TPF Users Group Spring 2005

Hardware Cryptography Support for SSL and User Data

Mark Gambino

AIM Enterprise Platform Software

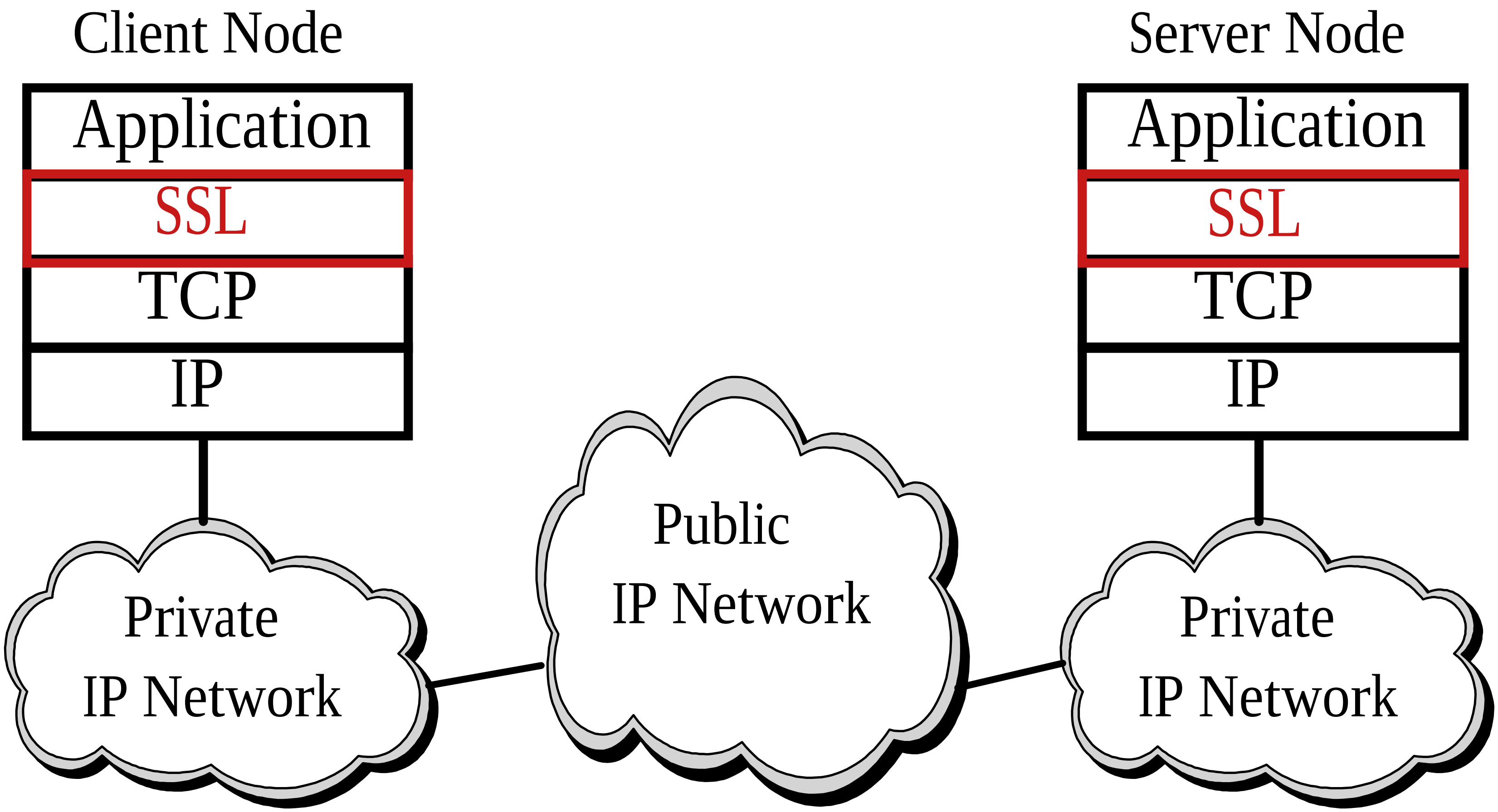
IBM z/Transaction Processing Facility Enterprise Edition 1.1.0

Any references to future plans are for planning purposes only. IBM reserves the right to change those plans at its discretion. Any reliance on such a disclosure is solely at your own risk. IBM makes no commitment to provide additional information in the future.

Secure Sockets Layer (SSL)

- Protocol layer that sits between the TCP layer and the application (or middleware)
- Enables applications to communicate in a secure manner over an insecure (public) network
- SSL evolved to the Transport Layer Security (TLS) open standard, defined by RFC 2246
  - Still referred to as "SSL" most of the time
- TPF 4.1 added SSL support on PUT 15
  - Included Apache Secure Web Server

SSL Network Example



Starting an SSL Session

- Client and server use RSA public key cryptography to exchange the following secret keys:
  - KEY1 - key used to encrypt and decrypt data messages flowing on this SSL session
  - KEY2 - key used to create and verify message digests appended to each data message on this SSL session
- RSA operations are very CPU-intensive
  - For example, an RSA private key decrypt operation can execute millions of instructions in software
- The secure key exchange using RSA is the heart of SSL security
- Using software for RSA operations, the number of SSL sessions that can be started is in the tens per second range

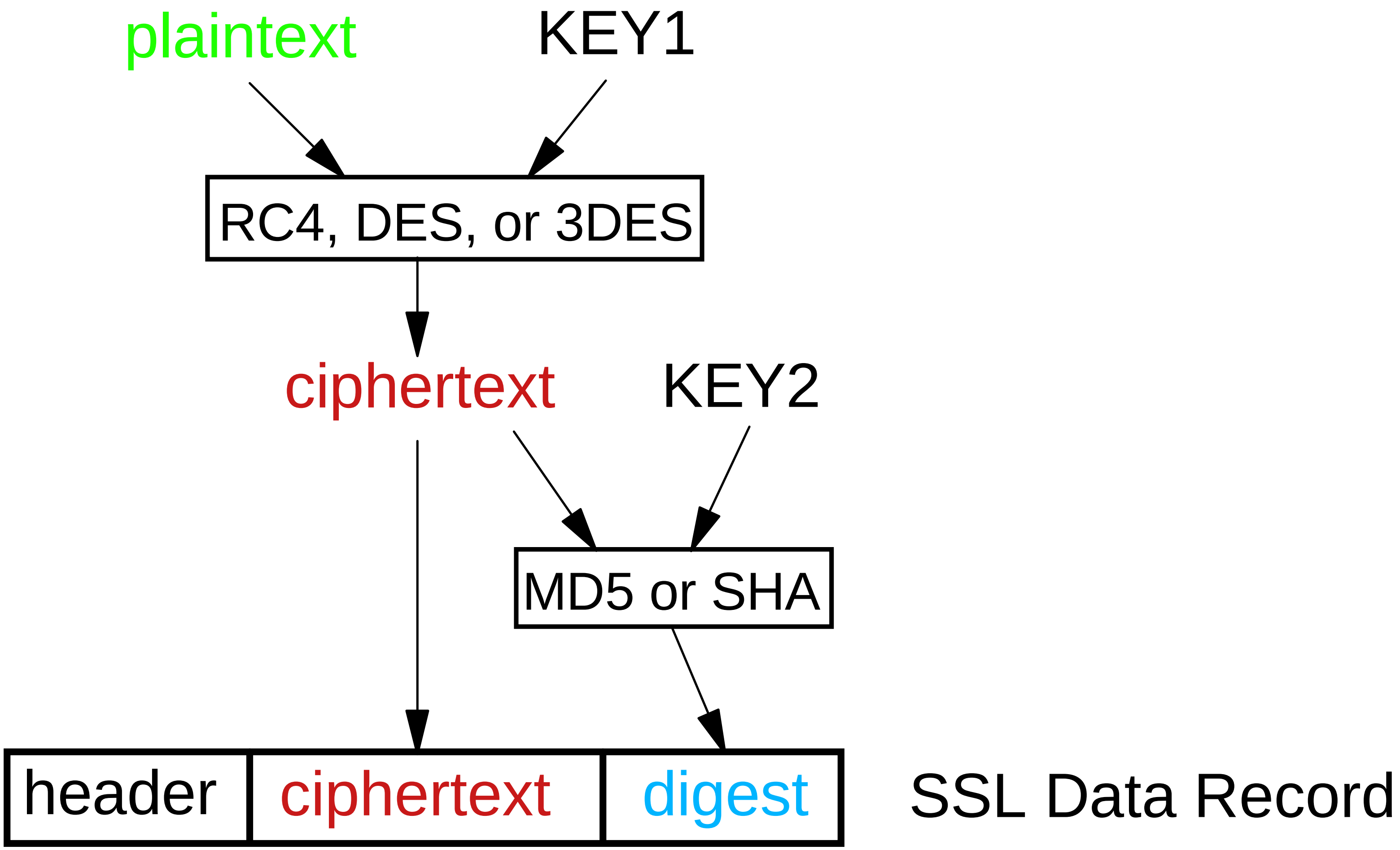
Hardware Acceleration for RSA Operations

- PCI Cryptographic Accelerator (PCICA)
- Hardware cryptographic accelerator card introduced on the IBM z900 server (supported on z900, z800, z990, 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 things like RSA key size)
- Using PCICA cards enables TPF to start thousands of SSL sessions per second
- SSL support in TPF automatically determines if PCICA(s) exist and uses them for RSA operations if they are installed
- APAR PJ30133 (in test phase) adds this support to TPF 4.1.

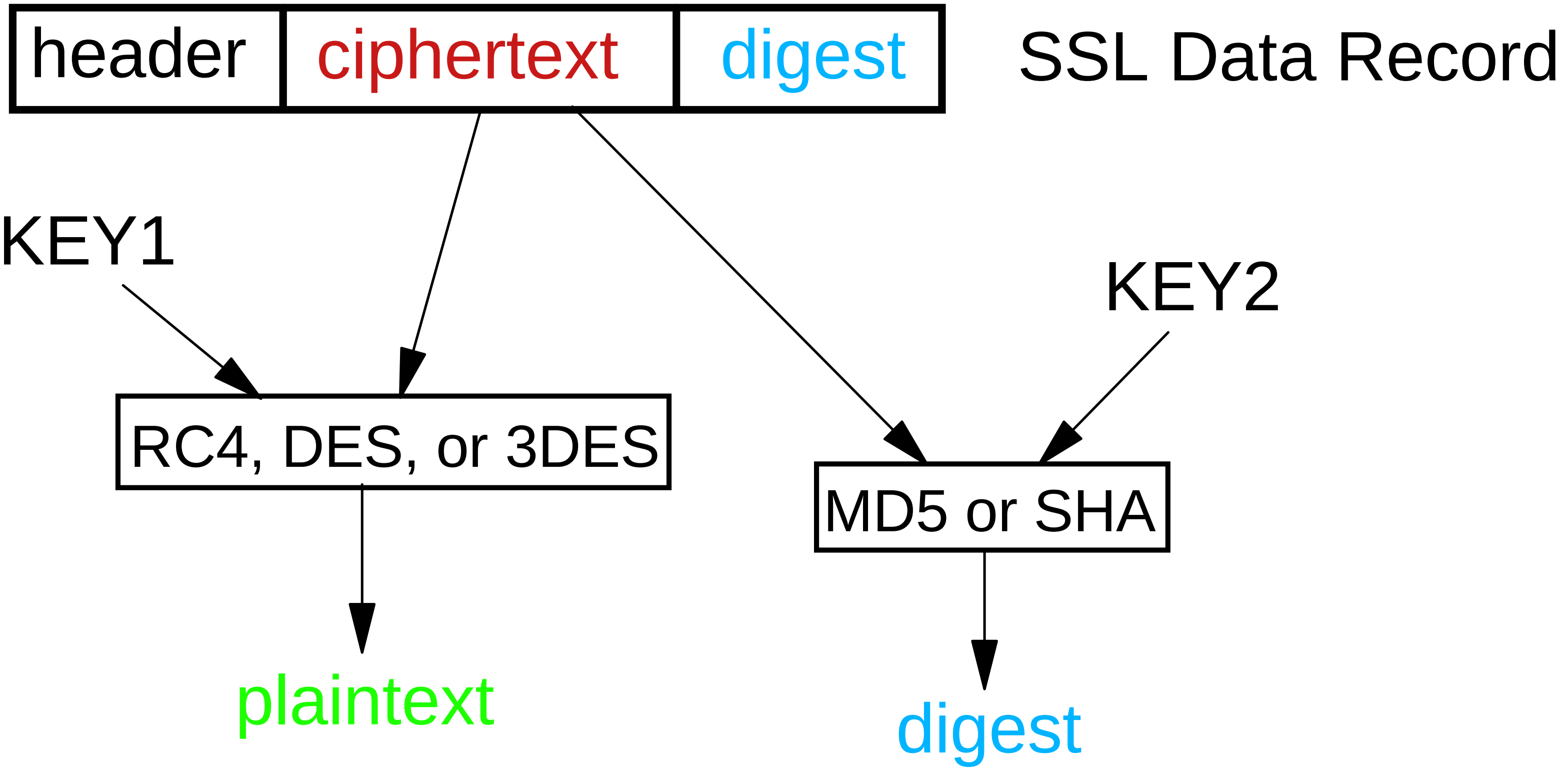
Exchanging Data Messages over SSL

- Each SSL data message is encrypted by the sender using one of the following symmetric cryptography algorithms:
  - RC4, DES, Triple-DES (3DES, TDES)
- Receiver decrypts the data using the same key (KEY1 in previous example) that the sender used to encrypt the data
- 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

Building an SSL Data Record



Processing an SSL Data Record



Hardware Acceleration for SSL Data Messages

- 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 does DES, 3DES, and SHA operations
- SSL support in TPF automatically determines if CPACF is installed and uses it for DES, 3DES, and SHA operations if CPACF is installed
  - Improves performance of data encryption/decryption as well as message digest creation/validation
- 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
- 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 has been created allowing you to encrypt/decrypt variable length user data using DES or 3DES
  - Both assembler and C language API interfaces
  - 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.

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.