Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Return to Legacy Security

This paper examines three mainframe security systems (Computer Associates' ACF2 (Access Control Facility, Computer Associates' Top Secret, and IBM's RACF (Resource Access Control Facility) to relate how they can be used as security servers for multiple operating system environmentsz.

Copyright SANS Institute
Author Retains Full Rights

AD

A Return to Legacy Security

Christopher Abramson
Version 1.2e
July 27, 2001

Introduction

Everyday we see more and more security breaches happening on networks all over the world. We as security people continue to fight this at every turn of the road. The underlying factor is that the systems that hackers prey on are the network operating systems. Microsoft Windows NT, Microsoft Windows 2000, Linux and Unix are all very susceptible; hence the need to secure them is of the utmost importance. Unfortunately, fighting the growing security problem on these operating systems is almost impossible. As security organizations and personnel come up with solutions, there are people out there figuring out ways to by pass these solutions.

Security administrators fight viruses, intrusions and on many occasions' people in there own companies, to try to protect their companies' network. What if you were told there is a security product available that has proven itself for over 30 years. The proof is in the companies that run these security systems. A PKI style setup or a PC security system is not the point of this paper. The point of this paper is mainframe security systems. Namely three products:

- Computer Associates' ACF2 (Access Control Facility 2)
- Computer Associates' Top Secret
- IBM's RACF (Resource Access Control Facility).

These are some pretty old security systems, but they have proven themselves over time as effective security systems. "Love it or hate it, the S/390 is likely to be with us for many years. Not at the bleeding edge of IT, I grant you but as a trusted repository for 80 percent of the world's business-critical data." sites Mark Lillycrop in his article The Mainframe: A strategic Platform for the future[1]. Companies all over the world are reevaluating the roll their mainframes are playing in their business. Companies are finding that many e-business systems can be successfully run on OS\390 and z\OS systems from IBM.

One thing that these security systems all have in common is that many companies have been running them for many years. The people who maintain these security systems swear by them. Each one is unique in the way that it secures the mainframe.

The purpose of this paper is not to prove that these systems have done the job they have been doing for over 30 years, which is securing the mainframe. The goal here is to show how they can be used as security servers for multiple operating system environments. Let us start off with a little history for those who are not familiar with this class of security software.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

A Brief History of Mainframe Security

IBM first created the RACF security system for the MVT operating system in 1976. The following historical information was found on the IBM web site at http://www-1.ibm.com/servers/eserver/zseries/zos/racf/racfhist.html

"September, 1976, Version 1 Release 1

- User identification/verification
- Data set authorization checking
- Journalizing "[2].

These were some of the high points of the RACF system at the time. As you can see, when IBM first decided to create a security system the only things that were necessary, were to provide user identification and verification, which at that time was sufficient security for the mainframe environment. The unfortunate thing about RACF was that it provided security only if it was installed and configured, in other words, RACF was not secured by default. It was up to security administrators to secure all resources on the system.

ACF2 however was a much different story. A Company called SKK, located in Illinois first released ACF2 in 1978. The writers of ACF2, Barry Schrager, Scott Kruger and Eberhard Klemens utilized what they knew about security and IBM's MVT operating system and created what became ACF2. In talking with Mr. Klemens, he explained what ACF2 provided at the time, "ACF2 had the same functionality as RACF. It provided user verification and identification, journaling and data set authentication. Where it was different was that ACF2 provided security by default." [3]As you can see ACF2 is not significantly different from RACF, but different enough to make it viable as a standalone product. ACF2 has changed hands over the years. SKK no longer exists as a separate company. They were purchased by another company called Ucell. In 1987 Ucell in turn was purchased by Computer Associates, giving Computer Associates ownership of ACF2.

ACF2 is not the only mainframe security system that Computer Associates owns. They own another system called Top Secret. Top Secret made its debut in the mainframe market in 1980. Originally Top Secret was a product of Cap Gemini Allen. Computer Associates acquired Top Secret from Cap Gemini Allen.

A description on Computer Associates web site at http://www3.ca.com/Solutions/Product.asp?ID=180 states that, "Top Secret enables controlled sharing of your computers and data, with features that prevent accidental or deliberate destruction, modification, disclosure and/or misuse of computer resources. It allows you to control who uses these resources. Unauthorized attempts to access resources are automatically denied and logged. Any authorized use of sensitive resources may also be logged for subsequent review. "[4]

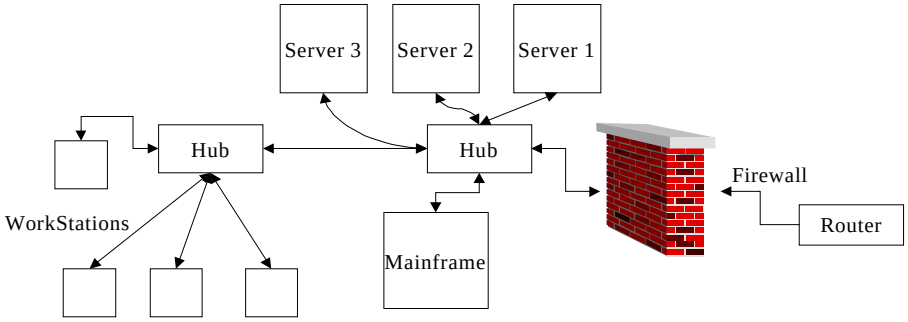
© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

One thing that is not mentioned above, that should be made clear is that Top Secret works like ACF2, in that it provides security by default. The only way to gain access to a resource is to have access granted by the security administrator. The above discussion sums up the history of mainframe security systems. Now that the reader has an idea of the history behind mainframe security systems, the remainder of the paper will explore how they can help enforce security in today's network oriented environments.

The Network As It Is Today

The introduction to this paper has shown that mainframe security systems have been available for a relatively long time. They have added value as a security system to companies all around the world. Now let's take their use as a security system a step further and apply them to network systems. The following diagram shows the network system in any typical company. This diagram includes the company's mainframe.

Diagram A.



As the reader can see, the network connection enters via the firewall. The firewall may filter or protect this company from some network vulnerabilities. However, it is still necessary to enable security on the companies' servers, mainframe and workstations. The need to enable the additional security is best described in an article by Luca Bertagnolio entitled, Security on the Network: What You Really Need to Know. Bertagnolio states, "How can I make my network 100 percent secure? The simple answer to this is that you can't. The security solutions available today offer risk management only. This means minimizing the vulnerabilities of, and threats to, the network."[5]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The author agrees with Bertagnolio's statement. It is the author's opinion that today security is about managing the risks to our systems. A vigilant watch must be kept using logs, network scanning tools and Antiviral scanning to protect our systems. Protecting our networks means knowing the Who, What, When, Where, Why and How. Who is accessing our networks? What are they doing on the network? When did they access the network? Where did they access the network? Why did they access the network? How did they access the network?

The above six questions should be asked by any network administrator or security administrator if they are to determine if the person accessing their network is an authorized user of the system. Without asking these types of questions network and security administrators are bypassing the very first step of good security, planning.

The next section shows how a mainframe security system can be used to help control the above situation.

Security by Legacy

Let us now take a look at an alternate view. The following diagram shows the same network rearranged to make the mainframe the security gateway.

Diagram B.

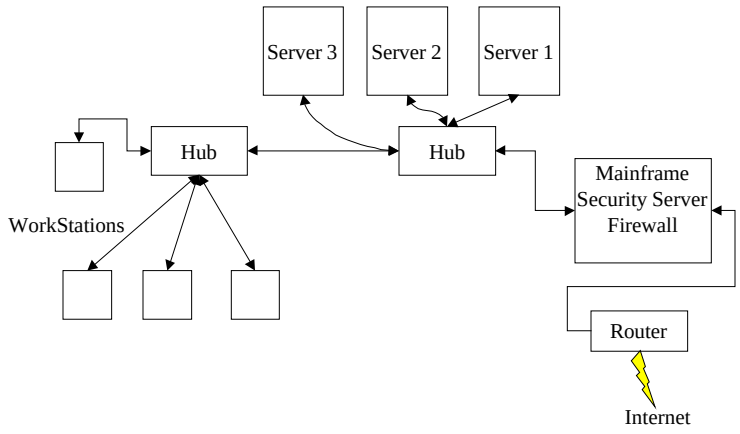


Diagram B shows how the mainframe can become the security gateway for the network infrastructure for any corporation that has a mainframe computer. The best way to look at this is by analyzing the six questions from the previous section.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

First, who is accessing our network? For over thirty years mainframe security systems have been the guard at the front door for the mainframe. The security system has been logging every single access for all that time. All three security systems discussed in the Introduction have been providing logging and reporting information about who has accessed the mainframe systems for years. Those same mainframe security systems can now record network traffic also. This means that mainframe security products can be used to provide the necessary information for security administrators.

Third party products have added to the logging and reporting features of the mainframe security systems by making logging easier, or by formatting reports so that they are easy to read and understand. If the security system is designed so that user access all systems including network and desktop systems is via the mainframe, logging user access and use would be easy for administrators to log, report and analyze.

Second, what are they doing on the network? Again, the logging and reporting capabilities of the mainframe come into good use. We can see explicitly what it is that the user is doing on the network. Are they accessing every server or just one server? Is the user accessing data that they should not be accessing? **Third, when did they access the network?** At what time did the user access the network, early in the morning or late at night? Security administrators can watch how long a user was logged on for. If a user was logged on for an amount of time that was unnecessary the user can be questioned about it.

Fourth and fifth, where and how are two questions that go hand in hand? These questions ask if the user is valid or not. If a user is accessing the network secretly via a port that was accidentally overlooked, obviously they are accessing the system illegally. **Sixth, why did they access the network?** With the capabilities of the mainframe this question can be easily answered. Information supplied by the security capabilities of the mainframe will tell the administrator whether or not the user logged on, were they there to work, or to play on the system.

Mainframe and Network Security Integration

Now how do we integrate the mainframe with the network so that we can do what has been proposed. Well, fortunately the mainframe has come along way since the beginning. IBM has provided an environment on the mainframe called Unix System Services. Unix System Services provides the security administrator with an environment that allows them to run services like firewalls, Virtual Private Networks, LDAP and digital certificates on the mainframe. With these tools the administrator can now use the mainframe as a security server and firewall.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

"Successful security requires many components, among them strong hardware isolation and system integrity to ensure that misbehaving or malicious applications and users cannot affect other applications or users, system level security to control and monitor the actions of users and applications on the system, network-level security to protect your system from outside attackers on the Internet, and transaction-level security to provide protection for business transactions on the Internet. " As stated on the IBM web site, http://www. -1.ibm.com/servers/eserver/zseries/zos/security.[6]
Security must still be divided out to protect the proper information on systems. So let us talk about security provided by the mainframe. Well we know that User ID and Passwords have been a mainstay of mainframe security since it was created. Another emerging tool in user identification is a digital certificate.

IBM has within the last two releases of RACF been providing identification for digital certificates. Computer Associates provides access via digital certificates in both ACF2 and Top Secret. Digital Certificates provide a unique function, they allow a user to access a secure once and only have to authenticate once. The digital certificate is stored in a mainframe user profile in the security system. When the user accesses data using the digital certificate, the mainframe security system grants that user access based on their profile. If your profile or security access does not match you are not granted access. The key here is that the profile being used is the strong RACF, ACF2 or Top Secret profile. An security administrator can double up on security by requiring an User ID and Password if necessary also. Well we have authenticated this user, but the user needs access to some information off of the mainframe. How do we authenticate him outside of the mainframe environment, because UNIX and Microsoft platforms do not understand the security databases of the mainframe.

LDAP combined with the security capabilities of ACF2 and Top Secret allows security administrators to maintain users across multiple platforms. "The new releases include the eTrust LDAP (Lightweight Directory Access Protocol) Server, enabling CA-ACF2 6.4 and CA-Top Secret 5.2 users to take advantage of the industry-standard LDAP protocol to query and update mainframe security information for use on distributed eBusiness systems. IT administrators will also be able to leverage the authentication policies established within their CA-ACF2 and CA-Top Secret implementations and apply them to any enterprise and/or eBusiness application using TCP/IP." As stated at the site http://www.itsecurity.com/tecsnews/jun2001/jun26.htm[7]. Instituting LDAP gives the security administrators the ability to define their users across multiple platforms. The advantage is that security administrators have not sacrificed strong security authentication via the mainframe. Users are held to the same security rules on their server systems as they are on the mainframe systems.

Allowing users to access systems and maintain their information is just one security function that is required. What about keeping out users that do not belong? One thing the author knows the mainframe is very good at is access control. If the person trying to access the mainframe does not have a valid User ID and password, that person is not getting on the mainframe. ACF2 and Top Secret allow access based on security rules

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

written by security administrators. RACF secures users via profiles containing information about the user. Users are then assigned to groups that grant them access to resources or applications. The point of this statement is to show that to access any resources via the mainframe the user must be a valid user on that system.

What about keeping out those who do not belong on the mainframe? Well for mainframe resources and applications, if that person does not have a User ID and password they will not be allowed to gain access.

The mainframe also needs to protect services that do not require user information. This is where the firewall comes into the picture.

As at the IBM website, http://www-1.ibm.com/servers/eserver/zseries/zos/firewall/whatisfw.htm , "OS\390 Firewall - The defense secure enough to protect a corporation's information on the platform recognized for reliability and scalability. OS/390 Firewall Technologies:

- Keeps your intranet secure from intrusion with Socks and FTP proxy servers
- Controls traffic through your network according to your specifications using IP filters
- Allows secure communications across a non-secure network using IP Security (IPSec)
- Works with RACF or other External Security Manager already on your OS/390 system
- Logs network activity and can work with SMF to complete your existing system security.

For many of our customers, IBM's OS/390 Firewall Technologies provide the basic firewall capabilities on the OS/390 platform to reduce or eliminate the need for non-OS/390 platform firewalls. The Firewall Technologies functions offered on OS/390 support the logging of information that could be used to perform security audits. The Firewall Technologies function included in the SecurewWay Security Server are:

- An ftp proxy server
- A version 4 socks server
- An ISAKMP server
- A Graphical User Interface (GUI) client and configuration server
- A command line interface "[8]

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Originally the mainframe worked on small internal company networks. Today the global community communicates on the Internet every day. Sometimes, traffic is passed on the Internet that no one wants. Unsecured ports are the plagues of some companies. They allow all types of problems in. So to secure those things that the mainframe security systems can only partially control enter an OS\390 firewall. Currently IBM is the only company that provides a firewall for the OS\390 environment. The firewall provides that on more extra layer of protection that the security systems can not.

The mainframe has been around for over 40 years. The systems that are running on these computers have been in development and redevelopment for over 30 years. Time and users have tested these systems over and over. It is the author's opinion that the mainframe and the security systems that are available on them can be very powerful tools in a security administrator's pocket. They have advanced from simple user verification and identification, to cross platform integration and system wide administration. By combining the strength of the mainframe security systems with the ideas of network systems, it will prove to be a powerful force in implementing the security policies that company's design to protect their systems.

Summary

The idea behind practical was to provide new ideas to security professionals. The mainframe is definitely not new, but the possibilities of how it can be used are endless. It is not a matter of being biased to one security product or the other. It is how we put those products together and how we use them to make the job of security administration more effective. The mainframe has been around for years. When client server systems became popular, many people assumed that mainframes were dead. These systems however came back stronger then ever. Mainframes are now the workhorses of the companies that run them. Acting, as a company's security server is just one more function the mainframe is more than capable of performing.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

References

1. Lillycrop, Mark. 2001. “The Mainframe: A strategic Platform for the Future.” Technical Support Magazine, August.

2. IBM, Corporation. “RACF History; Twenty Four years of RACF!” Last updated March 2001. http://www-1.ibm.com/servers/eserver/zseries/zos/racf/racfhist.html (August 19,2001).

3. Klemens, Eberhard. 2001. Interview by author. Written documentation. Rosemont, IL, 20 July.

4. Computer Associates Corportation, “CA-Top Secert Security for z\OS & OS\390” . http://www3.ca.com/Solutions/Product.asp?ID=180 (August 19, 2001).

5. Bertagnolio, Luca, 2001. “Security on the Network: What You Need to Know.” SCMagazine, Feburary.

6. IBM Corporation. “z\OS and OS\390 Security; Security A Key element of Business” http://www-1.ibm.com/servers/eserver/zseries/zos/security (August 19, 2001)

7. Townsend and Taphouse, “CA Enhances eBusiness Security Across Mainframe and Distributed Platforms” 8, June, 2001 http://www.itsecurity.com/tecsnews/jun2001/jun26.htm (August 19,2001)

8. IBM Corporation. “What is OS\390 Firewall Technologies.” http://www-1.ibm.com/servers/eserver/zseries/zos/firewall/whatisfw.htm. (August 19, 2001)

© SANS Institute 2001, Author retains full rights

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced