



While every attempt has been made to ensure the accuracy and completeness of the information in this document, some typographical or technical errors may exist. Hummingbird cannot accept responsibility for customers' losses resulting from the use of this document. The information contained in this document is subject to change without notice.

This document contains proprietary information that is protected by copyright. This document, in whole or in part, may not be photocopied, reproduced, or translated into another language without prior written consent from Hummingbird.

*This edition published December 2005*

## Table of Contents

> <b>The Security Challenge</b> .....	4
> <b>Security in Organizations</b> .....	4
> <b>Driving Security</b> .....	5
Structural Factors .....	5
External Factors .....	6
> <b>Connectivity — A Definition</b> .....	6
> <b>Security Risks in a Connectivity World</b> .....	7
Weak Authentication .....	7
Easy Protocol Decoding .....	7
Date Authenticity and Integrity Tampering .....	7
> <b>Solutions for Secured Connectivity</b> .....	8
> <b>SSL</b> .....	8
> <b>Kerberos</b> .....	9
> <b>Secure Shell</b> .....	10
> <b>Connectivity SecureTerm®</b> .....	11
> <b>Connectivity Secure Shell™</b> .....	12
> <b>Glossary of Terms</b> .....	14

## The Security Challenge

Security is the hot topic today. Although, companies have been slow to recognize the importance of security things have changed during the last decade. Security is a top priority and there are no indications that this will end any time soon.

The costs of security (or lack thereof) have now been clearly identified, and the picture does not look very good. The CSI (Computer Security Institute), in partnership with the FBI (Federal Bureau of Investigation), releases a Computer Crime and Security Survey every year. This survey is one of the longest-running surveys in the information security field and definitely one of its most relevant. The survey document can be downloaded at no charge from the CSI Website([www.gocsi.com](http://www.gocsi.com)).

In 2004, 53% of respondents identified some form of unauthorized use of their computer systems. This figure has been in constant decline since 2000 when it peaked at 70%. This decrease should however be mitigated by the fact that 10% of the respondents were not able to provide an answer in 2004 because of their inability to assess unauthorized use of their systems.

The number of incidents per respondent remains relatively low with 47% of them acknowledging between 1 and 5 incidents during the year. Twenty percent of the respondents reported between 6 and 10 incidents a year and 12% of them more than 10 incidents a year. When asked about the origins of the attack, respondents answers revealed an equal volume of internal and external incidents.

The nature of the attacks is also evolving. As seen in the report, there's been a significant decrease in reports of system penetration, insider abuse and theft of proprietary information.

Last year's survey revealed the total costs of security incidents (251 respondents) to be at \$201 M. A significant decline has occurred this year with total costs of security incidents (269 respondents) being at \$141 M. Top security incidents per cost (269 respondents) were virus attack (\$55 M), denial of service (\$26 M), theft of proprietary information (\$11 M), insider net abuse (\$10 M), abuse of wireless network (\$10 M) and financial fraud (\$7 M).

## Security in Organizations

This year's CSI Security Survey contains particularly interesting data on an organization's Security spending and deployed technologies. Although some of the data cannot be compared over years because they were not collected in previous surveys, their importance cannot be denied.

Security managers, like all other IT managers with domain expertise, have realized the importance of budgeting and financial management of Security.

What are companies spending on Security as a percentage of their IT budget? Among all respondents to this question in the survey (481), a large majority spent over 1% of their IT budget on Security related expenses. More than 50% of that group acknowledged spending over 5% of their IT budget in Security technologies.

Another interesting metric of this survey reveals that as a company's revenue grows, average reported computer Security expenditure per employee grows less rapidly. Investment and operating expenses per employee are the highest in such sectors as federal government (\$449), telecommunications, hightech and finance, with transportation topping the list with a figure of \$608 per employee. On the low end of Security expenditure were media, retail, local government, education and utility. These are the sectors where the least spending was reported.

When it comes to Security technologies in use, antivirus and firewalls are still the most commonly deployed security technologies (99% and 98% of the respondents respectively). Intrusion detection systems are also a dominant technology with 68% of the respondents using it, along with encryption for data in transit (64%). Smart cards or other password tokens (35%), PKI (30%) and biometrics (11%) are slowly gaining ground in corporations.

Audits are also a widely used tool with 82% of the 470 respondents acknowledging that Security audits are used within their organization. However, most respondents do not believe that adequate investments are being made in Security awareness programs.

## Driving Security

Beyond the potential for significant financial damages, many other factors are urging companies to investigate, purchase and deploy security technologies. These factors can be classified in two categories: structural and external.

### Structural Factors

- > Inability to operate without IT infrastructures. How many organizations would be able to effectively run their daily operations without their computer systems?
- > IT framework downtime impacts revenue and profit. How many millions per minute would investors lose if a bank or a stock exchange IT system went down?
- > Integrity of information is essential to accomplish daily operations. How many transactions rely on some form of trust between both the provider and the customer?
- > Theft of proprietary information can mean life or death situations for companies. What would become of a Biotech company if its latest groundbreaking drug was stolen after several years of development?
- > Businesses are becoming more and more interconnected. How many transactions per day are performed through electronic data exchange?
- > Exposure to the outside world. What would some companies do if they were not able to avail themselves to their providers and/or their customers?

## External Factors

- > Our world has become more security conscious. Amid heightened concerns for national security, every individual has fully realized that safety has been redefined.
- > Massive IT attacks (Code Red, Nimda, Sobig ...) have had a worldwide impact and prompted media attention. Because we live in an interconnected world, the security of IT infrastructure is not an expert reserved domain any longer.
- > Proliferation of standards and legislations with direct or indirect impact on Security: since 2001, numerous initiatives have been taken by the government that directly impact security policies of public and private organizations. (e.g. The Patriot Act, Sarbanes-Oxley and HIPAA).
- > Threat of legal liability by customers and/or partners. 2002 has been the year of legal liability from security. Organizations and software vendors are being held to a higher degree of accountability for security, if not in the courtroom, then by their customers. Organizations are challenged to prove they are managing security at a level that will satisfy their business partners and stakeholders. This goes beyond discussing what security products are installed, to communicating compliance and management practices of information security.

## Connectivity — A Definition

Connectivity is a domain where network communications are paramount. In its broader sense, Connectivity can be defined as the group of technologies that allow multiple systems (heterogeneous or not) to communicate. In a more popular sense, Connectivity designates TCP/IP client server technologies working with standardized protocols which allow systems to interconnect and exchange information.

Some of the most popular Connectivity technologies are:

- > **X-Window (or X11)**: is a windowing and graphic system developed at the MIT. Almost all UNIX graphic applications are X-Window based. One of X-Window most notable properties is its ability to separate the application processing layer, the logic, from its graphic layer, the user interface, which can be deployed on a remote machine.
- > **Telnet**: is a protocol for remote computing on a network. It allows a computer to act as a remote terminal on another machine, anywhere on the network. The remote computer (also called the telnet server) accepts input directly from the client computer and output for the client session is directed to the client screen. Many other protocols such as TN3270 (Mainframe) or TN5250 (AS/400) are derived from Telnet.
- > **FTP**: File Transfer Protocol, is a protocol for exchanging files over a network. FTP is most commonly used to download a file from a server, or to upload a file to a server using a network.

Many other Connectivity technologies are commonly used in organizations, such as HTTP (Hyper Text Transfer Protocol), which defines how the messages are formatted and transmitted over the world wide web or SMTP (Simple Mail Transfer Protocol) and POP3 (Post Office Protocol), which are used to send and retrieve messages from a mail server.

## Security Risks in a Connectivity World

Although some Connectivity protocols have been in use for more than a quarter century, very few of them come with a strong security model. Inherent security flaws exist in almost every Connectivity protocol and many organizations do not realize how vulnerable they are to these security issues.

### Weak Authentication

As surprising as it may seem, many protocols, such as Telnet and FTP, send their messages in clear text over the network. Such messages include username and passwords, as well as all other information displayed to the user during the session. Widely available network sniffing tools allow any attacker to easily capture that information and use it for their own profit.

### Easy Protocol Decoding

Although X-Window does not transmit user's input as a string of text to the X application, the protocol remains relatively easy to decode in order to retrieve the desired information. Keyboard inputs are transmitted in clear-text as numbers which can be easily obtained and interpreted to rebuild the original text that was entered by the user. Access to password protected X applications can be compromised by anybody with a network sniffing tool and a little bit of patience.

### Data Authenticity and Integrity Tampering

The Man in the Middle attack, or TCP hijacking, is a well known attack where an attacker sniffs packets from network, modifies them and inserts them back into the network. Sensitive information can be intercepted and altered without a chance for the victim to know that their data has been tampered with. Although this attack requires a superior level of skills than those required for simply sniffing a network, some program/code sources are available on the Internet for the enterprising hijacker.

Because of their widespread usage throughout organizations, Connectivity software is a target of choice. Their popularity does not allow companies to simply remove and replace them with more secure technologies without significant investment. The solution to this problem lies in applying robust security techniques to existing Connectivity protocols.

## Solutions for Secured Connectivity

Assuming that Connectivity protocols are still going to be around for a significant number of years, it becomes mandatory for organizations to implement complementary security solutions that can be built on top of their existing infrastructure.

Some of those solutions consist of building encryption and authentication within the network hardware. Although it sounds like an interesting way of increasing the security level of the network, such a solution is very expensive and involves significant disruption of the business operations.

Another solution consists in building a security layer within the existing protocols. High effectiveness, minimal business disruption and relatively low investments are some of the characteristics that have led many organizations to choose this path.

## SSL

SSL (Secure Sockets Layer), is a protocol which allows for the encryption of data transmitted between two computers. It was developed in the mid-90s by Netscape® to facilitate the transmission of sensitive information via the Internet. Since then, it has been built into all major browsers and web servers and is the industry standard for protecting information sent over the Internet.

SSL uses public and private keys. There are two strengths of SSL, 40-bit and 128-bit. The bits indicate the length of the session key — the longer the session key, the harder it is to crack the code. When a client wants to connect to a server using SSL, the client and the server go through a series of requests and acknowledgements (“the SSL handshake”). Briefly, the following occurs:

- > The client sends a request for a secure session to the server.
- > The server returns its digital certificate in response to the request. The certificate contains the server’s public key.
- > The client checks the certificate to make sure it is valid and the server is authenticated. The client creates a session key which is encrypted with the server’s public key and sends it to the server.
- > The server decrypts the session key information by using its private key.
- > Both the client and server are now using the same session.

All further information that is transmitted between the client and server will be encrypted automatically and safe from third-party prying.

SSL offers both encryption and authentication. Encryption is accomplished using various algorithms such as 3DES, AES or RC4 for instance. In contrast to server authentication, client authentication is not mandatory but can be accomplished by using client certificates.

SSL is used to secure a wide variety of protocols and has been adopted by a large number of organizations. As an example, SSL has become the de facto security standard for Mainframe and AS/400 Connectivity through the TN3270 and TN5250 protocol. It's also widely used to secure HTTP connections and many 3rd party protocols.

## Kerberos

Kerberos is a trusted third-party authentication mechanism. It is trusted in the sense that each of its clients believes Kerberos' judgment as to the identity of each of its other clients to be accurate.

Kerberos keeps a database of clients and their private keys. The private key is a large number known only to Kerberos and the client to which it belongs. In the case that the client is a user, it is an encrypted password. Network services requiring authentication register with Kerberos, as do clients wishing to use those services. The private keys are negotiated at registration.

Because Kerberos knows these private keys, it can create messages which convince one client that another is really who it claims to be. Kerberos also generates temporary private keys, called session keys, which are given to two clients and no one else. A session key can be used to encrypt messages between two parties.

Kerberos provides three distinct levels of protection. The application programmer determines which is appropriate, according to the requirements of the application. For example, some applications require only that authenticity be established at the initiation of a network connection, and can assume that further messages from a given network address originate from the authenticated party.

Other applications require authentication of each message, but do not care whether the content of the message is disclosed or not. In these instances, Kerberos provides safe messages. Yet a higher level of security is provided by private messages, where each message is not only authenticated, but also encrypted. Private messages are used, for example, by the Kerberos server itself for sending passwords over the network.

Kerberos is generally used in UNIX environments to provide authentication services. Kerberos is also available on the Mainframe and on AS/400. Microsoft® introduced operating system level support for Kerberos in Windows® 2000. Although interoperability between a "classic" Kerberos environment and its Microsoft counterpart was somehow challenging at the beginning, the two environments can now work seamlessly together.

Many companies are considering using Kerberos as their primary authentication mechanism, now that it can be used from the Windows environment. A Microsoft Windows server can easily become a Kerberos domain controller and thus serve as an authentication trusted tier for all third party authentication needs. Another factor that speaks to Kerberos is its ability to be used as part of a much wider security implementation. The Secure Shell protocol for instance, which provides authentication and encryption services, can use Kerberos as one of its authentication methods.

## Secure Shell

The Secure Shell protocol was created in 1995 by a young Finnish student named Tatu Yl\_nen after he was victim of a password-sniffing attack. The protocol was released to the public as free software with its source code. By the end of 1995, the software was used by more than 20,000 users in 50 countries and the amount of requests asking for technical support was close to 150 requests per day.

In 1996, SSH™ Communications Security Ltd introduced the 2nd version of the Secure Shell protocol in order to overcome certain weaknesses of the initial version. The draft for SSH-2 was submitted to the IETF in 1997. In 1999, OpenBSD shipped with OpenSSH, a derivative of the original free Ssh 1.2.12 which also supports the Secure Shell 2 protocol.

The Secure Shell protocol offers numerous answers to security issues among which:

- > It offers strong security against cryptanalysis and protocol attacks
- > It provides support for key and certificate management infrastructures
- > It can work in conjunction with existing certificate infrastructure if available
- > It is relatively easy to deploy and can be made easy-to-use
- > It does not require in-depth security knowledge from the user and can work transparently behind-the-covers.

Secure Shell offers a very flexible infrastructure allowing the protocol to evolve as new authentication methods are invented. Current supported authentication methods include:

- > Password
- > Keyboard Interactive which is a method to use with authentication devices for instance
- > Public/Private Keys
- > Certificates (not standardized yet)
- > Kerberos

## Connectivity SecureTerm®

Connectivity SecureTerm is Hummingbird's new secure terminal solution. Connectivity SecureTerm offers an easy and cost-effective solution to organizations that look for securing their desktop assets while carefully controlling their costs. Connectivity SecureTerm preserves the legacy of UNIX applications while providing a strong set of security standards and unparalleled terminal and file transfer functionalities.

Connectivity SecureTerm allows users to:

- > Access mission critical applications from their Windows desktop or a browser through a secured terminal
- > Transfer files securely from UNIX environments to their Windows desktop

Connectivity SecureTerm has been built to offer a large choice of security methods:

- > **Secure Shell 2:** Connectivity SecureTerm supports state-of-the-art Connectivity SecureTerm supports state-of-the-art secure shell 2 protocol standards. Based on the work of the Secsh group Connectivity SecureTerm implements the latest IETF RFC for secure shell 2 authentication and encryption
- > **SSL:** Connectivity SecureTerm offers support for SSL v2/3 and TLS encryption and authentication
- > **Kerberos:** Connectivity SecureTerm supports Kerberos v4 and Kerberos v5 based on the work of the MIT

Connectivity SecureTerm provides administrators with the latest technologies for securing their network communications. By getting the most from a wide range of encryption and authentication protocols, Connectivity SecureTerm ensures that mission-critical data is safely transmitted over the wires.

Migrating from a desktop-based product to a web-based solution can be risky, especially when it affects functions such as access to legacy applications and mission-critical data. Connectivity SecureTerm can help achieve this transition with maximum security and efficiency. Whether in desktop-based or web-based mode, Connectivity SecureTerm provides consistent interface, features, power and administrative options.

With its built-in web capabilities, auto-upgrade features, Microsoft SMS integration and powerful administrative features, Connectivity SecureTerm introduces users to a new world of terminal emulation solutions.

Thanks to its macro converter, terminal themes manager and advanced API support Connectivity SecureTerm provides an easy migration path from existing terminal emulators.

Connectivity SecureTerm offers an easy way to protect corporate investments in legacy data while letting users benefit from the latest in desktop and web-based technologies. It enables organizations to lower their total cost of ownership while deploying a state-of-the-art web-based terminal emulator. Corporations are able to provide every user with quick and convenient access to legacy information without having to undertake costly and painful installation on each desktop. Organizations that choose Connectivity SecureTerm save time and money by skipping the deployment process while increasing their productivity.

## Connectivity Secure Shell™

Connectivity Secure Shell is a security add-on which complements Hummingbird existing suite of Connectivity Software:

- > **Exceed®**: Exceed allows users to cost-effectively display graphic X-Window application on a PC desktop. Credited with 71.5% of the PC X market share by IDC (PC X Server Market Forecast and Analysis, 1999–2004), Exceed has become the de facto standard in X11 server for PC. Exceed offers the most comprehensive X11 protocol implementation in the market.
- > **HostExplorer®**: HostExplorer is a Hummingbird solution which provides access to mission critical enterprise data residing on legacy systems. HostExplorer offers TN3270E, TN5250E and Telnet emulation from Windows desktop to Mainframe, AS-400 and UNIX machines. HostExplorer offer a single solution for both traditional PC-to-host and web-to-host legacy access.
- > **Hummingbird FTP™**: Hummingbird FTP is a client implementation of the File Transfer Protocol that is completely integrated with Windows Explorer. Hummingbird FTP allows users to transfer files between a PC and a remote server. Hummingbird FTP includes a full feature set, easy to use interface and supports remote-to-remote transfers.

Connectivity Secure Shell	
General Information	
> Primary Function	> Secure Shell 2, SCP, SFTP, SSL v2/v3 & TLS, Kerberos v4/v5 client
> No Charge	
Applicable Technology	
> X11	√
> FTP	√
> VT	√
> TN3270	√
> TN5250	√
Applicable Product	
> Exceed PowerSuite™	√
> Exceed	√
> NFS Maestro Client™	√
> Host Explorer	√

Coupled with Exceed, HostExplorer and Hummingbird FTP, Connectivity Secure Shell offers:

- > Secure Terminal
- > Secure File Transfer
- > Secure X11 port forwarding
- > Secure generic port forwarding

The following authentication methods are supported:

- > Password
- > Keyboard Interactive
- > Public/Private Keys
- > Kerberos tickets

Additional features include:

- > Extensive ability to configure the protocol settings
- > Multiple trace levels
- > Choice among several strong encryption algorithms including AES
- > Choice of MAC algorithm
- > Support for Agent forwarding
- > Ability to automatically or manually select the X11 port settings
- > Choice of the Secure FTP listening interface

## Glossary of Terms

**Certificate:** An SSL certificate, or digital certificate, or X509 certificate, acts like an identification card. It serves three basic functions:

- > It verifies the identity of the owner and the owner's right to use a given set of encryption keys.
- > It holds the public and private keys used for encrypting content between the server and the browser.
- > It prevents others from impersonating the certificate holder.

**Certificate authority:** if the certificate is like a piece of ID, then the Certificate Authority (CA) stands for the ID issuing office. When you put in a request for a certificate, the CA will conduct a thorough check of the following information:

- > That your organization is a legal entity
- > That you have the right to use the domain name included in the certificate
- > That the person requesting the certificate has the right to do so on the organization's behalf.

Once the information has been verified, the CA will sign the digital certificate to authenticate the data contained within the certificate and validate its use. CAs can also revoke the certificate if the information on the certificate is incorrect or if the certificate holder has compromised or lost the private key.

**Encryption:** Encryption is altering data in such a way that only the intended recipient can read or use it. The intended recipient must have the proper decryption key to decipher the data. Unauthorized people with no knowledge of the correct key will have a very hard time deciphering the message.

**Key:** A key is a table or a password needed to decipher the encoded data. The length of the key is the factor that determines how difficult it is to decrypt the data if it falls in the wrong hands.

**Public and private keys:** SSL uses a method of encryption called public key encryption — a system that uses two keys. A public key is known to everyone and a private key is known only to the recipient of the message. The public key is mathematically linked to the private key in such a way that only the public key can be used to encrypt a message and only the private key can be used to decrypt it. Just in case the public key is intercepted by a third party, it is virtually impossible to guess what the private key is based on the public key.

**Session key:** A randomly generated key that is used for one transaction and then discarded when the session is closed.

PC X Server > Desktop Consolidation > X Window > Unix integration > NFS v4 > Mainframe > Terminal Emulation > Security > SSL > Web-to-host > Cost Reduction > AS/400 > Mobile Workers  
Standardization > Kerberos > Smart Card > X Desktop Sharing > WebNFS > Web Deployment > Linux > PC X Server > Desktop Consolidation > X Window > Unix integration > NFS v4 > Mainframe  
Reducing Business Disruption > TN3270E > TN5250E > Easy Migration Path > Bi-directional NFS > Desktop Standardization > Kerberos > Smart Card > X Desktop Sharing > WebNFS > Web Deployment  
Mobile Workers > Thin X Protocol > Public Private Keys Authentication > Secure Shell > Telnet > FTP > Reducing Business Disruption > TN3270E > TN5250E > Easy Migration Path > Bi-directional



**Hummingbird®**

Transforming Information into Intelligence™

**Corporate Headquarters**

1 Sparks Avenue, Toronto, Ontario M2H 2W1 Canada

Toll Free Canada/USA: 1 877 FLY HUMM (359 4866)

Tel: +1 416 496 2200

Fax: +1 416 496 2207

E-mail: [getinfo@hummingbird.com](mailto:getinfo@hummingbird.com)

For more information, visit <http://connectivity.hummingbird.com>

**North American Sales Offices**

Boston • Chicago • Dallas • Los Angeles • Mountain View

New York • Ottawa • Toronto • Washington DC

**International Sales Offices**

Amsterdam • Brussels • Frankfurt • Geneva • London • Milan

Munich • Paris • Rome • Seoul • Singapore • Stockholm • Sydney

Tokyo • Wokingham • Zurich

WP-03-00-EN-0045.12/05

Copyright © 2005, Hummingbird Ltd. All rights reserved.

®™ — Trademarks and logos are the intellectual property of Hummingbird Ltd.

All other company and product names are trademarks of their respective owners.