Hacking Mainframes
with
SNA and APPN
Session 1785

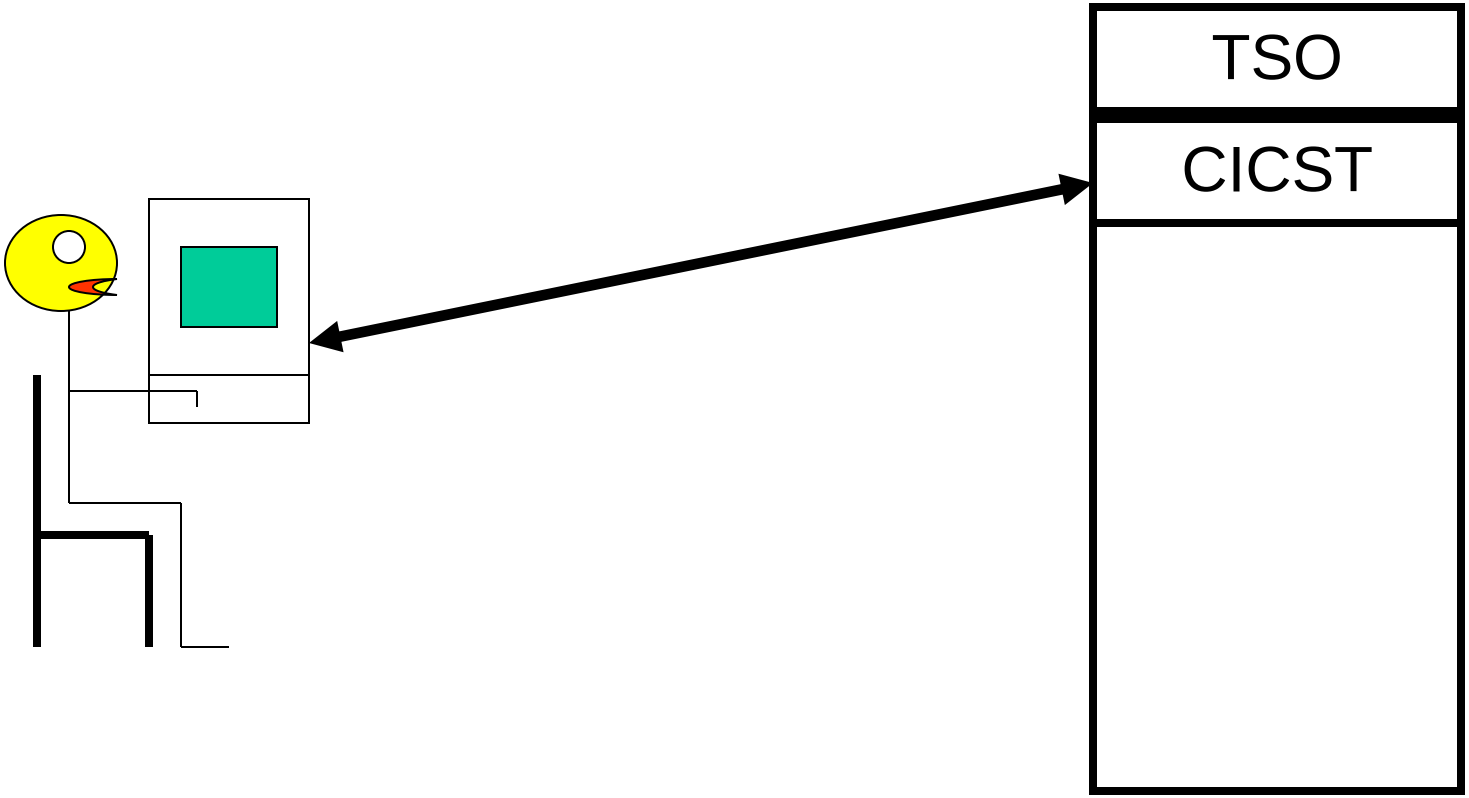
Stu Henderson,the Henderson Group
(301) 229-7187 www.stuhenderson.com
-^-
Peter Hager, Net'Q
(202) 470-2563, www.net-q.com

Abstract

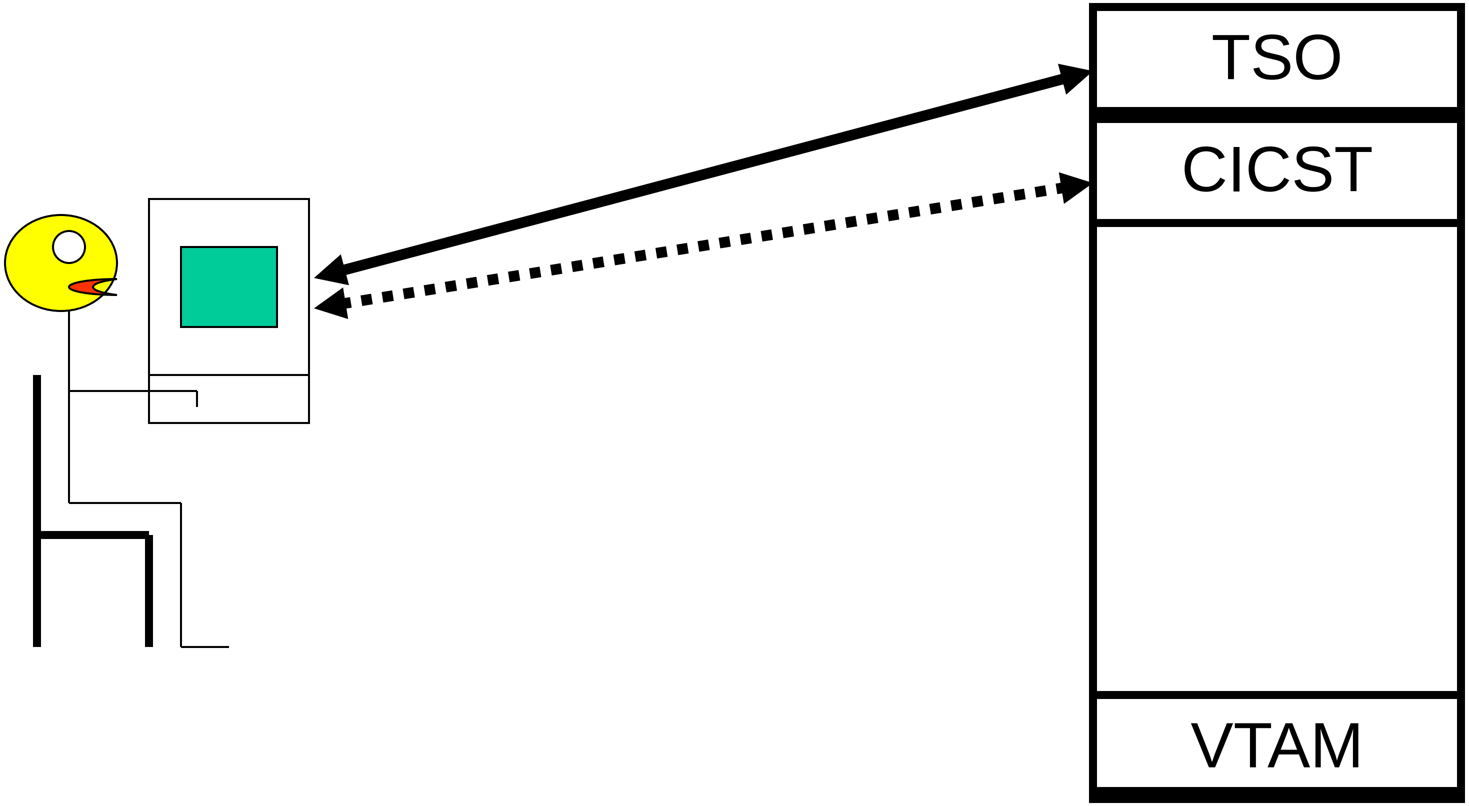
Most RACF (and ACF2 and TSS) administrators know that for effective security, you need to control every path into the system, including: TSO, NJE, RJE, started tasks, the internal reader, USS, and all the other APPLIDs. The path which is most often overlooked is APPN (Advanced Peer to Peer Networking), the protocol used to connect SNA networks to each other. (SNA is not going away, despite what the TCP/IP people claim.)

This session shows you what APPN is how how it works, the risks it introduces, and how to secure it with RACF/ACF2/TSS. Attendees should prepare by asking their VTAM system programmer the names of their SNA networks, the partner networks they connect to, and the networks their partners connect to.

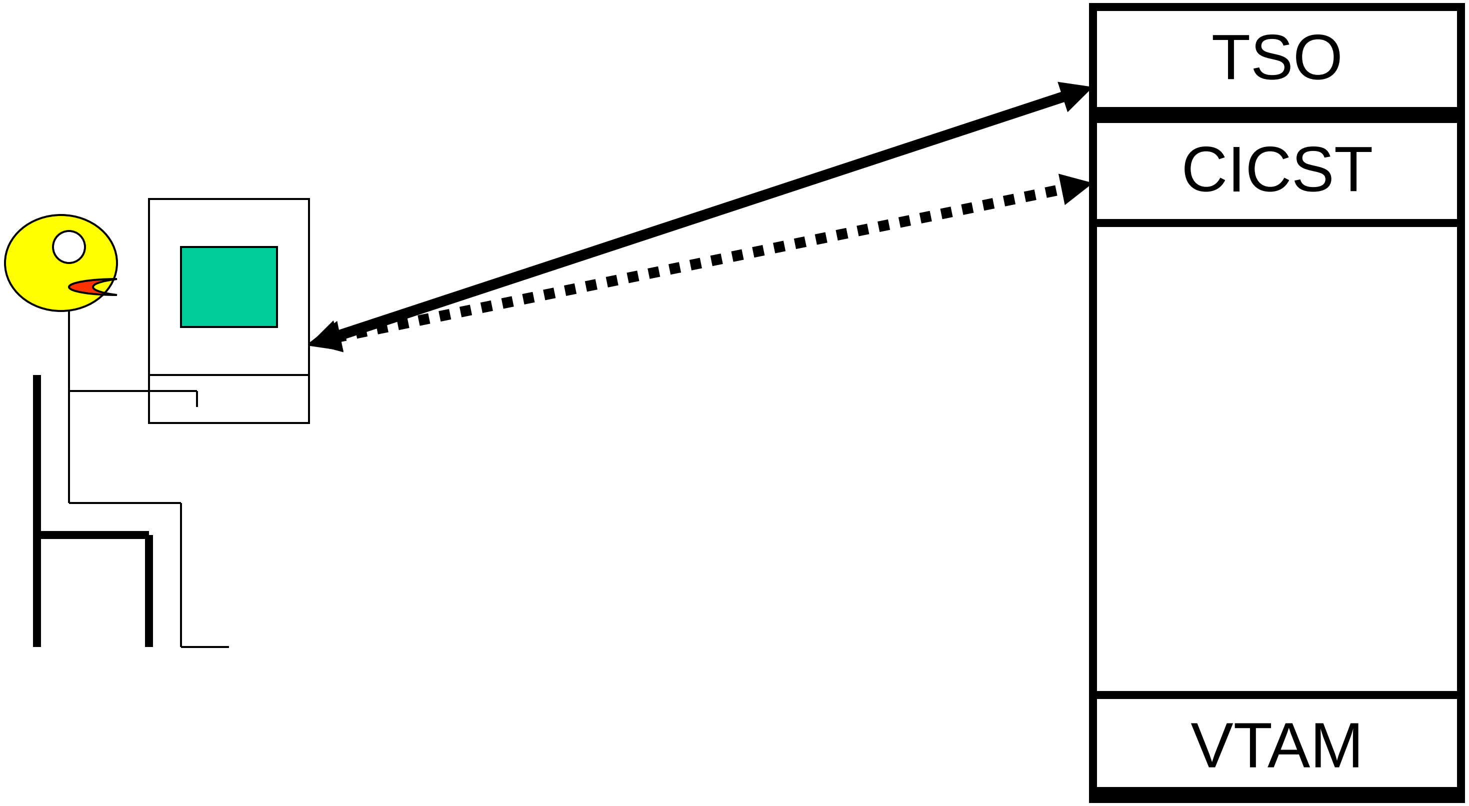
In the Beginning, Terminals Were Hardwired Into Mainframes (Phase 0)



Then with VTAM, a Terminal Could Switch Between Programs, Like TSO and CICS (Phase 1)



The Key to VTAM is That it Connects a Terminal to an APPLID (Program)



In VTAM, There Are Two Key Node Types

- LU (Logical Unit)

  VTAM treats its nodes as LUs Either:

  Terminals: 3270 Screen, Printer,
  RJE, NJE, ATM …

  OR

  Applications: IMS TSO CICS, TPX,
  TN270 Server ...

- VTAM (the VTAM Program Itself)

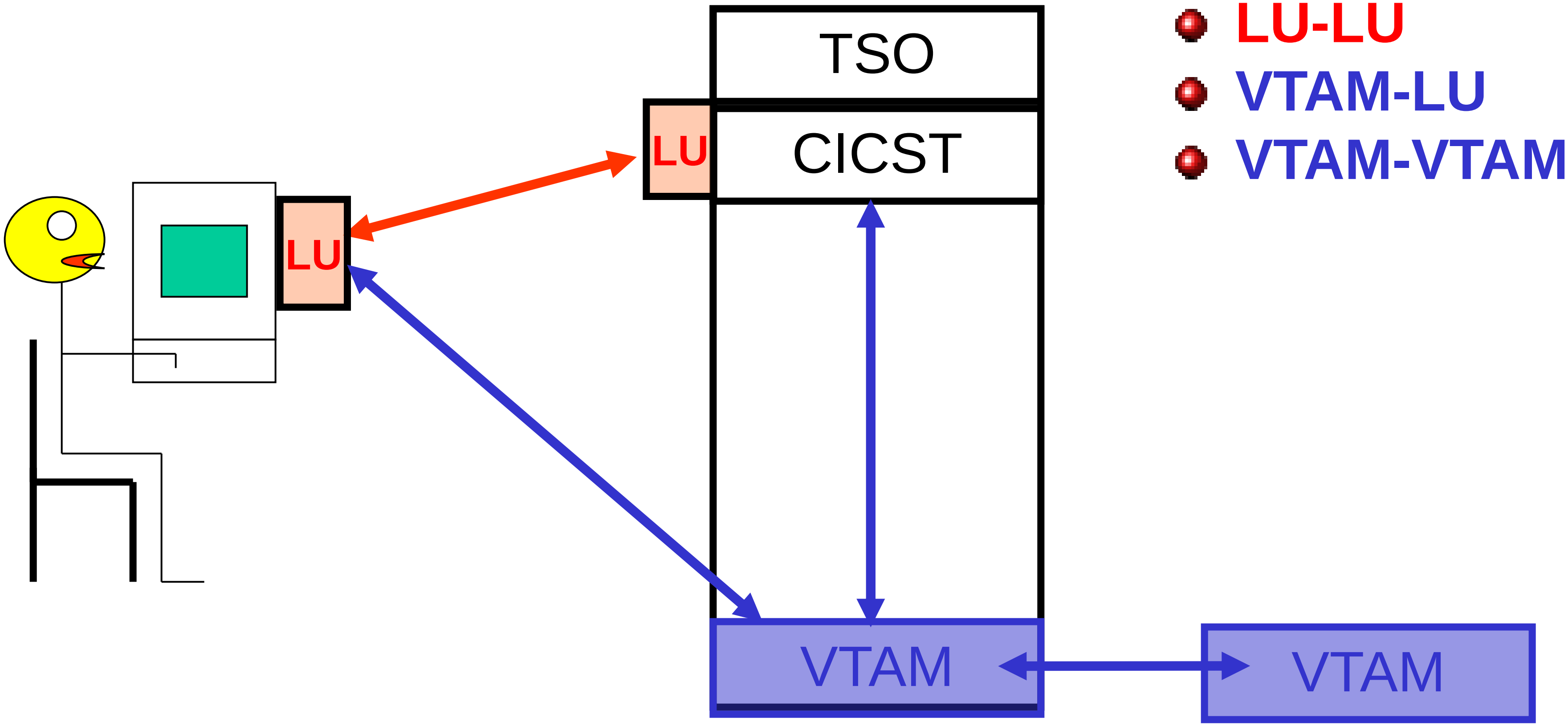
  SNA Name: System Services Control Point, or
  CDRM

  APPN Name: CP (Control Point)

An LU (either Terminal or Application Program) is an Entry Point to the Network.

- It is Similar to an IP address or a Phone Number, in That It Is Used for Routing
- You Will Find That APPN Makes VTAM More Like IP (More Dynamic and Less Master/Slave)
- This Results in APPN Being Subject to Risks Similar to Those We See With IP (Spoofing, Port Scanning, Man In the Middle)
- Fortunately, IBM Gives Us the Tools to Secure It

Three Session Types



- **LU-LU**
- **VTAM-LU**
- **VTAM-VTAM**

Session Start Commands

Sess Type	SNA/ APPN Command
LU-LU	**BIND**
VTAM-LU	**ACTLU**
VTAM-VTAM	**ACTCDRM(SNA), BIND(APPN)**

Basic Security Rules

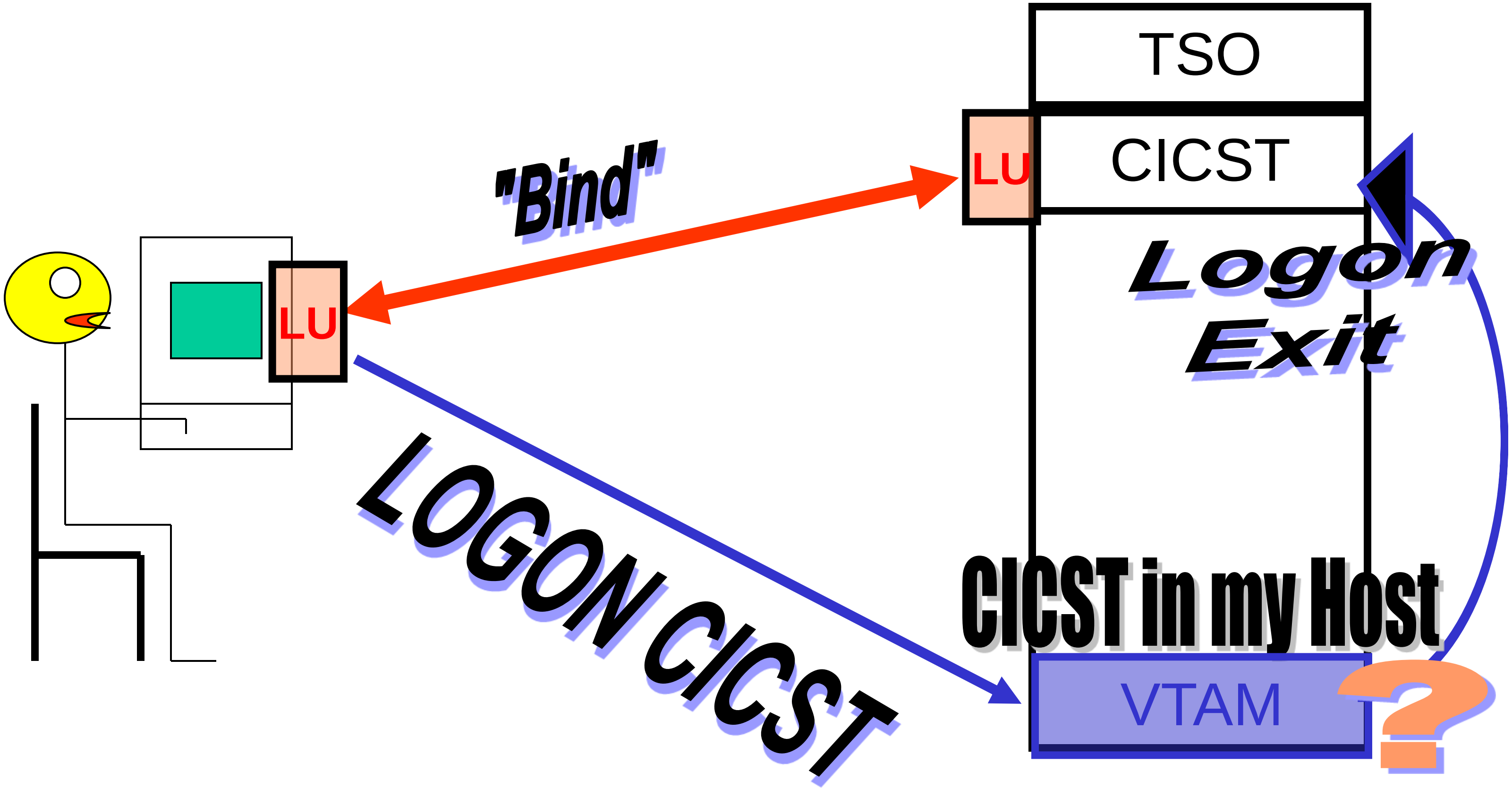
Rule 1

No Session = no Dataflow!

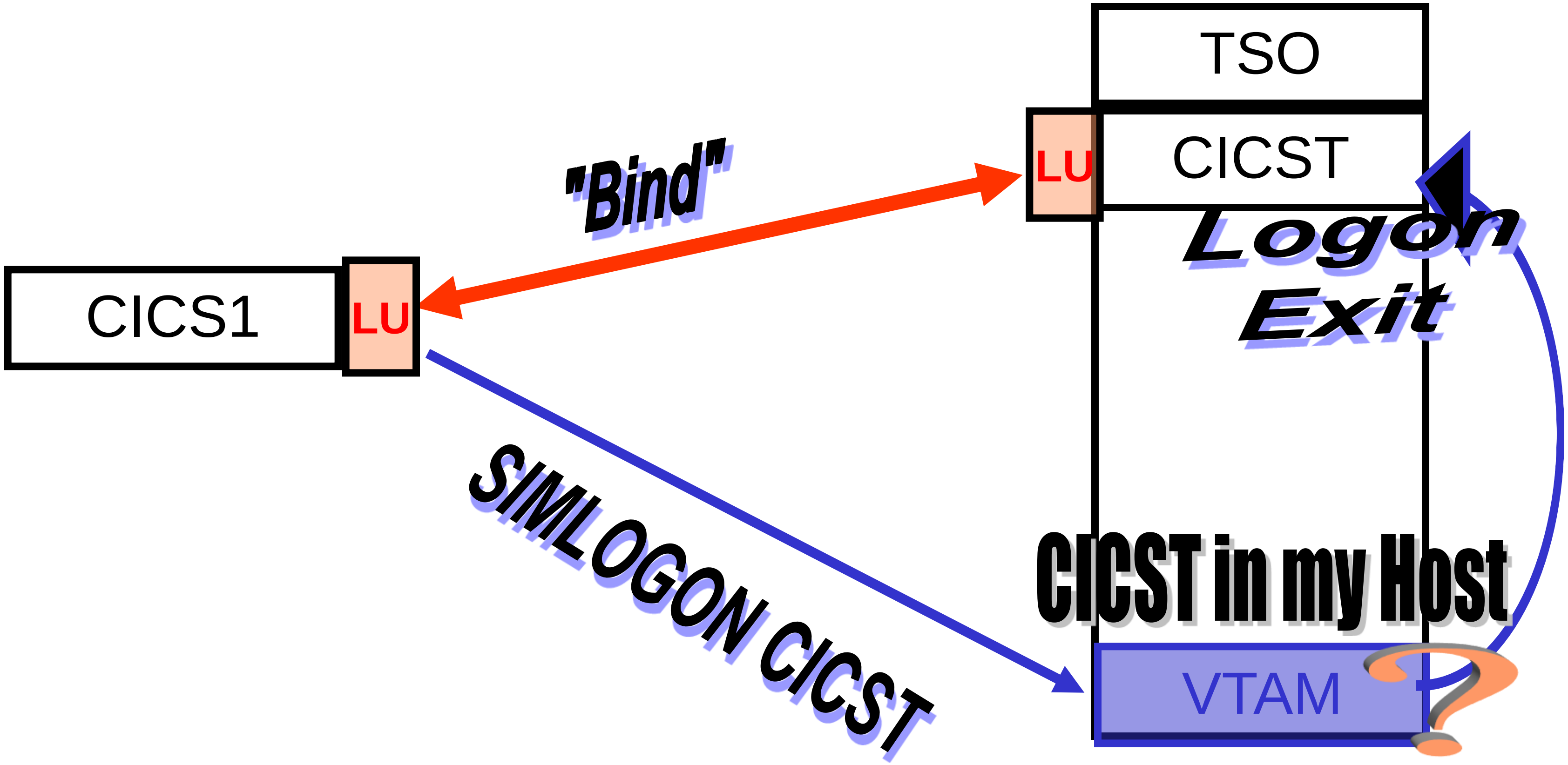
Rule 2

Session Security Profile is defined in session start command (Bindimage)

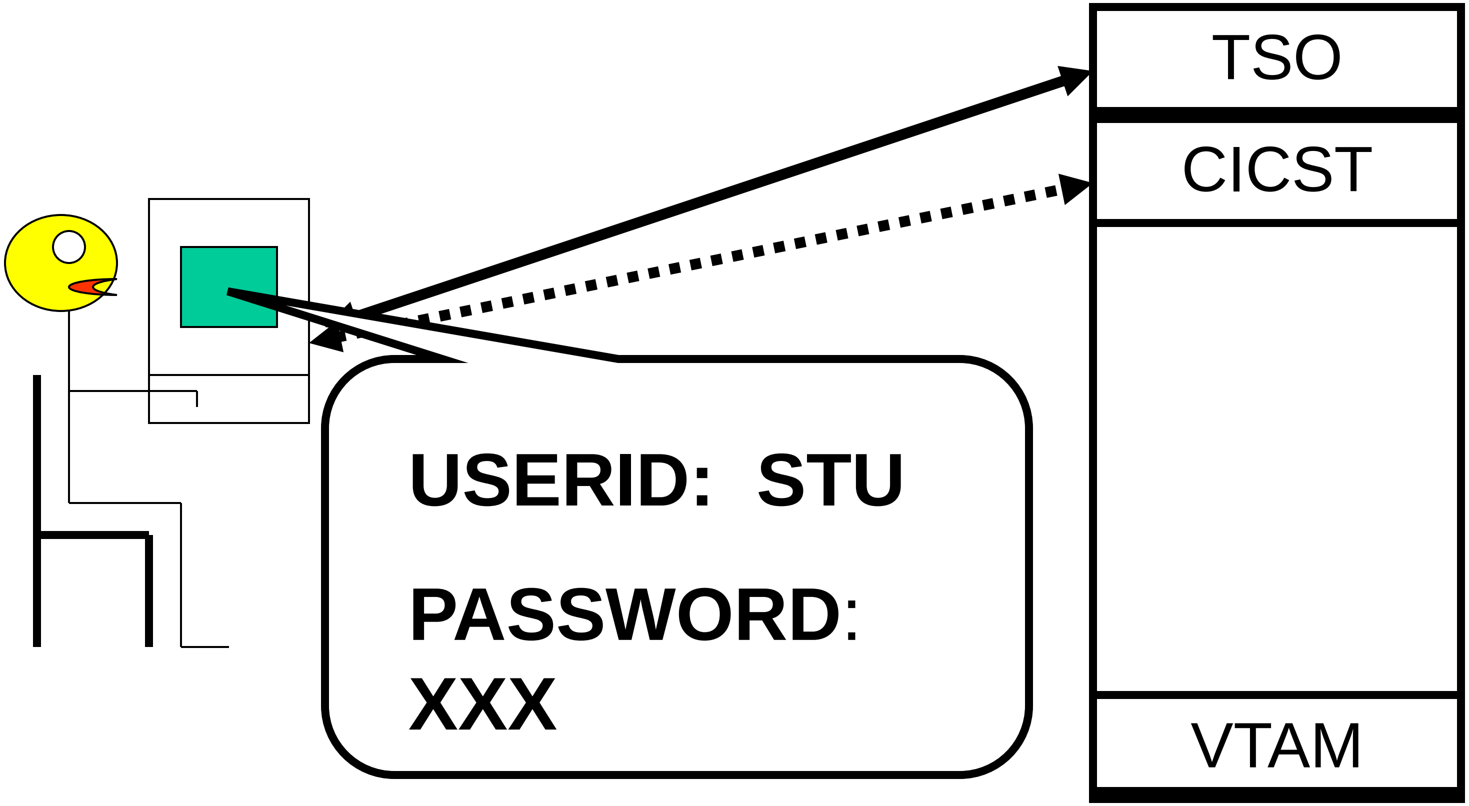
The Request for a Session is Called a "LOGON"



“LOGON” between Applications



The Result of a Bind is That Everything You Type Goes to The APPLID



USERID: STU

PASSWORD: XXX

TSO

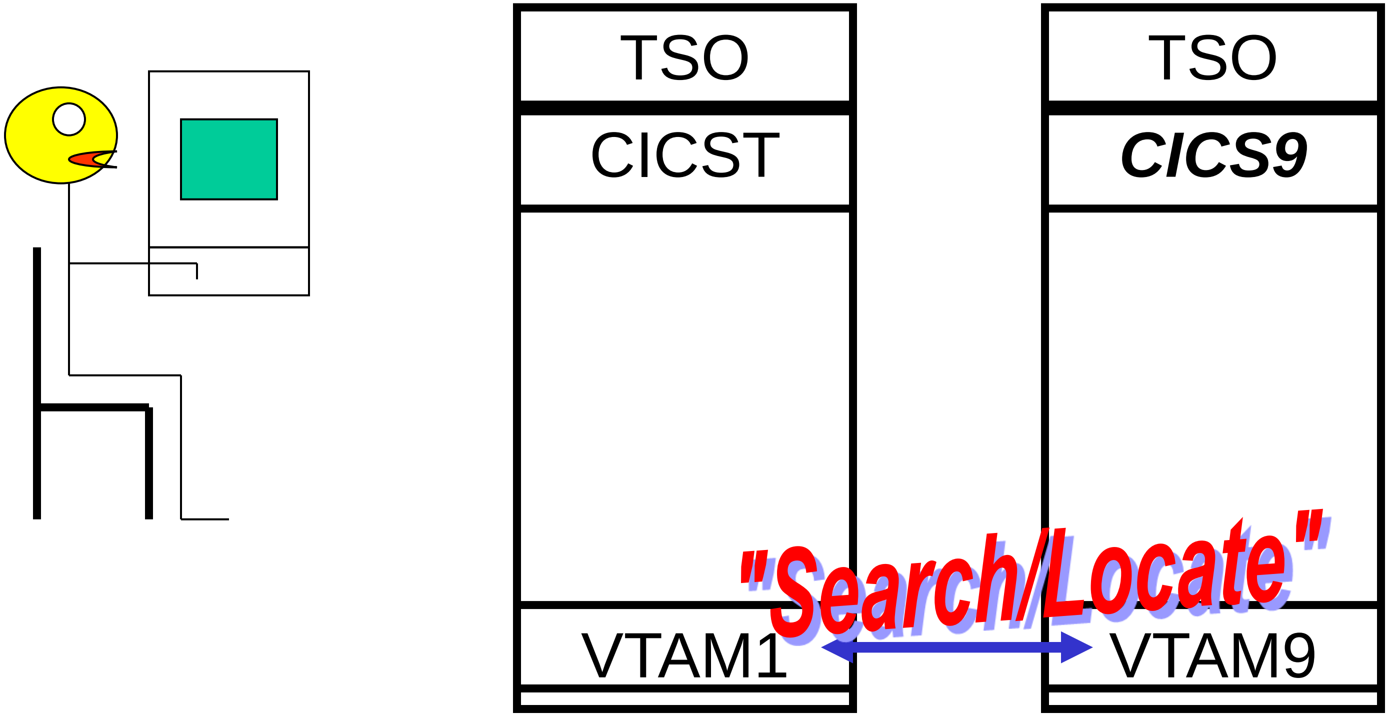
CICST

VTAM

But What IF (Phase 2)

- The Terminal is On Your Test CPU
- And the APPLID is on Your Production CPU? (all in the same network)
- The Two VTAMs Use CDRM (Cross Domain Resource Management) to Set Up the LU-LU Session

With Cross-Domain, the VTAMs Talk to Each Other exchanging Search/Locates



With SNA

We Have Security Because The CDRMs (Cross Domain Resource Managers)

- Must Be Pre-Defined to Each Other
- Are Behind an IBM-Designed Channel, Which Serves Sort of Like a Firewall
- Are Behind Locked Doors in a Data Center

<u>But They Can't Authenticate Each Other</u>

(perhaps don't need to)

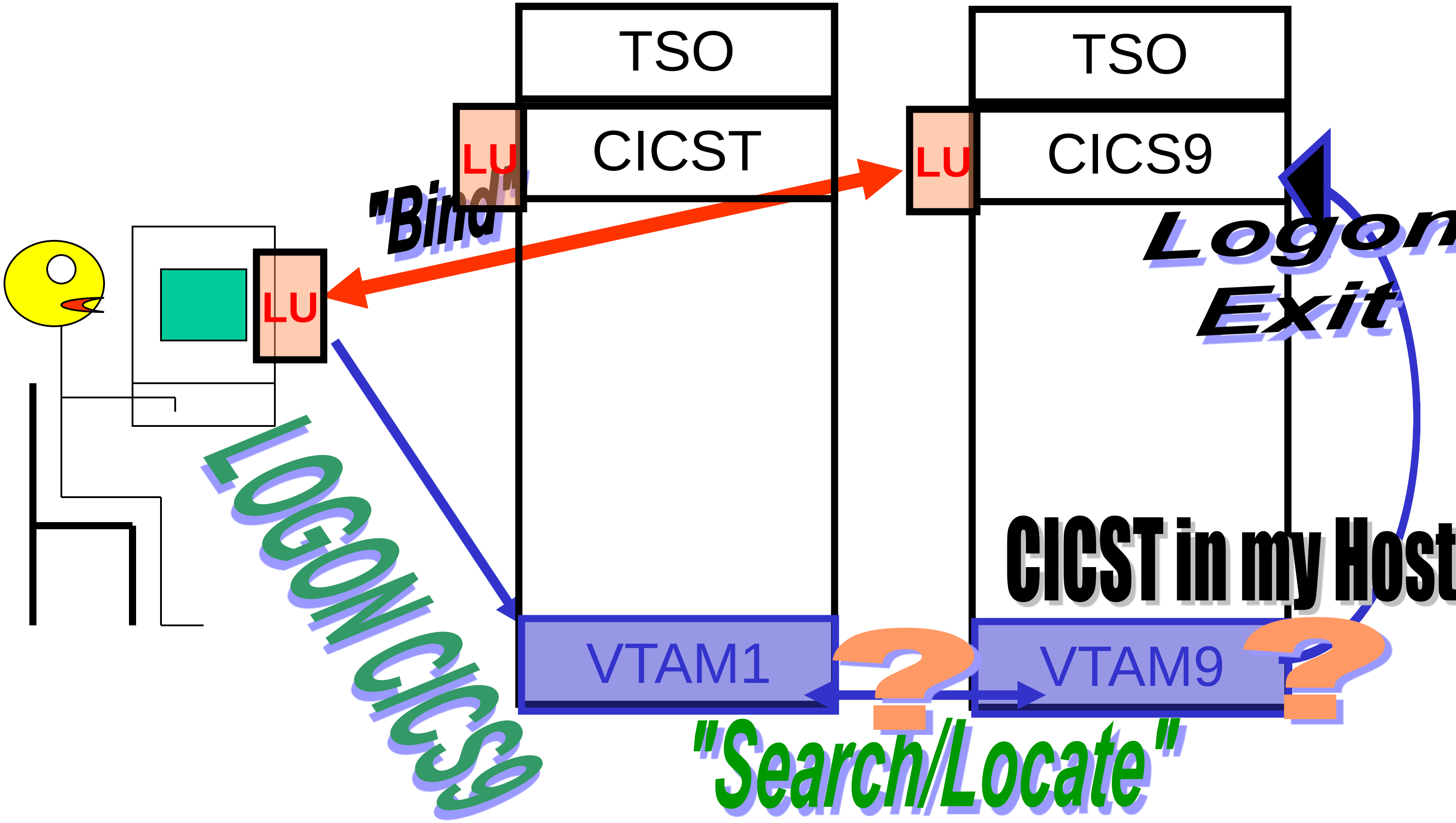
With APPN, Each VTAM Is:

- Called a CP or “Control Point”
- CPs Don’t Have to Be Pre-Defined to Each Other
- IBM Gives Us an Option for CPs Only to Talk to CPs Which Are Pre-Defined to Them. 99 Percent of Installations Take the Default: “Don’t Require Pre-Definition”

They Can Authenticate Each Other

(More than Half the Installations Don't Allow This)

The Terminal Can Be Defined in One Computer and the APPLID can be in Another. This is Called "Cross-Domain"



VTAM1 Asks Some Basic Questions:

- **Is CICS9 in My Host?**
- **Is It Predefined as a Resource in a Dedicated External Host?**
- **Is It In a Predefined Adjacent VTAM List?**
- **What Does My Default Algorithm Say to Do?**

But What IF (Phase 3)

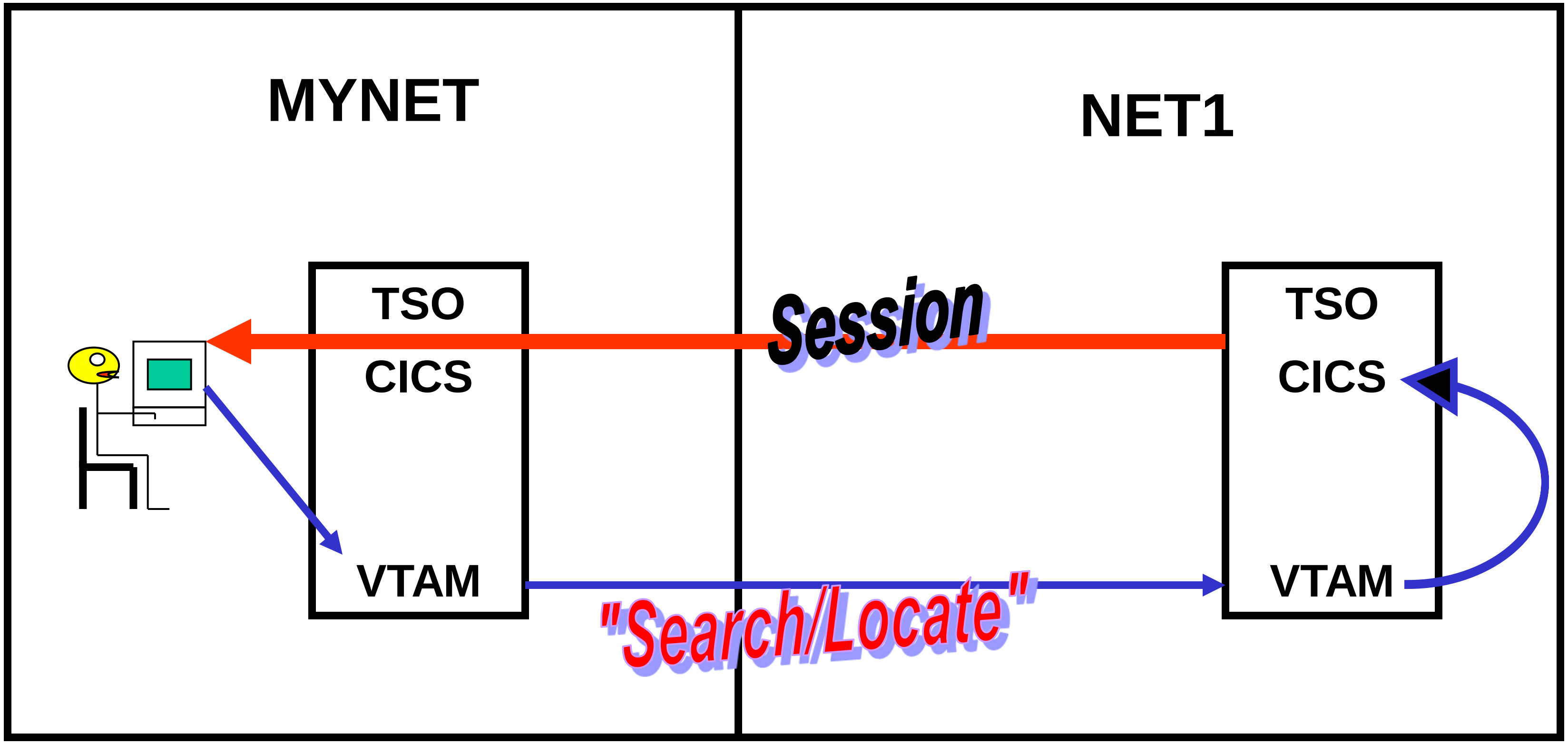
- The Terminal is On Your Test CPU
- And the APPLID is On a Different CPU in a ***Different*** **Network**?
- For This, You can Use
  1. SNI (SNA Interconnection)

     Crossnet over SNA Gateways
  2. APPN (Advanced Peer to Peer Networking).

     Crossnet over IBMs Enterprise Extender, tunneling APPN over IP

Both Cross Domain and Cross Net Execute on IBM’s SNA (System Network Architecture)

This is Cross-Domain Across Networks

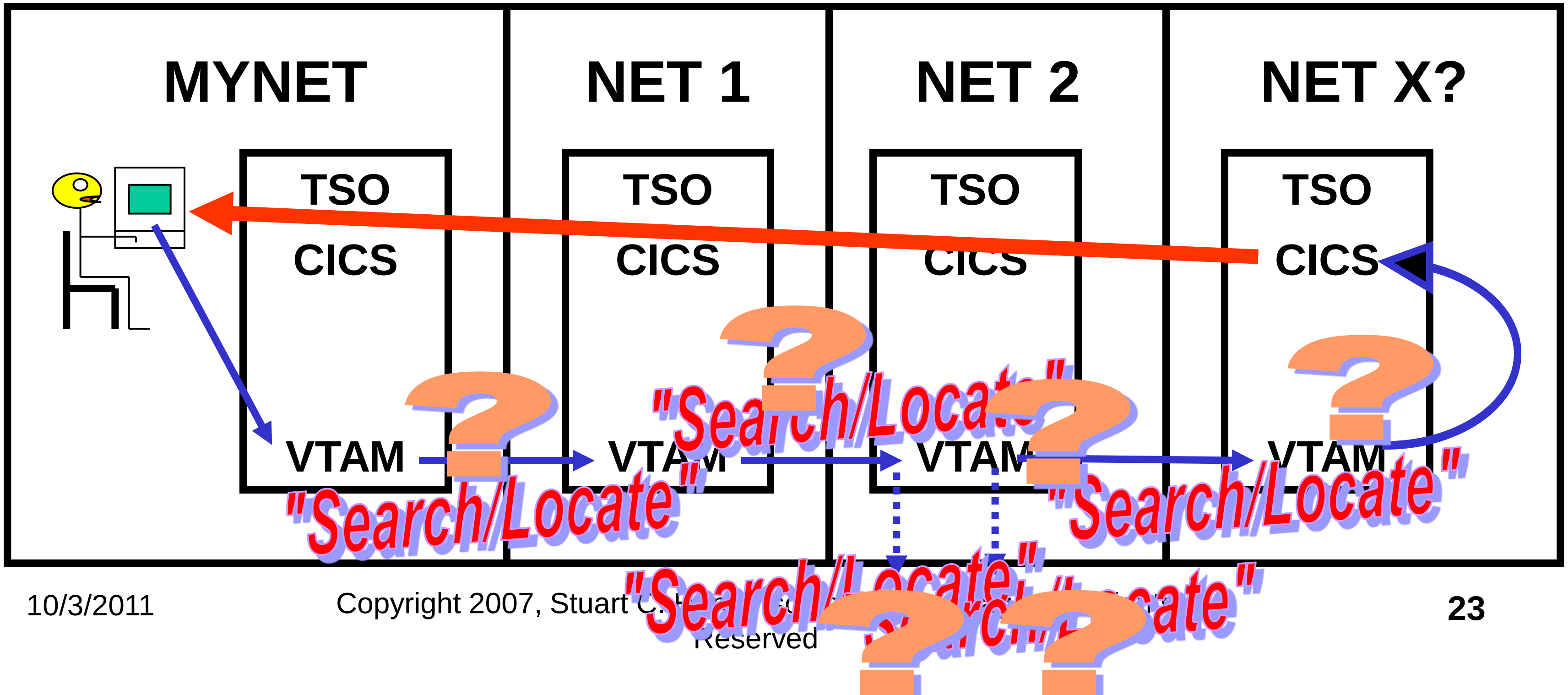


Some of the Requests That Can Be Made Over the Network

- BIND (Please connect my LU to that program)
- SEARCH (**ORIG-LUNAME . VTAMNAME . NETID**
  searches for
  DEST-LUNAME . VTAMNAME . NETID)
- LOCATE (**ORIG-LUNAME . VTAMNAME . NETID**
  locates
  DEST-LUNAME . VTAMNAME . NETID)

SEARCHES are more SNA/SNI like,
LOCATES are more APPN like

You Can Have APPN Across Many Networks (Some of Whom You May Not Know)



With Crossnet, the VTAMs:

- **Store Info About Each Others' Connections, Terminals, APPLIDs, etc in Resource Databases**

- **Answer Queries to/from Each Other About these Resources**

- **Broadcast and Respond to Requests from Terminals for a Bind to a Given APPLID**

- **Once a Search/Locate reaches your adjacent Network, it is out of your control!**

You Will Still Have APPN:

- **Even if You Make Your Terminals All Go to TCP/IP with OSA**
- **If You Are a Significant Financial Institution, Manufacturer, or Government Agency Whose Mainframes Talk to Other Mainframes**

To Know You Have Good Security,

You Need to Know Basic Info About Your Network Connections, Including APPN

You Can Have APPN Across Many Networks

- **What is the Name of Your Network?**
- **What Networks are You Connected to?**
- **What Networks are They Connected to?**
- **(And so on…)**

What’s Happening with TCP/IP and SNA?

- Many Mainframes are Using OSA (Open System Adapter) to Connect Terminals to the Mainframe with TCP/IP
- Many Mainframes are Using EE (Enterprise Extender) to Connect to Other Networks, Tunneling SNA Through UDP
- SNA is Here to Stay, Along with TCP/IP

Types of Protection:

- SNA FIREWALL
- SAF Calls (RACF, ACF2, Top-Secret)
  - APPCLU Resource Class
  - VTAMAPPL Resource Class
- VTAM Options (Several Dozen, in Startup Parms, in NAU Definitions, in COS Tables and other places) of your network

Summary and Call to Action

- If You Don’t Use APPN, or If You Don’t Connect to Other Networks, Then You Can Relax

- Else You Need to Address The Risks Outlined Here

- If You Want Further Information or Automated Analysis Tools, SNA Firewall, Please Contact:

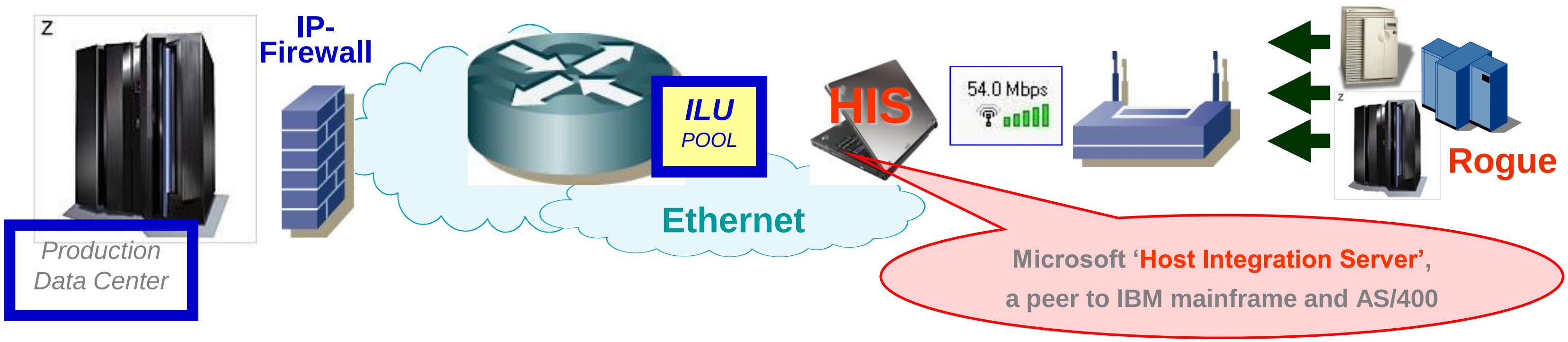
  www.net-q.com

Hacking Methods Applicable

Green Field for Hackers?

		MyHost	MyPlex	MyOrg	MyNet	OtherNet
1	Spoofing SAF (RACF-ACF2-Top Secret)	🚫	✓	✓	✓	✓
2	Spoofing SSCP or CP	🚫	✓	✓	✓	✓
3	Expand Capability to Hack	✓	✓	✓	✓	🚫
4	Transfer SAF Admin Rights to an ext. System	🚫	✓	✓	✓	✓
5	Man in the Middle	✓	✓	✓	✓	✓
6	Spoofing Application or Session Partners	✓	✓	✓	✓	✓
7	Enforce Innocent TERM/APPL to Rogue APPL	✓	✓	✓	✓	✓
8	Session Forwarding	✓	✓	✓	✓	✓
9	Rogue APPL Innocent TERM/APPL	✓	✓	✓	✓	✓
10	Bind Scan, (like Port Scan in IP)	✓	✓	✓	✓	✓
11	Denial of Service	✓	✓	✓	✓	✓
12	Spoofing NetID	✓	✓	✓	✓	✓

Security Violation Case 16



Microsoft ‘Host Integration Server’,
a peer to IBM mainframe and AS/400

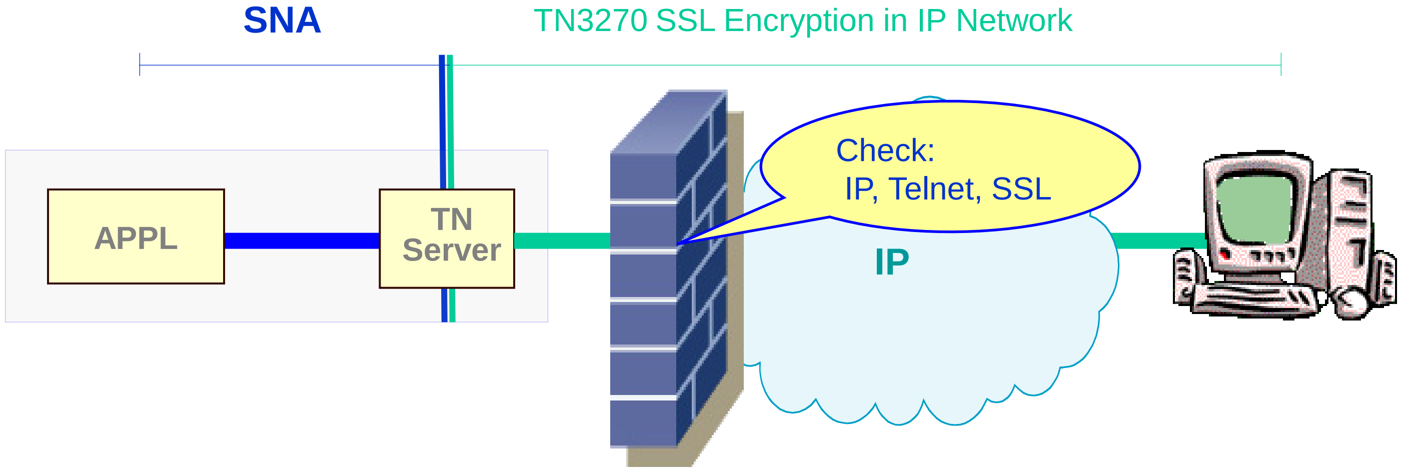
Datacenter no longer had any interconnection to external networks. Security Team felt their SNA/APPN network would be safe. Their mainframe access was secured by an IP Firewall

One day they detected a laptop connected to an Ethernet LAN port. This particular laptop did not belong to anyone on their team. Upon closer inspection of that suspicious laptop, they discovered that they were being hacked by external third parties using this small laptop

- **Microsoft Host Integration Server (HIS) acted as an extension to contact various external IBM Host Systems**
- **The physical connection to the external world was a fast wireless LAN linked to a WLAN router which was connected to the Internet somewhere in the neighborhood buildings**
- **From there, over the public Internet they were hacked by various external systems**
- **All external communication partners registered to their production center as internal resources**
- **There is a free download available: http://www.microsoft.com/hiserver/default.mspx**

Security Violation Case 17-1

TN3270 SSL was rerouted to a rogue 3rd Party



Situation SNA side:

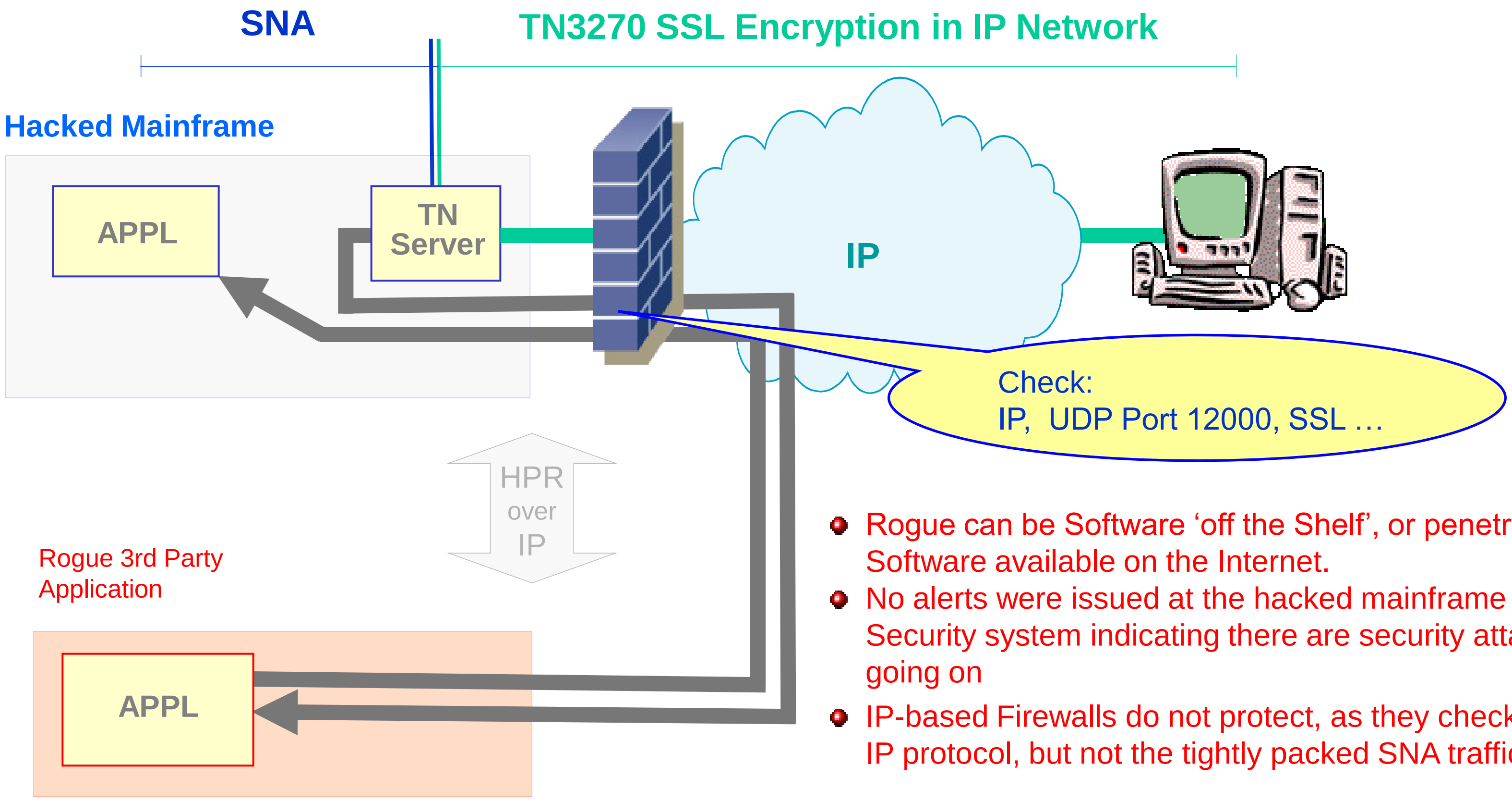
- Traditional SNA traffic between TN3270 and legacy Application
- No SSL encryption possible
- Passwords and data transported in cleartext format

Situation IP side:

- TN3270 data traffic is secured well as encryption takes place.
- In addition protection through the IP firewall is activated

Security Violation Case 17-2

TN3270 SSL was rerouted to a rogue 3rd Party

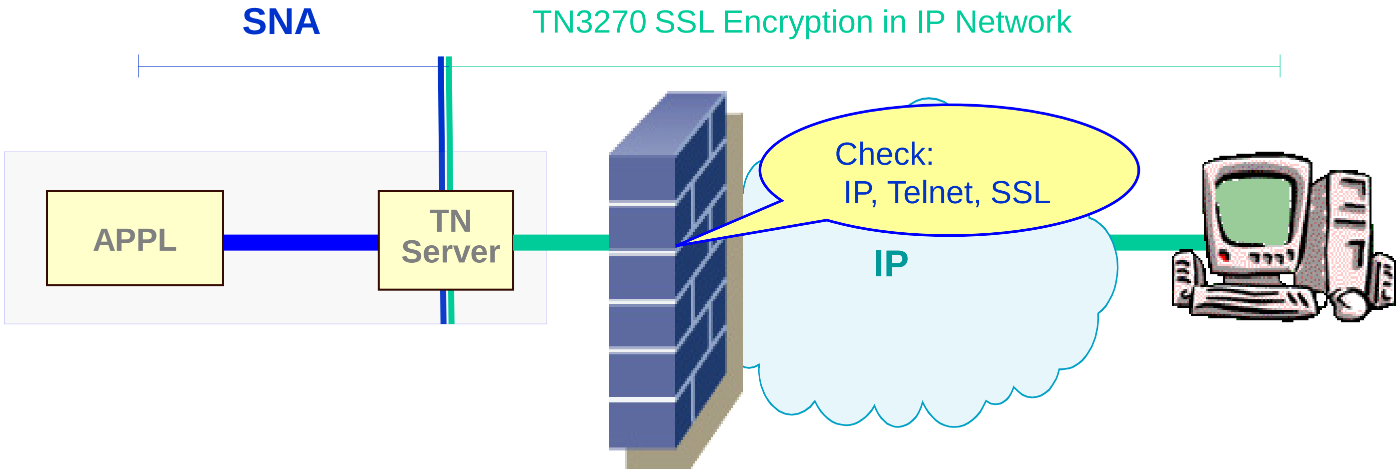

SNA
TN3270 SSL Encryption in IP Network
Hacked Mainframe
APPL
TN Server
IP
HPR over IP
Rogue 3rd Party Application
APPL

Check:
IP, UDP Port 12000, SSL …

- Rogue can be Software ‘off the Shelf’, or penetration Software available on the Internet.
- No alerts were issued at the hacked mainframe Security system indicating there are security attacks going on
- IP-based Firewalls do not protect, as they check only IP protocol, but not the tightly packed SNA traffic!

Security Violation Case 18-1

Phishing TN3270 SSL



Situation SNA side:

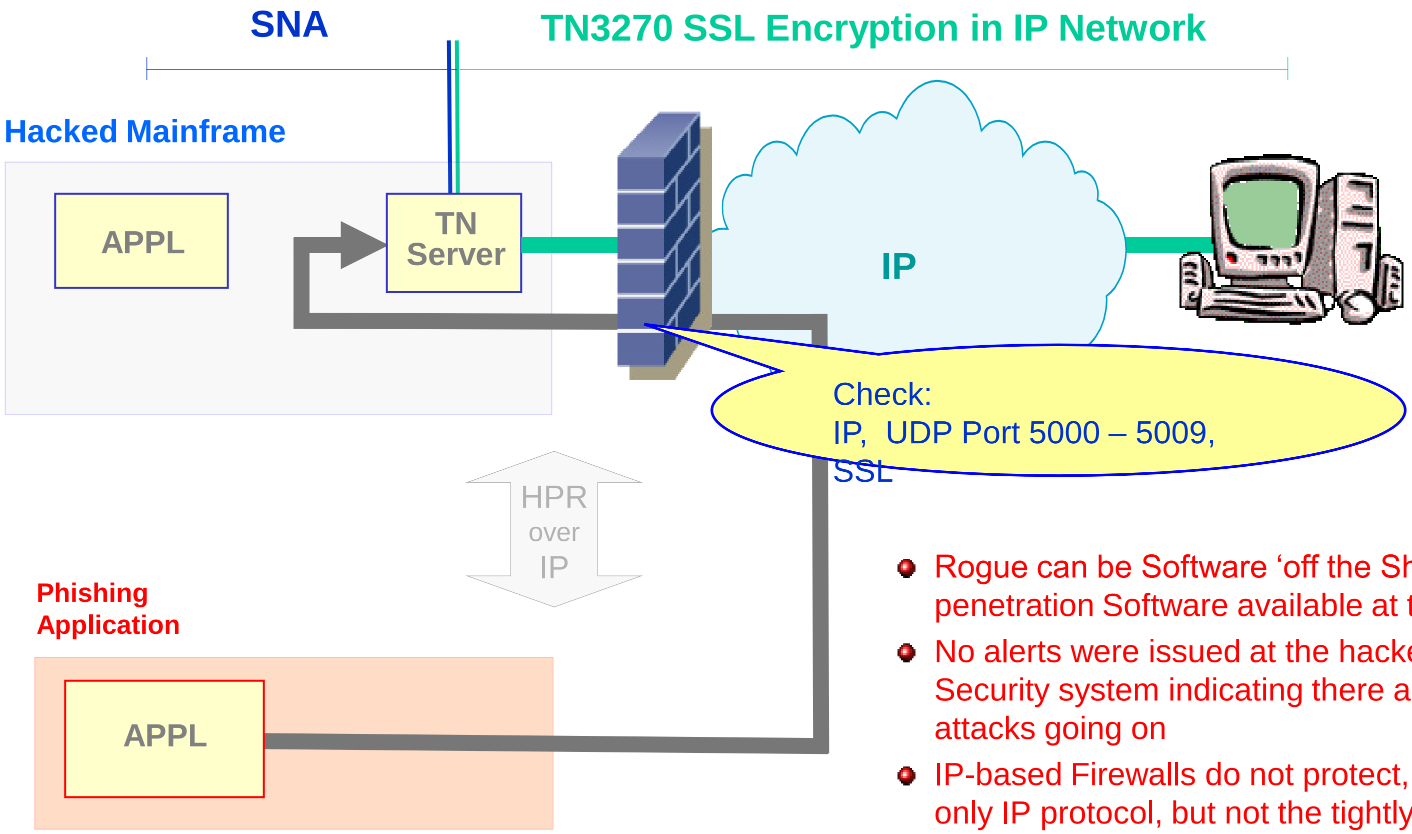
- Traditional SNA traffic between TN3270 and legacy Application
- No SSL encryption possible
- Passwords and data transported in cleartext format

Situation IP side:

- TN3270 data traffic is secured well as encryption takes place.
- In addition protection through the IP firewall is activated

Security Violation Case 18-2

Phishing TN3270 SSL



Check:
IP, UDP Port 5000 – 5009, SSL

- Rogue can be Software ‘off the Shelf’, or penetration Software available at the Internet.
- No alerts were issued at the hacked mainframe Security system indicating there are security attacks going on
- IP-based Firewalls do not protect, as they check only IP protocol, but not the tightly packed SNA traffic!

Hacking Platforms

You do not need to use traces for Penetration

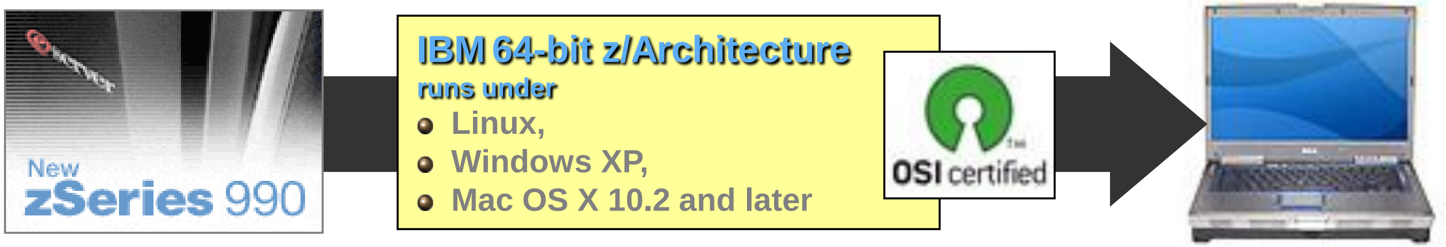
- Standard software can be used to attack at rogue mainframe, or use penetration software available.
- NO alerts are issued at the hacked mainframe Security system indicating there are security attacks going on
- IP-based Firewalls do not protect, as they check only IP protocol, but not the tightly packed SNA traffic!

Hacking Platforms

IBM z/OS Penetration Platform

IBM penetration platform can easily be realized on various ways:

A. Rent LPAR from one of the outsourcing companies available worldwide
B. Run penetration tests on your own IBM Test-LPARS.
C. Run penetration software at a PC or LAPTOP by installing Hercules on your PC.
D. Buy Microsoft Server 2003 hosting service for ~ 100 USD per month, install Hercules and z/OS
E. Eventually order z/OS on CD from eBay?



IBM 64-bit z/Architecture
runs under

- Linux,
- Windows XP,
- Mac OS X 10.2 and later

Microsoft HIS Penetration Platform

Microsoft’s HIS can be downloaded for free with temporary license for 3 months.
Microsoft's excellent technical guidelines and directions help to easily use and gain access
Download: www.microsoft.com/hiserver/evaluation/trial/default.mspx

Hack Case 17 & 18

Which software do you want to use?

A) Use software already available like

- **IBMs NetView Access or Supersession-**
- **McKinneys VTAM Switch**
- **Computer Associates TPX or Net Master**

B) Develop your own hacking software

Develop Hacking Software

Ways to compile and test on your Microsoft laptop:

- **Free download from Dignus Software Assembler**
- **Free download of MVS 3.8 (This old Release contains already everything needed for this attack!)**
- **Free download of Hercules, Learn more from WIKIPEDIA..**
- **Optionally run your newest z/OS software in your PC or laptop including Enterprise Extender**

Code Hacking Software

Hacking ‚Bible‘ for SNA?

Hackers ‚Bible‘ for writing SNA hacking software is IBMs 'SNA Programming manual' downloadable from IBM z/OS Internet Library

www-03.ibm.com/servers/eserver/zseries/zos/bkserv/r8pdf/cserver.html

If you want to code software to hack mainframe case 17 or 18 by yourself, you will find complete source code sample applications.

Have a special look for Chapter 16 - 'SAMP3 assembler language code'.

This sample describes the ACQUIRE functionality which is the key method to start active attacks for Case 17 and 18.

Phishing Program- Logic

Steps to complete:

1) Logon to innocent application
2) Store the welcome panel from innocent application (Enter USERID and Password)
3) OPNDST OPTCD=ACQUIRE to a list of innocent users. (This can be a whole TN3270 LUPOOL)

   Note: 'Acquire' has no effect on innocent users as long as they are logged on to their target application, it is just queued internally. As soon as the users log off, or if this session is terminated by any other reason, they are automatically logged on to the rogue application.
4) Send welcome panel.
5) Collect UserID and Password typed in by innocent users.

3rd Man in Middle Program- Logic

Steps to complete:

1) OPNDST OPTCD=ACQUIRE to innocent user. (This can be a whole TN3270 LUPOOL)

   Note: ‘Acquire’ has no effect on innocent users as long as they are logged on to their target application, it is just queued internally. As soon as the users log off, or if this session is terminated by any other reason, they are automatically logged on to the rogue application.

2) Logon to innocent welcome application

3) Collect UserID and Password and all subsequent data flows typed in by innocent users.

Most Dangerous Attack?

The German Government prohibits my disclosing details about that Hacking incident for fear that disclosure would make it easy for Hackers to attack mainframes using that method.
This is the only information I am allowed to give about that problem which affects all IBM z/OS Communication Servers, regardless of how their definition files are designed and how they are customized.

This Security gap allows hackers from inside or even from outside the target network to achieve

- all TCP/IP
- all SNA/APPN

Communication data flowing through the mainframes.

This security gap in combination with the latest security violation (Case16) which happened to a datacenter in summer 2006 can permit a disaster.

This also shows that the vulnerability of SNA / APPN becomes week by week worse even if nothing will be improved in SNA security. As more new technologies will become available and as more the world becomes interconnected.
Some samples are mainframes available on micro computers, WiFi, Internet, SNA on UNIX.
In other words **it does not matter if the terrorist comes by train or by plane**.

Summary and Call to Action

- If You Don't Use APPN, or If You Don't Connect to Other Networks, Then You Can Relax

- Else You Need to Address The Risks Outlined Here

- If You Want Further Information on:
  - Examine Network Software
  - On Demand Security Analysis
  - SNA/APPN Firewall
  - Sarbanes Oxley Validation for SNA/APPN

Please Contact: **www.net-q.com**