TPF Users Group Fall 2005

Hardware Cryptography Support
The Details

Name : Mark Gambino
Venue : Communications Subcommittee

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.

Central Processor Assist for Cryptographic Functions (CPACF)

- Hardware cryptographic accelerator coprocessor
  - ► Supported on z990, z890, and System z9
  - ► One CPACF coprocessor per CP (I-stream)
- CPACF does DES, TDES, and SHA-1 (SHA) operations
- APAR PJ30156 added CPACF support to TPF 4.1
- APAR PJ30456 added CPACF support to z/TPF

Hardware Acceleration for SSL Data Messages

- For SSL sessions with DES or TDES as the data cipher:
  - TPF uses CPACF (if installed) to encrypt/decrypt data messages flowing across the SSL session
- For SSL sessions with SHA as the digest algorithm:
  - TPF uses CPACF (if installed) to create/verify message digest appended to each SSL data message
- CPACF improves performance of data encryption/decryption as well as message digest creation/validation

SSL Data Message Test Environment

- Each test was run twice:
  1. All crypto operations performed in software (no CPACF)
  2. Crypto operations (TDES and SHA) performed by CPACF
- Multiple long-running SSL driver sessions used to:
  - Maintain high and consistent message rate for several minutes
  - Eliminate overhead of starting SSL sessions
- Data collection measured average CPU utilization
- Application (driver) path length is minimal; therefore:
  - The vast majority of the CPU was spent in the SSL layer
  - Results shown on the next page represent CPU savings of using SSL with hardware acceleration versus software SSL

SSL Data Message Test Results using TDES-SHA

Message	MSG Rate	Data Rate	CPU Savings
Size	(MSG/sec)	(MB/sec)	with CPACF
100	48,090	4.8	47.2%
250	44,820	11.2	53.1%
500	22,406	11.2	62.8%
1,000	23,013	23.0	64.2%
10,000	5,014	50.0	86.9%
32,000	1,707	54.6	89.7%

SSL Data Message Cipher Comparison Details

- Tests were done using 1000-byte messages over long running SSL sessions
- SHA used for message digest algorithm
- Variables:
  - Data cipher (RC4, DES, or TDES)
  - Whether or not CPACF is used
- CPU utilization was measured, then normalized based on message rate to produce CPU cost per message
  - This is the "CPU Utilization Ratio" column on the following chart

SSL Data Message Cipher Comparisons

Encryption	Message Digest		CPU Util
Algorithm	Algorithm	CPACF	Ratio
RC4(software)	SHA(hardware)	YES	1.00
RC4(software)	SHA(software)	NO	1.39
DES(hardware)	SHA(hardware)	YES	1.68
TDES(hardware)	SHA(hardware)	YES	1.84
DES(software)	SHA(software)	NO	2.50
TDES(software)	SHA(software)	NO	5.17

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 TDES
  - Both assembler and C language API interfaces
    - CRYPC macro
    - tpf_cryptc() function
  - Can process up to 1 MB of data on a single API call
  - Uses CPACF if installed to do the DES/TDES operation; otherwise, uses software encryption

Crypto API Test Results

- Each test consisted of a C language driver issuing *tpf_cryptc()* APIs in a loop for several minutes
- CPACF was used to do data encryption/decryption
- Variables for each test:
  - ► Size of the data to encrypt or decrypt
  - ► Cipher algorithm (DES or TDES)
- Charts of the following pages show average number of APIs issued per second
  - ► Average number of DES or TDES operations per second
- Results are per I-stream

Crypto API Rates to Encrypt User Data using DES

Cipher	Data Size	APIs/sec	Data Rate (MB/sec)
DES-CBC	64	110,468	7.07
DES-CBC	256	104,130	26.65
DES-CBC	1,024	87,600	89.70
DES-CBC	4,096	54,090	221.55
DES-CBC	65,536	6,187	405.47

Crypto API Rates to Encrypt User Data using TDES

	Data		Data Rate
Cipher	Size	APIs/sec	(MB/sec)
TDES-CBC	64	106,025	6.78
TDES-CBC	256	92,250	23.62
TDES-CBC	1,024	65,740	67.32
TDES-CBC	4,096	29,400	120.42
TDES-CBC	65,536	2,450	161.56

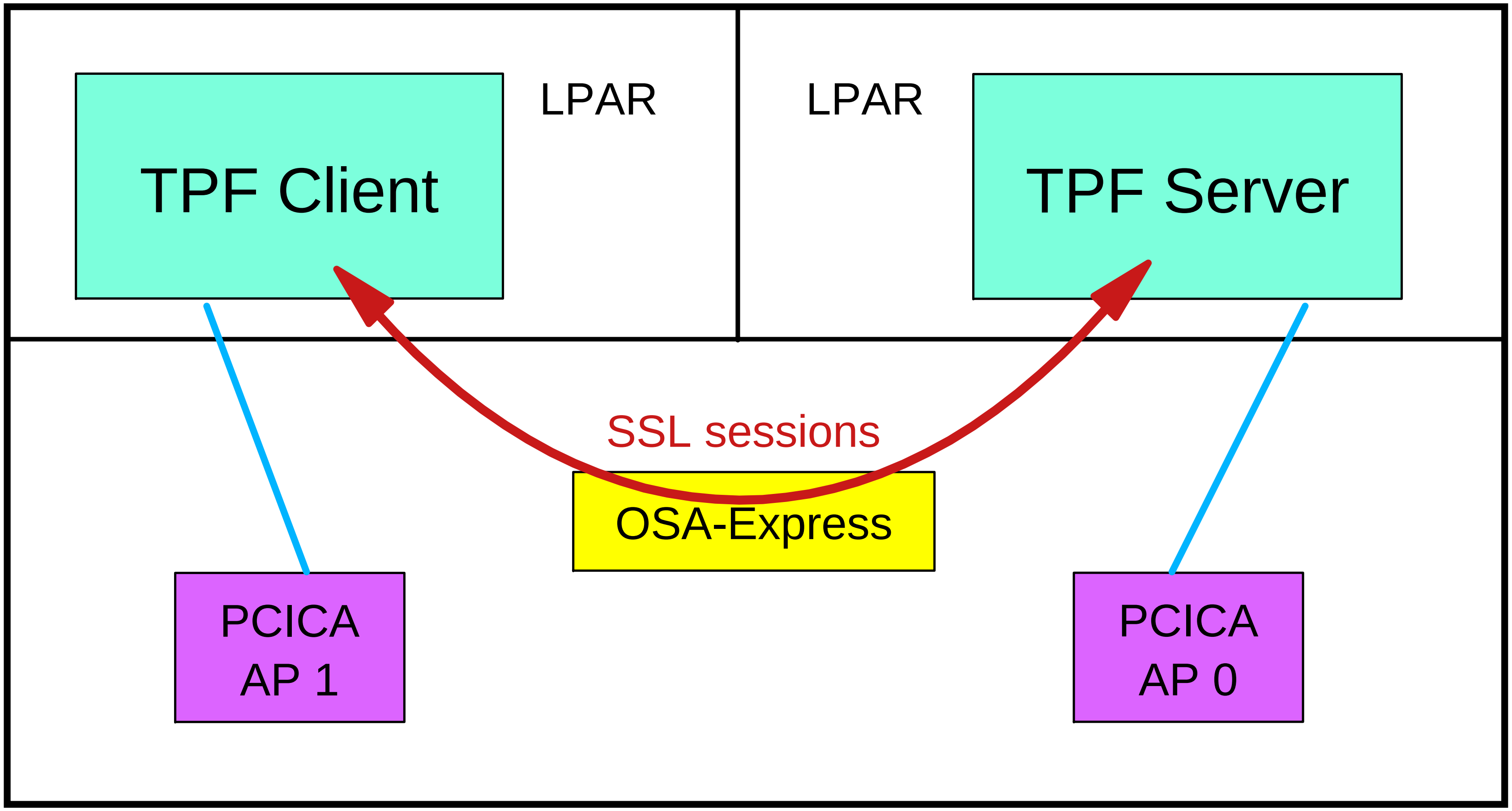
Starting an SSL Session

- Starting an SSL session uses RSA public key cryptography to exchange secret keys between the client and server nodes
- RSA uses a public/private key pair
- 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
- PCI Cryptographic Accelerator (PCICA) is a hardware crypto card that performs clear key RSA operations
- APAR PJ30133 added PCICA support to TPF 4.1
- APAR PJ30424 added PCICA support to z/TPF

Starting SSL Sessions Test Environment Details

- Multiple drivers on TPF client system start thousands of SSL sessions with the TPF server system
  - TPF client system uses PCICA for RSA public key operations when an SSL session is starting
  - TPF server system uses PCICA for RSA private key operations when an SSL session is starting
- Each instance of the client driver starts an SSL session, ends that session, and then starts another SSL session. This pattern repeats for several minutes.
- Variables in the test:
  - RSA key size (1024-bit vs 2048-bit)
  - Private key decrypt algorithm used (CRT vs ME)
  - How many PCICA cards (APs) are used by each system
  - Whether PCICA cards are dedicated or shared
- TPF data collection was used to measure PCICA usage

Starting SSL Sessions Test Environment #1

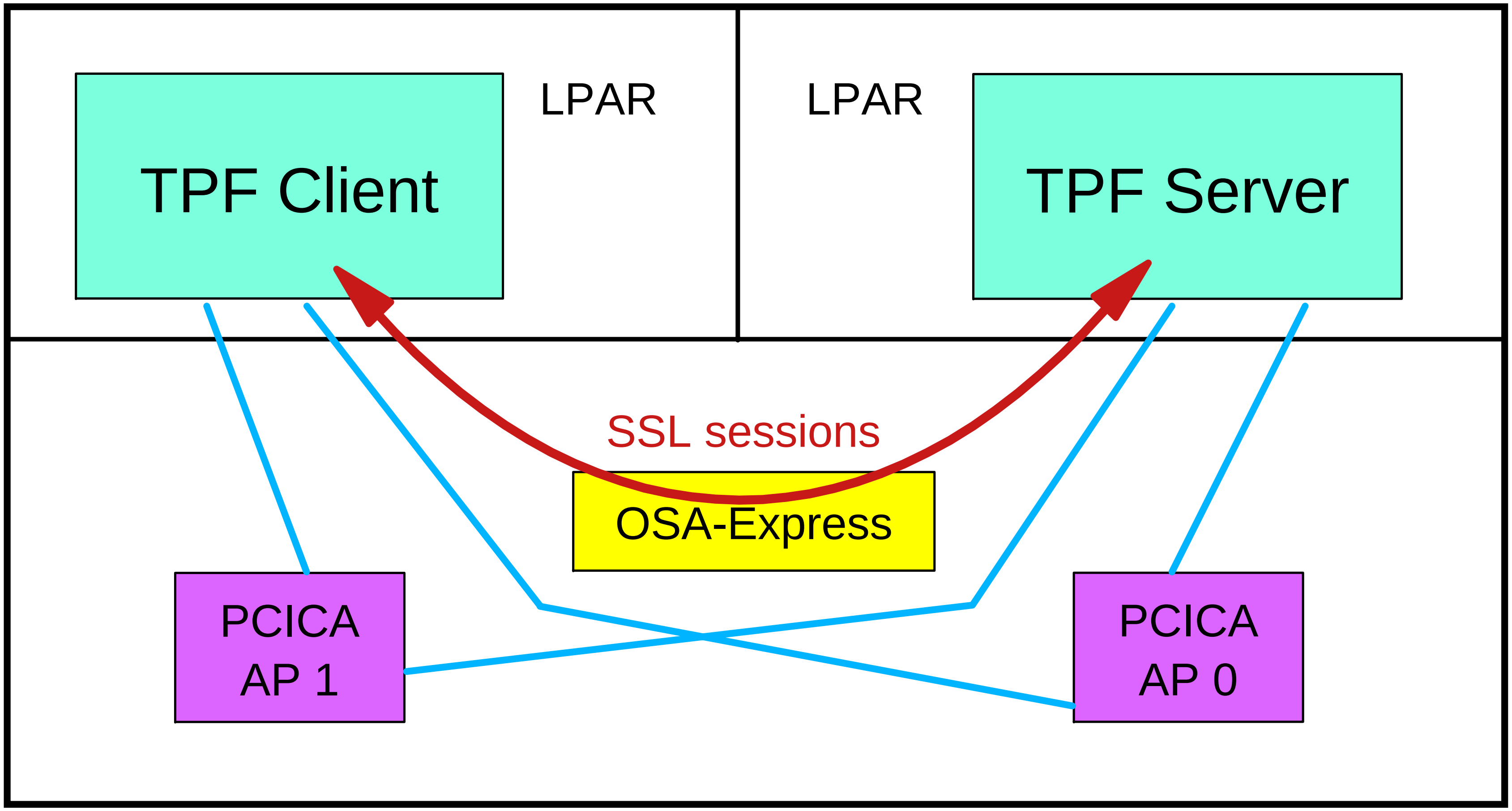


Starting SSL Sessions Test Environment #1 Results

RSA Key Size	Private Key Decrypt Algorithm Used by the Server	SSL Sessions Started per second
1024-bit	CRT	1093
1024-bit	ME	547
2048-bit	CRT	271
2048-bit	ME	70

- Client and server systems each have 1 dedicated PCICA
- Results indicate how many SSL sessions can be started per second per PCICA card

Starting SSL Sessions Test Environment #2

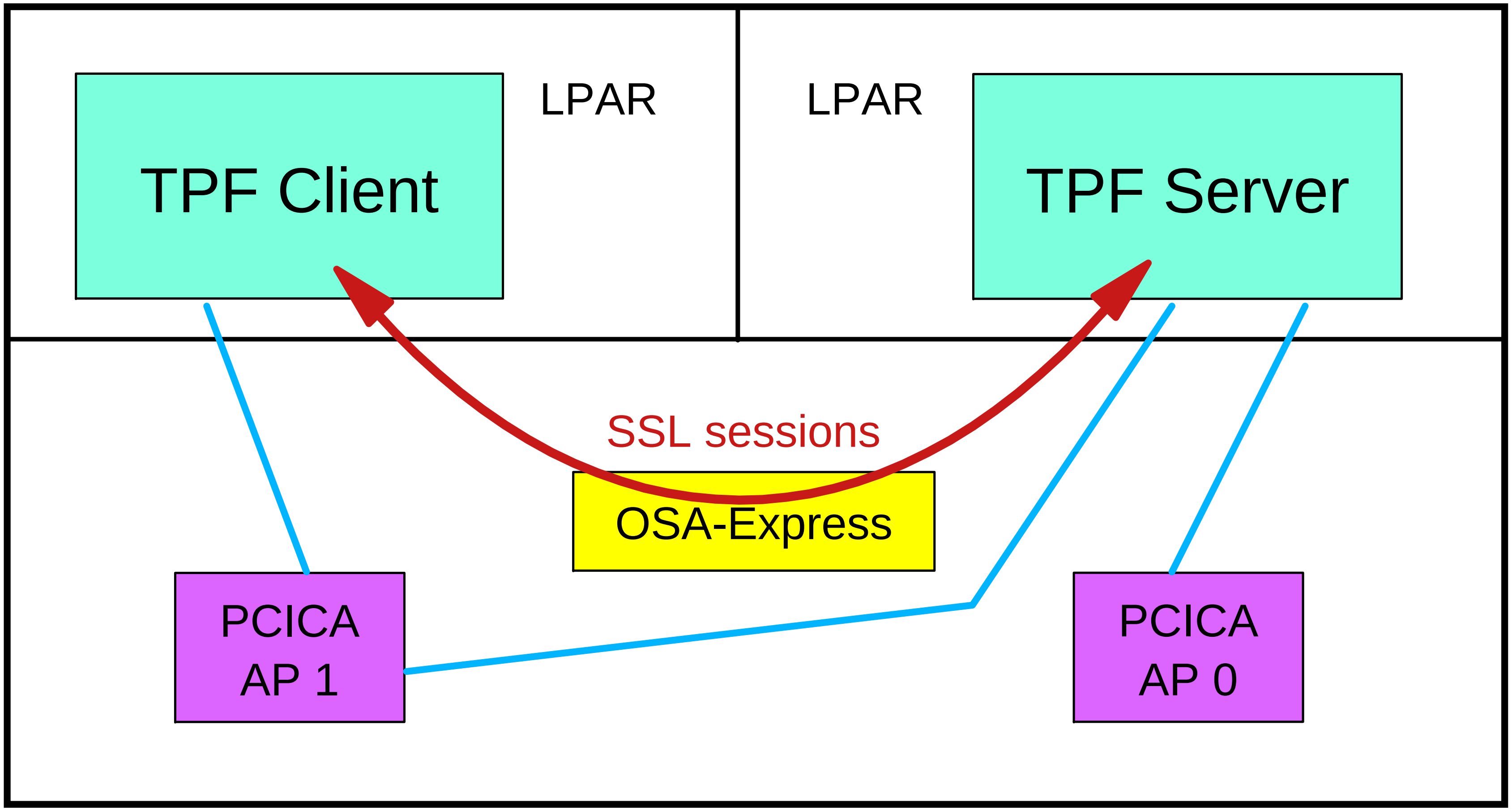


Starting SSL Sessions Test Environment #2 Results

```
PCICA     Client Operations/Second  Server Operations/Second
-----     ------------------------  ------------------------
 AP 0                  971                       968
 AP 1                  956                       959
          ------------------------  ------------------------
   TOTALS             1927                      1927
```

- Client and server systems each share both PCICA cards
- Each TPF balances requests roughly 50-50 across the available PCICA cards
- 1024-bit RSA keys were used
- Server used CRT for private key decrypt operations

Starting SSL Sessions Test Environment #3



Starting SSL Sessions Test Environment #3 Results

PCICA	Client Operations/Second	Server Operations/Second
AP 0	N/A	1047
AP 1	1912	865
TOTALS	1912	1912

- Client and server systems share one PCICA card (AP 1)
  - Server System also has one dedicated PCICA card (AP 0)
- TPF server detects the heavier overall load on the shared card (AP 1) and routes more requests to the dedicated card
- 1024-bit RSA keys were used
- Server used CRT for private key decrypt operations

Crypto Express2

- In January 2005, IBM announced the Crypto Express2 card on the z990
- Crypto Express2 combines the functions of PCICA (clear key RSA operations) and PCIXCC (secure key operations) into a single card
- On z990, the card runs as a Crypto Express2 Coprocessor (CEX2C)
  - Provides same performance for clear key RSA operations as PCICA
- z990 still supports PCICA
- On System z9, Crypto Express2 is configurable:
  - Crypto Express2 Coprocessor (CEX2C) - same as on z990
  - Crypto Express2 Accelerator (CEX2A)
    - Optimized for SSL performance
    - Processes clear key RSA operations only
    - Can perform roughly 3X the number of operations per second compared to PCICA
- System z9 does not support PCICA
- Statement of direction - TPF plans to support clear key RSA functions on Crypto Express2 configured as either CEX2C or CEX2A

Trademarks

IBM and z9 are trademarks 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.

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.