NexTalk

NexTalk, Inc

WHITE PAPER
"NexTalk SECURITY ISSUES"

A. INTRODUCTION

1. Overview of NexTalk

NexTalk is a TCP/IP network-based client/server communication system for text chat and text messaging. Once the NexTalk client software program is installed on a networked computer, this computer becomes accessible to the TTY devices used by the deaf and other NexTalk users for both incoming and outgoing calls and messages. Other benefits include text chat, text messaging, and secure instant messaging between desktop computers.

An organization wide NexTalk system can make every employee with a networked computer accessible to the deaf in a cost-effective manner. A NexTalk 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 desktops, 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, NexTalk can improve organizational network security by removing the need for analog phone lines and TTY modems at the desktop. Using NexTalk, 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.

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

2. Security issues

There are two separate "security" issues to be considered in implementing a NexTalk system:

(1) Are NexTalk messages and conversations themselves encrypted and secure? Can the NexTalk live text or messages be viewed or intercepted as they travel over the LAN/WAN or internet?

(2) Does NexTalk compromise the organization's network security?

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 NexTalk that the NexTalk 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 NexTalk's recommendations as described below. This latter type of organization will want to consider the later sections of this white paper as well.

The NexTalk network system is extremely secure, and it is not possible to "hack" into a network through phone lines connected to NexTalk servers or by using any NexTalk gateway or software module. NexTalk has been in use at extremely secure networks at federal agencies since 1996. For example, in late 2004 NexTalk 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 NexTalk so secure? The answer to this question lies in the NexTalk design and the following factors.

1. NexTalk is a single-purpose product for text chat and text messaging. All NexTalk operations are carried out via defined NexTalk "packets". It is not possible to "break out" of these defined NexTalk packets to do things not defined by the NexTalk feature list.

2. NexTalk 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 NexTalk because the underlying support for such access is simply not contained in the NexTalk product.

3. PSTN access: most NexTalk sites include a NexTalk 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 a NexTalk Telephony Server for several reasons, including:

    (1) The NexTalk Telephony Servers support only very low speed and primitive protocols such as the 45 baud 5-bit "Baudot" code used by

TTY's. NexTalk 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 NexTalk 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 NexTalk Telephony Server are locked into the NexTalk packet system.

(4) Reason 2 above. Persons connecting to the NexTalk Telephony Server cannot access RAS type functions because this functionality is simply not in the NexTalk product.

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

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

B. OVERVIEW OF THE NexTalk ARCHITECTURE

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

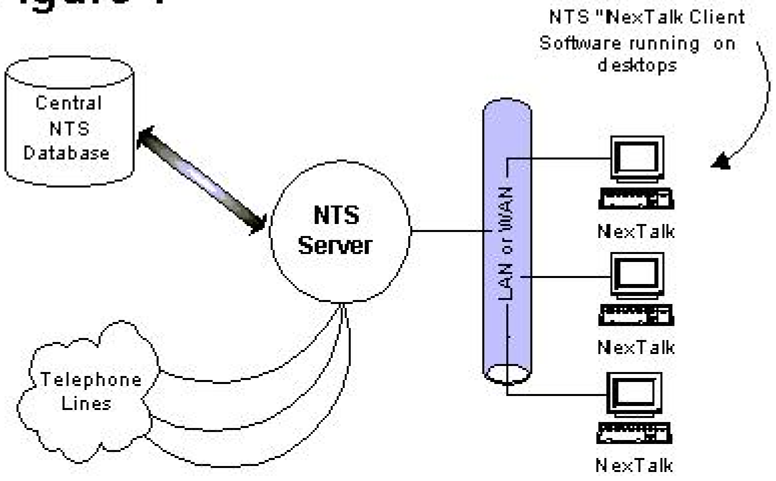
The NexTalk system can be broken into the following two primary pieces: NexTalk client software running on user’s computers, and NexTalk “services” running on the NexTalk server. NexTalk services come in two basic types: (a) “gateways” converting from some non-NexTalk protocol to the native NexTalk protocols,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

From a security standpoint, the NexTalk services which are “gateways” are of most interest. NexTalk gateways are discussed below.

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

A drawing of a typical NexTalk system is shown below.

Figure 1



"LAN/WAN view of a simple NexTalk system"

Figure 1 above shows a LAN or WAN, a single NexTalk server on the network, and a few desk top machines also on the network. The desktop machines will run the NexTalk client software called the "SimpliciTTY" client. The NexTalk server and desktop machines might be in a single building on a small local area network or might be separated by thousands of miles on a wide area network. NexTalk systems range from 5 users and can scale to many thousands of users.

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

So, each NexTalk client obtains a new encryption key on each login to NexTalk, and no two NexTalk 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.

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

NexTalk clients connect to NexTalk servers the same way, even if there are network segments or firewalls present on the LAN or WAN. As long as the NexTalk 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 NexTalk client to the NexTalk 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, and VDI environments.

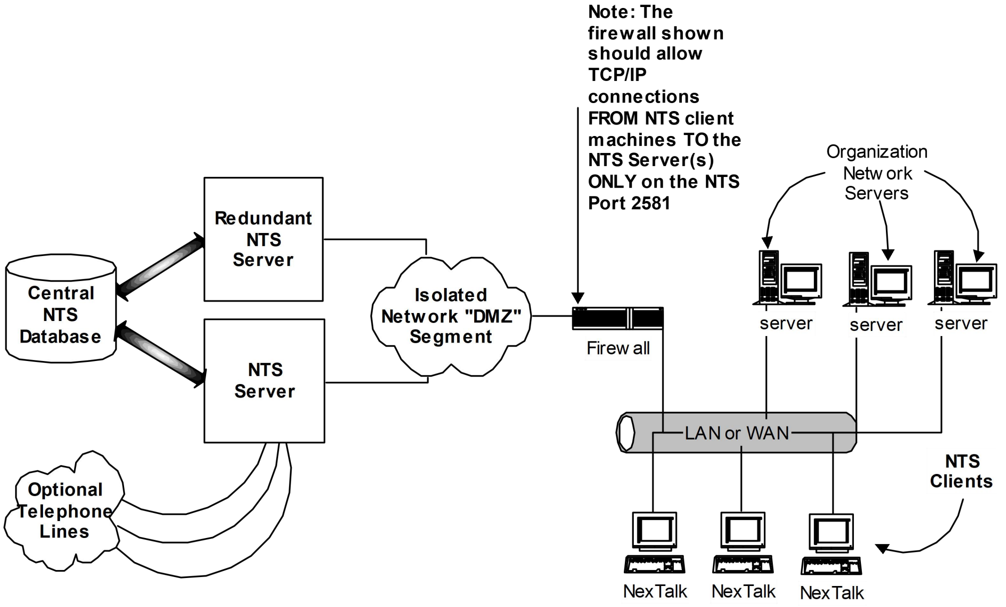
C. RECOMMENDED IMPLEMENTATION TECHNIQUES FOR NexTalk SYSTEMS

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

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

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



Note: The firewall shown should allow TCP/IP connections FROM NTS client machines TO the NTS Server(s) ONLY on the NTS Port 2581

Figure 2

"LAN/WAN view of an encapsulated NexTalk system"

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

D. NexTalk "GATEWAYS"

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

(1) RPS Gateway for client logins (RPS)
(2) Telephony Servers (TS)

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

NexTalk RPS Gateway:

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

NexTalk Telephony Servers:

NexTalk Telephony Servers connect to SIP “phone lines” and allow voice phones or the TTY/TDD devices used by the deaf to call or be called by the NexTalk system over the PSTN. A single NexTalk TS connected to one or more phone lines means that all NexTalk users are accessible to the TTY devices used by the deaf. All NexTalk 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 NexTalk, then all text communications are encrypted within NexTalk.

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

E. Communications between separate NexTalk servers within a NexTalk system.

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

In order to improve scalability to large systems, NexTalk does not normally encrypt communications between NexTalk server-side modules. Server modules include processes or executable modules such as the NexTalk Data Services, Locator Service, Message Delivery Service, RPS, Telephony Server, and so on. If a NexTalk system has only one NexTalk 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 NexTalk servers this issue should be considered.

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

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

F. NexTalk Hosted Environments.

As more and more organizations move away from on-premise solutions, and move to hosted environments, security becomes more of a concern as this could open other possible vulnerabilities. The security aspects and architecture described above applies to our secure hosted environments. There are different types of hosted options that are available to you.

1. General hosted platform: This platform is a good fit for most of our customers that want a "no frills", secure SaaS platform. This environment is hosted in our multi-tenant environment. All customers share the same database however, each NexTalk domain is "siloed", and others will not see your data.
    a. All traffic is secured with 256-bit AES encryption
    b. Connections from our servers to the database are encrypted
    c. Data at rest is encrypted as well using SQL Server's TDE (Transparent Data Encryption)
    d. All our hosted environments are SOC compliant

2. Hosted Private/Hybrid Servers: Customers that require a more secure environment such as banks, healthcare providers, etc. NexTalk will deploy This type of setup allows you to utilize your own SQL database, SAML, firewall rules, or even SIP telephony ports. This setup allows your organization full control of the environment.

G. Sumamry.

The network security of an organization using NexTalk is ensured by the single purpose design of the NexTalk product, and by "encapsulation" of the NexTalk system from the desk top machine and network resources. NexTalk 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 NexTalk system, and the NexTalk designers have never lost sight of network security issues in the design of the NexTalk system.