBC) mode
  - Triple-DES (3DES, TDES)
    - 168-bit, block cipher, operates in CBC mode
    - Considered highly secure
    - Most CPU overhead of the symmetric ciphers
- Receiver decrypts the data using the same key (KEY1 in previous example) that the sender used to encrypt the data

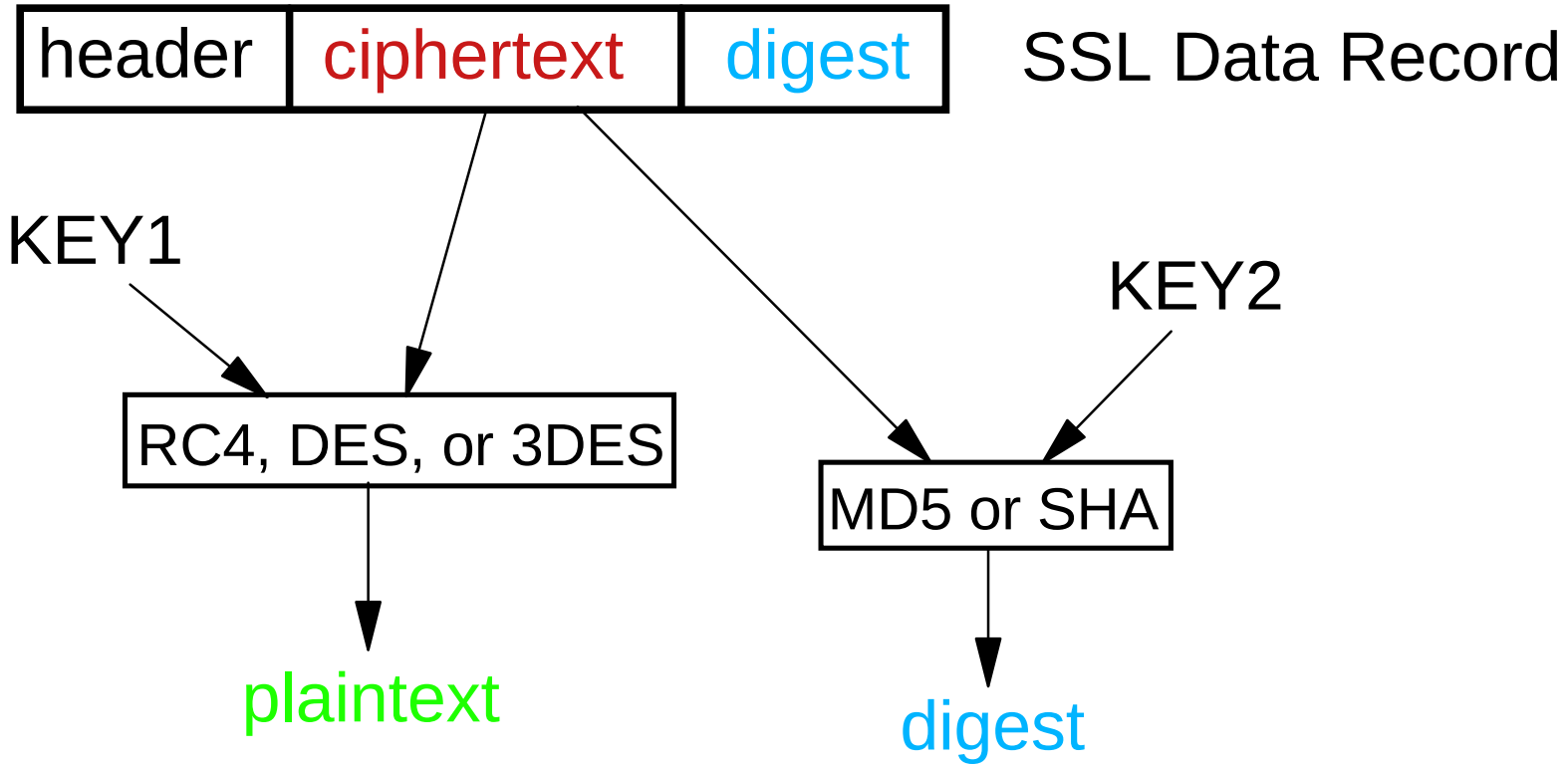
SSL Message Digests

- The encrypted data is run through a secure one-way hash algorithm (using KEY2 in the previous example) to produce a message digest that is the appended to the SSL data message
  - The MD5 or SHA (SHA-1) algorithm is used to produce the message digest
- The receiver calculates the message digest (using KEY2) and compares that to the digest appended to the message
  - If the two digests do not match, the data has been altered by some node in the network
- MD5 produces 128-bit hash
- SHA produces 160-bit hash and is recommended over MD5

Building an SSL Data Record



Processing an SSL Data Record



Central Processor Assist for Cryptographic Functions (CPACF)

- Hardware cryptographic accelerator coprocessor introduced on the IBM z990 server (supported on z990 and z890)
  - One CPACF coprocessor per CP (I-stream)
  - CPACF is not an adjunct processor (AP)
- CPACF does DES, 3DES, and SHA operations
  - CPACF comes with SHA enabled
  - Separate feature code to enable DES/3DES on CPACF
- Each CPACF can do DES at 300 MB/sec, 3DES at 100 MB/sec, and SHA at 250 MB/sec
  - Rates vary (up or down) based on data size
- CPACF is invoked via new assembler instructions. For example:
  - KM - encrypt/decrypt data using DES/3DES
  - KMC - encrypt/decrypt data using DES/3DES running in CBC mode
  - KIMD - compute intermediate message digest using SHA
  - KLMD - compute last message digest using SHA

Hardware Acceleration for SSL Data Messages

- SSL support in TPF automatically determines if CPACF is installed and which features (like DES/3DES) are enabled
- TPF uses CPACF for data encryption on an SSL session if all of the following conditions are true:
  - DES or 3DES is the algorithm selected for data encryption
  - CPACF is installed
  - The DES/3DES feature of CPACF is enabled
- TPF uses CPACF for message digest processing on an SSL session if both of the following conditions are true:
  - SHA is the algorithm selected for message digests
  - CPACF is installed
- CPACF improves performance of data encryption/decryption as well as message digest creation/validation
- APAR PJ30156 (in test phase) adds this support to TPF 4.1.

Hardware Acceleration for User Data Encryption

- Requirements exist to encrypt/decrypt user data outside the scope of SSL or other standard protocol
  - For example, encrypt credit card numbers or other sensitive data stored in your TPF database
- A new user API exists to allow you to encrypt/decrypt variable length user data using DES or 3DES
  - Both assembler and C language API interfaces
  - Can process up to 1 MB of data on a single API call
  - Uses CPACF if installed to do the DES/3DES operation; otherwise, uses software encryption
- APAR PJ30156 (in test phase) adds this support to TPF 4.1.

Tuning, Statistics, and Capacity Planning

- PCICA Support (APAR PJ30133):
  - Includes online displays and data collection updates
  - Shows RSA operations per second per PCICA information
  - Shows current and maximum queue sizes
  - Helps you determine if more PCICA adapters are needed
- CPACF Support (APAR PJ30156):
  - Includes online displays and data collection updates
  - Shows number of operations and bytes per second per I-stream for DES, 3DES, and SHA
  - Shows current and maximum rates

Summary

- SSL is now ready for mainline applications on TPF
  - PCICA adapters allow you to start thousands of SSL sessions per second
  - CPACF allows you to exchange tens of thousands of messages per second across SSL
- New user APIs enable you to encrypt/decrypt hundreds of MB per second of user data using CPACF to meet the ever growing security requirements of your business
- TPF system automatically determines whether PCICA and CPACF are installed
  - Uses software encryption if the appropriate hardware acceleration is not installed
    - Allows you to test applications running on back-level processors (using software encryption) and then run in production using hardware acceleration

Trademarks

IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Notes
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.