



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

NXi Communications, Inc

WHITE PAPER
"NTS 7 SECURITY ISSUES"

July 12, 2008

A. INTRODUCTION

1. Overview of NTS

NTS 7 is a TCP/IP network based client/server communication system for text chat and text messaging. Once the NTS client software program is installed on a networked computer, this computer becomes accessible to the TTY devices used by the deaf and other NTS users for both incoming and outgoing calls and messages. Other benefits include text chat, text messaging, and secure instant messaging between desk top computers, wireless PDAs (personal digital assistants), e-mail, and optionally, browsers and other devices.

An organization-wide NTS system can make every employee with a networked computer accessible to the deaf in a cost effective manner. An NTS system can bring many other advantages as well.

Most large organizations today provide some degree of communications access for the TTY devices used by the deaf. An analog phone line is typically placed at selected desk tops, and a TTY or TTY modem is connected. The PC at this location can then accept or make TTY calls. However, this analog phone line and TTY modem hardware are themselves a security concern. The computer at this station is usually networked, and it may be possible for someone to install a high speed modem and RAS (remote access server) protocols on this computer connected to the PSTN (Public Switched Telephone Network).

From a security viewpoint, NTS can improve organizational network security by removing the need for analog phone lines and TTY modems at the desk top. Using NTS, all phone lines and modem hardware can be centralized in one or more locations, and all employees of the organization can "share" these phone lines and modem hardware over the network for TTY calls, instant messaging, and text chat.

NTS improves network security by removing analog phone lines from networked computers, but it focuses security concerns on the NTS system itself. This white paper will discuss these security concerns.

2. Security issues

There are two separate "security" issues to be considered in implementing an NTS system:

- (1) Are NTS messages and conversations themselves encrypted and secure? Can the NTS live text or messages be viewed or intercepted as they travel over the LAN/WAN or internet?
- (2) Does NTS compromise the organization's network security?



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

These security issues will be discussed below.

3. "Security issues... the short answer"

Some organizations may require simply a short explanation and a written guarantee from NXI that the NTS system will not compromise the organization's network security. This section is for this type of organization. Some other organizations may wish to delve more deeply into details and/or follow NXI's recommendations as described below. This latter type of organization will want to consider the later sections of this white paper as well.

The NTS network system is extremely secure and it is not possible to "hack" into a network through phone lines connected to NTS servers or by using any NTS gateway or software module. NTS has been in use at extremely secure networks at federal agencies since 1996. For example, in late 2004 NTS passed an extensive security review and was approved for deployment on the Navy Marine Corp Intranet (NMCI) system, as well as many other U.S. Dept of Defense sites.

Why is NTS so secure? The answer to this question lies in the NTS design and the following factors.

1. NTS is a single-purpose product for text chat and text messaging. All NTS operations are carried out via defined NTS "packets". It is not possible to "break out" of these defined NTS packets to do things not defined by the NTS feature list.
2. NTS has never, nor will it ever, support "RAS" (Remote Access Server) protocols like PPP or SLIP for network access. It is not possible to "hack" into a network via NTS because the underlying support for such access is simply not contained in the NTS product.
3. PSTN access: most NTS sites include an NTS Telephony Server connected to phone lines for PSTN access for the TTY devices used by deaf persons. It is not possible to hack into an organization's network from an NTS Telephony Server for several reasons, including:
 - (1) The NTS Telephony Servers support only very low speed and primitive protocols such as the 45 baud 5-bit "Baudot" code used by TTY's. NTS may optionally also support low speed 300 baud connections, but higher speed modem protocols are not supported. Even 300 baud support can be disabled if desired, and this leaves only the 5-bit 45 baud "Baudot" TTY text protocol on phone lines.
 - (2) The NTS 7 Telephony Servers only use "voice cards" that are not modems. The 45 baud TTY protocol has been added to these voice cards, but high speed modem capability is not present or possible.
 - (3) Reason 1 above. Persons connecting to the NTS Telephony Server are locked into the NTS packet system.
 - (4) Reason 2 above. Persons connecting to the NTS Telephony Server cannot access RAS type functions because this functionality is simply not in the NTS product.



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

NXi Communications, Inc. stands behind the security of the NTS product. NTS has been designed from the ground up with network and organizational security in mind, and NTS will not compromise network security.

There are further steps that an organization can take to guarantee that NTS is in fact "encapsulated" from access to computers on the network. These additional steps are described below.

B. OVERVIEW OF THE NTS ARCHITECTURE

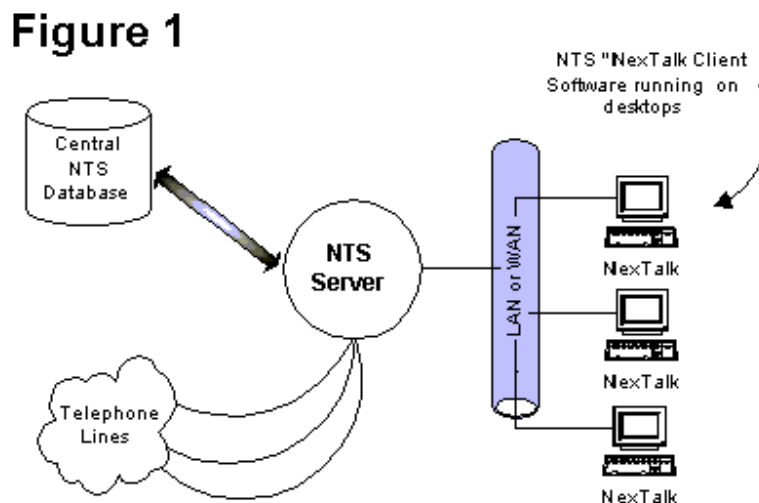
The present section provides an overview useful in the security discussion which follows.

The NTS 7 system can be broken into the following two primary pieces: NTS client software running on user's computers, and NTS "services" running on the NTS server. NTS services come in two basic types: (a) "gateways" converting from some non-NTS protocol to the native NTS protocols, and (b) other NTS services performing some function in the NTS system.

From a security standpoint, the NTS services which are "gateways" are of most interest. NTS gateways are discussed below.

An NTS "domain" is a community of NTS users and services sharing the same central databases and domain security rules.

A drawing of a typical NTS systems is shown below.



"LAN/WAN view of a simple NTS system"

Figure 1 above shows a LAN or WAN, a single NTS server on the network, and a few desk top machines also on the network. The desk top machines will run the NTS client software called "NexTalk". The NTS server and desk top machines might be in a single building on a small local



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

area network, or might be separated by thousands of miles on a wide area network. NTS systems range from 5 users and can scale to many thousands of users.

Every NTS client creates a "link" to an NTS RPS Gateway within an NTS server. "RPS" stands for "Remote Proxy Client". Each such NTS client logs into a RPS, and on log in each component negotiates with the RPS a unique encryption key using a 1024 bit Diffie Hellman technique. Each NTS link is then 256 bit AES encrypted. "AES" is the standard for encryption widely used by the U.S. federal government.

So, each NTS client obtains a new encryption key on each login to NTS, and no two NTS clients share the same encryption key. If someone could break the 256 bit AES encryption on a given client connection, a very difficult task, this feat would not help in decoding communications to any other client traveling over the network.

NTS is a bit unusual in its architecture. Every NTS link is a persistent TCP/IP socket connection that is kept in place even when there is no data flowing. Each NTS link from a client to the server is in effect an encrypted VPN "tunnel".

NTS clients connect to NTS servers the same way, even if there are network segments or firewalls present on the LAN or WAN. As long as the NTS client can create the single encrypted link needed to the server, it does not matter how the LAN or WAN network is segmented or the structure of the network topology. An important point is that the persistent TCP/IP connection above is established FROM the NTS client TO the NTS server and never in the reverse direction. The importance of this feature is discussed in the next section.

It should also be noted that the approach above works in a Citrix or Terminal Services environment.

C. RECOMMENDED IMPLEMENTATION TECHNIQUES FOR NTS SYSTEMS

Highly secure organizations may wish to implement NTS in the following manner. NXI stands behind the security of the NTS product on a network, and most NTS sites will not implement the security model described below. However, the three steps described can provide additional security guarantees.

First, the NTS server should be placed on an isolated network segment or network "DMZ", separated from the organization's LAN or WAN by a firewall.

Second, the firewall separating this NTS network segment from the organization's LAN/WAN should be opened only in this manner: all desk top machines running the NTS client should be allowed to connect to the NTS server, but only on the selected NTS port (default is port 2591). This "pinhole" one-way opening should be allowed FROM the LAN/WAN side TO the NTS server and not the reverse. Note that the NTS server(s) cannot make a connection to any organization server, or any other computer, outside its DMZ since the NTS server cannot initiate any connection outbound across the firewall.

A drawing of the suggested approach is shown below in Figure 2.



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

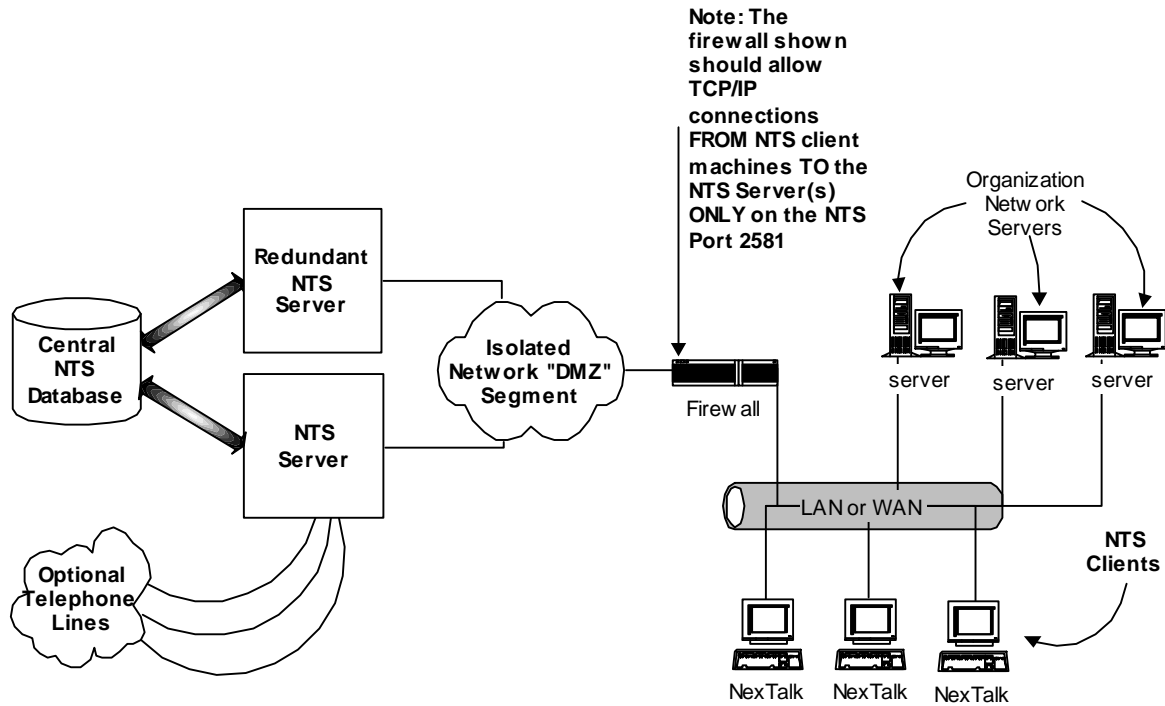


Figure 2

"LAN/WAN view of an encapsulated NTS system"

Note that Figure 3 shows an optional second NTS server. When two or more NTS servers are present there is automatic load balancing and redundancy set up between the NTS servers.



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

D. NTS "GATEWAYS"

NTS "gateways" allow access to the outside world for text chat or messaging. There are currently three types of NTS gateways:

- (1) RPS Gateway for client logins (RPS)
- (2) Telephony Servers (TS)
- (3) Internet Gateways (IG)

Individual NTS sites may implement one or more of these gateways. What does each gateway provide and how might each affect network security?

NTS RPS Gateway:

The NTS RPS Gateway was described above. All NTS clients connect to an NTS server by creating a single, persistent, encrypted TCP/IP connection to an RPS module. There can be multiple RPS modules on separate NTS servers for scalability and redundancy.

NTS Telephony Servers:

NTS Telephony Servers connect to phone lines, and allow voice phones or the TTY/TDD devices used by the deaf to call or be called by the NTS system over the PSTN. A single NTS TS connected to one or more phone lines means that all NTS users are accessible to the TTY devices used by the deaf. All NTS users "share" modems or voice cards present on Telephony Servers for TTY calls.

TTY, or voice, calls over normal phone lines are not encrypted on the phone line itself. However, once the text of a TTY conversation enters NTS, then all text communications are encrypted within NTS.

As discussed above, an NTS Telephony Server is not a danger to the network security of an organization. This is because (a) NTS does not contain any remote access protocols, (b) NTS does not support standard high speed modem protocols, and (c) the text communications onto phone lines supported by NTS is normally limited to the 5-bit 45 baud TTY protocol. Most people can type faster than TTYs can send.

NTS Internet Gateway (IG)

The NTS IG provides access from browsers. The NTS IG is a specialized web server that can serve custom NTS Java applets to browsers. The NTS Java applet creates a link to the IG, and in turn allows anyone on a browser to create calls or send messages into NTS domains.

Nxi Communications maintains an Internet Gateway on its freeware NTS system at www.nextalk.net. In this implementation, the Java applet delivered to a browser creates an encrypted SSL connection to a standard Apache web server in Nxi's data center, and this Apache server proxies this text connection to an NTS Internet Gateway in the NexTalk.net NTS system. Communications between the browser user and an NTS client, or other points in the NTS architecture, are end-to-end encrypted.

The NTS Internet Gateway is not normally run by individual NTS domains.



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

E. Communications between separate NTS servers within an NTS system.

In most NTS systems there is a single NTS server, and communications outside this server occur only via encrypted links between NTS clients and the RPS module. However, NTS 7 supports more than one NTS server in a system, and these servers in turn support dynamic load balancing, scalability to large systems, and redundancy in NTS operation. What about communications security between separate NTS servers ?

In order to improve scalability to large systems, NTS does not normally encrypt communications between NTS server-side modules. Server modules include processes or executable modules such as the NTS Data Services, Locator Service, Message Delivery Service, RPS, Telephony Server, and so on. If an NTS system has only one NTS server, then the communications between these server processes are all internal to the server, and encryption is not needed. But in the case where there are two or more NTS servers this issue should be considered.

A common situation is that multiple NTS servers are all on the same protected DMZ subnet, and in this case inter-server-module communications do not need to be encrypted on this protected network.

In the case where NTS servers are separated, and not on the same DMZ subnet, then the security of inter-server-module communications between NTS servers should be reviewed. Suppose two NTS servers are placed in two separate DMZ's at two separate data centers, and these two NTS servers are part of the same NTS system or domain. In this case, an obvious approach is to implement an encrypted VPN tunnel between these two data centers, and allow the NTS servers to communicate over this encrypted link. This approach will solve this issue.

NXi also offers a means to encrypt NTS inter-server-module communications. This approach will have some effect on the scalability and performance of the NTS system. Contact NXi for details in this area.

F. Summary

The network security of an organization using NTS is ensured by the single purpose design of the NTS product, and by "encapsulation" of the NTS system from the desk top machine and network resources. NTS has always been a text chat and text messaging product. File transfers, file attachments, document sharing, and remote network access have never been part of the base NTS system, and the NTS designers have never lost sight of network security issues in the design of the NTS system.