SNA Mainframe Security

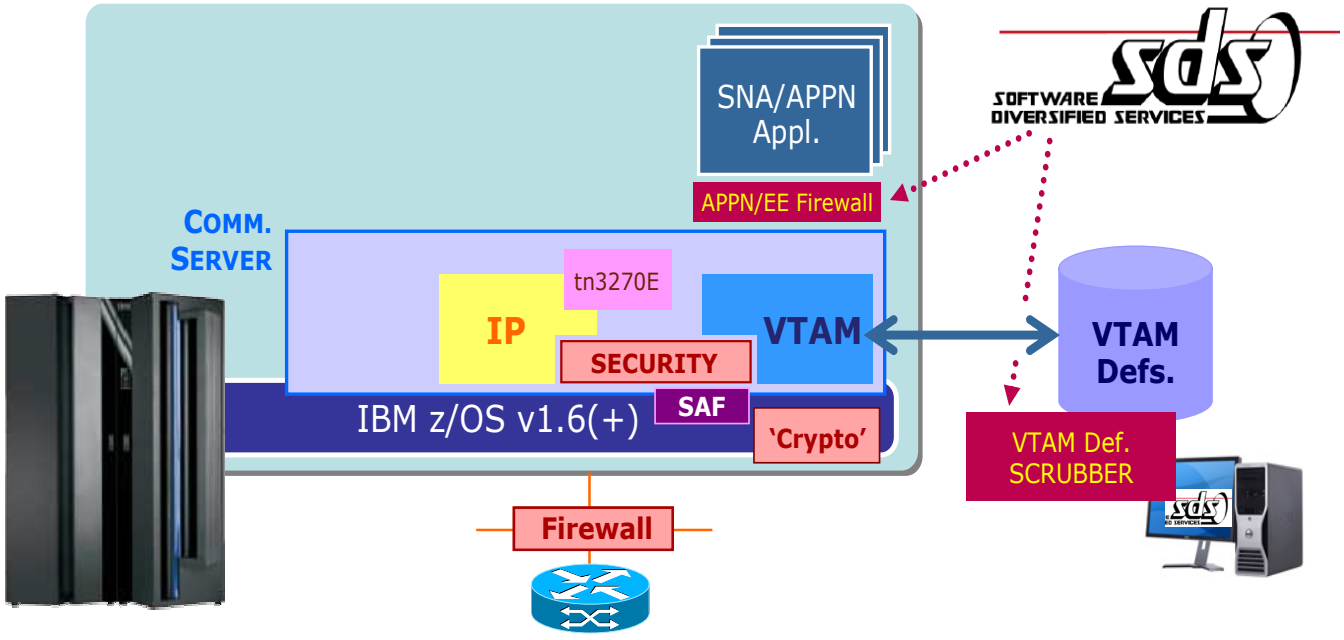
Because SNA isn't Hacked, Instead it is *INFILTRATED*

Hacking is for sport, infiltration is for gain

Software Diversified Services (SDS)

APPN/EE Mainframe Firewall & VTAM Definition Scrubbing from SDS

Internet firewalls are NOT designed to recognize and intercept SNA-specific, SNA-based threats to SNA mainframe applications. It is as simple as that.



Developed for SDS
by Anura ['SNA'] Gurugé
June 2009

www.sdsusa.com

Table of Contents

Key Acronyms

ACF2	(Computer Associates) Access Control Facility Mk. 2
APPN	Advanced Peer-to-Peer Networking
CP	Control Point
Do S	Denial of Service (attack)
EE	Enterprise Extender
FTP	File Transfer Protocol
HPR	High Performance Routing
IDS	Intrusion Detection System
IP	Internet Protocol
LU	(SNA) Logical Unit
MITM	Man-in-the-Middle Attack
RACF	(IBM) Resource Access Control Facility
SAF	Security Authentication Facility
SMF	(IBM) System Management Facility
SNA	Systems Network Architecture
SSCP	(SNA) System Services Control Point
VTAM	(IBM) Virtual Telecommunications Access Method

SNA Mainframe Security

Because SNA isn't Hacked, Instead it is *INFILTRATED*

Hacking is for sport, infiltration is for gain

SOFTWARE DIVERSIFIED SERVICES

APPN/EE Mainframe Firewall & VTAM Definition Scrubbing from SDS

That IBM's z/Center of Excellence, in 2008, would publish a 47 page manual entitled 'SECURING AN SNA ENVIRONMENT FOR THE 21ST CENTURY' *should have been a HUGE red flag.*

SNA mainframe applications are by no means immune to being compromised, and being compromised badly. Maintaining an ultra-secure, fully encrypted IP network, replete with state-of-the-art firewalls with intrusion detection, and insisting on 'clean' workstations running the best 'anti-threat' technology that money can buy, does not, alack, mean that your mainframe SNA/APPN applications are safe from infiltration. Nearly all of the ***current*** techniques being used to successfully infiltrate SNA mainframe applications are SNA-specific and SNA-based – with many being programmatic and artfully designed to interact with VTAM on a peer-to-peer basis.

Internet firewalls with their IP-orientation are not equipped to deal with these 'SNA Application Layer' threats. These threats also invariably go undetected by intrusion detectors, including the z/OS IDS, because they do not exhibit rogue characteristics. The current SNA threats are not from bored teenagers hacking for a 'hit,' but from seasoned professionals expertly infiltrating SNA applications for financial, political or espionage gain.

IBM, in addition to publishing the 47-page manual mentioned at the start, also did a *'SNA Security Considerations'* session at the March 2009, **SHARE** Conference in Austin [Session 3612]. That IBM in 2008 and 2009 is actively talking about SNA security should really be interpreted as more than a red flag, it is a clarion call. Other than about the dangers of SNA-over-IP (à la tn3270), unless measures such as SSL were being used, I do not recall IBM talking about SNA application security *per se* ten years ago, or fifteen years ago.

That was because SNA mainframes applications, primarily due to their reliance on physically secure private networks, were on the whole relatively immune to being compromised. But that has changed, and IBM, both in its manual and the SHARE presentation, point this out – upfront. SNA applications used to be secure, but not anymore. As for dealing with this new challenge, IBM strongly recommends capitalizing on as many layers of policy-based security as possible. **The APPN/EE Firewall and VTAM definition scrubbing product available from SDS is indeed a policy-based solution – designed to analyze and verify the validity of all SNA/APPN logon sequences via the intelligent and incisive application of sophisticated, context-sensitive APPN/EE-specific policies**. These provide an immediate, demonstrable deterrent to some of the threats identified by IBM and are consistent with the recommendations made by IBM.

At this juncture it is worth taking a minute to elaborate as to why IT departments, including most data center professionals, are not *au fait* with the current vulnerabilities of SNA mainframe applications. Simply put, there is close to zero publicity about SNA application compromise – which is what makes IBM's current initiatives both noteworthy and laudable. There are four primary reasons as to why we do not hear about SNA applications being compromised. These being:

1/ Enterprises that are compromised (which are invariably Fortune 1000 corporations or government agencies) do not, for very understandable reasons, want to tell the world that their mission-critical applications and databases were breached – particularly since in most cases they cannot accurately quantify the amount of 'assets' misappropriated and the volume of sensitive information exposed.

2/ There really are no dedicated, independent watchdog organizations that monitor and publicize SNA vulnerabilities, in marked contrast to all the groups and individuals that track threats to workstation software.

3/ Those infiltrating SNA applications, who are professionals engaged in what they perceive as a business endeavor, have no desire, whatsoever, to publicize their exploits – not only are they committing a crime, but the longer they can go without being detected the more they can 'steal.'

4/ Given the expert degree of stealth involved, many enterprises never realize that they have been compromised – or worse still, that they continue to be compromised.

So, that is the challenge facing us. Your mainframe SNA applications may have already been compromised. There could be data being siphoned off or rogue transactions being discreetly inserted even as you read this. Have you ever discovered, with a sickening thud in your stomach, that there was spyware on your PC? While we all now have decent 'anti-piracy' software on our PCs, the same is not the case when it comes to SNA mainframe applications – unless you decide, forthwith, to implement an APPN/EE firewall behind VTAM and install software that will scrub your VTAM definitions to eradicate known vulnerabilities.

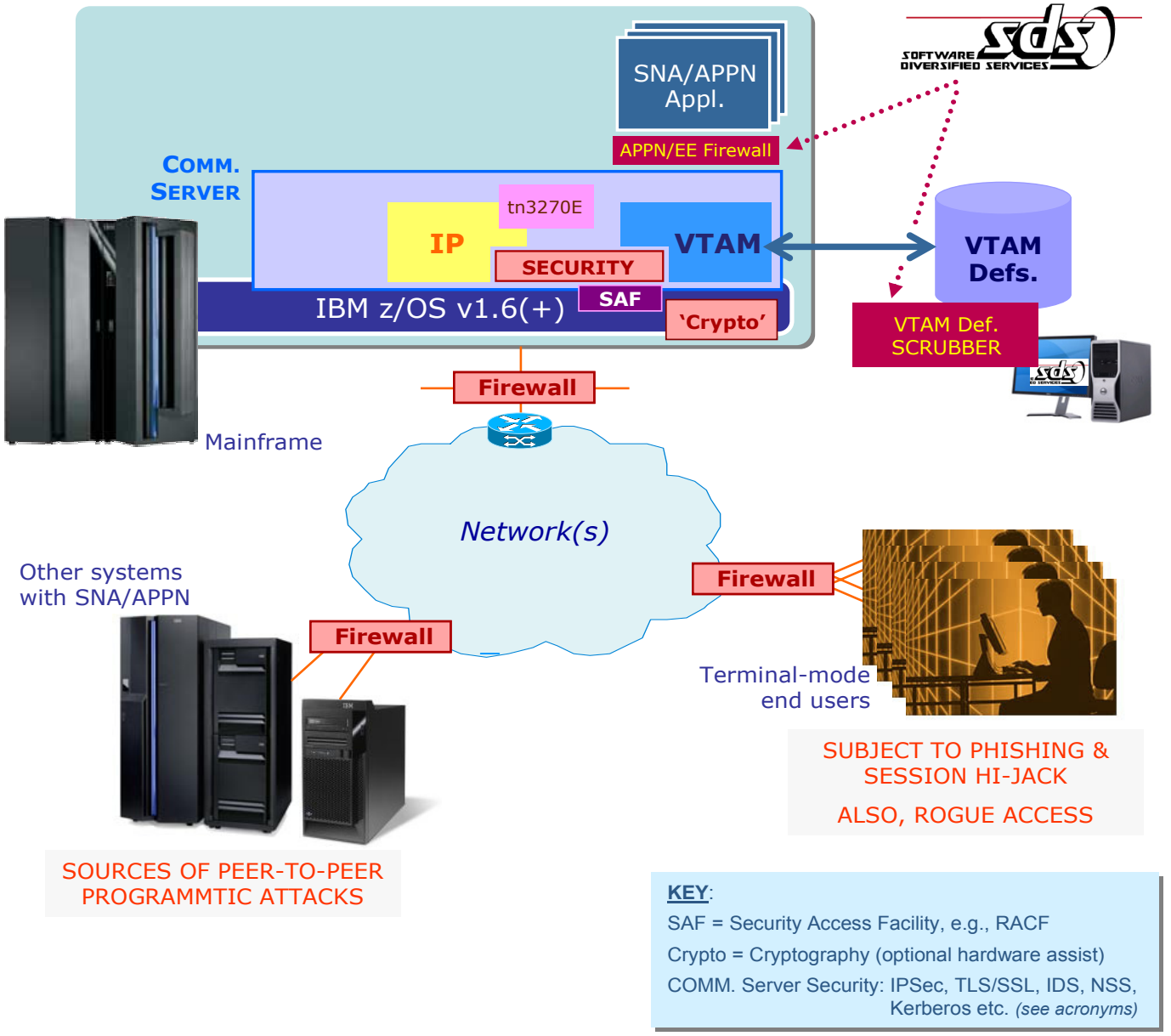


Figure 1: SDS's policy-based APPN/EE Firewall and VTAM definition scrubbing solution adds a much needed layer of SNA/APPN logon specific security to protect against mainframe infiltration.

Unexpectedness And Complacency Set The Stage

When confronted with the list of the currently known SNA mainframe threat scenarios it is easy to fall into the trap of going: *"Ah! That should never happen. You can fix that by doing this, that and the other."* This instinctive, knee-jerk reaction itself captures the challenge facing us. Yes, most likely, most of these vulnerabilities *could have* been fixed at their source when that SNA application was first implemented. But, what we do not know, unless we specifically test for it today, using the known attack methodologies, is whether the necessary safeguards are already in place. Practice versus theory.

If we take that saying about closing the barn door after the horse has fled, in this situation, the challenge facing us, right now, is determining not only whether that barn door is currently open or closed -- but whether it was properly installed, in the first place, to prevent the horse from being able to open it. To make matters worse, it is possible that this barn was never built, in the first place, to house animals as strong and smart as horses. I think you catch my drift.

A customer who recently implemented the **APPN/EE Firewall** discovered to their chagrin that because of some wrongly coded RACF parameters the administrator of a peer-connected Unix system could create userIDs and passwords for an SNA application. Now we all know that this particular vulnerability should never have come to be. But it happened, as accidents do – and was only discovered because the **APPN/EE Firewall** was able to automatically detect the incorrectly set parameters. IP-oriented firewalls cannot detect these vulnerabilities.

That SNA pre-Web was perceived to be invincible is now proving to be the major cause of its current vulnerabilities. Many of today's SNA mainframe applications were conceived in an era where security threats were very different to what they are today.

It is just as with air travel.

In the early 1970s, during the dawn of SNA, when it came to air travel, there were no metal detectors, X-ray machines or security checks. You never had to show an ID. You could travel under assumed names. Things are, obviously, very different today. The problem when it comes to SNA mainframe applications, however, is that we still haven't got around to installing all of the metal detectors, let alone the ID verification, as we should – and as we must. Think of the **APPN/EE Firewall** as that much-needed metal detector and the VTAM definition scrubber as a powerful, automated ID verifier for SNA mainframe applications.

The bottom line here is that so many of today's SNA mainframe applications were developed and implemented well before mainframe infiltration became a highly profitable, big stakes business. Consequently, these applications still have many

unplugged vulnerabilities. The problem is that today we have dedicated professionals, in some cases sponsored by what IBM politely refers to as 'unorthodox governments,' hell-bent on gainfully exploiting these vulnerabilities – to your cost.

SDS has the expertise and a **'Security Probing'** product that can be initially used to determine your level of exposure based on the currently *successful* SNA infiltration techniques. Given the sensitivity of what is being tested, this initial **SNA mainframe security audit** is best done as discreetly as possible, in a tightly controlled, self-contained environment. Thus SDS can help you conduct this audit on a test LPAR to avoid exposing your mission-critical production systems to even a trial infiltration.

The key here is to talk to SDS, ASAP. www.sdsusa.com.

As with any serious security threat, whether it is to a mainframe, Windows XP or to the homeland, it is best not to divulge all of the exact details as to how the threat works. Publicizing vulnerabilities could attract other 'vultures' to the scene. That is very much the case here. SDS, a long-time proponent of mainframe business, and a trusted IBM Partner, has made a conscious decision to *keep secret* the exact details of the known SNA mainframe vulnerabilities.

Bona fide SNA mainframe customers have to sign a non-disclosure agreement (NDA) so that the necessary confidentiality can be maintained for the mutual benefit of the entire mainframe community. Given the insidiousness of the attacks, and the nature of the professionals involved, this has to be a concerted community effort -- us '*mainframers*' protecting our beloved mainframes and maintaining their reputation for integrity. Hence, the discretion. Hence, the caution.

Consequently, in this White Paper, I too have to be somewhat vague as to how I describe these threats. We do not want this White Paper to provide the unscrupulous with ideas as to how to infiltrate SNA applications. I will tell you enough to convince you that the threat is real. Then you need to work with SDS to put together a security audit plan to see where you stand.

Fifteen Known SNA Mainframe Vulnerabilities.

SDS, working in conjunction with a strategic business partner who has been proactive in SNA mainframe security since 1995, has documented fifteen discrete techniques that are currently being used, *very successfully*, to infiltrate unprotected SNA mainframes. Precise details of how these attacks work, with network diagrams, data flows and references to the relevant VTAM 'features,' will be made available to you once SDS has established your credentials.

The fifteen documented threats fall into the following high-level categories:

1. SAF spoofing, whether it be RACF, ACF2 or Top Secret, whereby a mainframe SAF is led to believe that incoming rogue user logons have been authenticated by a 'trusted' partner SAF by inserting relevant credentials obtained through a technique known as 'BIND-scanning.'
2. SSCP or CP spoofing where a VTAM control point, *due to inadequate definition controls*, accepts rogue session initiation requests from an external system masquerading as an authenticated peer node.
3. Locating an old fixed function terminal [e.g., printer] defined to VTAM as a Type 1 Node and replacing it with a programmatic, Type 2.1 Node [e.g., PC with Comm. Server] that can send a peer-to-peer session initiate hoping that the existing VTAM definitions will accept and process the initiate thus providing a potential path into VTAM than can be further exploited.
4. Seeking 'holes' in SAF definitions that permit logons from peer systems to be accepted on the assumption that the logon was authenticated by a trusted SAF in the peer system, even though it was not – and then capitalizing on this unauthenticated access by trying to obtain administrative rights on the target mainframe.
5. SNA-specific variant of the active eavesdropping-based, 'Man-in-the-Middle' (MITM) attacks that have been used on the Internet where the attacker gets between two *bona fide* SNA systems and intercepts all the data flowing between the two.

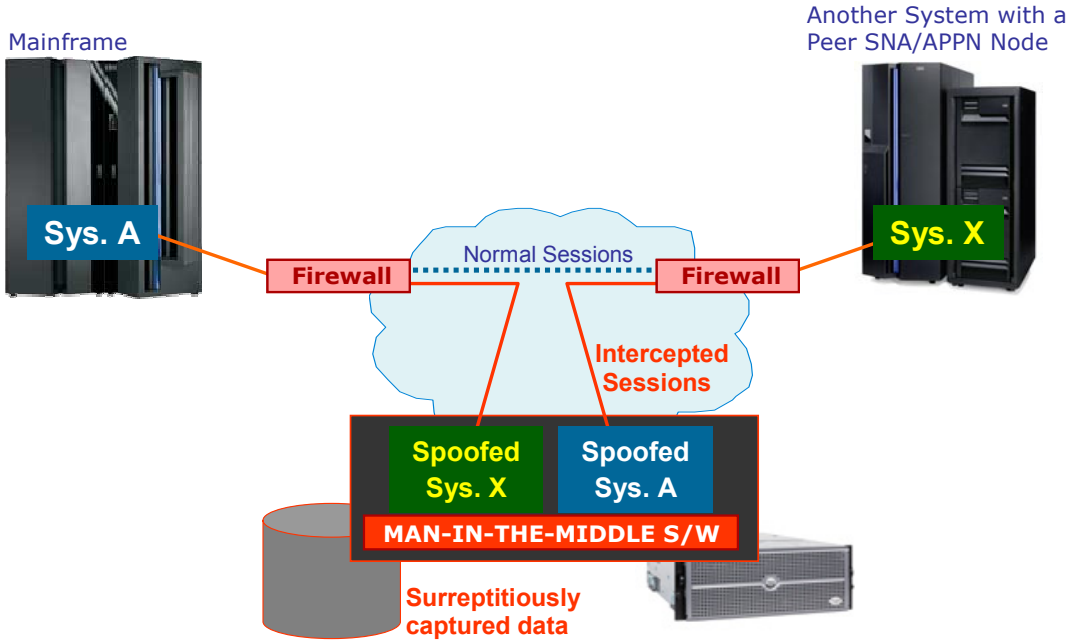


Figure 2: The basic notion of a 'Man-in-the-Middle' attack in the context of SNA mainframes.

6. A variant of the 'Man-in-the-Middle' (MITM) attack scenario when specific SNA applications (or session partners) are spoofed as opposed to the entire system (per the configuration shown in Fig. 2).

7. A variant of phishing, with elements of denial-of-service (Do S), whereby terminal users frustrated by not being able to logon to a desired system end up typing in userIDs and passwords into bogus logon screens hoping to establish a connection.

8. 'Session forwarding,' another variant of the 'Man-in-the-Middle,' this time exploiting the dynamic resource search capabilities of APPN/HPR given that the protocols used in these searches contain a wealth of 'address' information pertaining to both the source and destination in their headers.

9. Attempted session capturing with queued, pending session initiation requests – awaiting a session termination that might activate the queued request.

10. 'BIND-scanning,' mentioned in #1 above, is an SNA/APPN-specific variant of the oft practiced 'Port Scanning' attack used in IP networks to programmatically locate open, unsecured host ports – with infiltrators, in the case of SNA, intercepting and analyzing as many BINDs as they can find to determine if a target SNA mainframe application may accept rogue BINDs with a less secure 'mode entry' profile.

11. Expert and precise use of denial-of-service (Do S), to one or both ends of a networked system, hoping that the added load on the systems might expose infiltration opportunities; e.g., vulnerabilities caused by buffer overflow or credentials exposed in an obscure, not often seen error message to do with the unexpected session rejections precipitated by the Do S.

12. NetID spoofing, with the aid of Type 2.1 node emulation software (e.g., Microsoft's Host Integration Server (HIS) or IBM's Communications Server), in some instances exploiting Wi-Fi wireless connections, whereby a rogue system masquerades as a valid node within a known network.

13. Sophisticated, SNA application specific phishing, sometimes by actually tapping into the SNA side of a data center resident tn3270(E) server, to programmatically harvest large volumes of valid userIDs and passwords that can then be used to infiltrate applications without any push-backs from SAF.

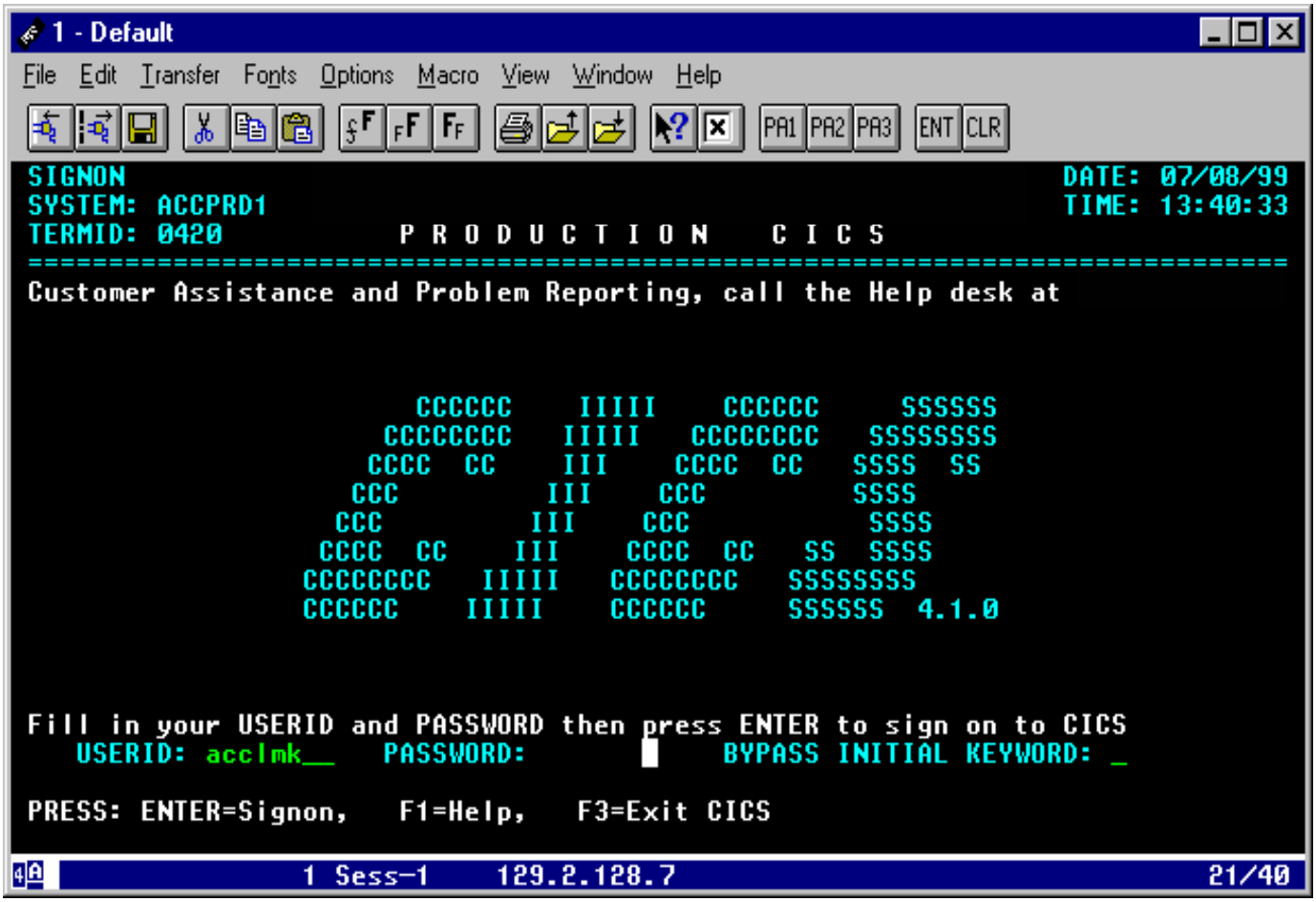


Figure 3: Quintessential, 'nothing-but-text,' logon screens such as this from SNA mainframe applications, devoid of any logos, graphics or topical news stories, can be easily replicated by professional infiltrators to mount very effective phishing attacks to harvest valid userIDs and passwords.

14. Session hijacking by monitoring session timeout intervals and faking a timeout at the remote end and diverting still active mainframe session to a rogue end point (typically a PC with Type 2(.1) node terminal emulation software).

15. Mainframe application replication (à la PC virus schemes), typically in conjunction with session hijacking as described in #14 above, and then masquerading as a *bona fide* application interacting with real end users and trying to submit bogus transactions to other applications on a trusted, peer basis.

Some Background To The Attack Scenarios

Exactly how a professional infiltrator will unleash these attacks against a specific mainframe environment will obviously depend on numerous criteria and will vary

from one target to another. Invariably the attacks are painstakingly customized for each system targeted to best exploit the perceived (or known) security vulnerabilities of that system. It is also important to keep in mind that the SNA mainframe application specific attacks might not be included within the opening rounds of offensives launched against your system.

As IBM and others repeatedly point out, your IP network, despite all of 'batten-down-the-hatches' technology available, may still be your weakest security link. Then there is always tn3270(E) and FTP – particularly if you are not using the necessary precautions. The attacks may be launched per a well laid out campaign spanning weeks, if not months, starting with the IP network.

Once infiltrated, the malicious activity, like spyware on a PC, could be ongoing for protracted periods of time. Take a successful phishing attack as an example. Once the perpetrators harvest a batch of valid userIDs/passwords, they can use these to repeatedly gain access to the target application without in any way rousing suspicion. If the goal is surreptitious eavesdropping for commercial or political espionage, this activity could go on for a long time until the password comes due for renewal.

[These valid credential-based, rogue logons are likely to be detected by the policy-based **APPN/EE Firewall** which will spot any changes in 'incoming characteristics' or 'logon behavior' (e.g., changes in logon times). The APPN/EE Firewall can also facilitate powerful ***session auditing*** by generating **SMF** records journaling each session start and session end. This SNA/APPN session specific auditing, combined with a suitable script, will enable you to quickly establish if there are any incongruous logons that should be further investigated. It is SNA/APPN-specific auditing capabilities such as these that will, in future, let you sleep soundly at night without recurring nightmares about infiltrators.]

Professional infiltrators will invariably try to pick the easier 'locks' first. So they are likely to start with the IP network, tn3270(E) server and any other Web-to-host 'gateways' you may have. In some cases they might need to tap into the IP network to obtain userIDs/passwords, NetIDs, BIND parameters or screen formats they need in order to launch an SNA mainframe attack. In some instances they might combine network infiltration with a mainframe infiltration method to maximize their haul.

There is also a possibility that multiple categories of SNA mainframe attacks may be launched against the same mainframe, serially or in parallel. What is crucial to note is that these attacks, in marked contrast to what is often the case with attacks on Windows, are not being done for sport, publicity or vandalism. Given

that they are done for gain, the attacks will be carefully planned, very deliberate in their nature, and well orchestrated when it comes to execution. There are unlikely to be any warning signs beforehand. These professionals do not launch exploratory probes against the target system. They have test systems that they use for that type of testing and staging. Consequently, intrusion detection systems typically do not notice any suspicious activity prior to an attack. Hence the need for an intelligent, incisive, policy-driven **APPN/EE Firewall** (with auxiliary SMF-based session auditing) to try and intercept these very insidious attacks.

These professionals also try hard not to leave any traces of their attack. Usually somebody discovers that something is missing or is not right. But most times the experts have to surmise how the attack came to be – was it a session hijack, 'Man-in-the-Middle' (MITM) or phishing? Often, it is hard to tell. So the goal, in all cases, is to try to proactively prevent the attacks from taking place by implementing the relevant technology to block all of the currently known attack scenarios. That means closing the newly strengthened barn door, with its heavy-duty lock, before the horse gets any ideas about stretching it legs.

That, Unfortunately, Is Not All

The fifteen malicious infiltration techniques categorized above are, unfortunately, not the sum total of the SNA mainframe application vulnerabilities now being regularly exposed. It can now be divulged that over the last five years, there were several instances of users (in some cases 3rd party customers) or company employees accidentally stumbling upon major security loopholes in SNA mainframe applications. In some of these instances the vulnerability had to do with inadequate data access security when it came to the partitioning of sensitive data being maintained by a single SNA application.

In one case, two competing financial services corporations, both subscribing to a 3rd party SNA mainframe application, discovered, to their initial glee, that they could 'eavesdrop' on the activities of their competitor – each believing, however, that this was strictly a one-way loophole, and that the other was not able to spy on them. Suffice to say things soon turned very ugly when both parties discovered to their mutual horror that each had been eavesdropping on the other. But, there was unanimity on one crucial issue – they, for obvious reasons, wanted a total embargo on any publicity pertaining to this breach. There is a possibility that this breach may have violated some laws – but a court case was the last thing that anybody wanted.

So yet again, the desire for secrecy, when it comes to any and all infractions involving mainframes, prevailed. But there is a definite downside to this secrecy. It, at a disservice to others which includes you and me, continues to foster that complacency about SNA mainframe applications being immune to compromise – when, in reality, they are not. If the mainframe world was not such a 'closed community,' so to speak, people would genuinely claim that this was indeed a conspiracy!

Then there is the always thorny and sensitive matter of intentional sabotage by disgruntled employees. In this unsavory arena, we, if you stop and think about it for a second, are now in the midst of 'THE PERFECT STORM' when it comes to SNA mainframe applications. So many of the enterprises so greatly impacted by the recent mayhem in the global financial sector are by and large blue-chip mainframe customers! We have all heard of the layoffs. We know the names of the once mighty corporations that have suffered, the mergers that have occurred and the data centers that have gone dark.

In the case of SNA mainframe applications there is also another pivotal factor that exacerbates matters even further. The knowledge required to detect a potential sabotage is restricted to a very small, specialized group of 'veterans.' Most enterprises no longer have too many of these 20 plus year 'Sys. Progs.' Who really do know all the ins-and-outs of SNA/APPN and VTAM. Of late many have opted to retire. Some, unfortunately, got caught in the mayhem. But the bottom line here is that there are a lot of disgruntled data center folks out there, and not enough qualified 'good cops' to keep them all at bay. And this, alack, gets worse, though I really don't want to start getting into specifics here.

We have all heard the stories about the dedicated 'mainframers' who have preserved an old rescued mainframe in their basement or garage. But today you don't need an old mainframe, let alone a decent size server, in order to mount a subterfuge attack on corporate data assets masquerading as an 'in-network' peer node. You can run a fairly effective mainframe emulation on a $799 laptop. Plus, in today's world of APPN/HPR and EE, you don't need to have an SSCP capability in order to wreak havoc. Just a Type 2.1 node will suffice – and you can even get freeware 2.1 emulations for Windows, Linux and Unix.

So this is the challenge. The stakes are inordinately high. A lot can be gained, financially and politically, by infiltrating SNA mainframe applications. Hence why this is a business – a very lucrative business at that. The ever increasing disgruntlement among the data center community increases the pool of prospects that can be tempted into discreetly leaving open a 'back door.' At the

same time, the pool of experts with the requisite arcane VTAM know-how is on the decline – with some already among the disgruntled! And to cap it all, nobody wants to tell the world that their mainframe was compromised. Misplaced complacency, thus, continues.

But at least you are reading this White Paper.

The Call For Action Re. SNA Mainframe Applications

The best course of action when it comes to further securing your SNA mainframe applications is to follow the adage that goes: 'forewarned is forearmed.'

The first thing that has to be done forthwith is to get a much deeper understanding of the currently documented attack scenarios. What I have described here is but an outline. SDS has presentations and documents with the pertinent technical details, such as the **OPNDST** statements that may be used, the exact step-by-step process of an attack scenario and the reference numbers of ***IBM SNA programming manuals*** used by the professional infiltrators to develop their attack software. SDS will also help you identify and establish the different **'security spheres'** you may need to protect – depending on which categories of attacks you are likely to be vulnerable to.

The 'security spheres,' in essence, deal with the potential span of an SNA/APPN session. An LU 6.2 session between two SNA/APPN Appls. running within the same LPAR is likely to be considerably more immune from attack than say a LU-LU Session Type 0 that spans two autonomous SNA networks (via say SNI or an Extended Border Node). SDS, in conjunction with a strategic technology partner, have identified six 'security spheres' in the context of the fifteen attack scenarios described above – with a categorization of which 'security spheres' are vulnerable to each of the fifteen types of attack. For example, 'SSCP or CP spoofing' (the #2 scenario) can not occur if a session is contained within a single LPAR. This is also true for scenarios #1 and #3. But these attack scenarios are possible in the other 'security spheres,' including sessions contained within a Parallel Sysplex or an in-house intranet.

Once you have contacted SDS and have established your *bona fides*, you can immediately start working with qualified SDS staff to scope out exactly how vulnerable your SNA mainframe applications are – at present. At this juncture, I will remind of you of my earlier observation. It is easy, even natural, to look at the list of documented vulnerabilities and claim that there is no way that any of these attacks will succeed against your systems. You could, very well, be right. There is also a possibility, however slim, that your faith and optimism is misplaced.

Remember that in today's society you can never totally rule out the possibility that you have been 'sold down the river' by a disgruntled employee. The VTAM definitions that you were sure are as watertight as possible may have been tampered with to permit infiltration.

Given what is at stake, and the insidiousness of the attacks, you really cannot take a chance here. Have you ever done a full-scale, bleeding bodies on the ground, disaster recovery (DR) drill? So many seasoned IT professionals used to be so confident about the absolute infallibility of their DR scheme – until that first real drill. DR, particularly since 2002, is now on a different plane. We now have to do the same when it comes to SNA mainframe application security.

SDS, as previously mentioned, will also be able to set up realistic probe scenarios that you could use against a test configuration to determine, unequivocally, the vulnerabilities of your SNA systems vis-à-vis the known threats. By this stage you probably would have decided that implementing the **APPN/EE Firewall** (with its auxiliary SMF-based session auditing) in conjunction with the **VTAM definition scrubbing** is imperative – with time being of the essence. This is like buying insurance. It is difficult to calculate the immediate ROI, but we all know that the real returns are going to be HUGE.

The Bottom Line

That SNA mainframe applications are in some way magically immune to being compromised is now, alack, but a myth. Yes, it is true that SNA mainframe applications used to be secure fifteen to twenty years ago – but that was in a different era. In those simpler days, you could fly without having to put your shoes through an X-ray machine, buy goods with a credit card without the vendor having to instantly verify your card with an online terminal or check into a hotel without having to produce an ID. Things have changed, and in this instance not for the better.

That the transition, in the late 1990s, from mainly private, leased-line networks to IP network technology (with tn3270(E)) created numerous security exposures was well known. Much was done, particularly in terms of powerful, end-to-end encryption and user authentication (e.g., with SSL/TLS), to minimize if not totally eradicate these IP-network related vulnerabilities – but, obviously, this was totally contingent on enterprises implementing all the necessary safeguards. It is sobering, though, that IBM still cites lack of IP-network security as one of the major threats facing SNA customers.

Since 2008, IBM appears to have noticeably ratcheted up its advocacy when it comes to SNA mainframe application security. That it published a 47-page

manual entitled *'Securing an SNA Environment for the 21st Century'* and did a session at the March 2009 SHARE Conference on a similar theme is highly noteworthy. Let's face it. Despite its continuing strategic importance to customers, from IBM's perspective SNA/APPN is in 'end game' mode.

That IBM has suddenly started emphasizing SNA security, when there is really no SNA/APPN specific R&D effort *per se*, is telling to any seasoned 'IBM watcher' – and I will confess that I do fall into those ranks. That is why I agreed to write this White Paper. There is a real and present danger. Given my 35-year association with SNA, it would have been remiss for me not to use my platform, however rickety, to share with you what I have learned of late.

The fifteen attack scenarios described above are plausible and potential. I have seen some of the documentation. Though I would very much like to do so, I cannot directly share this documentation with you. So you have to first talk to SDS. If you are reading this, there is a fairly good chance that you have already had prior interactions with SDS. They are committed to mainframe solutions. They have been serving the mainframe community for a very long time.

The policy-based **APPN/EE Firewall** (with SMF-based session auditing) and the companion **VTAM definition scrubbing** definitely plugs a hitherto unprotected opening in SNA mainframe security. Today it is nearly impossible to implement an IP-network without some kind of firewall – even Windows has a built-in firewall. Thus, it makes sense to have an APPN/EE-aware firewall, running above VTAM, that can be finely customized with policies specific to your configuration. Hence, this recommendation.

So the bottom line here is rather simple and straightforward. Contact SDS, www.sdsusa.com, and tell them you want to find out more about SNA security. The ROI of this call, alone, could be great.

Selected Glossary

APPN	A landmark 1986 rework of the original SNA architecture to enable plug-and-play, peer-to-peer networking unhampered by centralized control from a mainframe.
BIND	The SNA/APPN command used to activate an LU-LU session following the successful completion of the SNA/APPN session initiation processing.
Comm. Server	IBM's all inclusive, multi-platform, software bundle that provides a plethora of terminal emulation, Web-to-host and networking capabilities.
Control Point	SNA/APPN/HPR functionality that performs authorization, directory services and configuration management.
Denial of Service	An insidious, carefully orchestrated attack on computer systems or networks to overload their resources with a barrage of requests in the hope of discovering overload induced vulnerabilities within the targets or to just disrupt the mission-critical activities of an enterprise.
DLSw	Widely used SNA/APPN(/NetBIOS)-over-TCP/IP transport mechanism which, however, unlike EE, does not support SNA COS or routing.
EE	HPR-over-UDP/IP, created by committee and codified in RFC 2353 in 1998, which permits SNA/APPN networking, replete with native COS and routing, across IP networks.
Firewall	Specialized software designed to prevent unauthorized access to a computer system while permitting validated, non-harmful interactions to get through.
HPR	An SNA architecture developed by IBM in the early 1990s to imbue SNA/APPN with dynamic alternate routing, nimble intermediate node routing and proactive congestion control in order make SNA networking more competitive with TCP/IP.
Intrusion Detection System	Intelligent systems that attempt to intercept unauthorized access into computer systems or networks by proactively monitoring suspicious activity based on previously identified policies.
IP	The primary, underlying, connectionless protocol which is the basis for all Internet Protocol Suite based networking.
LU	SNA's software interface (or 'port') through which end users gain access to the SNA network.
LU 6.2	SNA's protocol suite for program-to-program communications.
Man-in-the-Middle	Data siphoning scheme where fraudulent software manages to insert itself, undetected, between two network partners by actively emulating the two partners being deceived.
Node	In SNA, a total unit of network-attachable functionality, realized in software, that gets implemented within a device or runs on a computer.

Phishing	A malicious scheme to obtain the credentials necessary to access a secure system by masquerading as that system and fooling people into entering the sought after credentials.
SAF	Security Authentication Facility; e.g., RACF, ACF2 or TopSecret.
SSCP	SNA's System Services Control Point, in an hierarchical network, typically implemented on a mainframe within VTAM, that is responsible for directory services and configuration management. Now superseded by the peer-to-peer oriented functionality of APPN/HPR control points.
tn3270(E)	Widely used, client-server technology that permits TCP/IP clients to access mainframe-resident SNA applications using 3270 data streams.
Type 2.1 Node	A peer-to-peer capable node in SNA/APPN that has since evolved into APPN end and network nodes.
VTAM	IBM's mainframe-based software for implementing an SNA/APPN/HPR node within an LPAR.

Software Diversified Services

Software Diversified Services (SDS), [www.sdsusa.com] based in Minneapolis, MN, has been providing premium mainframe solutions to the IBM world since 1982. It currently has in excess of 1,000 mainframe customers worldwide.

SDS' mainframe product repertoire now includes over twenty z/OS, VM and VSE products, with the highly regarded Vital Signs VisionNet IP Monitor (VIP) being one of these. SDS also markets PC software related to mainframe operations. The products marketed by SDS focus on network management, performance monitoring, report distribution and data compression.

SDS is noted for having the highest quality software, documentation, and technical support in this industry sector. SDS technical support has been rated #1 by the prestigious IBEX Bulletin.

The Author

Anura Gurugé [www.guruge.com] is an ex-IBMer who used to be 'Mr. SNA' for the longest time. His first book, *'SNA: Theory and Practice'* was published in 1984. He was heavily involved with Token-Ring switching, APPN, Frame Relay and Web-to-host.

These days he is a consultant and a professional writer. His latest book, critically acclaimed, is *'Popes and the Tale of Their Names.'*

He can be contacted at (603) 455-0901 or anu@wownh.com.