AT-TLS Implementation and Diagnostics at U.S. Bank

Conrad Sanders : U.S. BanCorp
Nalini Elkins : Inside Products, Inc.

Conrad.sanders@usbank.com
Nalini.elkins@insidethestack.com

August 4, 2010

Our SHARE Sessions – Boston

- Proactive Network Management at the DTCC
  Monday, August 2, 2010: 11:00 AM-12:00 PM
- TCP/IP Performance Management for Dummies
  Monday, August 2, 2010: 4:30 PM-5:45 PM
- AT-TLS Implementation and Diagnostics at U.S. Bank
  Wednesday, August 4, 2010: 11:00 AM-12:00 PM
- Best Practices for Certificate Management – (Panel)
  Thursday, August 5, 2010: 11:00 AM-12:00 PM

Agenda

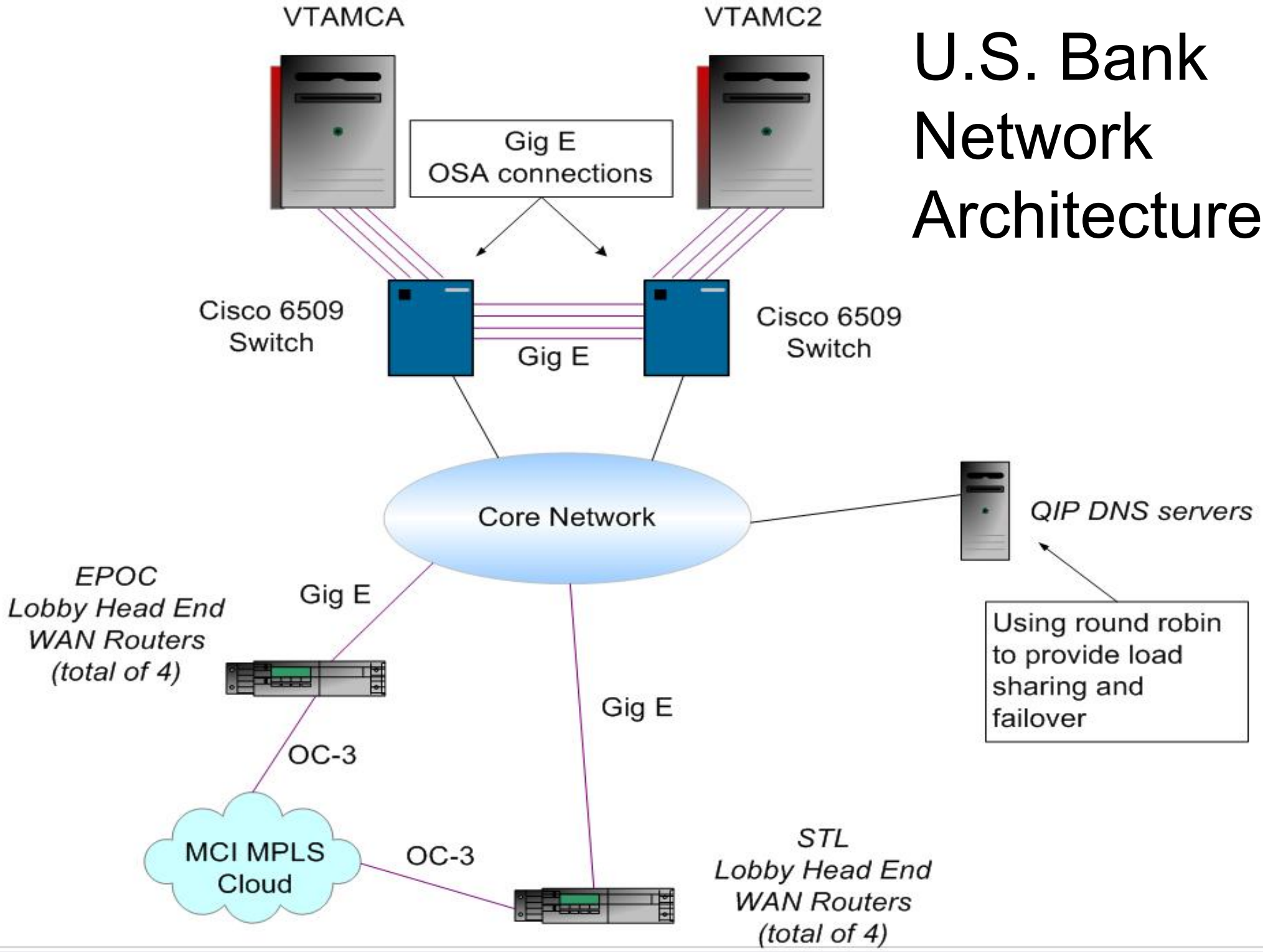
- Business requirements for encryption
- History of implementation
- Problems encountered
- Integration into our operational systems
- Diagnostic methods
- Future plans

Introduction

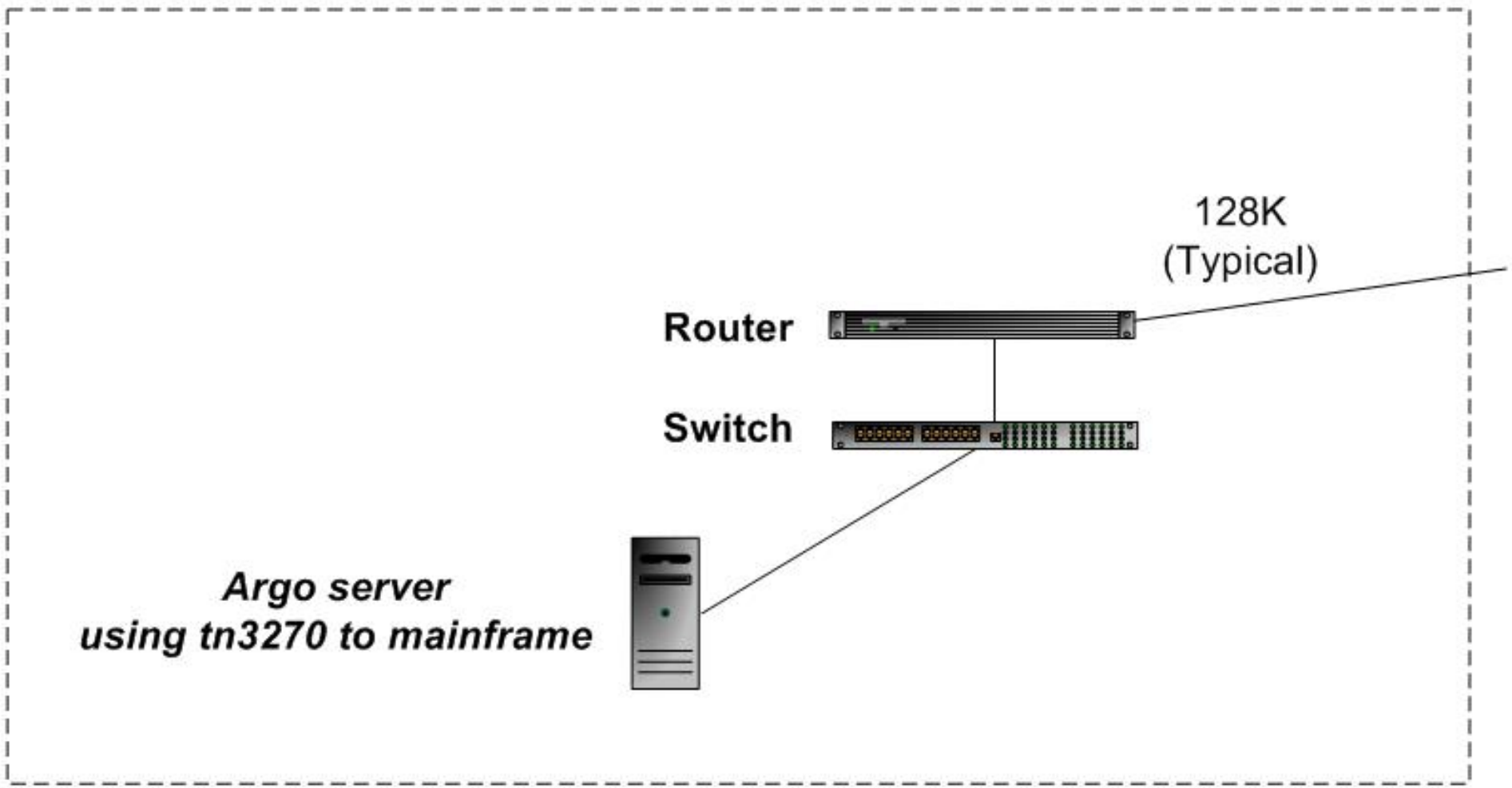
- The US Bank Corporation is the 6th largest bank in the country. Secure transmission of financial data is imperative. This session will discuss how we have implemented AT-TLS on the TCP/IP network to secure our network.

- US Bank has more than 3,000 branches and 5,000 ATMs. We have over 36,000 Telnet sessions split between two LPARs with 21,000 Telnet sessions just for our branches.

U.S. Bank Network Architecture

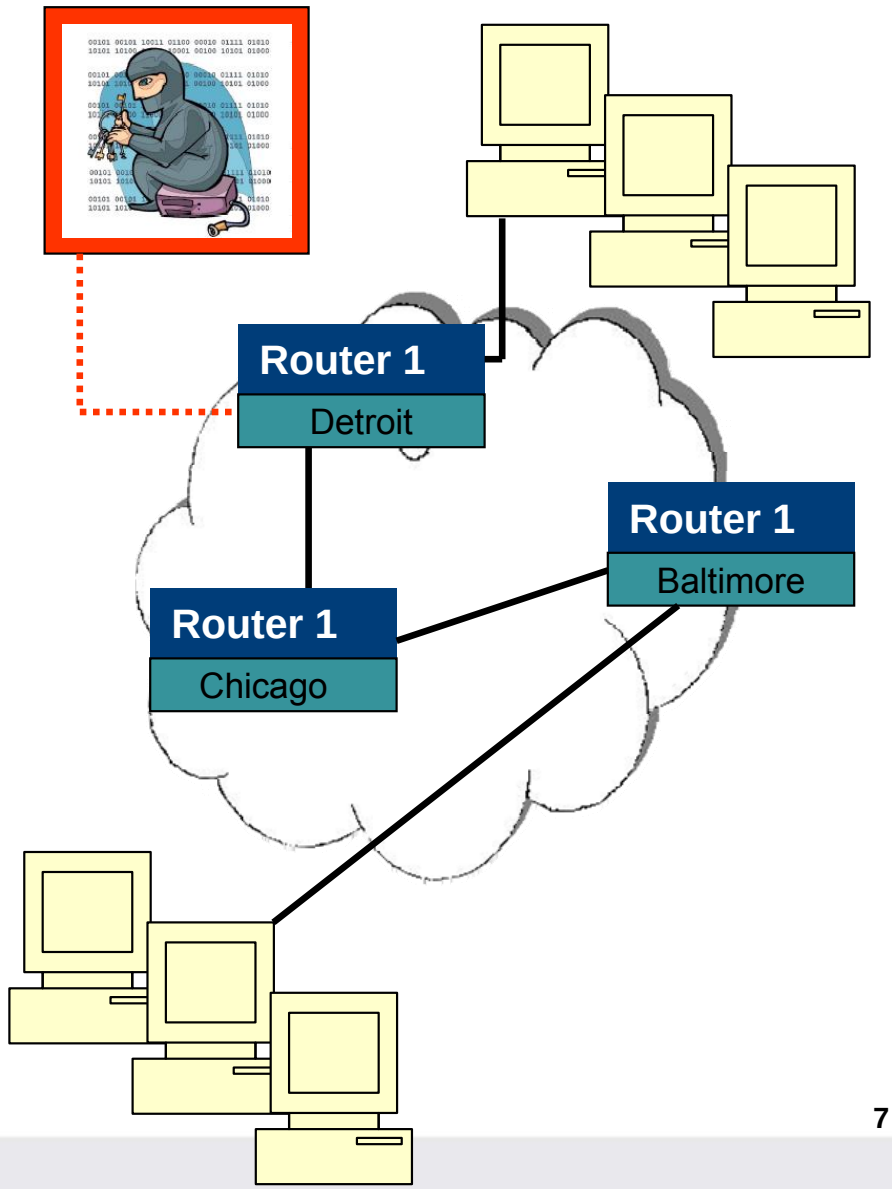


Typical Branch Connectivity (TN3270)



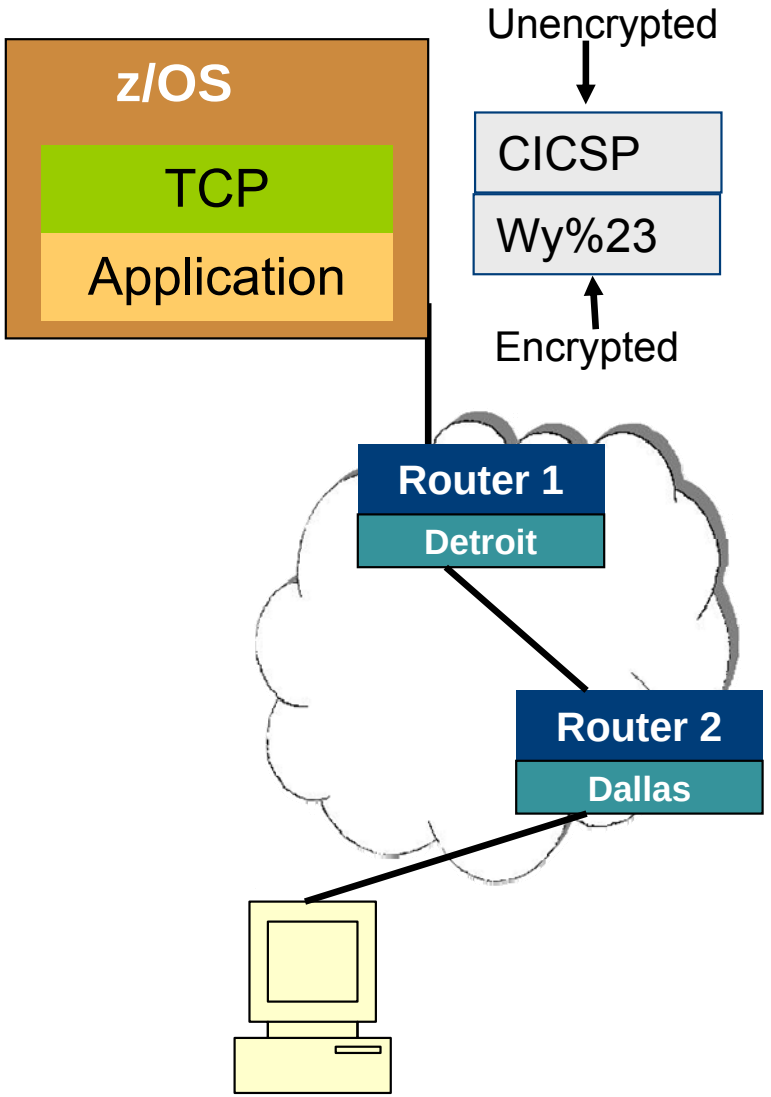
Business Reasons for Encryption

- Today, we have vast communications networks (Internet, Digital (GSM), cell phones, Automatic Teller Machines) offering instant ‘secure’ communication.
- The future of Electronic Commerce, and, in fact, the electronic world, rests on secure digital communication.
- Unfortunately, so does the success of terrorists, drug rings, people smugglers, child porn, organized crime, spy rings, and ‘cyber crime’.



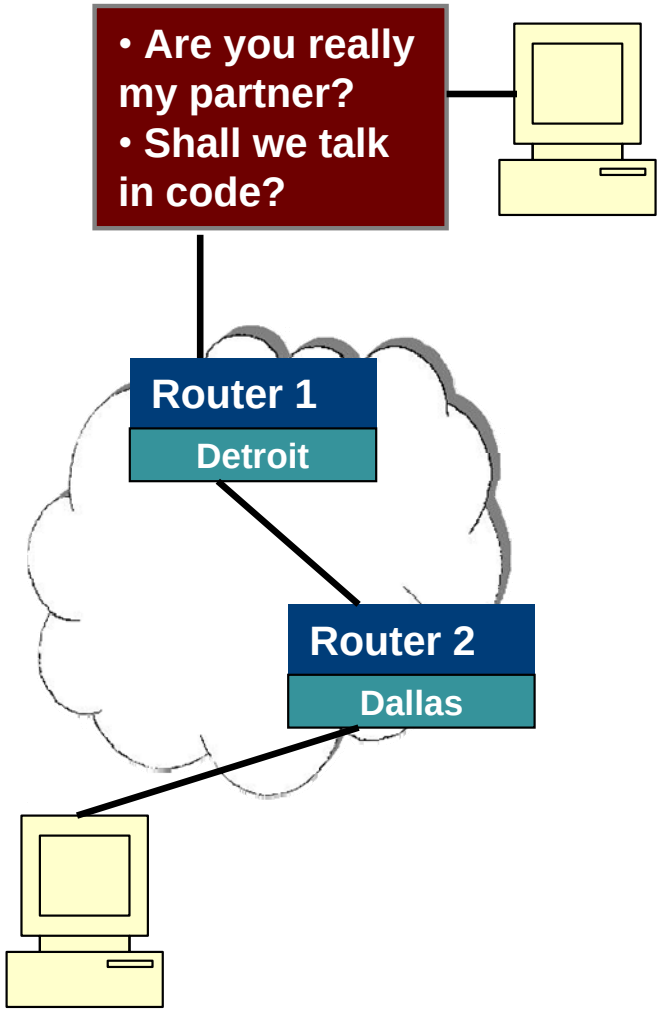
History of Implementation

- We started with using SecurePort for our TN3270 connections.
- We found some problem areas.
- We evaluated AT-TLS by implementing it on our test system.
- We learned to configure Policy Agent for AT-TLS.
- We had some issues because of client handshake problems.
- These were resolved and we now have AT-TLS running in production for our branches.



What is Secure Sockets Layer?

- Secure Sockets Layer (SSL) is a protocol developed by Netscape for transmitting private documents via the Internet.
- The main functions of SSL are:
  - Server authentication
  - Data privacy and integrity
  - Optional client authentication via digital certificate
- Multiple versions of SSL exist: SSL V2.0 and SSL V3.0.
- The SSL protocol became the Internet standard Transport Layer Security (TLS) described in RFC 2246 and updated in RFC 3546.
- TLS V1.0 is the current version of the secure sockets layer protocol.
- There are slight differences between SSL 3.0 and TLS 1.0, but the protocol remains substantially the same.

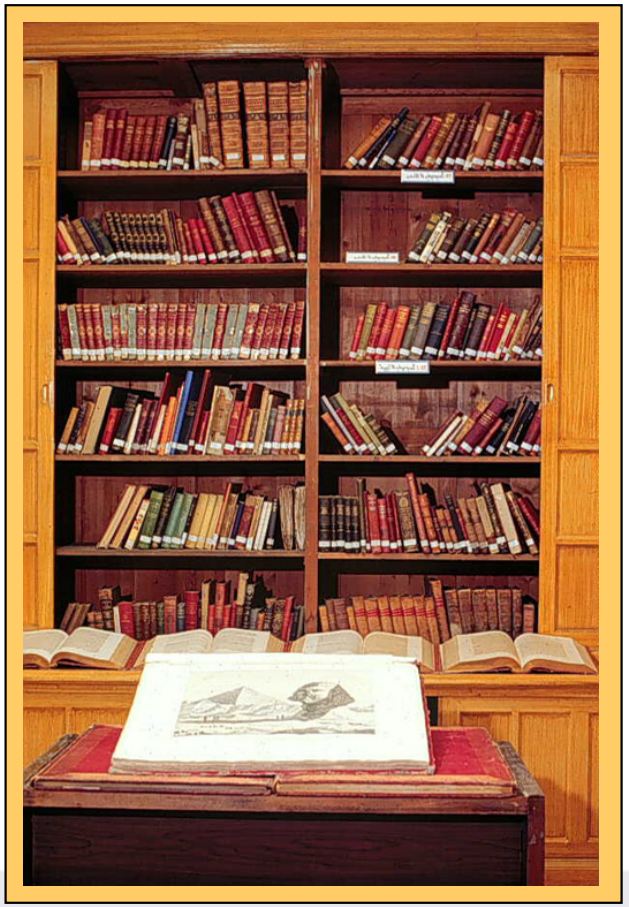


How to Implement SSL

- To implement SSL, the application program must use special SSL socket calls.
- As far as the TCP stack is concerned, SSL is just a TCP application. It is transparent to the stack.
- Languages such as C/C++ or Java provide application programming interfaces that interface with the sockets APIs for the platform (z/OS, Windows, Linux) to allow applications to establish secure sockets communications.
- SSL is available for TCP applications only. UDP, ICMP or other higher level protocols are not supported.

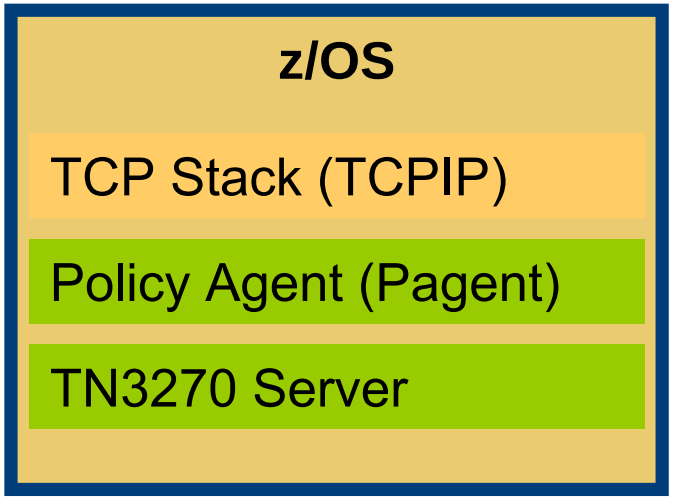
SSL Socket Library:

TCP Only



What is SecurePort

- SecurePort is when the TN3270 server itself is doing SSL.
- The TN3270 server may be configured with:
  - Port : insecure connections
  - SecurePort : connections with TN3270 using SSL
  - TTLSPort : connections with TN3270 using AT-TLS
- The Policy Agent is required to define security policies if you are using AT-TLS

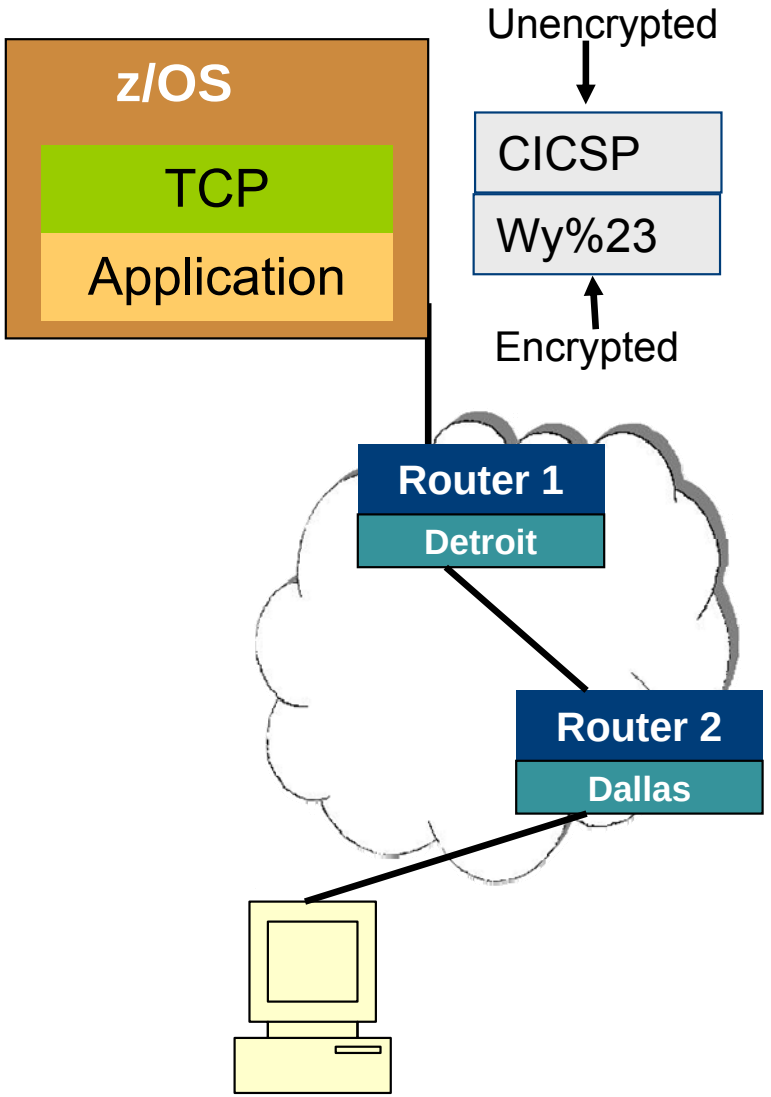


TN3270 Profile

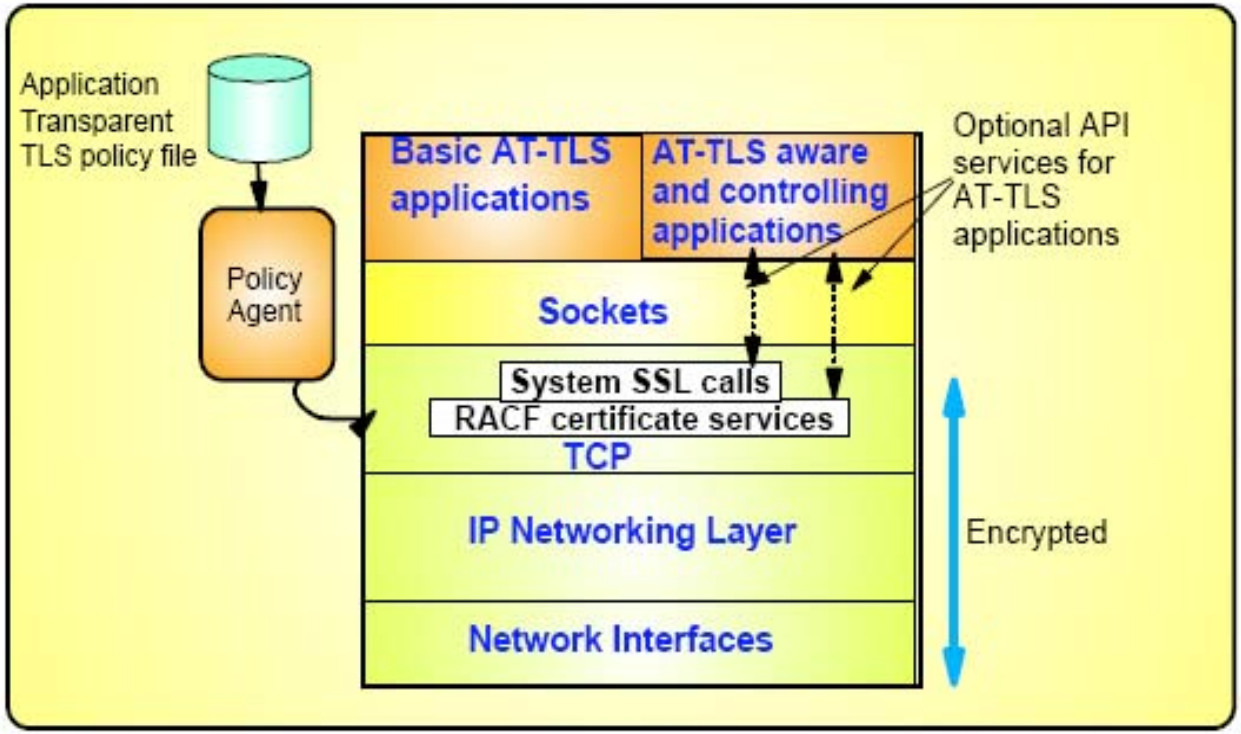
Port, SecurePort, TTLSPort…..

Shortcomings of SecurePort

- We started with using SecurePort for our TN3270 connections.
- We found shortcomings – mostly in the area of problem diagnostics and packet decryption.
- When we had a problem in the application, we had to do simultaneous packet and component trace for hours to see the data. There was lots of CPU overhead and we used many volumes of DASD!



AT-TLS Overview

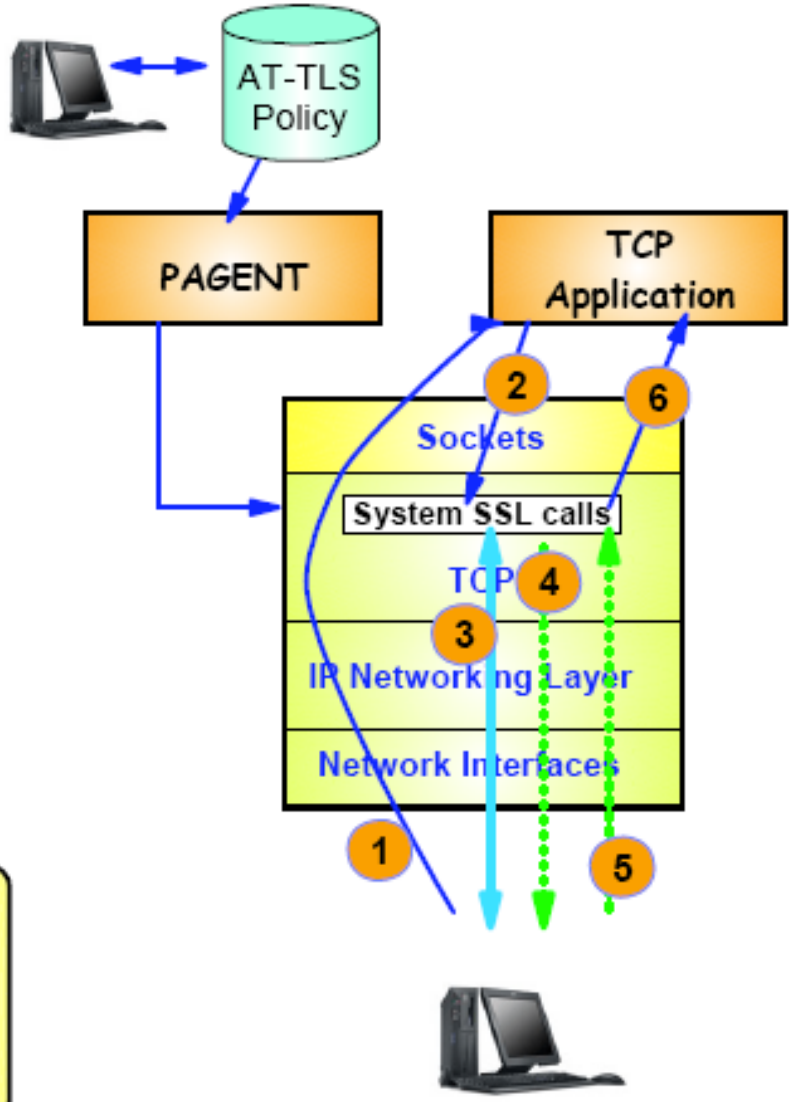


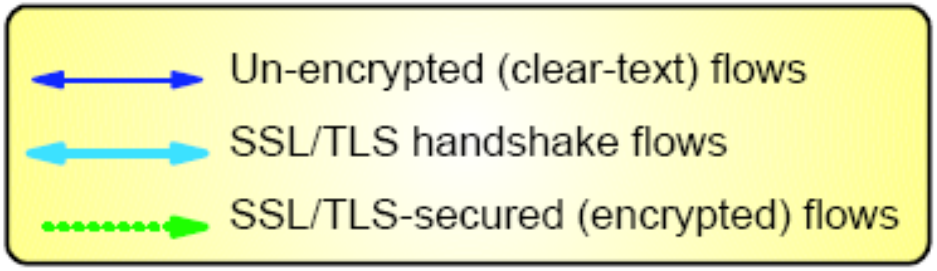
- **AT-TLS performs TLS process at the TCP layer for the application**
  - ►AT-TLS policy controls when and how to use AT-TLS
    - – AT-TLS policy managed by Policy Agent and configured by manual edit or Configuration Assistant for z/OS Communications Server
- **Most applications require no change to use AT-TLS**
  - ►AT-TLS Basic applications
- **Applications can optionally exploit advanced features using new SIOCTTLSCTL ioctl call**
  - ►AT-TLS Aware applications
    - – Extract information (policy, handshake results, x.509 client certificate, userid associated with certificate)
  - ►AT-TLS Controlling applications
    - – Control if/when to start/stop TLS, reset session / cipher

AT-TLS basic principles

- **Configured AT-TLS policy for the TCP application to use AT-TLS:**

1. Client connects to server and connection becomes established
2. Server sends data in the clear and TCP layer queues it.
3. TCP layer invokes System SSL to perform SSL handshake under identity of the server.
4. TCP layer invokes System SSL to encrypt queued data and sends it to client.
5. Client sends encrypted data, TCP layer invokes System SSL to decrypt.
6. Server receives data in the clear.





Why Go to AT-TLS?

- The following issues were important to us:
- Being able to look at the encrypted data without compromising the key if we needed to take a trace to see the data to look for patterns.
- We started to get requests from some of our internal customers wondering if we could support FTPs using AT-TLS.
- Network management possibilities in the future. (Alert on handshake failure, see encryption algorithm used.)
- Performance enhancements would be in AT-TLS (TTLS) not SecurePort.

TCPIP and Telnet Profile Changes

```
TCPCONFIG  RESTRICTLOWPORTS      ; Appl must be in PORT to use lowports
        TCPSENDBFRSIZE 262144
        TCPRCVBUFRSIZE 262144
        TTLS

; Telnet parameters for AT-TLS Port 992  (-> TN&SC.* LUs)
TELNETPARMS
   TTLSPort 992              ; AT-TLS Telnet (Also see in Profile.PORTS)
   CONNTYPE Secure           ; Default - Also consider NEGTSECURE
   EXPRESSLOGON              ;
   DEBUG Exception
ENDTELNETPARMS
```

TTLS Policy Agent Changes

```
TTLSConnectionActionRef          cAct3
 }
 TTLSRule                           TN3270_TLS_Rule~5
 {
   LocalAddr                        ALL
   RemoteAddr                       ALL
   LocalPortRangeRef                portR5
   RemotePortRangeRef               portR1
   Direction                        Inbound
   Priority                         251
   TTLSGroupActionRef               gAct1
   TTLSEnvironmentActionRef         eAct3
   TTLSConnectionActionRef          cAct3
 }
 TTLSGroupAction                    gAct1
 {
   TTLSEnabled                      On
 }
 TTLSEnvironmentAction              eAct1
 {
```

TTLS Policy Agent Changes (cont).

```
TTLSCipherParms                 cipher1~AT-TLS__Gold
{
  V3CipherSuites                TLS_RSA_WITH_3DES_EDE_CBC_SHA
  V3CipherSuites                TLS_RSA_WITH_AES_128_CBC_SHA
}
PortRange                       portR1
{
  Port                          1024-65535
}
PortRange                       portR2
{
  Port                          21
}
PortRange                       portR3
{
  Port                          25021
}
PortRange                       portR4
{
  Port                          23023-23024
```

Implemented on Test system

- We first implemented AT-TLS on our Test systems for our test branches using the Zephyr TN3270 Emulator for a month or so.
- We did not have any issues so we decided to move forward into production.
- We decided to only implement AT-TLS on one of our production CMCs using just one Telnet port for our corporate users who were using Attachmate Extra 9.0.
- We did not want to implement it on our production branches until we exercised about 1,000 Telnet sessions using AT-TLS.

Problems in Production Implementation

- One of the first problems we noticed is we started to see errors codes in syslogd and the Telnet Server log using Attachmate Extra TN3270 emulator that we did not see on our Test system using the Zephyr TN3270 emulator.
- Listed below are listed some of error codes we were getting during the SSL handshake:

```
Apr 20 09:55:03 plexprd-C0/TCPSTC   TCPCA01  TTLS[327704]: 09:55:03
TCPIP    EZD1286I TTLS Error GRPID: 00000001 ENVID: 00000001
CONNID: 004ECD9A JOBNAME: TN32CA01 USERID: TELNSTC RULE:
TN3270_TLS_Rule~5  RC: 5003 Data Decryption

Apr 20 09:55:03 plexprd-C0/TCPSTC   TCPCA01  TTLS[327704]: 09:55:03
TCPIP    EZD1286I TTLS Error GRPID: 00000001 ENVID: 00000001
CONNID: 004ECD9A JOBNAME: TN32CA01 USERID: TELNSTC RULE:
TN3270_TLS_Rule~5  RC:  406 Initial Handshake 00000000 7EC1FA98
```

Looking up the Error Codes

We had to look up the AT-TLS codes in two different IBM manuals to try determine if we had an issue. No users were reporting any problems because they would almost immediately reconnect to a different port when the initial handshake failed.

Rcode is a System SSL or AT-TLS return code that indicates why the event failed. rcode values under 5000 are generated by System SSL and are defined in z/OS Cryptographic Services System SSL Programming.

Rcode values over 5000 are generated by AT-TLS and are defined in Diagnosing AT-TLS problems in z/OS Communications Server: IP Diagnosis Guide.

Error Code 406

406 **Error while reading or writing data.**

Explanation: An I/O error was reported while the System SSL runtime was reading or writing data.

User Response: Ensure that there are no network errors. Collect a System SSL trace containing the error and then contact your service representative if the error persists.

Error Code 5003

5003	Connection Init	Clear text data was received on the connection from the remote partner instead of secure data. The connection has been terminated. Check the following: • Ensure that the remote client is enabled for secure connections. • If the policy is defined with ApplicationControlled **On**, ensure that the application read all the cleartext data before shaking the secure handshake. If configuring using the IBM Configuration Assistant for z/OS Communications Server, the Application Controlled setting done in each Traffic Descriptor.

Error Codes from the Telnet Server Log

09.55.03 STC09792 EZZ6034I TELNET CONN 004ECD9A LU **N/A** **CONN DROP ERR 1030** 852

852 IP..PORT: X.X.X.X..1903 EZBTTXPL

1030 TTLS Ioctl failed for query or init HS.

The PARM1 value is the return value, the PARM2 value is the return code, and the PARM3 value is the reason code for the ioctl failure.

How We Resolved Them

- We decided to run a very large trace for about 4 hours on one of our CMCs to catch the Telnet Sessions that were getting the error.
- Once I had a couple of hits, I stopped the trace and filtered the trace by the failing IP address and Port Number.
- We opened an ETR with IBM and sent them the trace and also fed the trace into SSL Problem Finder.
- We found out that our 3270 Emulator from Attachmate called Extra Extreme 9.0 was not following SSL Handshake protocols. I opened a ticket with Attachmate and they recommended we migrate to SP2.

Other Issues started to surface

- After running few days on one of our CMCs, we started to getting ABENDs on Telnet Server and then the TCPIP stack because of the Telnet Server problem.
- We suspected something with AT-TLS and the bad handshake with using Extra so we backed out AT-TLS while we had opened a SEV1 ticket with IBM.
- There were no immediate plans to update our Extra to SP2 so we hoped that IBM could come up with a fix.
- IBM came up with a PTF UK26977 to resolve the problem but we were not able to put it on for a number of months so the AT-TLS implementation was delayed about 4 months.

IBM Fixes

D140897 Problem Overview:

Embedded blanks and the # character are not allowed to be specified for the IPSec CaLabel parameter on the RemoteSecurityEndpoint statement, or for the CertificateLabel parameter on the TTLSConnectionAdvancedParms statement. Use of embedded blanks or the # character results in the parameter values being truncated.

D140908 Problem Overview:

A connection was made to the Telnet server. The server requested a SSL handshake be started. The handshake timedout before the timer could run, a SSL client hello was received on the connection. AT-TLS flagged the data as SSL handshake data and queued a request to a task to process the data. The timer routine ran and reset the AT-TLS flags before the request could be processed. The handshake data was moved to the applications receive queues. When Telnet attempted to read the data, EZBTCMR abended due to non zero band data being on the receive queue.

IBM Fixes

D140925 Problem Overview:

Telnet is writing an SMFTERM record and needs the TCP/IP stack hostname. The connection is terminating because the stack was terminated. A control block no longer exists when Telnet tries to access it for the hostname causing an abend.

D140949 Problem Overview:

It appears that somehow the IPv4 listening socket got dropped. Acceptfails with EBADF and ERRNO2 of 76620446 JRSOCKETCONDROPPED.
After the accept error, we loop back and do another select()

Another Recommended AT-TLS fix

- PE PTF List: PTF List: Release 1A0 : UK47489 available 09/07/24 (F907)
  Release 190 : UK47490 available 09/07/24 (F907)

- ERROR DESCRIPTION: A connection is using AT-TLS to implement SSL security. The connection was closed by the application, causing AT-TLS to send a SSL close alert and a FIN. The remote SSL application responded with a SSL close alert, another SSL alert, and a FIN. AT-TLS loops trying to read the second SSL alert because every read to SSL returns with a 437, indicating the SSL connection is closed. The alert is never consumed from the TLSX control block, causing AT-TLS to schedule another attempt to read the alert. This loop will continue until the timewait timer expires and the connection is freed.

- VERIFICATION STEPS: 1) High CPU seen in TCPIP address space. D GRS,C may show contention on the SYSZRACF AHSTUSERxxxxxxx resource for the TCPIP address space. 2) TCPIP ctrace option TCP will show AT-TLS processing function code x'19', trying to read control data for the same connections in TIMEWAIT.

SSL Problem Finder Analysis

SSL PROBLEM FINDER

Show SSL Traffic / Error Analysis

Summarized By Host
E081 : plextst-d0
Sort Order : Date / Time Descending
Showing Entries : 1 -10
Trace File:BAD992h

Total SSL Handshakes	Total Good SSL Handshakes	Total Bad SSL Handshakes	Minimum SSL Handshake Time (Microseconds)	Average SSL Handshake Time (Microseconds)	Maximum SSL Handshake Time (Microseconds)
2	1	1	55K	55K	55K

Drill Down	Total Bad Handshakes by Error Code	Error Code	Error Code Decoded
	1	202	Bad or Incomplete Certificate (202)

Drill Down	Total Good Handshakes by Performance Warning	Warning Code	Warning Code Decoded
	1	253	> 99 milliseconds between Server Done and Client Key Exchange (253)

SSL Problem Finder
Bad Handshake Analysis

SSL PROBLEM FINDER

Show Bad Handshake Analysis

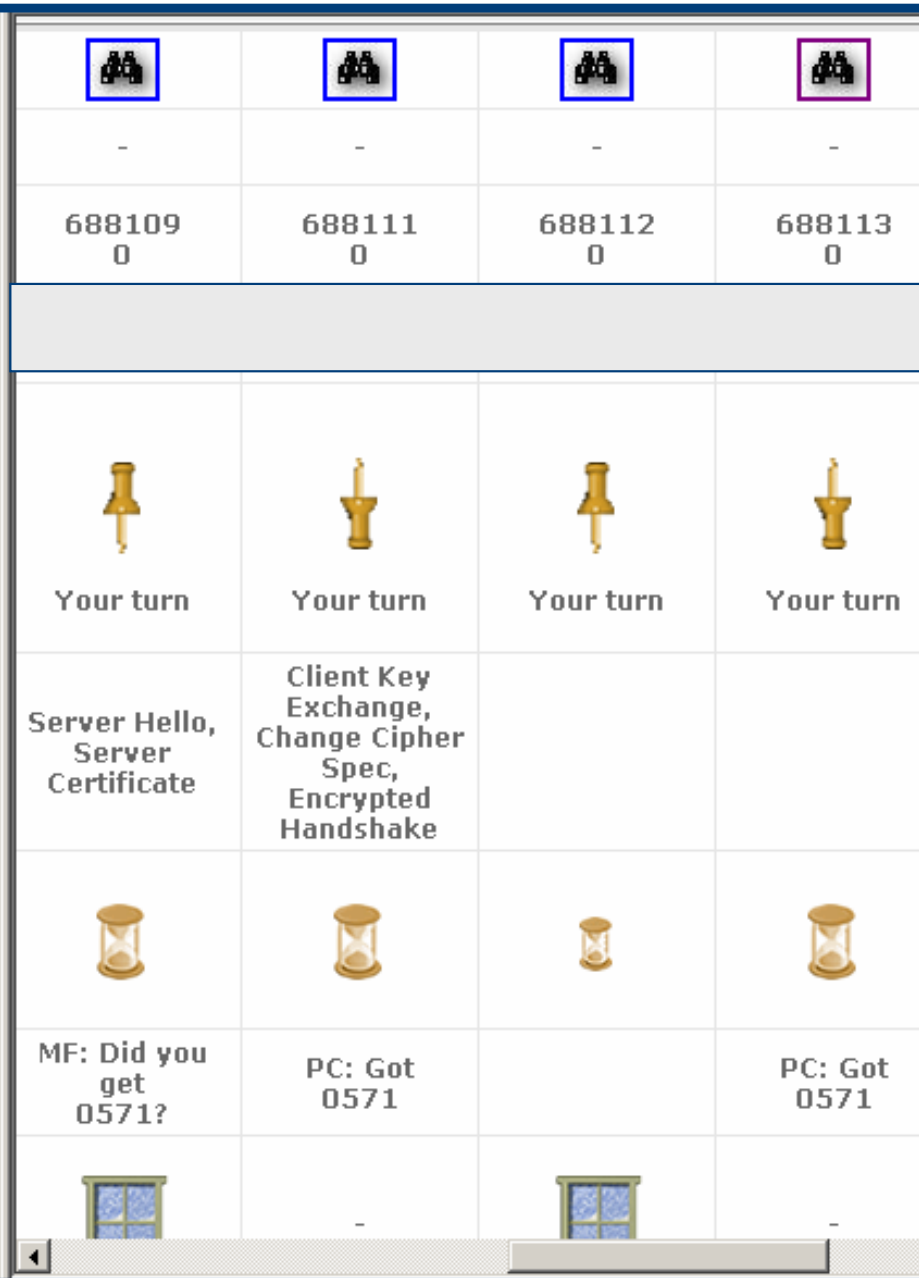
Sort Order : Packet Date
Showing Entries : 1 -10
Trace File:BAD992

-	Packet Date	Addresses	Error Code	Events
1	2010-04-21 11:38:40.0	Source:	202	Handshake from client IP address: to server IP address did not complete properly. • The Client Hello was sent at 2009-05-05 17:59:52.359972. • The next packet expected is the Server Hello. • A Server Hello was sent at: 2009-05-05 17:59:52.361635. • The Cipher Suite used is: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x0A). • The next packet expected is from the server and it is a Server Certificate. • A Server Certificate was sent at: 2009-05-05 17:59:52.361635. • This indicates that agreement was reached between the client and server on t Cipher Suite. • The Server Certificate may be sent in multiple packets. • The next packet expected is from the server and it is a Server Done packet. • No Server Done packet was sent. • The Server Certificate may not have been completely sent. There may be a pr at the server. Timing Analysis • The time between the TCP handshake and the Client Hello was: 0 seconds, 0 milliseconds, 0 microseconds. • A time of less than 100 milliseconds is generally not a problem.

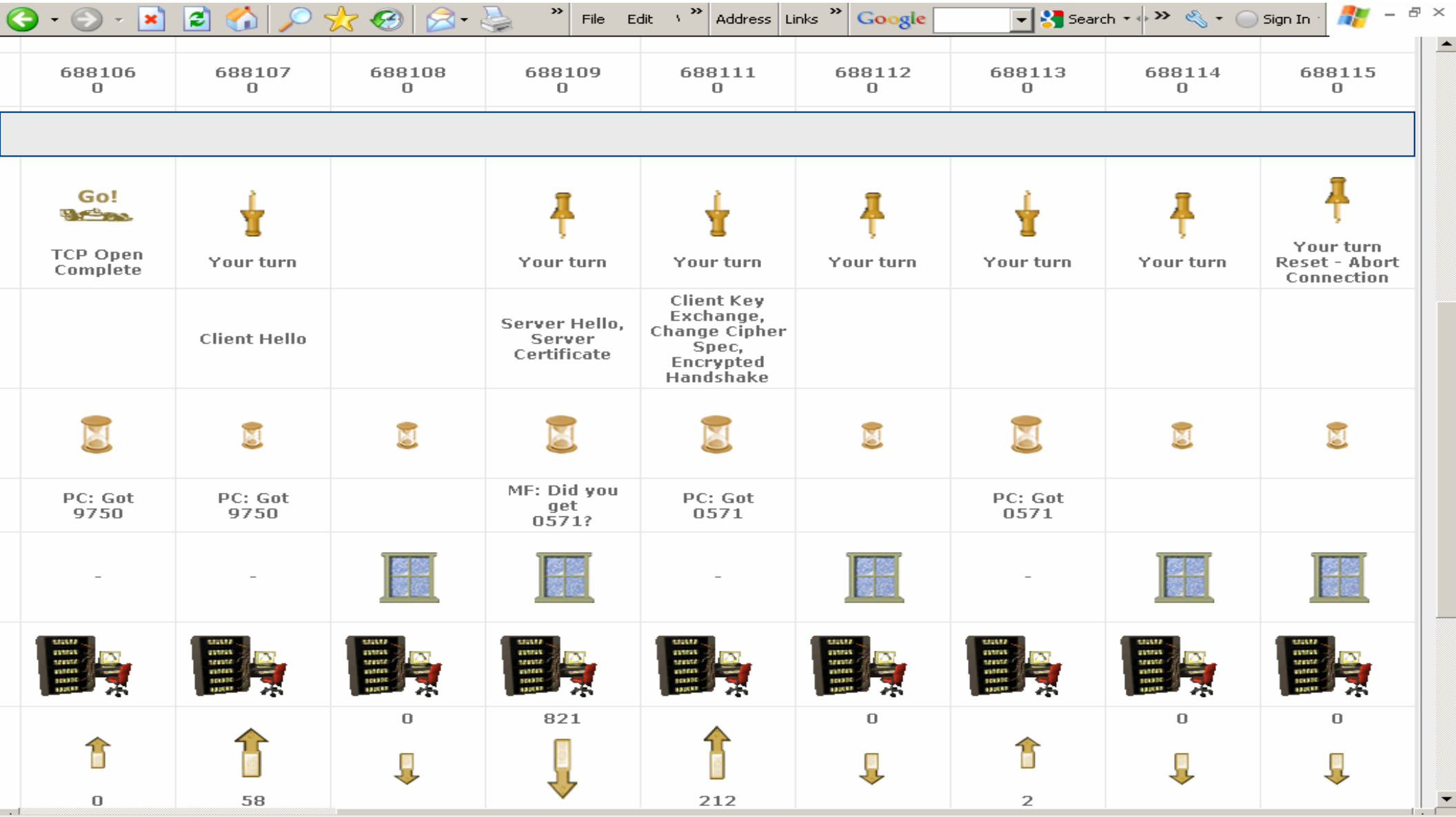
Using SSL Problem Finder

Good Handshake

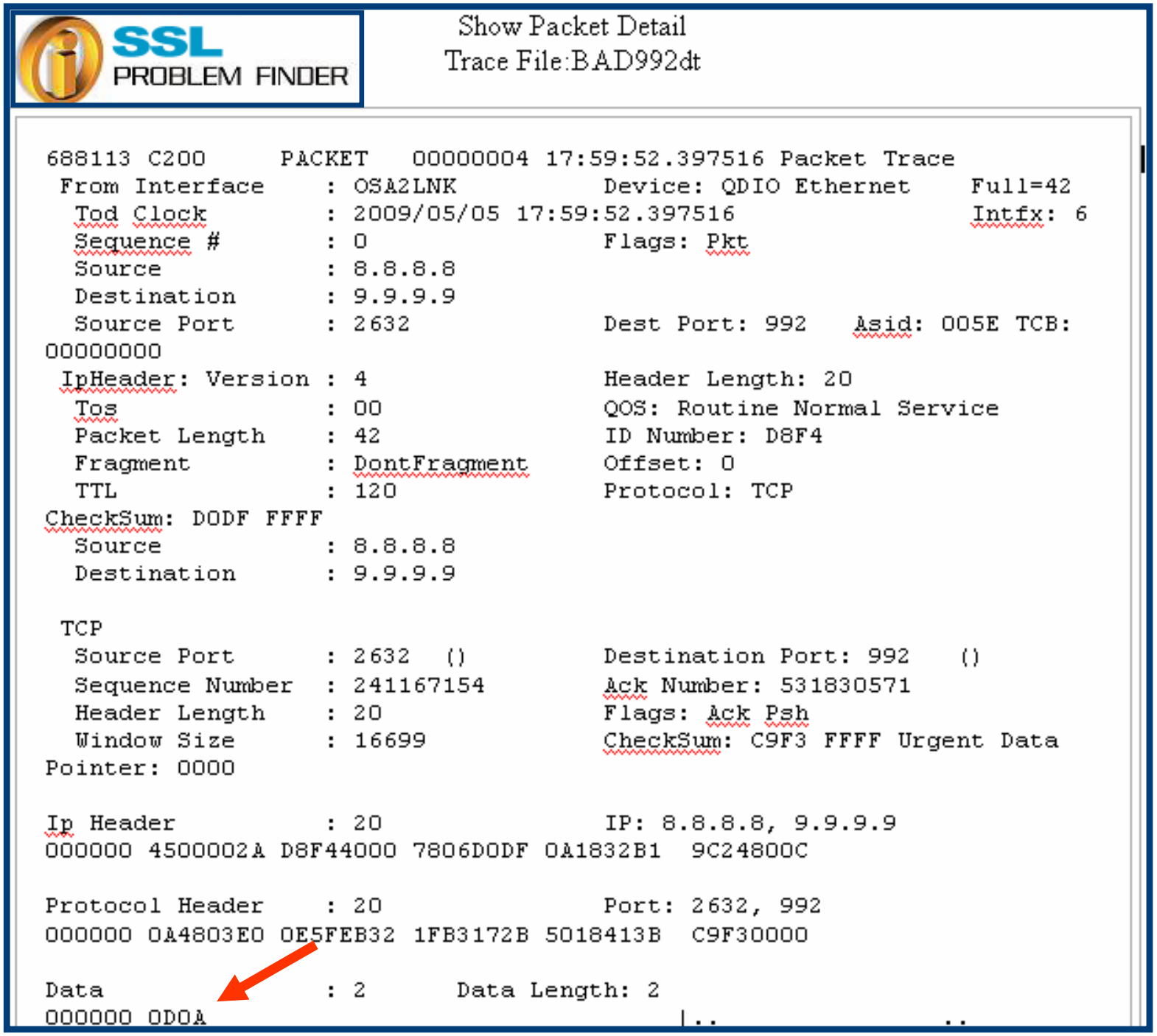
Bad Handshake



SSL Problem Finder (cont).

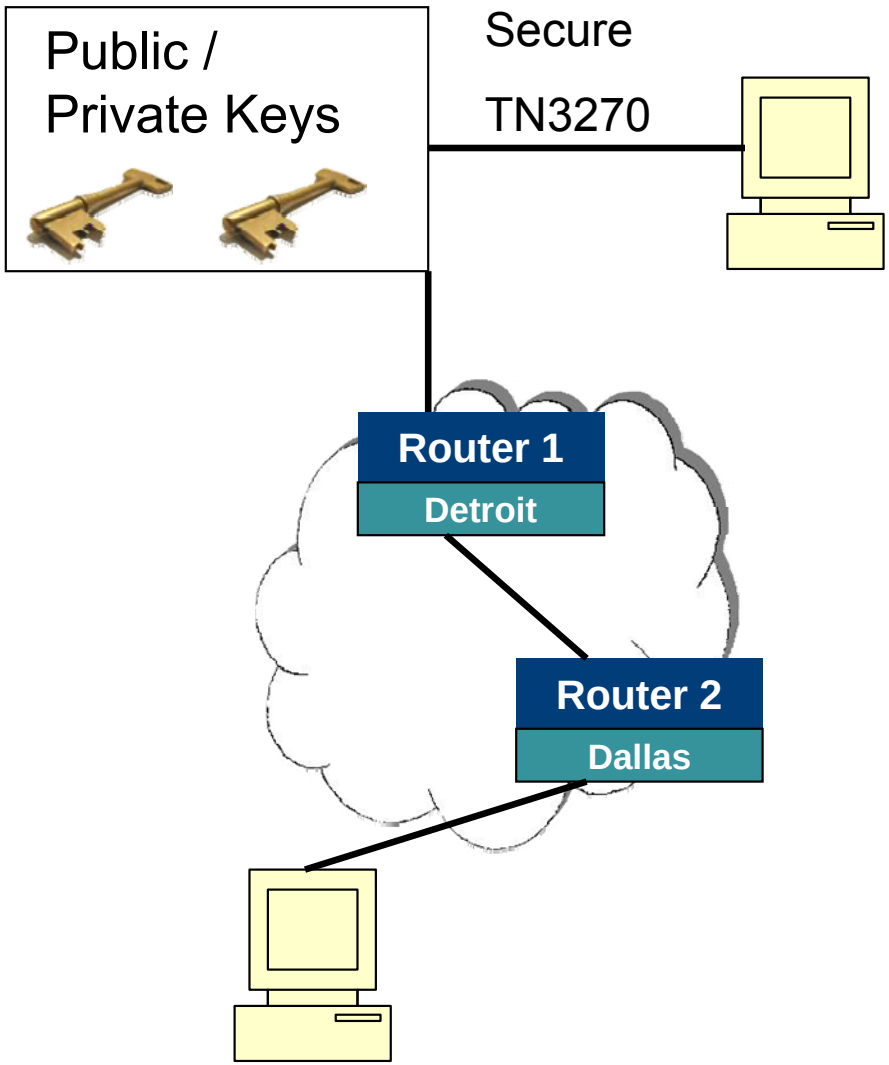


Client sends CRLF (x'0D0A') to the host during the SSL handshake



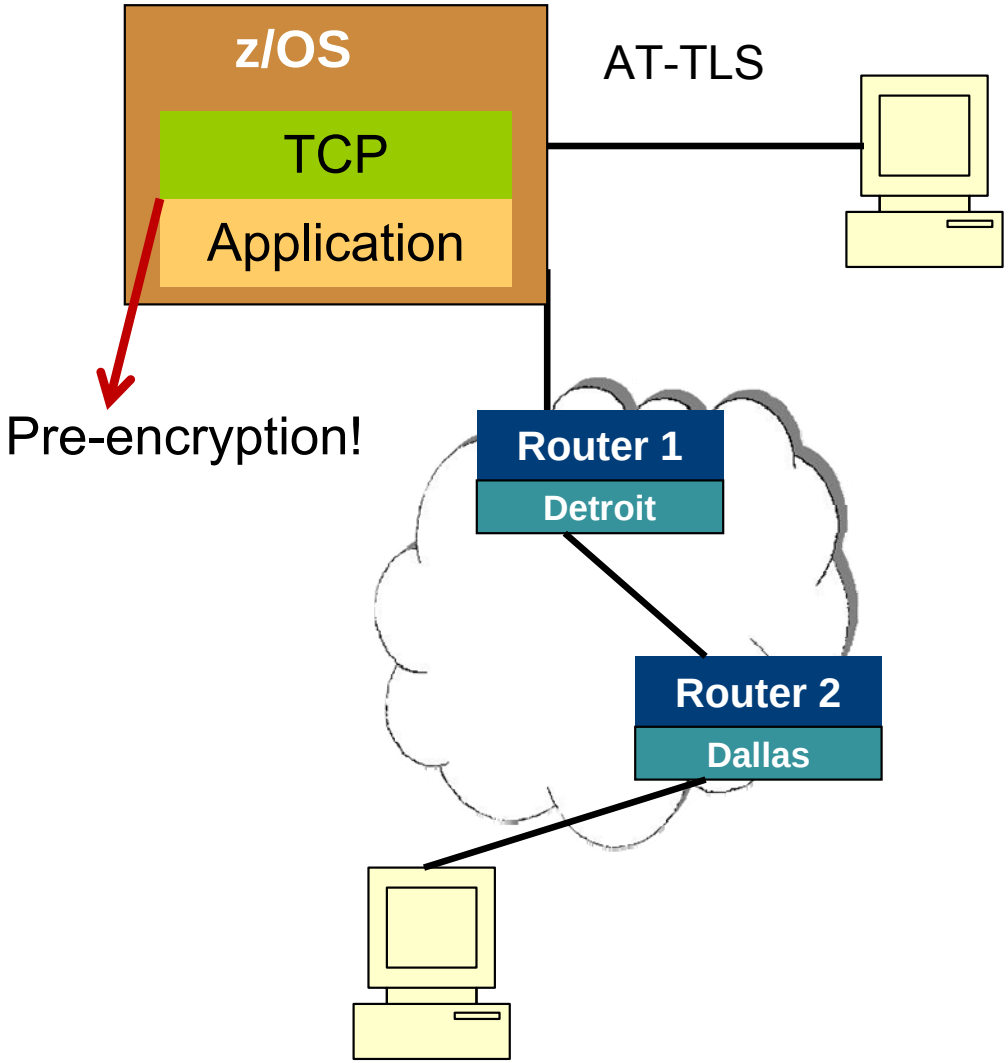
How To Decrypt SSL

- Depends on what method is used to encrypt the data.
  - SSL / TLS
  - AT-TLS
- Usually, SSL uses two keys to encrypt data − a public key known to everyone and a private or secret key known only to the recipient of the message.
- To decrypt these messages, the private key is required.
- Security folks don't care for this method.
- But, this is the reality. If you could break the decryption without the key, then it would not be secure!



How to Decrypt AT-TLS

- If Application Transparent TLS (AT-TLS) is used on z/OS to provide SSL encryption, then a data trace which captures data at the API layer can be used to see data before it is encrypted.
- You may either capture the data trace using the IBM External Trace Writer or the IBM Network Management Interface (NMI). This trace has only the unencrypted data at the API layer (ie. no IP headers).

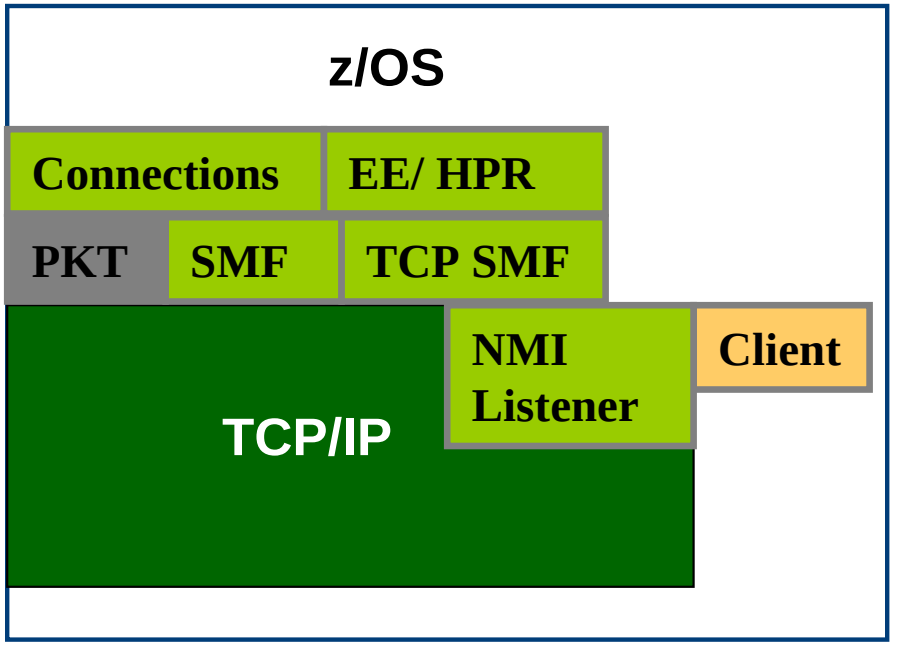


Implementation Considerations

- If the NMI option is chosen, then a capture program must be written to collect the data from the NMI after doing a :

  V TCPIP,,DATTrace

  command. Note that in the configuration for AT-TLS, you have to indicate that you would like to see the data unencrypted in the CTRACE.



- In the TTLSConnectionAction statement specify CtraceClearText.

- If the external writer is used, then just print to SYSTCPDA.

Matching Packets with Packet Trace

```
9153 T000     DATA     00000005 09:50:19.099043 Data Trace
  Jobname            : XXXX001          To                        Full=10
   Tod Clock         : 2009/01/30 09:50:19.099043                  Cid: 0000103E
   Sequence #        : 0                Flags: Dat Out
   Source            : xxx.xx.xxx.x     Destination       : xx.xxx.xx.xxx
   Source Port       : 2025             Dest Port: 1487  Asid: 006C TCB: 0000000

 Data                : 10     Data Length: 10
 000000 FFFA2803 04000204 FFF0              |.........0       ..(.......      |
 ---------------------------------------------------------------------------

9154 T000     PACKET   00000004 09:50:19.099075 Packet Trace
  To Interface       : OSA1LNK          Device: QDIO Ethernet     Full=77
   Tod Clock         : 2009/01/30 09:50:19.099075                 Intfx: 8
   Sequence #        : 0                Flags: Pkt Adj Out
  TCP
   Source Port       : 2025  ()         Destination Port: 1487  ()
   Sequence Number   : 357267317        Ack Number: 2144402221
 Data                : 37     Data Length: 37
 000000 17030000 20F99794 C3DD546D 3F7F3703 |.....9pmC..._."..  ....  .....Tm?.7.|
 000010 F882EF44 A773A936 CF9E1E02 DB46F653 |8b..x.z.......6.  ...D.s.6.....F.S|
 000020 EEE58B91 87                         |.V.jg             .....           |
```

If it is TO the foreign device, the data trace packet will be before the Packet trace.

Here is one FROM the remote

```
9159 T000     PACKET   00000004 09:50:40.172410 Packet Trace
 From Interface    : OSA4LNK          Device: QDIO Ethernet    Full=93
  Sequence #       : 0                Flags: Pkt Adj
  Source           : xx.xxx.xx.xxx    Destination      : xxx.xx.xxx.x
  TCP
  Source Port      : 1487  ()         Destination Port: 2025  ()
  Sequence Number  : 2144402221       Ack Number: 357268567
Data               : 53     Data Length: 53
000000 17030000 30FF2AC5 FF79CE94 B91C860F |.......E.`.m..f. ....0.*..y.....|
000010 0C981F58 4823E6FD 36E11A5E 9F7396D7 |.q....W....;..oP ...XH#..6..^.s.|
000020 3703D7AC FE2ECDCA 49DEE5D7 473EE3B7 |..P.......VP..T. 7.......I...G>..|
000030 FA949DFA DA                         |.m...            .....          |

-------------------------------------------------------------------------------
9160 T000     DATA     00000005 09:50:40.174272 Data Trace
 Jobname           : XXXX001         From                      Full=25
  Tod Clock        : 2009/01/30 09:50:40.174271                Cid: 0000103E
  Sequence #       : 0                Flags: Dat Adj
  Source           : xx.xxx.xx.xxx    Destination      : xxx.xx.xxx.x
  Source Port      : 1487             Dest Port: 2025  Asid: 006C TCB: 00000000
Data               : 25     Data Length: 25
000000 07000100 00939687 96954081 97979389 |.....logon appli ..........@.....|
000010 844DA3A2 96855DFF EF                |d(tsoe)..        .M.......       |
```

If it is FROM the foreign device, the data trace packet will be after the Packet trace.

Data visualized as TN3270 Screen

SSL PROBLEM FINDER

```
                        ---------- TSO/E LOGON ----------

   Enter LOGON parameters below:              RACF LOGON parameters:

   Userid    ===>                             Seclabel     ===>

   Password  ===>                             New Password ===>

   Procedure ===>                             Group Ident  ===>

   Acct Nmbr ===>

   Size      ===> 32768

   Perform   ===>

   Command   ===>

   Enter an 'S' before each option desired below:
          -Nomail         -Nonotice        -Reconnect        -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
```

Future Plans

- We are continuing to add AT-TLS sessions beyond TN3270.
- We plan to change all of our FTPs to use AT-TLS for security reasons.
- Other application groups are approaching us to provide security through AT-TLS.