Securing NSK Communications With Software Based Encryption

by XYPRO Technology Corporation

Introduction

The computer security industry has reached an understanding of the value of computer security. Most host systems are competently if not fully secured. Unfortunately, host systems are rarely isolated these days. Hosts talk to other mainframes for peer to peer transmission of data, to users who access the host for interactive sessions and to both PCs and other hosts for file transfer. With all of these access methods, the communications media open wide the window of risk.

Communications media are subject to risks based on their public and intra-company availability. A truly private network that has no external access points does not represent a risk. But few private networks are truly private - they often have an access point available to the telephone provider or they are located in a building that is not completely occupied by the network owner. Surprisingly, FBI surveys reveal that 80% of successful breaches are launched internally, by users who have legitimate access to some systems and using that legitimate access, they compromise other systems.

When a computer is compromised internally or externally, the owner of the computer loses in many ways. First, the direct dollar value of the loss is high. Next, the high cost of recovery must be taken into account. After all the costs are totaled, the bottom line can be a shocking surprise to management.

Since the Compaq NSK Himalaya is often used for financial applications, a financial incident is used to show the losses that can result from a single breakdown of security. Table 1 shows the approximate recovery cost for a hypothetical banking incident where 1,000 accounts were defrauded of $1,000 apiece. Initially, this seems to be a small incident, but when all the direct and indirect costs are added in, the recovery becomes quite expensive.

Expense	**Cost**
Returning Funds Stolen From Account ($1,000 from 1000 accounts)	$1,000,000
48 hours downtime beefing up security ($2M/hr)	$96,000,000
Emergency audit of 250,000 looking for tampering	$1,000,000
[Corporate Image] PR damage control for 3 months	$6,000,000
Increased fraud insurance premiums	$5,000,000
Loss of 10,000 accounts to other banks ($250/account)	$2,500,000
Total	**$111,500,000**

From COMPAQ Presentation at RSA 2000 Conference

Table 1: Direct and Indirect Losses

In this paper, we will discuss effective security measures for reducing the window of security exposure on your NSK by limiting the exposure of your corporate intranet and Internet access.

The Problem

Lack of security on a network can lead to compromise of Userids and passwords and data transactions. Compromise of Userids and passwords can lead to direct misuse of host resources or can set up a situation where the host is then used as a base for attacking other systems, both inside and outside of the host's network community. Transaction compromise can lead to direct monetary loses or compromise of private customer identity information.

Sessions

An interactive session is a session in which a user is sitting in front of a workstation or personal computer accessing the resources of a host system, such as the NSK. This access is enabled through the use of a terminal emulator that replicates the functionality of a standard terminal on the host, such as a 6530 on the NSK Himalaya. The session generally starts by transmitting a Userid and password from the user to the host in order to authorize the user. After authorization, the user can then access whatever resources are available to him, such as a Pathway application screen or a TACL interactive command session. Figure 1 shows a typical interactive session layout.

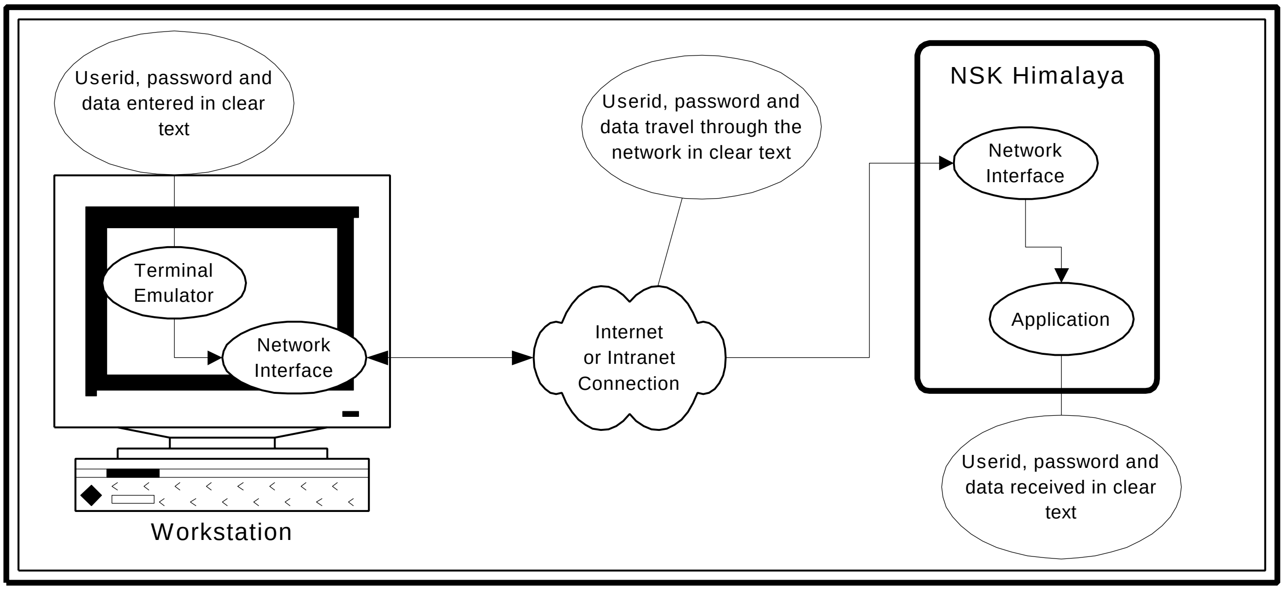
Userid, password and data entered in clear text
Terminal Emulator
Network Interface
Workstation
Userid, password and data travel through the network in clear text
Internet or Intranet Connection
NSK Himalaya
Network Interface
Application
Userid, password and data received in clear text

Figure 1: An Interactive Session

From that point on, the user could be a developer directly accessing system resources, an operator managing the Pathway application environment or a customer using the NSK Himalaya to perform application transactions. If the Userid and password are divulged, any of these functions can be compromised. Unauthorized possession of the data may lead to direct monetary loss. Unauthorized possession of the Userid and password lead to indirect loss that occurs because the computing resource is hijacked, set to purposes not approved by the resource owner.

Additionally, compromise of your security also reduces the accountability of authorized users. If a hacker might have stolen a user's Userid and password, the user can and will argue that no erroneous action can be absolutely matched to the user, because the hacker might have done it.

Once human factors are eliminated, the most common method available to compromise a Userid, password or other data is by using a program to monitor the communications medium. This type of program, called a "sniffer", can be used between the network interface card and the Internet or internal network or it can be used by someone who has access to the network. Figure 2 shows where "sniffers" can sit watching your transactions.

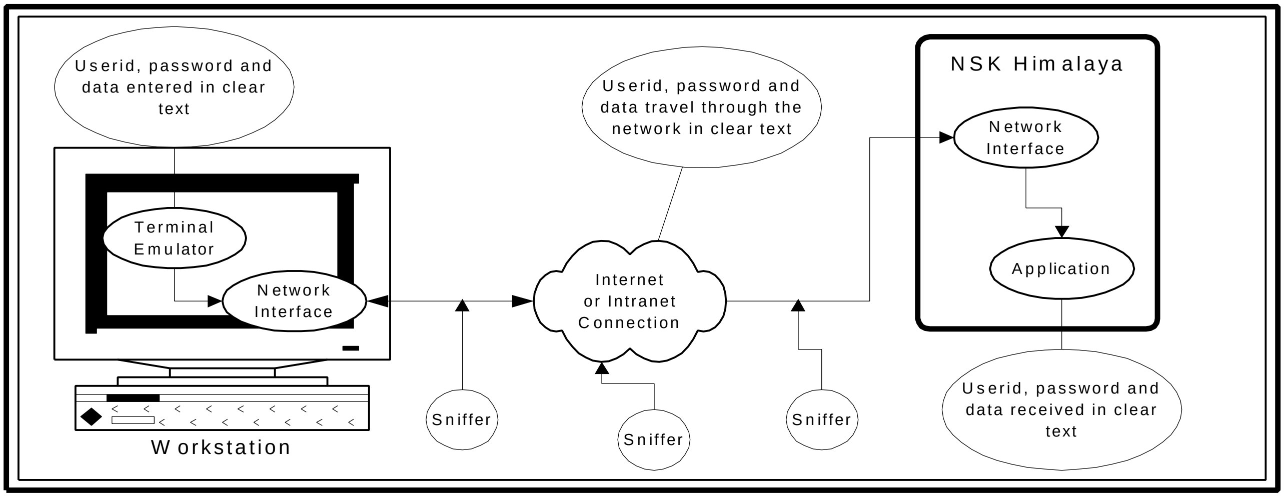
Userid, password and data entered in clear text
Userid, password and data travel through the network in clear text
NSK Himalaya
Network Interface
Terminal Emulator
Network Interface
Application
Internet or Intranet Connection
Userid, password and data received in clear text
Sniffer
Sniffer
Sniffer
Workstation

Figure 2: An Interactive Sessions Is Sniffed

A sniffer is a passive watcher of all your information as it goes by. Once the sniffer has gathered information, unauthorized attacks can begin. Figure 3 shows the hacker imitating legitimate access in order to gain unauthorized access for himself. In some situations, the legitimate access can continue, without any way for the user on the workstation to know that someone else is also using his Userid.

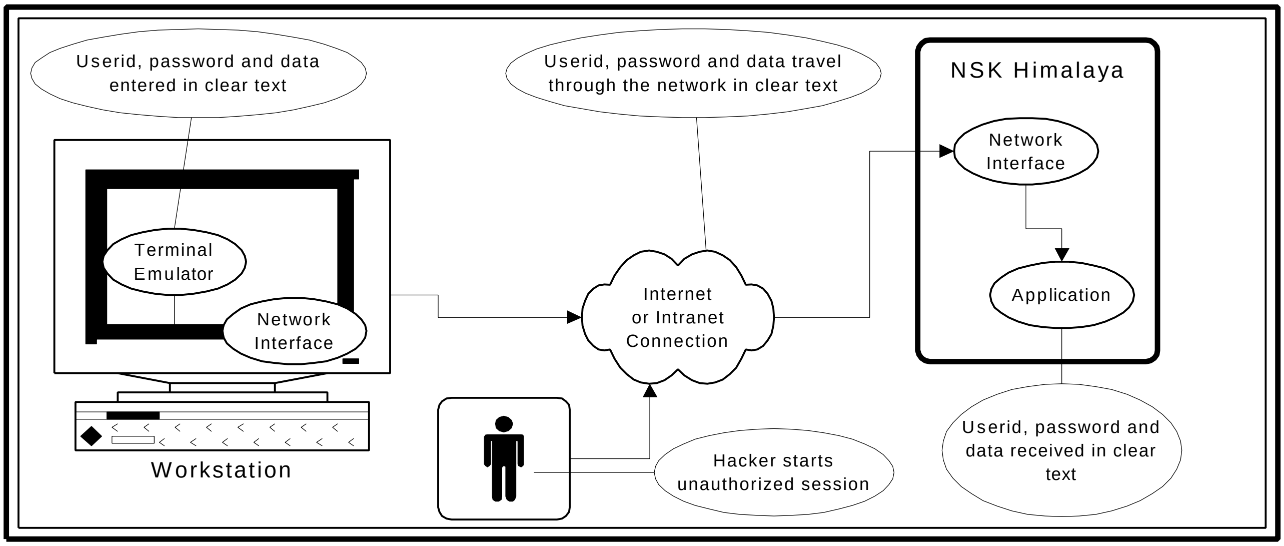
Userid, password and data entered in clear text
Userid, password and data travel through the network in clear text
NSK Himalaya
Network Interface
Terminal Emulator
Application
Internet or Intranet Connection
Network Interface
Userid, password and data received in clear text
Workstation
Hacker starts unauthorized session

Figure 3: An Interactive Session Is Attacked

The unauthorized attacker mimics an authorized session. Based on the sophistication of the attacker's tools, he might steal resources to dedicate to his own purposes, use the online application to create seemingly legal transactions or even use the compromised host's resources to attack another system. Examples of this occur every day when systems are hacked by "script kiddies" from the Internet for the purpose of using the system to attack someone else. Industrial espionage follows this same pattern, except the industrial spy is not using the resource to attack someone else, but to find out company trade secrets instead. Something as simple as a business plan or the test key algorithm may be extraordinarily valuable. Simple thieves use this method to create unauthorized transactions, such as funds transfers from valid accounts to accounts belonging to the thief.

File Transfer

A file transfer session on the NSK Himalaya generally starts by transmitting a Userid and a password, followed by the file to be transferred. The file generally contains data and instructions for an application's batch processing of transactions. Figure 4 is a diagram of a simple file transfer session.

When the file is transferred, the data is generally in clear text. A sniffer can gather the text and compile enough information to start the attack. Figure 5 shows where file transfer sniffing can occur.

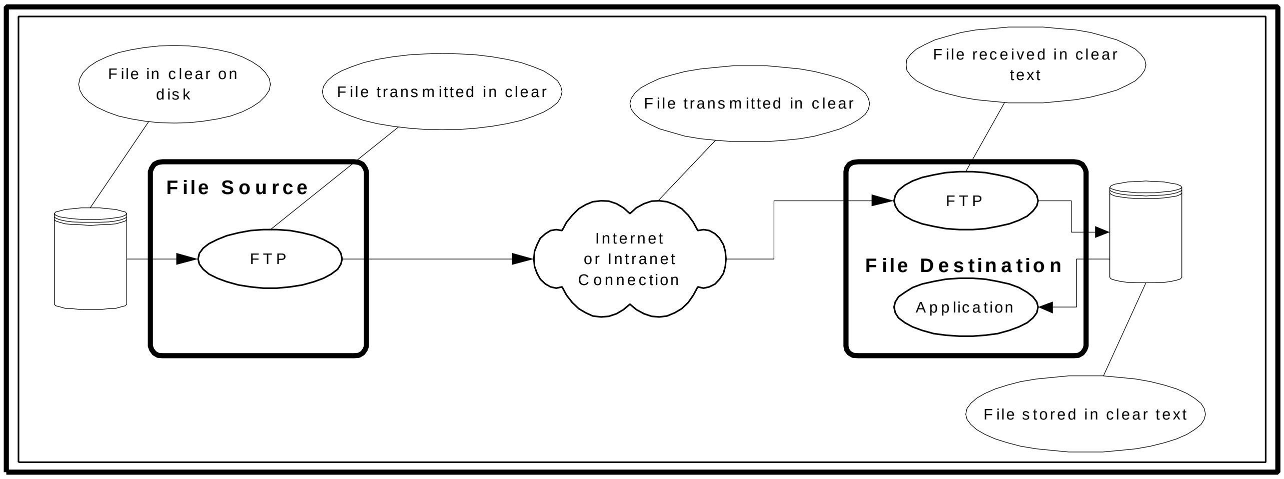
File in clear on disk
File transmitted in clear
File transmitted in clear
File received in clear text
File Source
FTP
Internet or Intranet Connection
FTP
File Destination
Application
File stored in clear text

Figure 4: A File Transfer Session

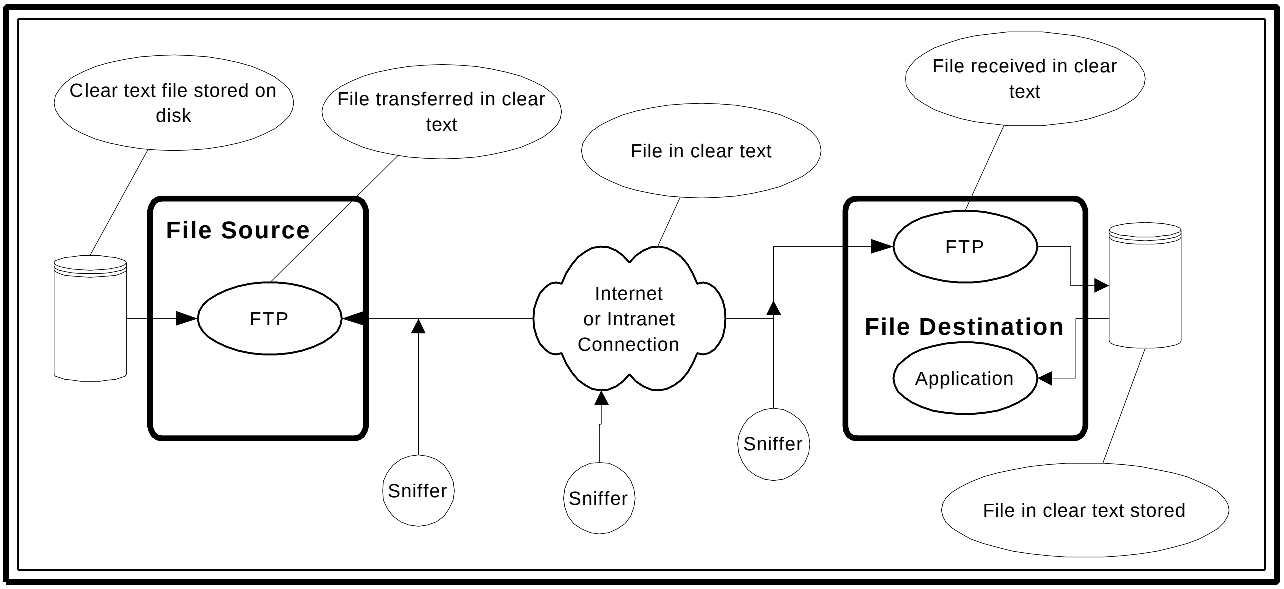
Clear text file stored on disk
File transferred in clear text
File in clear text
File received in clear text
File Source
FTP
Internet or Intranet Connection
FTP
File Destination
Application
Sniffer
Sniffer
Sniffer
File in clear text stored

Figure 5: A File Transfer Session Is Sniffed

Since these file transfers are often a client submitting a list of commands and transactions, such as ACH payroll transactions or service bureau customers submitting the day's transactions, compromise of these files will most likely be a commercial theft situation. Figure 6 shows a hacker using file transfer to submit an unauthorized file to the host application.

A variation of the unauthorized use of file transfer is the use of file transfer to hijack data space on the disk of some host. This is often done by Internet users looking for someplace to store an unauthorized game or movie. The manager of the host system may suffer no monetary loss, but the high impact of other traffic accessing this unauthorized data storage can destroy response time, indirectly becoming a denial of service situation.

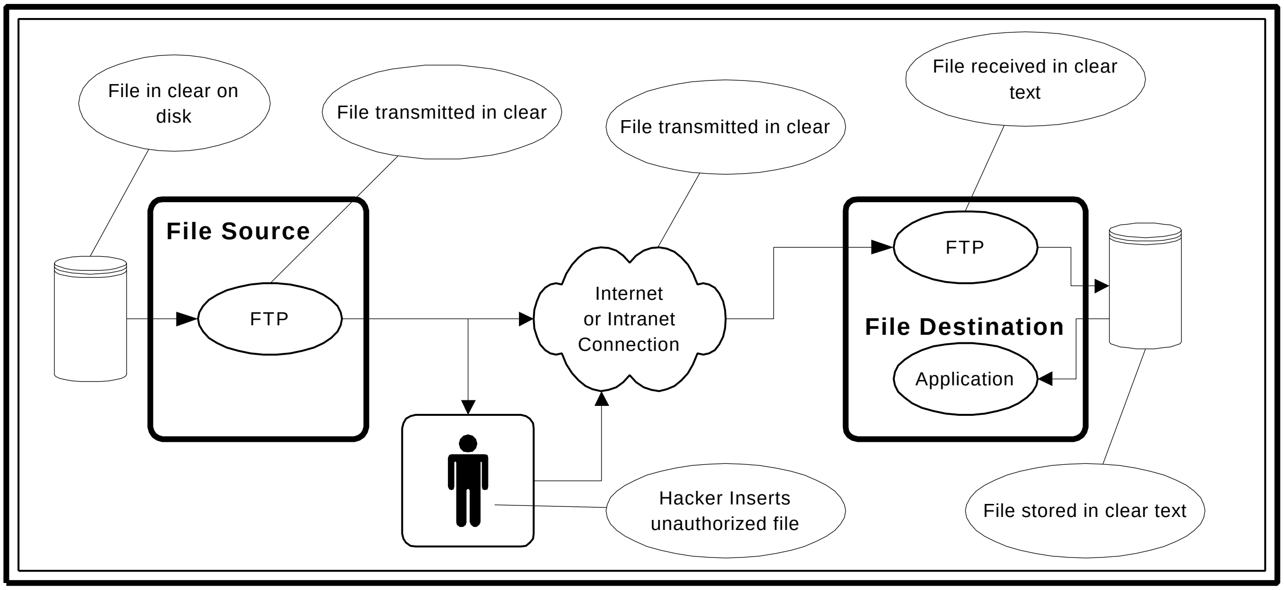
File in clear on disk
File transmitted in clear
File transmitted in clear
File received in clear text
File Source
FTP
Internet or Intranet Connection
FTP
File Destination
Application
Hacker Inserts unauthorized file
File stored in clear text

Figure 6: A File Transfer Session Is Attacked

Peer-to-Peer

The peer-to-peer network connection is used between multiple host systems to provide data from one application for use by another. Often, this data is mutual - either system may be using it at any time. Peer-to-peer data transfers often use some commercial transaction package such as RJE (multi-platform), Connect:Direct, XMODEM, YMODEM, and Information Exchange Facility to supply information from one host to another. NSK specific transaction packages include TOP and RSC. Figure 7 shows a typical network of hosts communicating via a shared network.

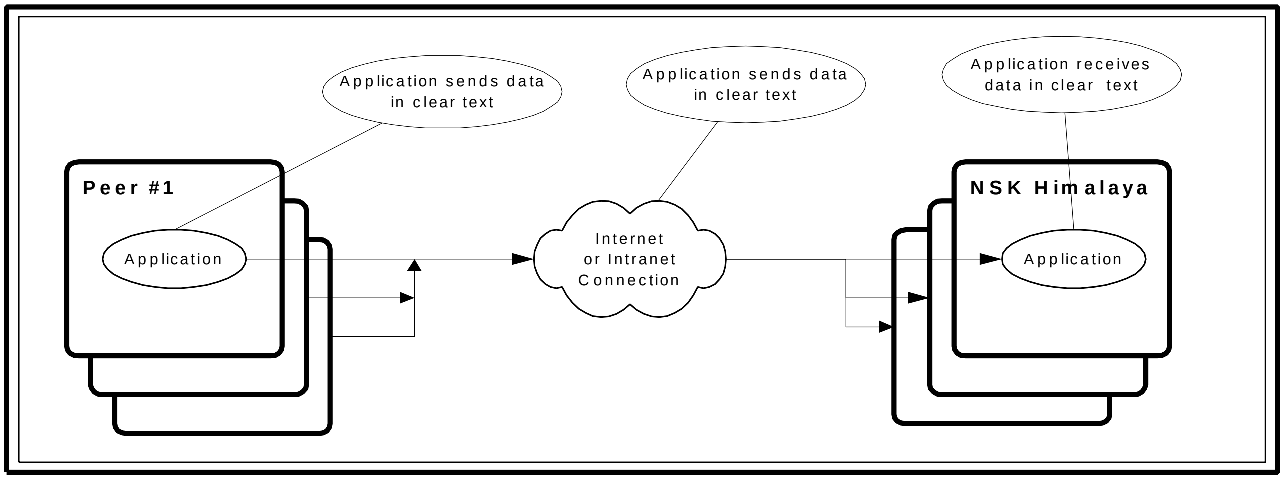
Application sends data in clear text
Application sends data in clear text
Application receives data in clear text
Peer #1
Application
Internet or Intranet Connection
NSK Himalaya
Application

Figure 7: A Peer-To-Peer Session

Peer-to-peer sessions are vulnerable to sniffing primarily for faking unauthorized financial transactions Figure 8 shows where a peer-to-peer session is vulnerable to being monitored.

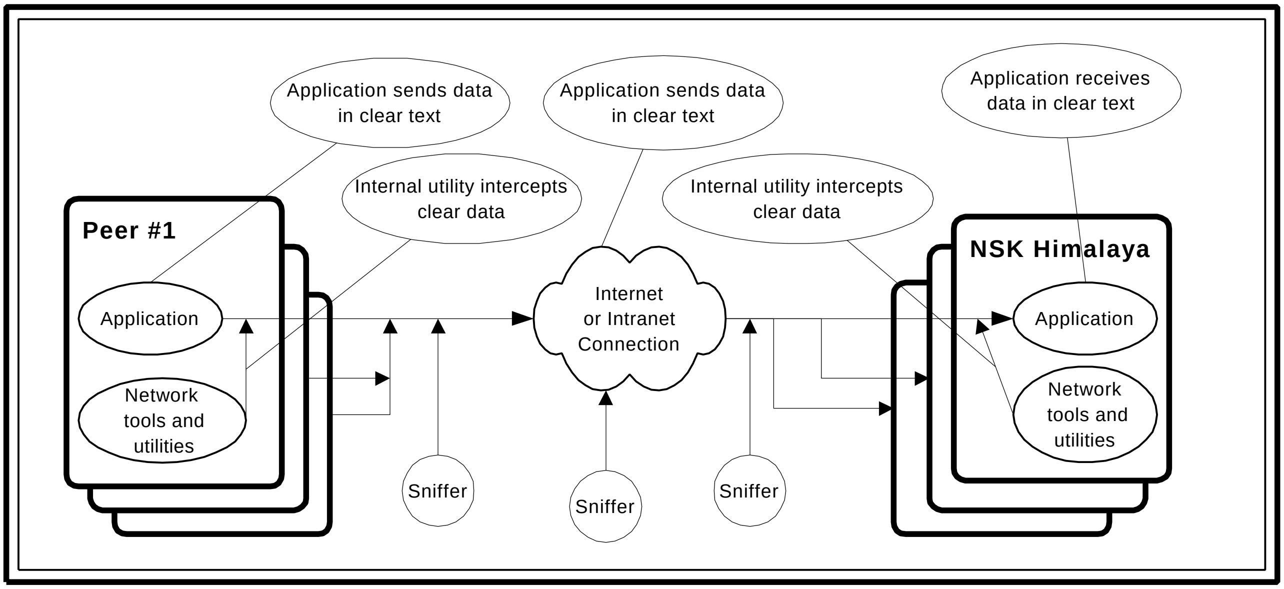
Application sends data in clear text
Application sends data in clear text
Application receives data in clear text
Internal utility intercepts clear data
Internal utility intercepts clear data
Peer #1
Application
Network tools and utilities
Internet or Intranet Connection
NSK Himalaya
Application
Network tools and utilities
Sniffer
Sniffer
Sniffer

Figure 8: A Peer-To-Peer Session Is Sniffed

Peer-to-peer sessions are subject to the threat of unauthorized transactions being inserted - a hacker emulating one end of a transaction. For example, a hacker emulating a wire transfer originator could send a transfer to the receiving system, which would then credit an account, which would then be emptied by the hacker and his assistants. Figure 9 shows the hacker inserting data into the transaction stream.

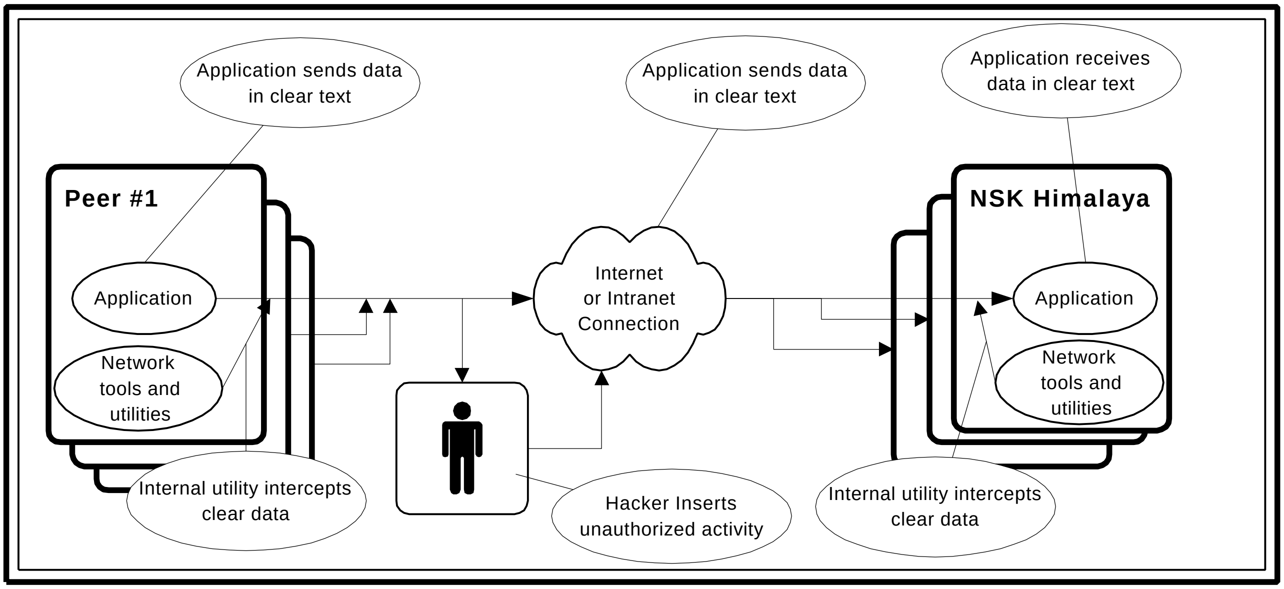
Application sends data in clear text
Application sends data in clear text
Application receives data in clear text
Peer #1
Application
Network tools and utilities
Internet or Intranet Connection
NSK Himalaya
Application
Network tools and utilities
Internal utility intercepts clear data
Hacker Inserts unauthorized activity
Internal utility intercepts clear data

Figure 9: A Peer-To-Peer Session Is Attacked

The Solution

A good solution conceals the contents of the transmission end to end, whether it is Userid and password or transaction data and it makes more difficult the task of inserting false data. Since the NSK Himalaya often communicates with other platforms, a good solution must be supported across many platforms. It must be standardized in the market place and inexpensive enough to be a reasonable solultion for both small and large installations.

Encryption of the Userids, password and data fulfills this requirement. The contents of the transmission must be decrypted in order to be useful. Unauthorized data cannot be added without having compromised the encryption keys, which is a costly and computationally-intensive activity for properly constructed encryption. Encryption algorithms are standard, supported both nationally and internationally. A good encryption/decryption tool would make it easy for small and large businesses to encrypt Userids, passwords, and data across multiple hardware platforms and multiple communications media.

Encryption can be performed in hardware or software. The cost of hardware devices for each host and workstation, however, is prohibitive for all but very large or affluent companies. A further expense is the management of the "keys" necessary to control encryption and decryption. This task alone can be a full time job for members of your Security Administration staff. The hardware itself also requires inventory control, repair and replacement. End to end protection is difficult to achieve.

Encryption in software provides a method of moving the encryption as close to the data origination as possible. Additionally, key management can also be automated, requiring only minimal setup. Without any hardware, there is no burden of physical management. Finally, encryption in software is easily upgraded when a new algorithm is adopted for commercial use.

On the NSK Himalaya, this encryption can be implemented as a server process, encrypting data as a service for the application. It can also be implemented in the application, calling routines that perform the encryption/decryption as a part of the application's normal functionality.

The following discussion shows how encryption in software can protect each of the three types of network communication.

Sessions

For greatest protection, an interactive session should be secured as close as possible to the user and to the application. The terminal emulator is an ideal place to implement security measures; it protects the session as early as possible. On the host end, the security measures need to be as close as possible to, if not integrated into the application.

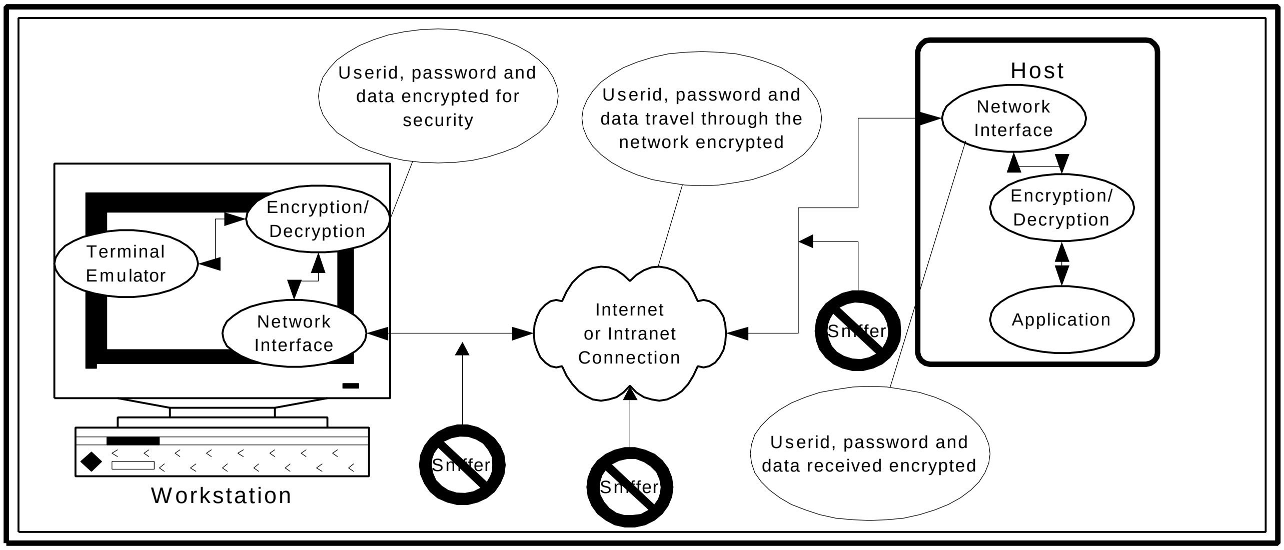
Userid, password and data encrypted for security
Userid, password and data travel through the network encrypted
Host
Network Interface
Encryption/ Decryption
Terminal Emulator
Encryption/ Decryption
Network Interface
Internet or Intranet Connection
Sniffer
Application
Sniffer
Sniffer
Userid, password and data received encrypted
Workstation

Figure 10: An Interactive Session Protected By Encryption

With encryption in place, the session is protected. Additionally, an encryption module that has been developed to work with a terminal emulator and the applications that drive it will take into account the need to keep terminal display transactions within a certain size range. It will also avoid control characters that might affect the hardware that controls the network interface.

File Transfer

With encryption in place, file transfer becomes completely secure. No one copying the file from the network will be able to decrypt it in a computationally-feasible manner before the data is processed by the destination application. Unauthorized files cannot be inserted because they will not be encrypted with the session keys that exist between the file source and destination. Figure 11 shows how sniffers are blocked, unable to monitor an encrypted file.

In addition, if the file is also encrypted on the disk and only decrypted when it is used by the application, the entire window of exposure is closed - the only way to monitor the data would be to break the encryption or have a physical method of reading active memory in the CPU of the system running the application.

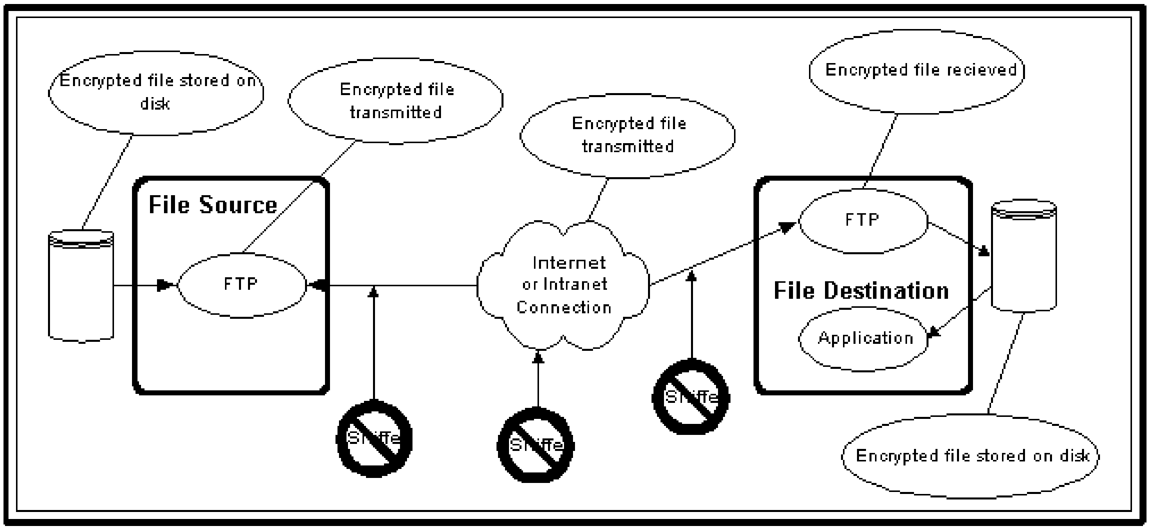
Encrypted file stored on disk
Encrypted file transmitted
Encrypted file transmitted
Encrypted file recieved
File Source
FTP
Internet or Intranet Connection
FTP
File Destination
Application
Sniffer
Sniffer
Sniffer
Encrypted file stored on disk

Figure 11: A File Transfer Session Is Protected With Encryption

Peer-to-Peer

A solution for peer-to-peer must protect the transmission before it exits from the originating host. Decrypting must occur after it reaches the receiving host. Encryption and transmission facilities used must take into account the control characters that matter to the transmission protocol, so no interference occurs in the transmission. Figure 12 shows a peer-to-peer transmission with encryption in place.

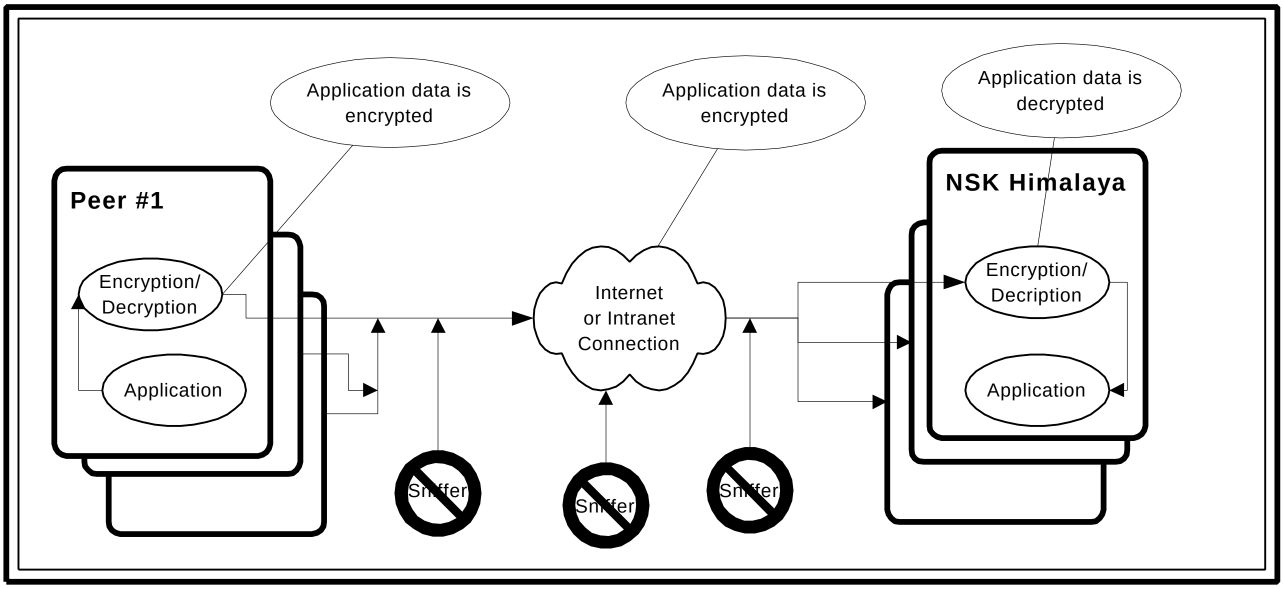
Application data is encrypted
Application data is encrypted
Application data is decrypted
Peer #1
Encryption/ Decryption
Application
Internet or Intranet Connection
NSK Himalaya
Encryption/ Decription
Application
Sniffer
Sniffer
Sniffer

Figure 12: A Peer-To-Peer Session Is Protected With Encryption

Summary

With a properly secured NSK Himalaya system, the window of vulnerability to security incidents is moved to the network used by other hosts and workstations that exchange data with the secured NSK Himalaya. It only makes sense to ensure that the network is as secure as the NSK Himalaya.

The Internet is not owned by any particular organization and even internal intranets can be compromised where the physical net passes out of control of the application. Computer networks can also be compromised from within. In order to reduce the window during which the information can be compromised, the controls on information passing out onto the network must be as close as possible to the application that creates or processes the data, the emulator that allows a user to input data or to the file that will be transmitted.

The closest protection possible is encryption in software. The encryption of the information occurs locally, reducing exposure to the smallest possible window. The encryption software uses standardized algorithms, and can generally be upgraded to new algorithms as they are developed. Encryption software can be used on many different platforms.

With encryption in place, the network traffic can be as secure as the NSK Himalaya host itself.

For additional information on software based encryption for the NSK Himalaya or any system that communications with an NSK Himalaya, please contact

XYPRO Technology Corporation
3325 Cochran Street, Suite 200
Simi Valley, CA 93063
USA

+1 805-583-2874

info@xypro.com