Multi-Gigabit SSL & TLS Record Layer Protocol Processor
and
Multi-Gigabit IPsec Processor

David Chin (david@broadcom.com)
Terry Tham (ttham@broadcom.com)
Outline

• SSL/TLS Protocol Overview
• BCM5850 SSL/TLS Record Layer Protocol Processor
  – Key Features
  – Implementation Challenges
  – Technology and Performance
• BCM5841 Multi-Gigabit Security Processor
  – Key Features
  – Description
  – Performance
• Summary
Where Security is Implemented

- **Secure Router, Switch, Appliance**
  - Must do Security at Gigabit rates

- **VPN Tunnel**
  - Large payload traffic
  - Few connections
  - Long life per connection

- **Secure Server or Load Balancer**
  - Must manage sessions fast
  - Exchange keys quickly

- **Secure SSL Sessions**
  - Small payload traffic
  - Many connections
  - Short life per connection

- **Secure Gigabit, Terabit Routers**
  - Must do Security at Multi-Gigabit rates

- **Headquarters**
  - Internet
  - Central Office
  - Service Provider
  - Server Farm
  - Load Balancer
  - Web Switch

- **Branch Office**
  - SOHO/Remote Users
  - Internet
  - Service Provider
  - Web Browsers

- **Central Office**
  - Secure Gigabit, Terabit Routers
  - Secure SSL Sessions

- **Service Provider**
  - Secure Gigabit, Terabit Routers
  - Secure SSL Sessions

- **Web Switch**
  - Secure Gigabit, Terabit Routers
  - Secure SSL Sessions

- **Server Farm**
  - Secure Gigabit, Terabit Routers
  - Secure SSL Sessions
Introduction to SSL/TLS

- http, telnet, ftp, etc. (e.g., web server): User Data
- Sits right below application in the network stack
- Sits directly above TCP
- Usually requires application to be modified

<table>
<thead>
<tr>
<th>Application</th>
<th>SSL/TLS</th>
<th>TCP</th>
<th>IP</th>
</tr>
</thead>
</table>

Input to SSL/TLS
### SSL/TLS Record

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>1 byte</td>
</tr>
<tr>
<td>version</td>
<td>2 bytes (major, minor)</td>
</tr>
<tr>
<td>length</td>
<td>2 bytes</td>
</tr>
<tr>
<td>data_fragment</td>
<td>$2^{14}$ bytes max. (MAC security consideration)</td>
</tr>
<tr>
<td>MAC</td>
<td>16 (MD5) or 20 (SHA-1)</td>
</tr>
<tr>
<td>pad</td>
<td>0-8 bytes, count in last byte, only for block cipher</td>
</tr>
</tbody>
</table>

Encrypted

**Hot Chips 2003**

(C) Broadcom Corporation. All rights reserved.
SSL/TLS Fragments
User Data into Records

- SSL records are independent of user buffers
  - One user buffer may be fragmented across multiple records
  - Multiple user buffers may be aggregated into one record
  - However, one-to-one is quite common
TCP Segments Records into Frames (Packets)

SSL Record

n
n+MSS
n+MSS+1
n+2xMSS

Segment

IP TCP

Rest of record (less than MSS)

IP TCP

IP TCP

Retain until acknowledged
Re-transmit if timeout

IP TCP

IP TCP

Hot Chips 2003  (C) Broadcom Corporation. All rights reserved.
BCM5850 Key Features

• SSL/TLS Record Layer Processing
  – 3DES, ARCFour, AES, SHA-1, MD5
  – Single Pass Authentication / Encryption for SSLv3/TLSv1
  – Key derivations for SSLv2, SSLv3, and TLSv1
  – Finished message Processing/client certificate verification
  – Support for SSL v2 record processing:
    • Single-pass authentication/encryption for inbound records
  – Streaming record buffer processing w/ TCP segmentation
  – TCP partial checksum computation
  – Maintains > 500K complete connections

• 32-bit and 64-bit Addressing Mode Support
  – All 16 combinations of the Bus/Processor endians supported
DMA Data Flow

INPUT RING (IRING)
- D1
- D2
- D3

Control
- Application Descriptors
- Control
- Application Data 1
- Application Data n

OUTPUT RING (ORING)
- Dx

Control
- Application Descriptors
- Control Pkt Status
- Application Data 1
- Application Data n

BCM5850

(C) Broadcom Corporation. All rights reserved.
SSLv3/TLSv1 Record Stream Cipher (Decrypt)

Record In

- ALEN = 33
- 0x00
- 0x00

<table>
<thead>
<tr>
<th>Content Type</th>
<th>Version (Major)</th>
<th>Version (Minor)</th>
<th>Len[15:8]</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA</td>
<td>(8 Bytes)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Buffer Out

- ALEN = 8
- Content Type
- 0x00

<table>
<thead>
<tr>
<th>Application Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA (8 Bytes)</td>
</tr>
</tbody>
</table>
SSLv3/TLSv1 Record Block Cipher (Encrypt)

Buffer In

<table>
<thead>
<tr>
<th>ALEN = 8</th>
<th>Content Type</th>
<th>0x00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Context</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DATA (8 Bytes)

Record Out

<table>
<thead>
<tr>
<th>ALEN = 37</th>
<th>Content Type</th>
<th>0x00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Context</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Content Type</th>
<th>Version (Major)</th>
<th>Version (Minor)</th>
<th>Len[15:8]</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA (8 Bytes)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Message Authentication Code (20 Bytes)

<table>
<thead>
<tr>
<th>0x03</th>
<th>0x03</th>
<th>0x03</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x03</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PAD

AUTH = 13

ENC = 32
### SSLv2 Record Block Cipher (Decrypt)

#### Record In

<table>
<thead>
<tr>
<th>ALEN = 35</th>
<th>0x00</th>
<th>0x00</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Context</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FLAGS / LENGTH</th>
<th>Pad Count</th>
<th>0x04</th>
</tr>
</thead>
</table>

**Message Authentication Code**
(16 Bytes)

#### Buffer Out

<table>
<thead>
<tr>
<th>ALEN = 12</th>
<th>0x00</th>
<th>0x00</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Context</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DATA**
(12 Bytes)

<table>
<thead>
<tr>
<th>0xXX</th>
<th>0xXX</th>
<th>0xXX</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>ALEN = 35</th>
<th>DATA (12 Bytes)</th>
<th>0xXX</th>
</tr>
</thead>
</table>

**PAD**

**AUTH = 16**  
**DEC = 32**
SSLv2 Record Stream Cipher
(Encrypt)

<table>
<thead>
<tr>
<th>ALEN = 12</th>
<th>0x00</th>
<th>0x00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Context</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA (12 Bytes)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ALEN = 30</th>
<th>0x00</th>
<th>0x00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Context</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FLAGS / LENGTH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key Stream (16 Bytes)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DATA (12 Bytes)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HASH VALUE FIELD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Authentication Code (16 Bytes)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Record Out
Finished Message Processing

<table>
<thead>
<tr>
<th>HLEN</th>
<th>PROTO</th>
<th>0x00</th>
</tr>
</thead>
<tbody>
<tr>
<td>512 bits 512 bits 512 bits</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Handshake Context

Client Hello

Server Hello

n-1 block

512 bits 512 bits 512 bits

BCM5850

20 | LEN = 36 | MD5 HASH (16 bytes)

20 | LEN = 36 | MD5 HASH (16 bytes)

20 | LEN = 36 | SHA1 HASH (20 bytes)

20 | LEN = 36 | SHA1 HASH (20 bytes)

Client Finished Message

Server Finished Message
TCP Partial Checksum

INPUT MESSAGE

<table>
<thead>
<tr>
<th>31</th>
<th>FLAGS</th>
<th>PRD</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>CTAG 0</td>
<td></td>
</tr>
<tr>
<td>ALEN</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Application Descriptor List

Application Payload

OUTPUT MESSAGE

<table>
<thead>
<tr>
<th>31</th>
<th>FLAGS</th>
<th>PRD</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>CTAG 0</td>
<td></td>
</tr>
<tr>
<td>ALEN</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Application Descriptor List

Application Payload

Partial ChkSum

ALEN

Application Payload

= Control Data

= Network Data

MSS

Application Descriptor OFFSET

Application Descriptor OFFSET

(©) Broadcom Corporation. All rights reserved.
Crypto Processing Unit Datapath

```
Parser

Hash Engines, SHA-1, MD5, HMAC

Digest Results

Post-Parser

CDU

Digest Results

Data to Digest

Cryptographic Engines, ARCFOUR, AES, 3DES

Digest Results

Connection State Retirement

Bypass

CMU

(C) Broadcom Corporation. All rights reserved.
Connection State Management Unit Datapath

Coherence Logic for CPU (x4)  
Coherence Logic for KDU (x1)

Record and CS Look-up Path  
Record and CS Issue Path  
Record and CS Retire Path

CAM  
CAM Arb  
Read Arb  
Write Arb  
Channel Buffer

CS Hit/Miss Detection

CS Hit/Miss Detection

Memory Access Path

CAM  
CAM Arb  
Read Arb  
Write Arb  
Channel Buffer

Hot Chips 2003  
(C) Broadcom Corporation. All rights reserved.
Technology and Performance

- 0.18 micron, 5LM CMOS technology
- 480-pin EBGA package
- 166MHz core, 133MHz DDR I/O, 400MHz HT™, and 133MHz PCI-X
- 2.4Gbps record layer processing and 10K/s SSL/TLS connections
- Worst case power of 3.8W
- Power saving features
BCM5841 Key Features

- Scalable Architecture
  - Multiple Crypto engines work in parallel, but maintain consistent order
- Support single pass 3DES/AES combined with HMAC (SHA-1/MD5)
- On-chip True Random Number Generator
- Key Encrypting Key to protect SA keys
- Interface supports FIFO 8/16/32 or PL3
The Packet Format

Control Word
SA Data
Buffer Data

Parser

Control Word
SA Data
Buffer Descriptor
Auth Offset
Auth Length
Crypto Offset
Crypto Length

IPsec Engine

Output Data

---Control Word---

---Status Word---
The Crypto Engine & RNG

- Supports single pass 3DES/AES combined with HMAC (SHA-1/MD5)
- Contains a 667 Mbps 3DES engine and a 800 Mbps AES engine
- Performs full range ESP pad checking
- Performs ICV checking
- On-chip random number generator
  - Provide on-chip IV generation
  - Provide host with random number
Dual Interface Mode

• With the same set of pins, BCM5841 supports two modes of interface
  • FIFO32 interface
    – FIFO32 interface is a source clock interface
    – Run up to 200 MHz, providing 6.4 Gbps bandwidth
  • POS-PHY Level3 (PL3) interface
    – Run up to 133 MHz, providing 4.2 Gbps bandwidth
Chip Performance
FIFO32 @200 MHz

BCM5841 Performance with FIFO32 interface

- Output BW
- 4.8 Gbps
- 1.2 Gbps
Chip Performance
PL3 @133 MHz

BCM5841 Performance

- Output BW
- 4.8 Gbps
- 1.2Gbps

Payload Size (Bytes)

Bandwidth (Mbps)
Technology

- 0.18 micron, 5LM CMOS technology
- 256-pin TBGA and 256-pin FPBGA package
- 166MHz core, 200MHz FIFO and 133 MHz PL3
- Maximum power of 5W
Summary

• BCM5850 accelerates all of the computation-intensive SSLv2, SSLv3, and TLSv1 protocol processing
  – Handshake, Key Derivation, Record Layer Processing, Client Certificate Verification, Data Management
• BCM5850 delivers 2.4Gbps record layer processing and 10K new SSL/TLS connections per second performance
• BCM5850 performance can be further enhanced by reducing the number of short reads/writes on the system bus
• BCM5841 processes IPsec ESP or AH transformations in a single pass
• BCM5841 achieves 4.8 Gbps with FIFO32 interface