Potential Vulnerabilities of Timbuktu Remote Control Software

This document is intended to explain the functionality and potential vulnerabilities of the Windows Remote Access/Remote Control Software application called Timbuktu. It has been said that "A picture is worth a thousand words." This is certainly the case when working with end-users who experience problems using a particular piece of software or perform some process with their Windows workstation. Using remote control software to identify the specific error messages or observe a series of dialog boxes can be dramaticall...

Potential Vulnerabilities of Timbuktu Remote Control Software
David Batz
October 9, 2002

Abstract:

The Problem: In today's connected world, there is often a need for help desk personnel or support staff to access end-user Windows workstations or remote servers. Many times, the devices being accessed may be geographically dispersed (hundreds or thousands of miles away) from support personnel.

Timbuktu – A Solution to the Problem? Disclaimer: The reader should understand that although this paper is neither for nor against the use of Timbuktu software as a Windows Remote Access /Remote Control solution, there are a number of potentially serious vulnerabilities that may be encountered through the use of the product. After reviewing the issues and potential responses the reader will be better equipped to make an informed decision about remote control products in general, and Timbuktu specifically.

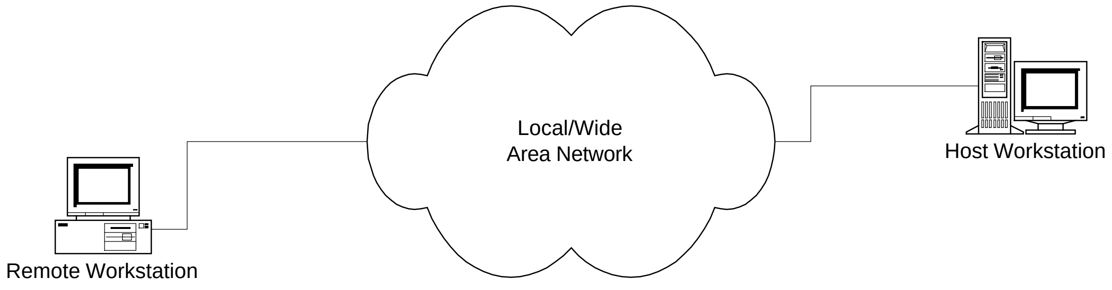
Introduction:

This document is intended to explain the functionality and potential vulnerabilities of the Windows Remote Access/Remote Control Software application called Timbuktu.

It has been said that "A picture is worth a thousand words." This is certainly the case when working with end-users who experience problems using a particular piece of software or perform some process with their Windows workstation. Using remote control software to identify the specific error messages or observe a series of dialog boxes can be dramatically more efficient than attempting to wade through fuzzy or inaccurate descriptions of problems.

There are a number of technical solutions available to address the challenge of remote access to windows hosts. These solutions include: Symantec PC Anywhere, VNC, Citrix, and Windows Terminal Service. This paper is concerned with Timbuktu Pro 2000 (Version 2.0 Build 815 Es) deployed on Windows 2000 devices (Professional and Server.) The product is developed by Netopia Inc., http://www.netopia.com/en-us/software/products/tb2/index.html.

Communications Overview



Client software on the remote workstation connects to a set of services on the host. In order to provide for total unattended connectivity on the Timbuktu host, several programs are started as services. A detailed explanation of the connection process will be covered later in the paper.

Remote access privileges to the host machine are controlled by a single file; tb2.plu. By default, this file is located in the following directory structure:
C:\Program Files\Timbuktu Pro. –1 (Blue Boar-insecure.org)

Communication Services

Timbuktu software supports seven flavors of functionality:

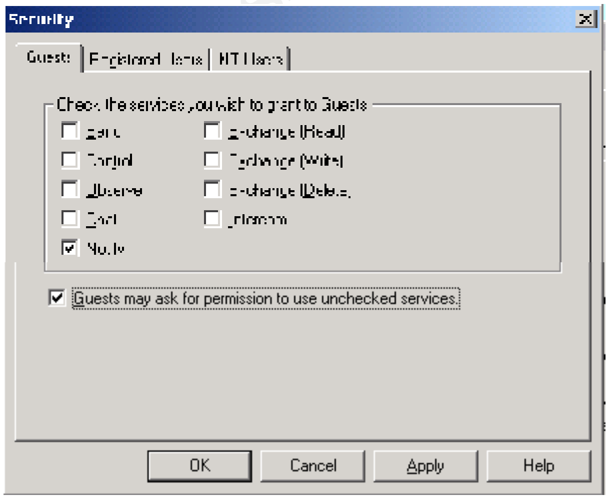
- **Send** allows users to send messages with attached files and folders to a remote host
- **Exchange** allows users to access the hard drive of a remote Timbuktu Pro host — even a Macintosh. Authorized users can copy and move files and folders between computers and delete files from either computer
- **Control** allows users to control a remote host from their own desktop
- **Observe** allows users to observe a remote host without controlling it
- **Notify** alerts users when a remote Timbuktu Pro host becomes active.
- **Chat** allows users to carry on a keyboard conversation with a remote user
- **Intercom** allows users to speak directly to a remote user through a host's audio hardware

Timbuktu supports three different types of users

- Guest Users (which include Ask for Permission Users and Temporary Guests)
- Registered Users
- Windows Domain Users. –2 (Netopia Help File)

On a Windows 2000 machine, a graphical user interface is used to configure Timbuktu User-Ids, passwords, and user access rights.

Guest Access



Check the services you wish to grant to Guests

□ Send
□ Control
□ Observe
□ Chat
☑ Notify
□ Exchange (Read)
□ Exchange (Write)
□ Exchange (Delete)
□ Intercom

☑ Guests may ask for permission to use unchecked services.

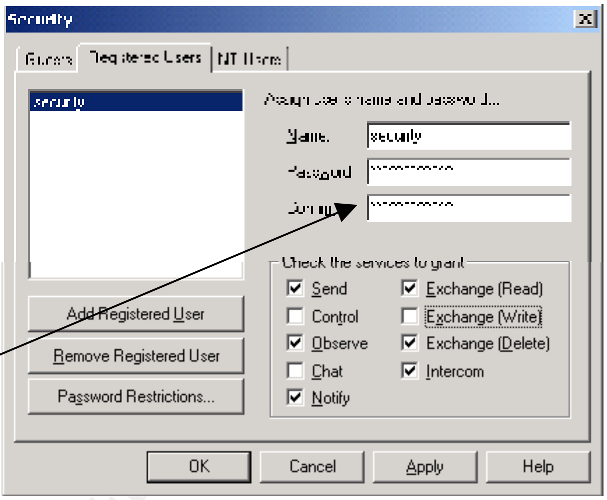
In Timbuktu, Guests function as a global "Everyone" group. Any rights granted to Guest users are implicitly granted to all workstations with the Timbuktu software. Rights granted to the "Guests" group may **not** be removed from "Registered Users" or "NT Users." **Extreme caution should be used when defining "Guest" access**. Guest privilege information is stored in the following directory structure: C:\Program Files\Timbuktu Pro\tb2.plu.

Registered User Access

In this dialogue, the system administrator can define specific users, and their associated privileges. Registered User names, encoded passwords, and privileges are also stored in the tb2.plu file.

This file will be examined in detail later in this paper.

Although the password entry field looks quite large, the maximum password length is 15 characters.


Security

security

Assign user's name and password...

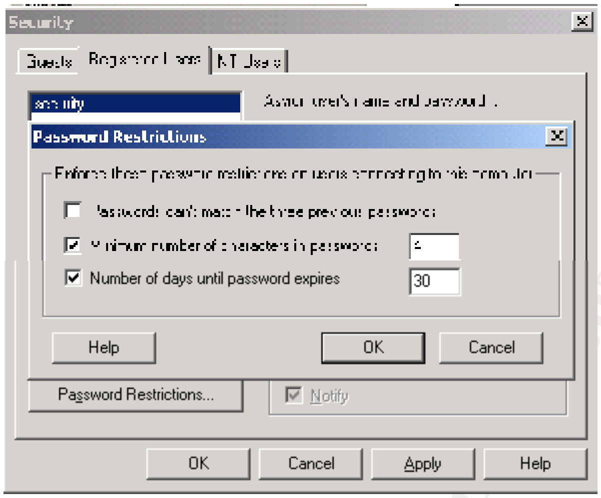
Name: security
Password: ***************
Confirm: ***************

Check the services to grant
☑ Send
☐ Control
☑ Observe
☐ Chat
☑ Notify
☑ Exchange (Read)
☐ Exchange (Write)
☑ Exchange (Delete)
☑ Intercom

The system administrator can also define *some* Password Restrictions for Registered Users.

As can be seen in the dialog box, the abilities to enforce specific password restrictions (policies) are limited to:

- A password may not match any of the previous three passwords
- Passwords must be a minimum length (the application does not support password lengths greater than 15 characters)
- Passwords can be set to expire in the future


Security

security

Assign user's name and password...

Password Restrictions

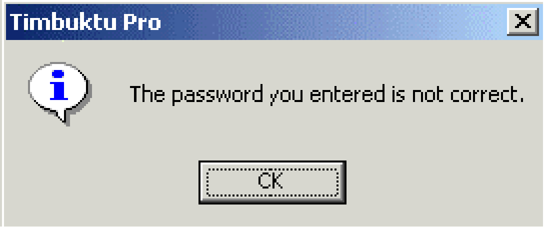
Enforce these password restrictions on users connecting to this computer
☐ Passwords can't match the three previous passwords
☑ Minimum number of characters in password: 4
☑ Number of days until password expires: 30

Timbuktu does **not** prevent "weak" passwords:

- Dictionary words (including foreign and technical dictionaries)
- Anyone's or anything's name
- A person, place or thing
- A proper noun
- A phone number
- Passwords of the same character (e.g aaa)
- Simple pattern of letters on keyboards (e.g. qwerty)
- Any of the above reversed or concatenated (e.g. ytrewq)
- Any or the above with digits prepended or appended (e.g. aaa1)

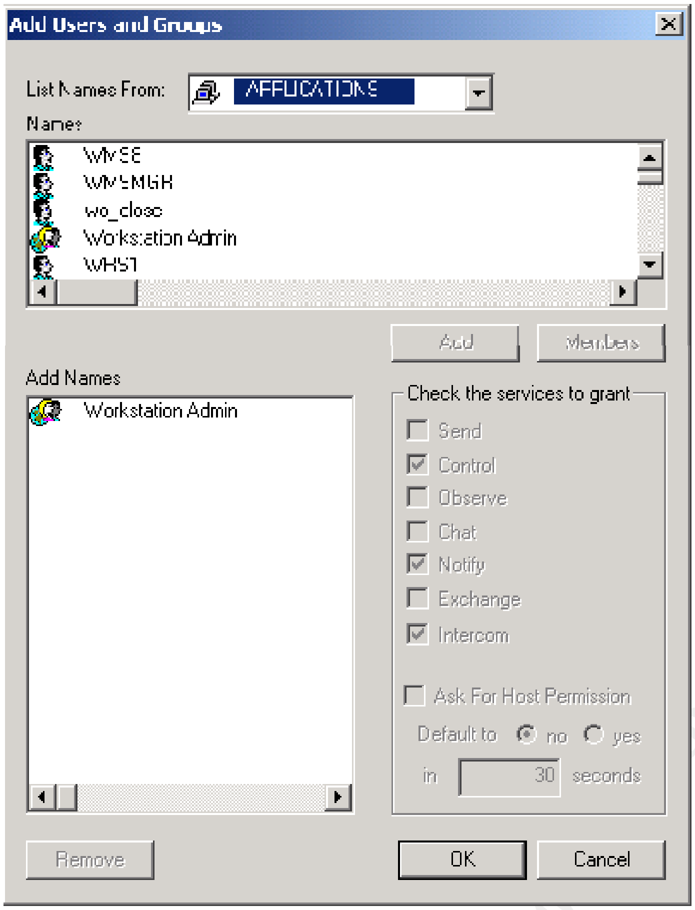
-3 (Maui High Performance Computing Center Kerberos Password Policy)

Timbuktu does not support a "Hard" lockout in the event that a Registered User supplies an incorrect password repeatedly. An attacker can keep banging on a host machine.


Timbuktu Pro

The password you entered is not correct.

NT User Access



Add Users and Groups

List Names From: APPLICATIONS

Names:
- WMSE
- WMSMGR
- wo_close
- Workstation Admin
- WRST

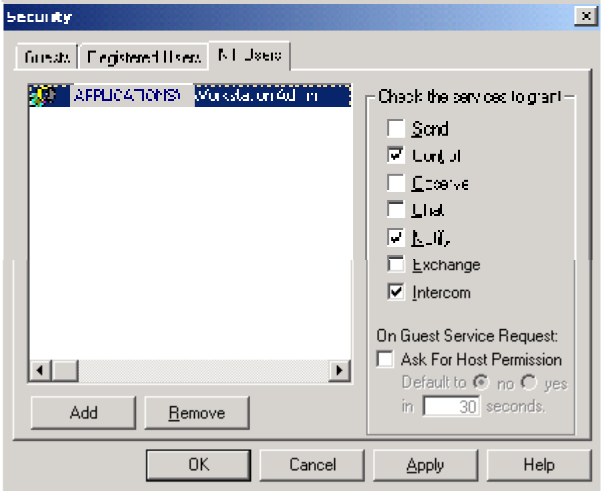
Add Names:
- Workstation Admin

Check the services to grant
- □ Send
- ☑ Control
- □ Observe
- □ Chat
- ☑ Notify
- □ Exchange
- ☑ Intercom

□ Ask For Host Permission

Default to ● no ○ yes

in 30 seconds



Security

APPLICATIONS\Workstation Admin

Check the services to grant
- □ Send
- ☑ Control
- □ Observe
- □ Chat
- ☑ Notify
- □ Exchange
- ☑ Intercom

On Guest Service Request:

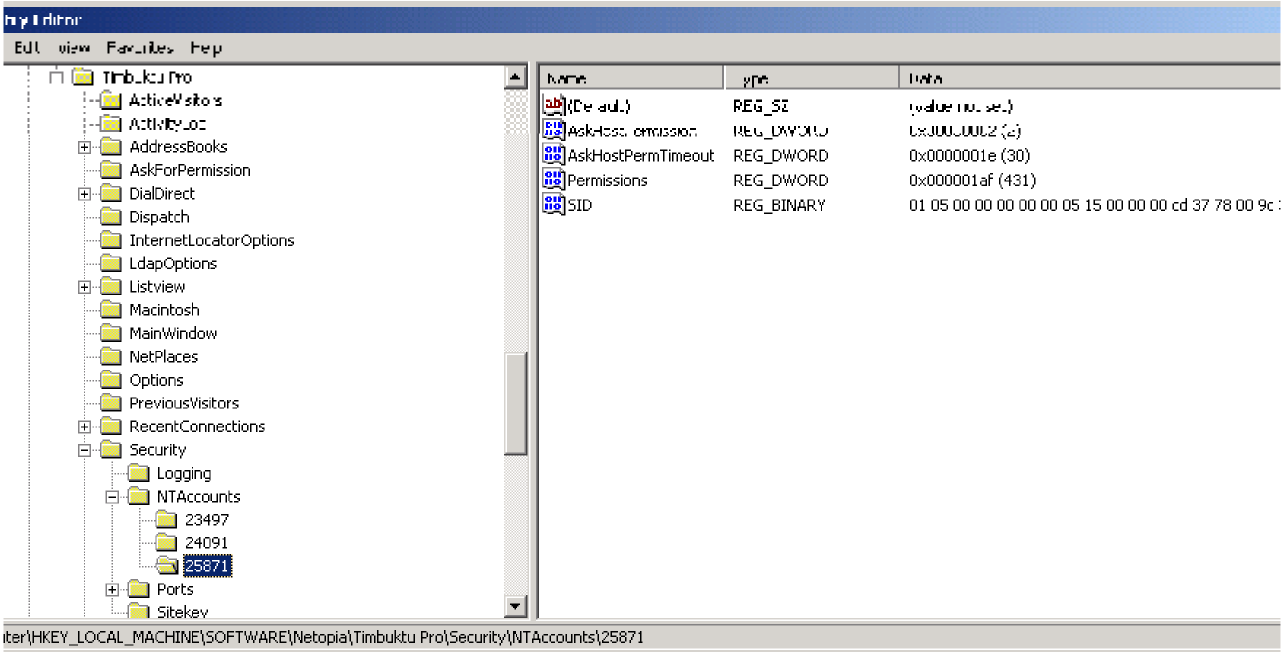
□ Ask For Host Permission

Default to ● no ○ yes

in 30 seconds.

If the Timbuktu host is part of a NT Domain, the system administrator may add individual NT user or group account access. In this situation, there is no opportunity to use a password policy specific to Timbuktu. The password policy of the NT domains is inherited, and used by Timbuktu. When NT Users are selected, information about the specific User ID and rights attributes are placed into the NT registry, rather than a configuration file in the Timbuktu sub-directory.

This graphic shows the Registry entries for a Timbuktu configuration with three NT Users identified. Each User has their own registry Key defined under the NTAccounts Key.

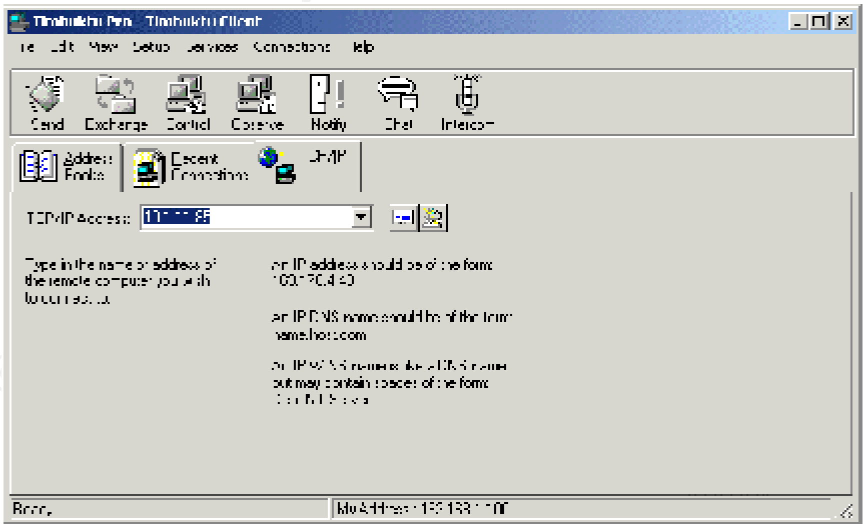


Name	Type	Data
(Default)	REG_SZ	(value not set)
AskHostPermission	REG_DWORD	0x00000002 (2)
AskHostPermTimeout	REG_DWORD	0x0000001e (30)
Permissions	REG_DWORD	0x000001af (431)
SID	REG_BINARY	01 05 00 00 00 00 00 05 15 00 00 00 cd 37 78 00 9c :

...ter\HKEY_LOCAL_MACHINE\SOFTWARE\Netopia\Timbuktu Pro\Security\NTAccounts\25871

Using the product:

The Graphical User Interface of Timbuktu (as a client) has the following appearance:



TCP/IP Access: 17[illegible]85

Type in the name or address of the remote computer you wish to connect to.

An IP address should be of the form: 100.170.4.40

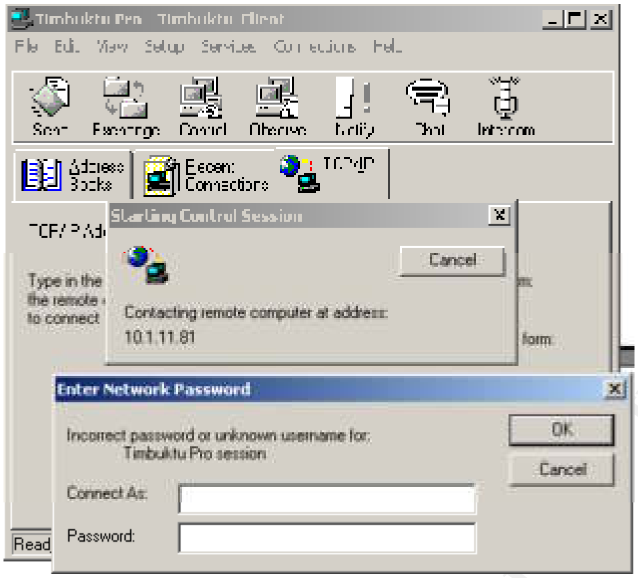
An IP DNS name should be of the form: name.host.com

An IP WINS name is like a DNS name but may contain spaces of the form: [illegible]

My Address: 192.168.1.100

After typing a computer name or address, the end-user clicks on the appropriate function, such as Send, Exchange, Control, etc.

On Windows 2000 platforms, the Timbuktu Host software assumes that the primary application authentication will be based on Windows Domain membership. When this is not the situation, the client will be shown the following dialog:



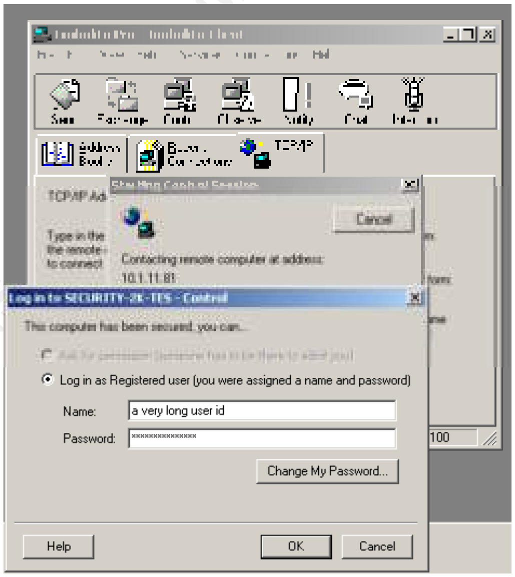
Contacting remote computer at address:
10.1.11.81

Incorrect password or unknown username for:
Timbuktu Pro session

Connect As:

Password:

“Registered and Guest Users” must press the Escape key to encounter the following dialog:



Contacting remote computer at address:
10.1.11.81

This computer has been secured, you can...

○ Ask for permission (Someone has to be there to admit you)

● Log in as Registered user (you were assigned a name and password)

Name: a very long user id

Password: ***************

At this point, the client can enter the Registered User credentials, or if the host system is configured, the client can ask for permission to connect.

Once the Timbuktu client is connected to the host, the client inherits the rights and permissions of the end-user who is logged into the host system. If the Timbuktu host is logged in as an administrator, the remote client gains those privileges.

Let’s take a look at what happens under the covers.

After a default installation, a Timbuktu host will be running the following programs:

Name	**Memory Used**
Tb2RCAssist.exe	1,312 K
Tb2pro.exe	13,796 K
Tb2logon.exe	1,532 K
Tb2launch.exe	884 K

After these programs have started, but before a remote session is established, a Windows Timbuktu host will listen on port 407/UDP.

After a remote session is established, a Windows Timbuktu host will listen on the following ports, depending on the services negotiated during session startup:

Service	**Host Listening Port**
Control	1417 /TCP
Observe	1418 /TCP
Send Files	1419 /TCP
Exchange Files	1420 /TCP
Chat	Dynamic TCP Ports
Notify	Dynamic TCP Ports
Intercom	Dynamic TCP and UDP Ports
Ask for Permission	Dynamic TCP and UDP Ports

-4 (Netopia FAQ Article)

The Following Windump output shows the communications between the Timbuktu Client and Host. This example shows an initiation of a **“Control”** session:

```
22:47:11.358305 timb-client.1540 > Timbuktu-host.407:  udp
22:47:11.363389 Timbuktu-host.407 > timb-client.1540:  udp
22:47:15.324970 timb-client.1541 > Timbuktu-host.407:  udp
22:47:15.330155 Timbuktu-host.407 > timb-client.1541:  udp
22:47:15.332263 timb-client.1542 > Timbuktu-host.407:  udp
22:47:15.341369 Timbuktu-host.407 > timb-client.1542:  udp
```

First two attempts to exchange credentials fail

Third try is the charm

```
22:47:15.342409 timb-client.1543 > Timbuktu-host.1417: S 3257468345:3257468345(0)
win 16384 <mss 1460,nop,nop,sackOK> (DF)      [Now, the initial Syn]
22:47:15.342833 Timbuktu-host.1417 > timb-client.1543: S 3281877292:3281877292(0)
ack 3257468346 win 17520 <mss 1460,nop,nop,sackOK> (DF) [Syn, Ack]
22:47:15.342870 timb-client.1543 > Timbuktu-host.1417: . ack 1 win 17520 (DF) [Ack –
The TCP communications channel is now open,]
```

```
22:47:15.343240 timb-client.1543 > Timbuktu-host.1417: P 1:17(16) ack 1 win 17520 (DF)
[The Timbuktu session starts]
22:47:15.475504 Timbuktu-host.1417 > timb-client.1543: . ack 17 win 17504 (DF)
22:47:15.482306 timb-client.1543 > Timbuktu-host.1417: P 17:32(15) ack 1 win 17520 (DF)
22:47:15.675746 Timbuktu-host.1417 > timb-client.1543: . ack 32 win 17489 (DF)
                                        n
                                        n
                                        n
22:47:19.871644 Timbuktu-host.1417 > timb-client.1543: P 17471:17478(7) ack 88 win 17433 (DF)
22:47:19.965540 timb-client.1543 > Timbuktu-host.1417: R 3257468433:3257468433(0) win 0 (DF) [The client is done with the session, tears down session]
```

Only after the negotiations are complete, is TCP used. -4 (Netopia FAQ Article)

One of the interesting aspects of the session startup is that it relies on the User Datagram Protocol (UDP) for the exchange of user credentials prior to the establishment of the communications channel. Using UDP for exchange of user credentials is rather counter intuitive:

- Sender and recipient of do not keep any information about the state of the communication session between the two hosts
- UDP Simply provides best-efforts delivery; No guarantee that data is delivered reliably or in order
- Endpoints do not maintain state information about the communication
- UDP data is sent and received on a packet-by-packet basis
- Datagrams must not be too big, because if they must be fragmented, some pieces might get lost in transit
- In addition, the use of UDP raises **additional security concerns**:
    - When a socket receives data on a UDP port, it will receive packets sent to it by any host, whether it is participating in the application or not
    - This possibility can present a security problem for some applications that do not distinguish between expected and unexpected packets
      (read: buffer overflow)
    - For these reasons, many network firewall administrators block UDP data from being sent to a protected host from outside the security perimeter
      -5(Australian National University)
      -6(Levier, Laurent)

The exchange of credentials is not particularly time sensitive, nor bandwidth intensive, so the selection of UDP to accomplish this communication is a mystery.

Issue: Stealth Observation or Control of Timbuktu Host Workstations.

Normal (Not connected)	**Timbuktu Connection Type**	**Active Session**	**Greyed-out** (inactive)
	Control		
	Observe		
	File Exchange		

A Timbuktu Host can be observed or controlled with very little notification (to the individual who is using the Host machine.) There is a small Timbuktu status icon located in the lower right corner of the System Tray. This icon is used to display the current status of the Timbuktu software. When the Timbuktu Host is not being controlled, Observed, Exchanging files, etc, the Timbuktu icon appears to be a small computer.

When the Timbuktu Host is **Observed** by a remote client machine, the Normal icon is alternated with the Observe icon. The Timbuktu Status flips between the Normal icon and Observe icon about every five to seven seconds.

When the Timbuktu Host is **Controlled** by a remote client machine, the Normal icon is alternated with the Control icon.

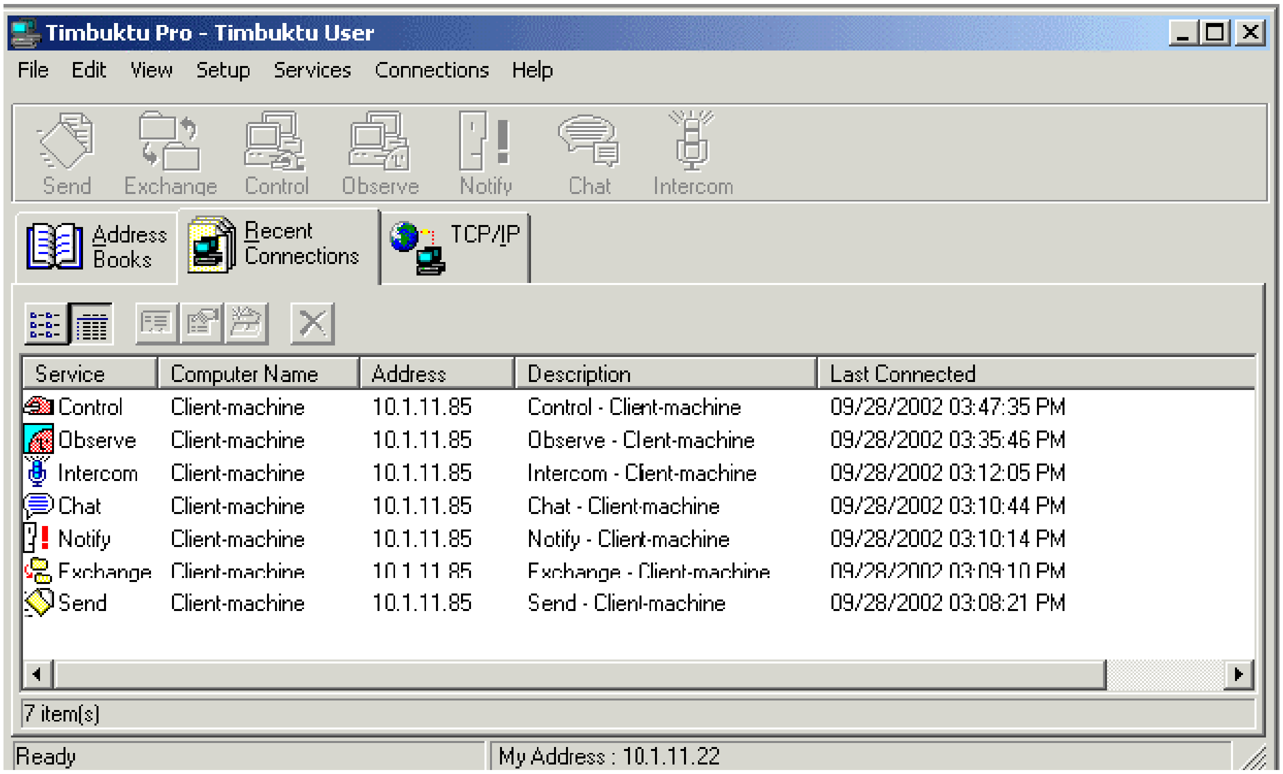
After a Timbuktu session is complete, the Timbuktu status icon alternates between the Normal icon and a "greyed-out" version of the icon based on the function(s) used during the remote session. For example:

Because Timbuktu can not be configured to splash a large notification message/warning across the screen in a remote contol / observe / file exchange situation, there is a risk of an attacker or rogue administrator controlling or observing workstations without the end-user being aware of it.

Potential Attack:
Many users may never notice or understand the significance of a tiny little icon on their task bar changing. Some end users hide the task bar altogether in order to obtain the maximum computer desktop real estate.

Consider the potential damage to a corporation if proprietary business plans or even payroll schedules were being accessed by an individual who was being monitored without their knowledge.

Logging of Timbuktu Events:
There are some tools available to the Timbuktu host machine to identify remote access. When the user of a Timbuktu Host machine double clicks on the Timbuktu status icon, and selects the Recent Activities Tab, they will see *some* entries in the C:\Program Files\Timbuktu Pro\activity.log file. The GUI presentation is below:



Service	Computer Name	Address	Description	Last Connected
Control	Client-machine	10.1.11.85	Control - Client-machine	09/28/2002 03:47:35 PM
Observe	Client-machine	10.1.11.85	Observe - Clent-machine	09/28/2002 03:35:46 PM
Intercom	Client-machine	10.1.11.85	Intercom - Client-machine	09/28/2002 03:12:05 PM
Chat	Client-machine	10.1.11.85	Chat - Client-machine	09/28/2002 03:10:44 PM
Notify	Client-machine	10.1.11.85	Notify - Client-machine	09/28/2002 03:10:14 PM
Exchange	Client-machine	10.1.11.85	Exchange - Client-machine	09/28/2002 03:09:10 PM
Send	Client-machine	10.1.11.85	Send - Client-machine	09/28/2002 03:08:21 PM

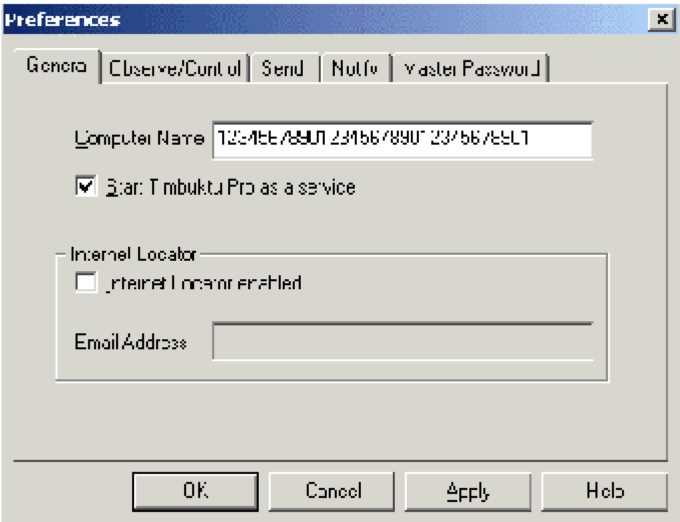
7 item(s)

Ready | My Address : 10.1.11.22

There are some deficiencies with this log:

- It only reports activity where the machine functioned as a Timbuktu host
- The Timbuktu Host end-user can delete entries with ease
- An end-user does not require any form of password or authentication to view or delete entries from this screen
- Once a connection entry has been deleted, it can't be recovered (using Timbuktu)
- It would be reasonable to assume that an attacker would delete entries from this file to cover their tracks
- Another point of interest is the data used to populate the field "Computer Name." This name is not necessarily the NetBIOS name of the remote Workstation. The Administrator of the remote workstation can name the Timbuku Remote Client anything desired.

The maximum Timbuktu Computer name is 31 characters. The following dialog shows where this name can be defined under Setup → Preferences:



Computer Name: 1234567890123456789012345678901

☑ Start Timbuktu Pro as a service

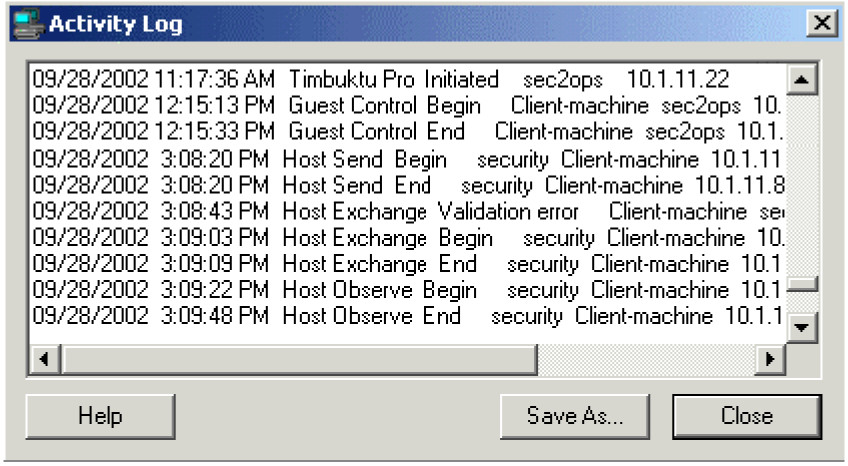
Internet Locator

☐ Internet Locator enabled

Email Address:

An attacker using Timbuktu to remotely control another workstation could modify their Timbuktu station name in an attempt to mask the origin of unauthorized access.

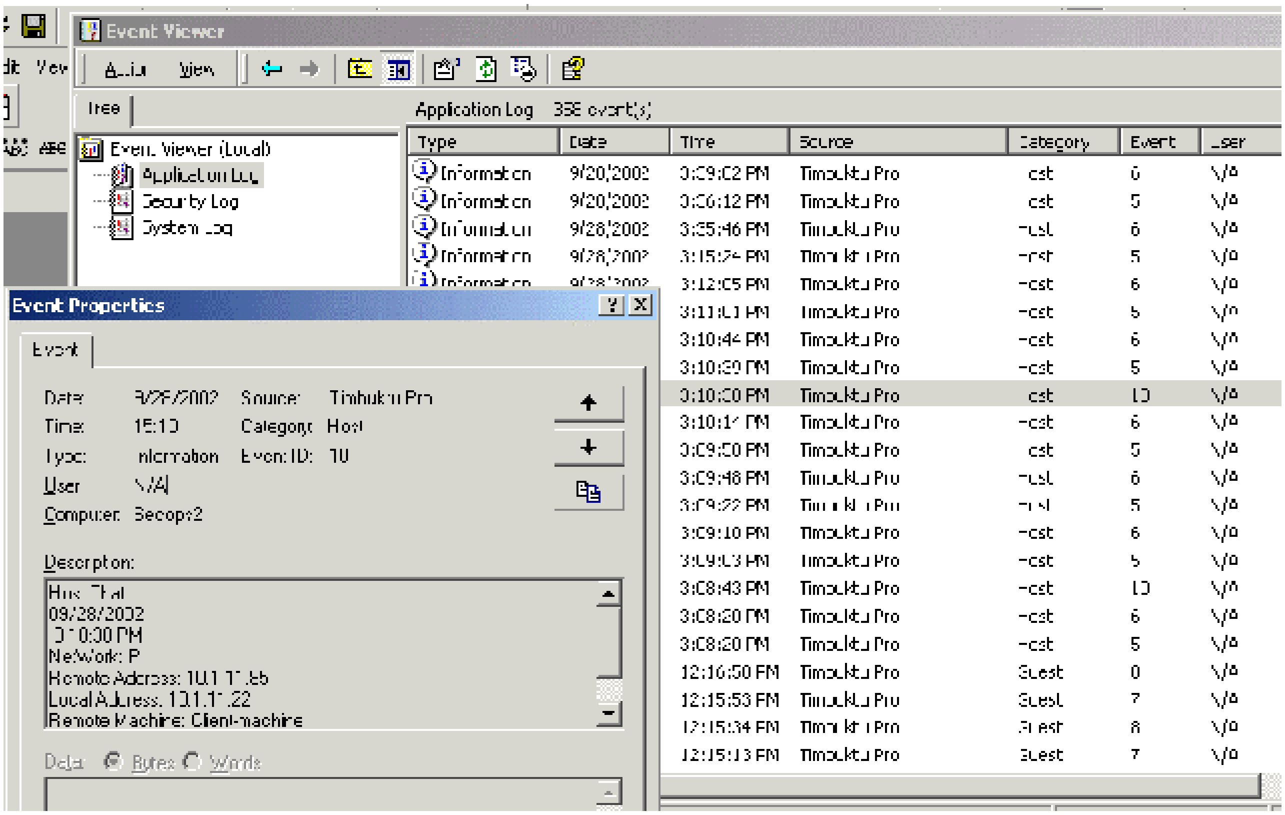
There are two other places to look for Timbuktu activity as either a Remote Client or a Host: When the user of a Timbuktu machine double clicks on the Timbuktu status icon, and selects
Connections → Activity log, the following dialog is displayed:



```
09/28/2002 11:17:36 AM  Timbuktu Pro  Initiated    sec2ops    10.1.11.22
09/28/2002 12:15:13 PM  Guest Control  Begin    Client-machine  sec2ops  10.
09/28/2002 12:15:33 PM  Guest Control  End    Client-machine  sec2ops  10.1.
09/28/2002  3:08:20 PM  Host Send  Begin    security  Client-machine  10.1.11
09/28/2002  3:08:20 PM  Host Send  End    security  Client-machine  10.1.11.8
09/28/2002  3:08:43 PM  Host Exchange  Validation error    Client-machine  se
09/28/2002  3:09:03 PM  Host Exchange  Begin    security  Client-machine  10.
09/28/2002  3:09:09 PM  Host Exchange  End    security  Client-machine  10.1
09/28/2002  3:09:22 PM  Host Observe  Begin    security  Client-machine  10.1
09/28/2002  3:09:48 PM  Host Observe  End    security  Client-machine  10.1.1
```

This is a much more complete log of Timbuktu related events. This dialog will allow the end user to see the entire contents of the C:\Program Files\Timbuktu Pro\activity.log file. By default, the activity.log file is read-only. In a typical installation, only an Administrator or Power-user would be able to delete or manually edit this file. It is reasonable to believe that an attacker would modify or delete this file to hide their activities.

The final tool to review Timbuktu related activities is with the Application Event Viewer:



Application Log 338 event(s)

Type	Date	Time	Source	Category	Event	User
Information	9/28/2002	3:39:02 PM	Timbuktu Pro	Host	6	N/A
Information	9/28/2002	3:36:12 PM	Timbuktu Pro	Host	5	N/A
Information	9/28/2002	3:35:46 PM	Timbuktu Pro	Host	6	N/A
Information	9/28/2002	3:15:24 PM	Timbuktu Pro	Host	5	N/A
Information	9/28/2002	3:12:05 PM	Timbuktu Pro	Host	6	N/A
		3:11:01 PM	Timbuktu Pro	Host	5	N/A
		3:10:44 PM	Timbuktu Pro	Host	6	N/A
		3:10:39 PM	Timbuktu Pro	Host	5	N/A
		3:10:30 PM	Timbuktu Pro	Host	10	N/A
		3:10:14 PM	Timbuktu Pro	Host	6	N/A
		3:09:50 PM	Timbuktu Pro	Host	5	N/A
		3:09:48 PM	Timbuktu Pro	Host	6	N/A
		3:09:22 PM	Timbuktu Pro	Host	5	N/A
		3:09:10 PM	Timbuktu Pro	Host	6	N/A
		3:09:03 PM	Timbuktu Pro	Host	5	N/A
		3:08:43 PM	Timbuktu Pro	Host	10	N/A
		3:08:20 PM	Timbuktu Pro	Host	6	N/A
		3:08:20 PM	Timbuktu Pro	Host	5	N/A
		12:16:50 PM	Timbuktu Pro	Guest	0	N/A
		12:15:53 PM	Timbuktu Pro	Guest	7	N/A
		12:15:34 PM	Timbuktu Pro	Guest	8	N/A
		12:15:13 PM	Timbuktu Pro	Guest	7	N/A

Event Properties

Event

Date: 9/28/2002 Source: Timbuktu Pro
Time: 15:10 Category: Host
Type: Information Event ID: 10
User: N/A
Computer: Secops2

Description:

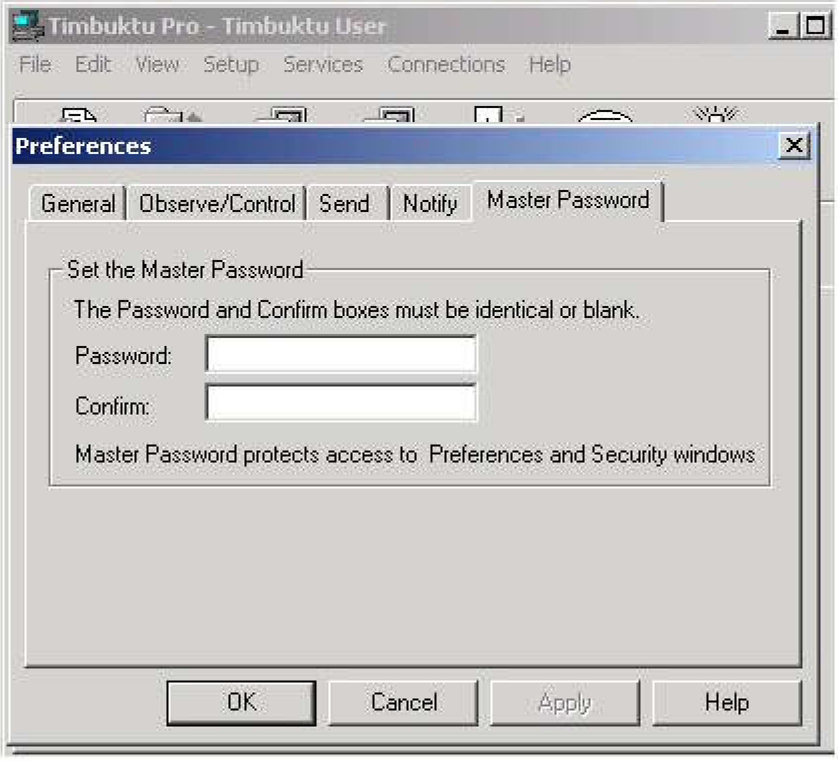
Host: Trial
09/28/2002
3:10:30 PM
Network: IP
Remote Address: 10.1.1.55
Local Address: 10.1.1.22
Remote Machine: Client-machine

Data: ● Bytes ○ Words

Using the Windows Application Event Viewer, one can obtain very specific and detailed information about Timbuktu related events. Again, it is reasonable to believe that an attacker would clear the event log to cover their tracks.

Configuring Access:

Access to the Security Setup screen is controlled by the “Master Password.” If you know the “Master Password” you can add or delete Timbuktu users, or modify their access privileges. –7 (DR.Timbuktu.Database.Insecurity Posting)



Set the Master Password

The Password and Confirm boxes must be identical or blank.

Password:

Confirm:

Master Password protects access to Preferences and Security windows

This password in stored in an encoded form in the following directory\file: C:\Program Files\Timbuktu Pro\tb2.plu.

The password is limited to 15 alpha-numeric characters, and can include spaces and special characters. The password can also include [ALT+Numeric Keypad Sequences] such as [ALT+3333] ♣ .

There are a number of vulnerabilities associated with the tb2.plu file. By default, this file can be read by all users of the computer system. Administrators, Power Users and SYSTEM can write to this file. If Timbuktu is installed on a disk without NTFS or on a Windows 95, 98 or ME workstation, there is no opportunity to create access control lists.

Issue: Passwords are not Strongly Encrypted
“The password hashes that are generated are not salted. As a result, it is possible to build a dictionary with which the Master Password can be attacked. “
– 8 (Wilson, Rich Security Focus Posting)

Salting password hashes brings randomness, that encoding alone cannot.

- The attacker may pre-compute (offline) encrypted versions of your dictionary. Even if the process is slow, or takes significant storage it may not matter to the attacker, they can just burn a CD or DVD with a database mapping encrypted text to clear-text.

- It's this pre-computation attack which a salt thwarts. A salt makes it impractical to build up a dictionary of encrypted → clear text mappings, because a given clear text has millions of encrypted equivalents. -9(Skoll, David postgres.org posting)

A related problem with the hash for the Master Password, is that it employs the identical algorithm used for encoding passwords for Registered Users. This would allow an attacker to systematically build a dictionary by entering known passwords and recording the encoded output.

The following is an example of the encoding output:

Encoded Password Hexadecimal Value	Plain Text
BCCD E7B6 708A 99D9 6CC5 C49C E31A 1B	aaaaaaaaaaaaaaa
E612 8A75 6E94 11AA AE95 BEB4 3C33 96	bbbbbbbbbbbbbbb
6CB0 EDA0 CAD1 5F60 A5B3 CF5C 1284 CD	ccccccccccccccc
B53A 306F 4E58 78F6 2899 7F97 26B0 A8	ddddddddddddddd

Issue: Registered User Names are Stored in Clear Text

Putting Registered User Names in clear text provides an attacker significant assistance in compromising a system. With knowledge of a valid User name, an attacker can attempt to grind or guess at valid passwords. Historically, passwords have proven to be an extremely weak form of protection from unauthorized access.
–10(Krishna, Arvind Five Steps for Keeping Hackers at Bay)

Issue: Deletion of C:\Program Files\Timbuktu Pro\tb2.plu Escalates Privileges

One method to defeat the requirement to enter the Master Password is to use the following procedure:

1. Stop the Timbuktu User interface (Tb2pro.exe)
2. Delete C:\Program Files\Timbuktu Pro\tb2.plu
3. Restart the Timbuktu User interface (Tb2pro.exe)
4. Within the Timbuktu User interface, Select Setup, then Preferences
5. Enter a new Master Password of your choice
6. Enter new “Registered Users”, “NT Users”, or modify Guest User privileges as desired

This procedure will also have the effect of removing or damaging valid Timbuktu Registered User Ids and passwords, which could lead to detection of the attack.

THE ATTACK:

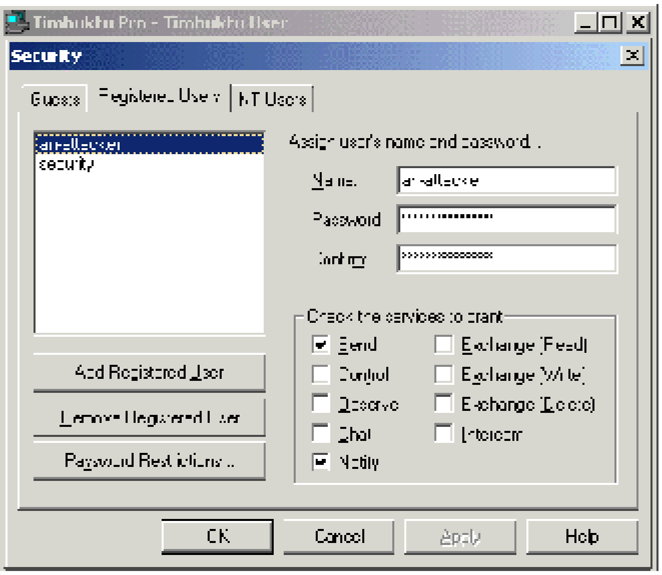
An attacker now has a customized version of the tb2.plu file. From here, the attacker could use a Word Macro virus, Mail Macro Virus, other automated batch or command scripts, or good old fashioned, social engineering to induce victims to place the modified tb2.plu file onto their machines. After the file is placed onto a victim machine, an attacker can take control or "Observe" the machine the next time that Tb2pro.exe starts.

Issue: Modification of C:\Program Files\Timbuktu Pro\tb2.plu Escalates Privileges Part 1

Let's consider a scenario where the attacker has a valid Registered User name and a password. But the attacker is not happy because they can only send messages or provide notification to Host computers, and they wish to control Host computers. Modification to the tb2.plu file is a trivial exercise. Armed with nothing more than a hexadecimal editor, an attacker can change 2 bytes, and achieve total power.

Consider the following user setup:

We have a "Registered User" defined with the name of an-attacker. This user does have a password, but has few rights. Only Send and Notify services have been granted.



an-attacker
security

Assign user's name and password.

Name: an-attacker

Password: ••••••••••••••

Confirm: ••••••••••••••

Check the services to grant

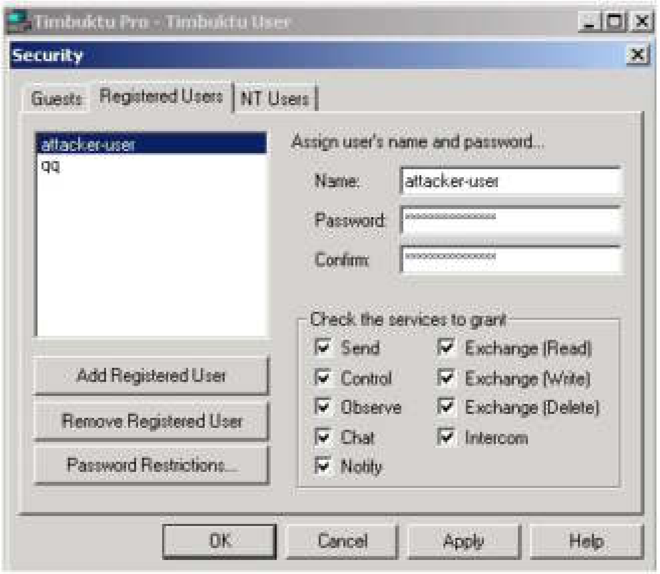
☑ Send
☐ Control
☐ Observe
☐ Chat
☑ Notify
☐ Exchange (Read)
☐ Exchange (Write)
☐ Exchange (Local)
☐ Intercom

This tb2.plu file excerpt shows the attacker-user with these user rights

```
Byte
Offset   |------------Hexadecimal-------------| |----ASCII-----|
00000200 0000 0000 0000 0000 0000 0000 FF23 0261 .............#.a
00000210 6E2D 6174 7461 636B 6572 0000 0000 0000 n-attacker......
00000220 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000230 000F 6ED6 54FB EDCD 95F2 81C2 B221 145E ..n.T........!.^
00000240 1B0F 6ED6 54FB EDCD 95F2 81C2 B221 145E ..n.T........!.^
00000250 1BCA 1C95 3D0F 90BB F8EB F256 CCA5 AF7E ....=......V...~
00000260 6FE3 1661 C900 0000 0000 0000 0000 0000 o..a............
00000270 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000280 0000 0000 0009 20                      ......
```

Now, let's look at the user setup:

We have now given the attacker-user **all** access rights.


Timbuktu Pro - Timbuktu User

Security

Guests | Registered Users | NT Users

attacker-user
qq

Assign user's name and password...

Name: attacker-user

Password: ***************

Confirm: ***************

Check the services to grant

☑ Send ☑ Exchange (Read)
☑ Control ☑ Exchange (Write)
☑ Observe ☑ Exchange (Delete)
☑ Chat ☑ Intercom
☑ Notify

This tb2.plu file excerpt shows the attacker-user with all user rights

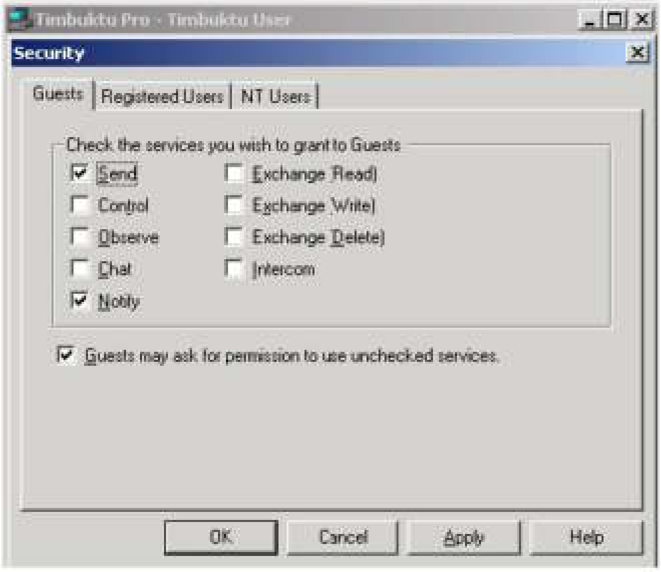
```
Byte
Offset   |------------Hexadecimal--------------| |----ASCII-----|
00000200 0000 0000 0000 0000 0000 0000 0000 0261 ...............a
00000210 7474 6163 6B65 722D 7573 6572 0000 0000 ttacker-user....
00000220 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000230 000F 224E 35E1 D2DE 3614 7EAC B416 C763 .."N5...6.~....c
00000240 E20F 224E 35E1 D2DE 3614 7EAC B416 C763 .."N5...6.~....c
00000250 E20F DC94 3D00 0000 0000 0000 0000 0000 ....=...........
00000260 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000270 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000280 0000 0000 00FF 23                       ......#
```

Two bytes in the configuration file was all it took to take a Registered User from few privileges to all privileges. Due to the nature of the file, an attacker can modify the hexadecimal contents 118 bytes from the start of the clear text user name, and gain all privileges.

Issue: Modification of C:\Program Files\Timbuktu Pro\tb2.plu Escalates Privileges Part 2

Earlier, the reader was cautioned about privileges granted to Guests. Using concepts from the previous issue, an attacker could modify the tb2.plu file to escalate privileges of Guests (and in effect, **everybody**.)

In this example, Guests have been given the ability to Send messages, notify the host, and request additional privileges. As a result, **all** users have at least these privileges.


Timbuktu Pro - Timbuktu User

Security

Guests | Registered Users | NT Users

Check the services you wish to grant to Guests

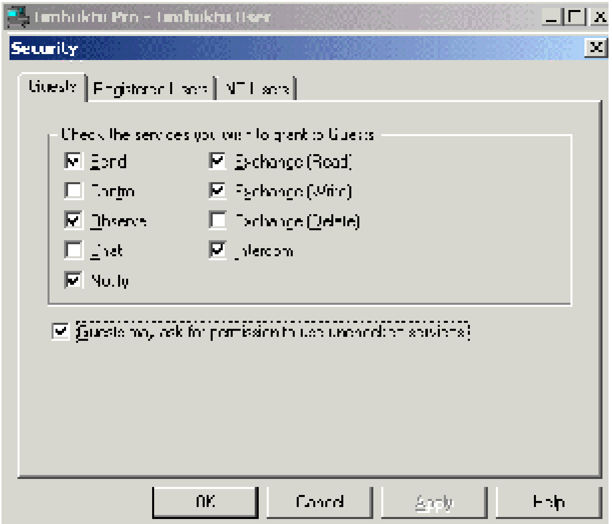
☑ Send ☐ Exchange (Read)
☐ Control ☐ Exchange (Write)
☐ Observe ☐ Exchange (Delete)
☐ Chat ☐ Intercom
☑ Notify

☑ Guests may ask for permission to use unchecked services.

This tb2.plu file excerpt shows the Guest Account with minimal user rights

```
Byte
Offset    |------------Hexadecimal--------------| |----ASCII-----|
000000A0 DB09 6001 3C54 656D 706F 7261 7279 2047 ..`.<Temporary G
000000B0 7565 7374 3E00 0000 0000 0000 0000 0000 uest>...........
```

In this example, additional rights have been granted to Guests.



Timbuktu Pro - Timbuktu User

Security

Guests | Registered Users | NT Users

Check the services you want to grant to Guests

☑ Send ☑ Exchange (Read)
☐ Control ☑ Exchange (Write)
☑ Observe ☐ Exchange (Delete)
☐ Chat ☑ Intercom
☑ Notify

☑ Guests may ask for permission to use unchecked services

This tb2.plu file excerpt shows the Guest Account with the added rights

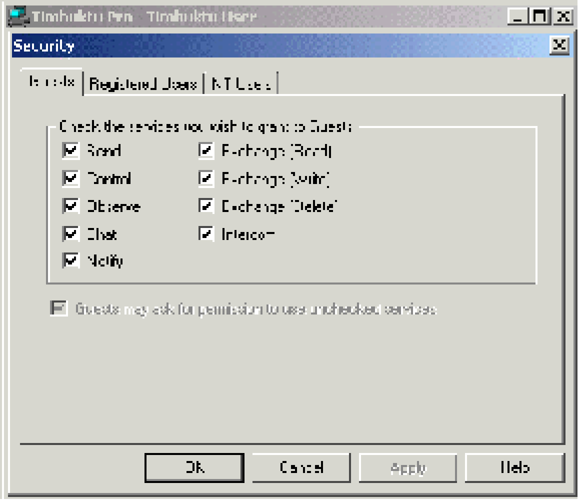
```
Byte
Offset    |------------Hexadecimal--------------| |----ASCII-----|
000000A0 DB7D 6201 3C54 656D 706F 7261 7279 2047 .}b.<Temporary G
000000B0 7565 7374 3E00 0000 0000 0000 0000 0000 uest>...........
```

Two bytes in the configuration file was all it took to modify Guest Privileges. Look at Hex Offset address 0x000000A1 and 0x000000A2. What happens if the attacker modifies the data at these addresses in a manner similar to the previous example?

```
Byte
Offset    |------------Hexadecimal--------------| |----ASCII-----|
000000A0 DBFF 2301 3C54 656D 706F 7261 7279 2047 ..#.<Temporary G
000000B0 7565 7374 3E00 0000 0000 0000 0000 0000 uest>...........
```

By simply placing the values 0xFF, 0x23 beginning at Hex Offset address 0x000000A1 an attacker can grant the following privileges to everybody.

Results of the modification as seen in the Timbuktu graphical user interface.



Timbuktu Pro - Timbuktu User

Security

Guests | Registered Users | NT Users

Check the services you wish to grant to Guests

☑ Send ☑ Exchange (Read)
☑ Control ☑ Exchange (Write)
☑ Observe ☑ Exchange (Delete)
☑ Chat ☑ Intercom
☑ Notify

☑ Guests may ask for permission to use unchecked services

Issue: Modification of C:\Program Files\Timbuktu Pro\tb2.plu Escalates Privileges Part 3

What if the attacker wanted to be more subtle? Deleting the tb2.plu file with the associated Registered Users and privileges might be detected when an authorized person attempted to access a Timbuktu host that had been compromised. The following is an example of a tb2.plu file with two users defined.

```
Byte
Offset   |------------Hexadecimal-------------| |----ASCII-----|
00000000 0300 0300 0F67 8651 4C0D 4BB8 DBF9 1253 .....g.QL.K....S
00000010 9398 882B 0000 0000 0100 0000 0000 0000 ...+............
00000020 0000 0000 0000 0000 0500 003C 4775 6573 ...........<Gues
00000030 743E 0000 0000 0000 0000 0000 0000 0000 t>..............
00000040 0000 0000 0000 0000 0000 0000 000F A241 ...............A
00000050 0543 9663 E032 9065 46F6 9F6C DB0F A241 .C.c.2.eF..l...A
00000060 0543 9663 E032 9065 46F6 9F6C DB00 0000 .C.c.2.eF..l....
00000070 000F A241 0543 9663 E032 9065 46F6 9F6C ...A.C.c.2.eF..l
00000080 DB0F A241 0543 9663 E032 9065 46F6 9F6C ...A.C.c.2.eF..l
00000090 DB0F A241 0543 9663 E032 9065 46F6 9F6C ...A.C.c.2.eF..l
000000A0 DB01 4001 3C54 656D 706F 7261 7279 2047 ..@.<Temporary G
000000B0 7565 7374 3E00 0000 0000 0000 0000 0000 uest>...........
000000C0 0000 0000 0000 0000 0000 0000 0000 0000 ................
000000D0 0000 0000 0000 0000 0000 0000 0000 0000 ................
000000E0 0000 0000 0000 0000 0000 0000 0000 0000 ................
000000F0 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000100 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000110 0000 0000 0000 0000 0000 0F60 063C 4174 ...........`.<At
00000120 7465 6E64 6564 2041 6363 6573 733E 0000 tended Access>..
00000130 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000140 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000150 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000160 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000170 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000180 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000190 0000 00FE 0302 616E 2D61 7474 6163 6B65 ......an-attacke
000001A0 7200 0000 0000 0000 0000 0000 0000 0000 r...............
000001B0 0000 0000 0000 0000 0F90 BBF8 EBF2 56CC ..............V.
000001C0 A5AF 7E6F E316 61C9 0F90 BBF8 EBF2 56CC ..~o..a.......V.
000001D0 A5AF 7E6F E316 61C9 1C14 953D 0000 0000 ..~o..a....=....
000001E0 0000 0000 0000 0000 0000 0000 0000 0000 ................
000001F0 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000200 0000 0000 0000 0000 0000 0000 0000 0273 ...............s
00000210 6563 7572 6974 7900 0000 0000 0000 0000 ecurity.........
00000220 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000230 000F 82B6 0D61 EA5E B6F4 F634 1C0E 3F43 .....a.^...4..?C
00000240 5A0F 82B6 0D61 EA5E B6F4 F634 1C0E 3F43 Z....a.^...4..?C
00000250 5A1C 1495 3D0F AED0 2234 9B8B 3075 626F Z...=..."4..0ubo
00000260 369F ACC6 D600 0000 0000 0000 0000 0000 6...............
00000270 0000 0000 0000 0000 0000 0000 0000 0000 ................
00000280 0000 0000 00FF 23                       ......#
```

The Registered User names can be seen beginning at offset 0x0196 “an-attacker”, and at offset 0x020F “security.” An attacker can modify their own password, then examine the file again, looking for changes. Close observation of changes to the file when the password changes show that one can always predict where the current password will be located in relation to the Registered User name. The current password always starts 35 bytes after the beginning of the Registered User name. In addition, the encoded password is always 15 bytes in length, even if the password itself is only one character long. Further experimentation shows that the Master Password field always begins at offset 0x05. Therefore, an attacker could perform the following steps to gain Master Password level access:

1. Use the Timbuktu application to generate an encoded password for a known password
2. Make a note of the original encoded Master Password beginning at offset 0x05 for a length of 15 bytes
3. Stop the Timbuktu User interface (Tb2pro.exe)
4. Modify C:\Program Files\Timbuktu Pro\tb2.plu, placing the known encoded password at offset 0x05
5. Start Timbuktu User interface (Tb2pro.exe)
6. Enter the known password
7. Enter new “Registered Users”, “NT Users”, or modify Guest User privileges as desired
8. Stop the Timbuktu User interface (Tb2pro.exe)
9. Modify C:\Program Files\Timbuktu Pro\tb2.plu, placing the original encoded password (of the valid Master Password) at offset 0x05.

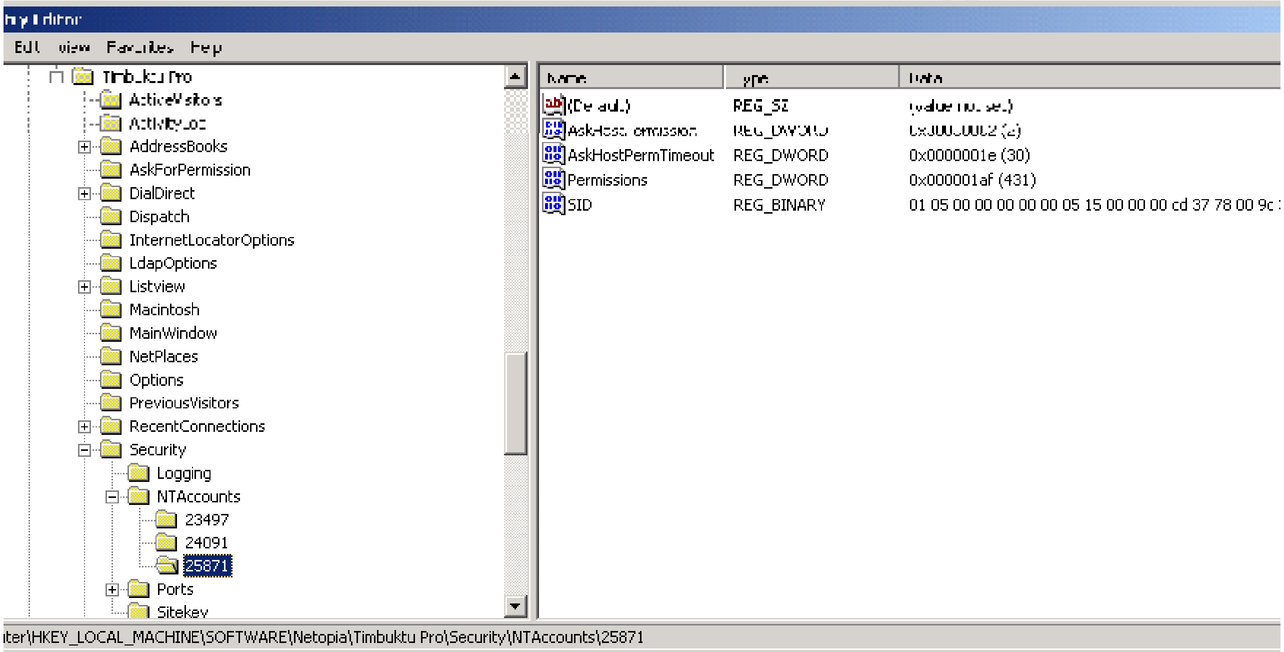
Issue: Modification of C:\Program Files\Timbuktu Pro\tb2.plu Escalates Privileges Part 4

What if the attacker wanted to be subtle but did not want to have to mess around with copying an encoded password to a known password? There is an even easier way of defeating the “security” of the Master Password. Looking at the example tb2.plu file, one notices several patterns. One of the patterns is that it appears that the encoded password is repeated multiple times for each Registered User Id. It appears that this repeated hash is the mechanism that Timbuktu uses to detect if a user attempts to reuse a password within three generations. The other pattern that can be seen is a sequence of 0x0F preceding each encoded password. This sequence also precedes the encoded Master Password. Testing has shown that if the sequence of 0x0F at offset 0x04 is modified to be 0x00, one is no longer prompted to enter the Master Password in order to add or modify Timbuktu users.

1. Stop the Timbuktu User interface (Tb2pro.exe)
2. Modify C:\Program Files\Timbuktu Pro\tb2.plu, placing value 0x00 at offset 0x04
3. Start Timbuktu User interface (Tb2pro.exe)
4. Enter new “Registered Users”, “NT Users”, or modify Guest User privileges as desired
5. Stop the Timbuktu User interface (Tb2pro.exe)
6. Modify C:\Program Files\Timbuktu Pro\tb2.plu, placing value 0x0F at offset 0x04

Issue: Access to NT Registry may allow attacker to Modify or Destroy Timbuktu NT User Account information

Timbuktu NT User(and Group) membership information is stored in the registry. If an attacker has the ability to make manual changes to the registry using a tool such as Regedit, they may modify permissions to escalate privileges. Although this type of attack is possible, it is more difficult to perform successfully, as the attacker would need to understand the mapping of the NT User/Group information to the SID values. A more likely possibility is that the attacker would simply delete keys located below \HKEY_LOCAL_MACHINE\SOFTWARE\Netopia\Timbuktu Pro\Secuity\NTAccounts.



- Timbuktu Pro
  - ActiveVisitors
  - ActivityLog
  - AddressBooks
  - AskForPermission
  - DialDirect
  - Dispatch
  - InternetLocatorOptions
  - LdapOptions
  - Listview
  - Macintosh
  - MainWindow
  - NetPlaces
  - Options
  - PreviousVisitors
  - RecentConnections
  - Security
    - Logging
    - NTAccounts
      - 23497
      - 24091
      - 25871
    - Ports
    - Sitekey

Name	Type	Data
(Default)	REG_SZ	(value not set)
AskHostPermission	REG_DWORD	0x00000002 (2)
AskHostPermTimeout	REG_DWORD	0x0000001e (30)
Permissions	REG_DWORD	0x000001af (431)
SID	REG_BINARY	01 05 00 00 00 00 00 05 15 00 00 00 cd 37 78 00 9c

iter\HKEY_LOCAL_MACHINE\SOFTWARE\Netopia\Timbuktu Pro\Security\NTAccounts\25871

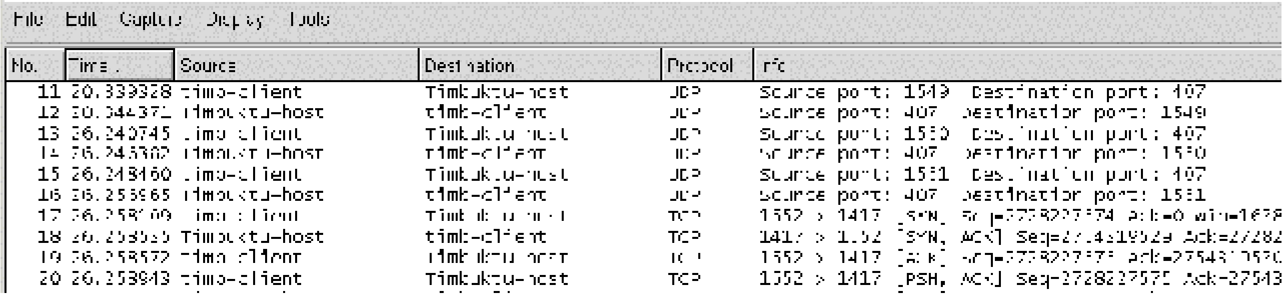
Issue: Registered User Ids are sent in clear text during initial session establishment.

Although this might not seem to be a very large vulnerability, it can lead to a severe breach in security. Organizations or individuals may use Timbuktu software on Windows devices that are directly connected to the Internet.

Without launching into a lengthy discussion on the perils of leaving unprotected Windows machines connected to the Internet, let's just focus on the Timbuktu access issues.

It was previously identified that all Timbuktu session negotiation and credential exchange occurs on UDP port 407. Therefore it is reasonable to expect that a high percentage of computers that have UDP port 407 open, function as Timbuktu hosts. If an attacker can get valid user credentials for a particular Timbuktu host, at least half of the work of compromising a system has been completed.

The following is a Ethereal packet capture of a Timbuktu session negotiation:

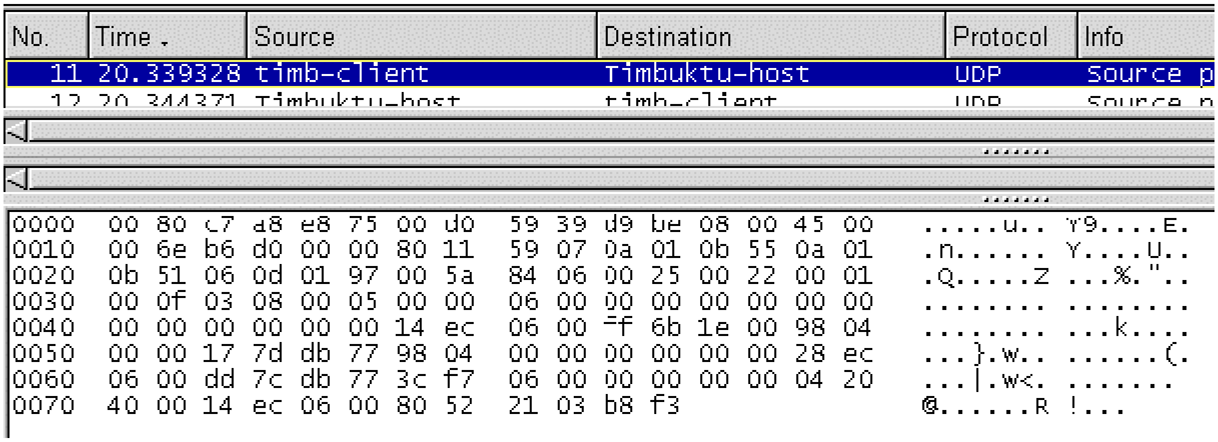


```
No. Time     Source         Destination    Protocol Info
 11 20.339328 timb-client    Timbuktu-host  UDP      Source port: 1549  Destination port: 407
 12 20.344371 Timbuktu-host  timb-client    UDP      Source port: 407  Destination port: 1549
 13 26.240745 timb-client    Timbuktu-host  UDP      Source port: 1550  Destination port: 407
 14 26.243302 Timbuktu-host  timb-client    UDP      Source port: 407  Destination port: 1550
 15 26.248160 timb-client    Timbuktu-host  UDP      Source port: 1551  Destination port: 407
 16 26.253965 Timbuktu-host  timb-client    UDP      Source port: 407  Destination port: 1551
 17 26.253109 timb-client    Timbuktu-host  TCP      1552 > 1417 [SYN] Seq=2728227574 Ack=0 Win=1638
 18 26.253535 Timbuktu-host  timb-client    TCP      1417 > 1552 [SYN, ACK] Seq=2754319529 Ack=27282
 19 26.253572 timb-client    Timbuktu-host  TCP      1552 > 1417 [ACK] Seq=2728227575 Ack=275431953C
 20 26.253943 timb-client    Timbuktu-host  TCP      1552 > 1417 [PSH, ACK] Seq=2728227575 Ack=27543
```

In frames 11 through 16, the client is talking to destination port UDP 407. In frames 17 through 19 the three-way TCP handshake is completed. The actual remote control session begins in frame 20.

Let's take a look at the traffic exchanged in frames 11 through 16 and see if there is any information present that would be interesting to an attacker.

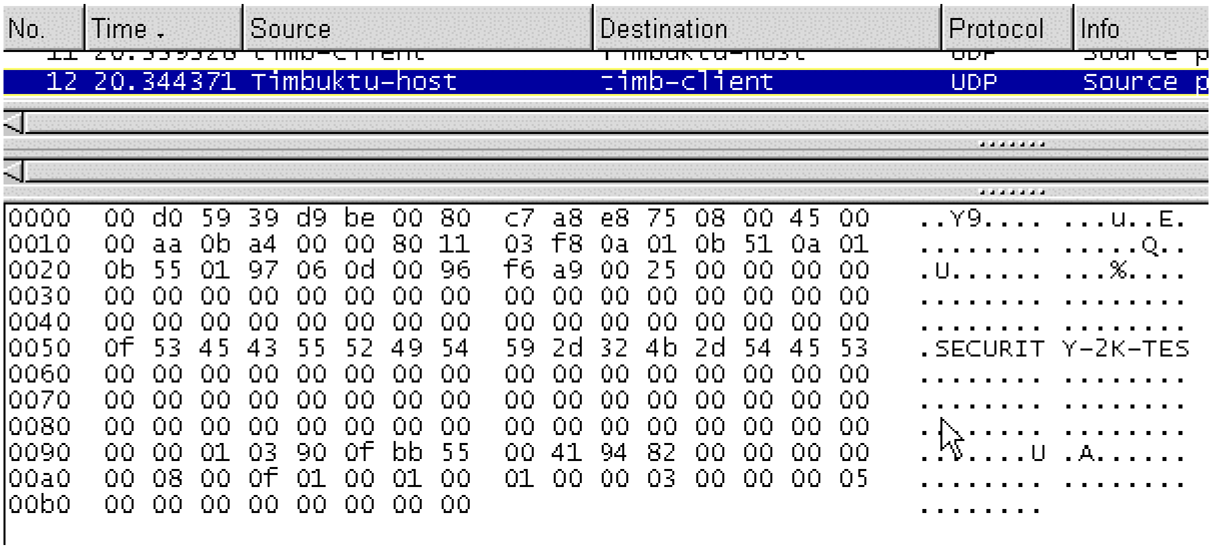
In frame 11, there is no obviously useful information



```
No. Time      Source         Destination    Protocol Info
 11 20.339328 timb-client    Timbuktu-host  UDP      Source p
 12 20.344371 Timbuktu-host  timb-client    UDP      Source p
```

```
0000  00 80 c7 a8 e8 75 00 d0  59 39 d9 be 08 00 45 00   ......u.. Y9....E.
0010  00 6e b6 d0 00 00 80 11  59 07 0a 01 0b 55 0a 01   .n...... Y....U..
0020  0b 51 06 0d 01 97 00 5a  84 06 00 25 00 22 00 01   .Q.....Z ...%."..
0030  00 0f 03 08 00 05 00 00  06 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 14 ec  06 00 ⁻f 6b 1e 00 98 04   ........ ...k....
0050  00 00 17 7d db 77 98 04  00 00 00 00 00 00 28 ec   ...}.w.. ......(.
0060  06 00 dd 7c db 77 3c f7  06 00 00 00 00 00 04 20   ...|.w<. .......
0070  40 00 14 ec 06 00 80 52  21 03 b8 f3               @......R !...
```

Let's look at frame 12.

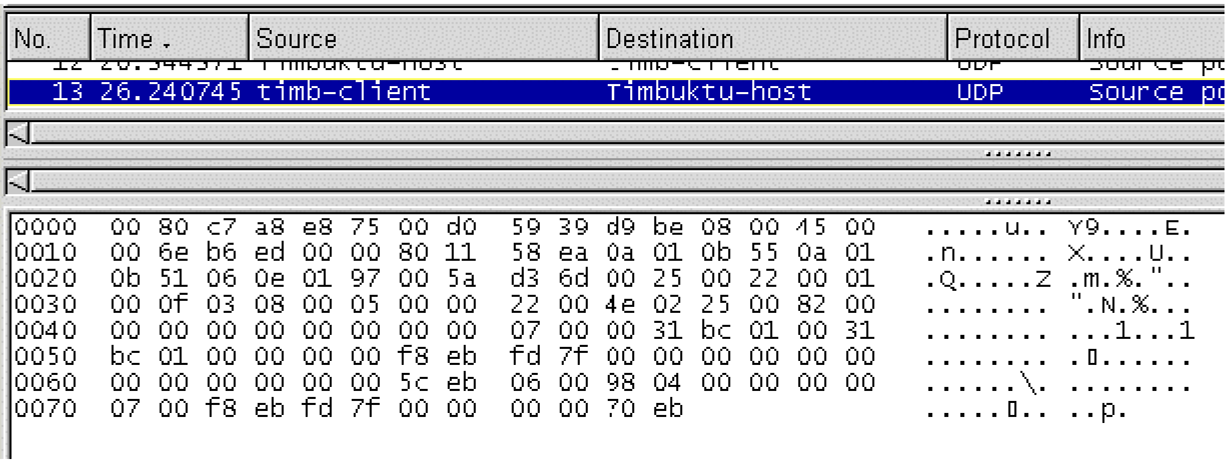


```
No.  Time .     Source          Destination     Protocol  Info
  12 20.344371 Timbuktu-host   timb-client     UDP       Source p

0000  00 d0 59 39 d9 be 00 80  c7 a8 e8 75 08 00 45 00   ..Y9.... ...u..E.
0010  00 aa 0b a4 00 00 80 11  03 f8 0a 01 0b 51 0a 01   ........ .....Q..
0020  0b 55 01 97 06 0d 00 96  f6 a9 00 25 00 00 00 00   .U...... ...%....
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  0f 53 45 43 55 52 49 54  59 2d 32 4b 2d 54 45 53   .SECURIT Y-2K-TES
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 01 03 90 0f bb 55  00 41 94 82 00 00 00 00   .......U .A......
00a0  00 08 00 0f 01 00 01 00  01 00 00 03 00 00 00 05   ........ ........
00b0  00 00 00 00 00 00 00 00                            ........
```

Now we have something of interest. Take a look at Hex offset 0x0051. That is the Timbuktu name of the Host machine (SECURITY-2K-TES). An attacker will use this and any other available information to develop a victim vulnerability profile.

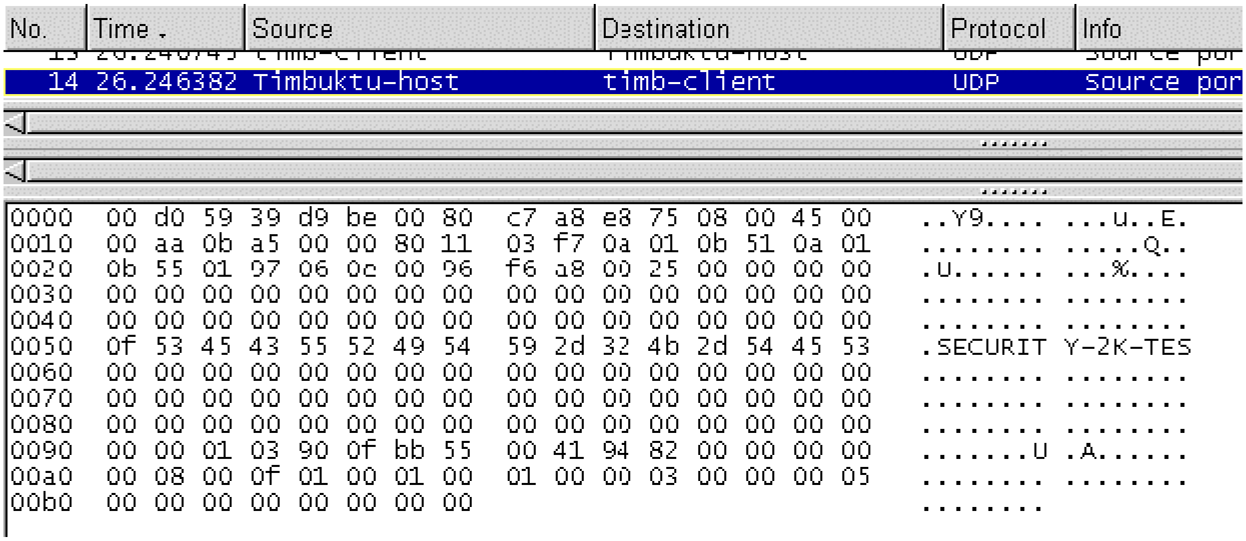
Frame 13: In this frame, there is no obviously useful information.



```
No.  Time .     Source          Destination     Protocol  Info
  13 26.240745 timb-client     Timbuktu-host   UDP       Source po

0000  00 80 c7 a8 e8 75 00 d0  59 39 d9 be 08 00 45 00   .....u.. Y9....E.
0010  00 6e b6 ed 00 00 80 11  58 ea 0a 01 0b 55 0a 01   .n...... X....U..
0020  0b 51 06 0e 01 97 00 5a  d3 6d 00 25 00 22 00 01   .Q.....Z .m.%."..
0030  00 0f 03 08 00 05 00 00  22 00 4e 02 25 00 82 00   ........ ".N.%...
0040  00 00 00 00 00 00 00 00  07 00 00 31 bc 01 00 31   ........ ...1...1
0050  bc 01 00 00 00 00 f8 eb  fd 7f 00 00 00 00 00 00   ........ .▯......
0060  00 00 00 00 00 00 5c eb  06 00 98 04 00 00 00 00   ......\. ........
0070  07 00 f8 eb fd 7f 00 00  00 00 70 eb               .....▯.. ..p.
```

How about Frame 14?

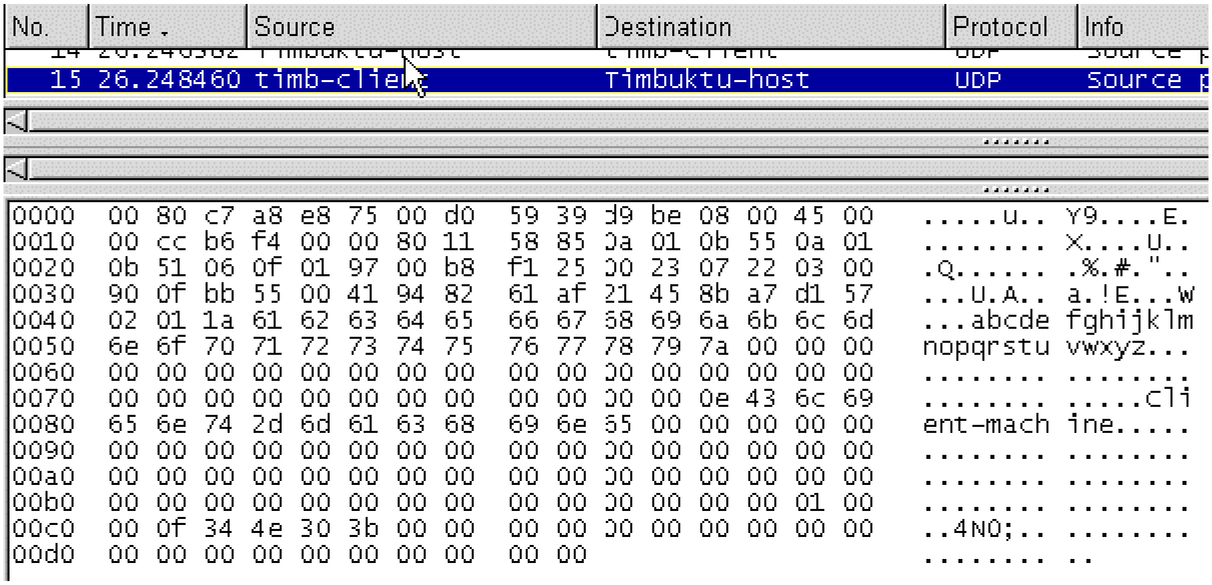


```
No.  Time .     Source          Destination     Protocol  Info
  14 26.246382 Timbuktu-host   timb-client     UDP       Source por

0000  00 d0 59 39 d9 be 00 80  c7 a8 e8 75 08 00 45 00   ..Y9.... ...u..E.
0010  00 aa 0b a5 00 00 80 11  03 f7 0a 01 0b 51 0a 01   ........ .....Q..
0020  0b 55 01 97 06 0c 00 96  f6 a8 00 25 00 00 00 00   .U...... ...%....
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  0f 53 45 43 55 52 49 54  59 2d 32 4b 2d 54 45 53   .SECURIT Y-2K-TES
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 01 03 90 0f bb 55  00 41 94 82 00 00 00 00   .......U .A......
00a0  00 08 00 0f 01 00 01 00  01 00 00 03 00 00 00 05   ........ ........
00b0  00 00 00 00 00 00 00 00                            ........
```

This seems to be nearly a repeat of frame 12. Other than the repeated host name, there is no obviously useful information

How about Frame 15?

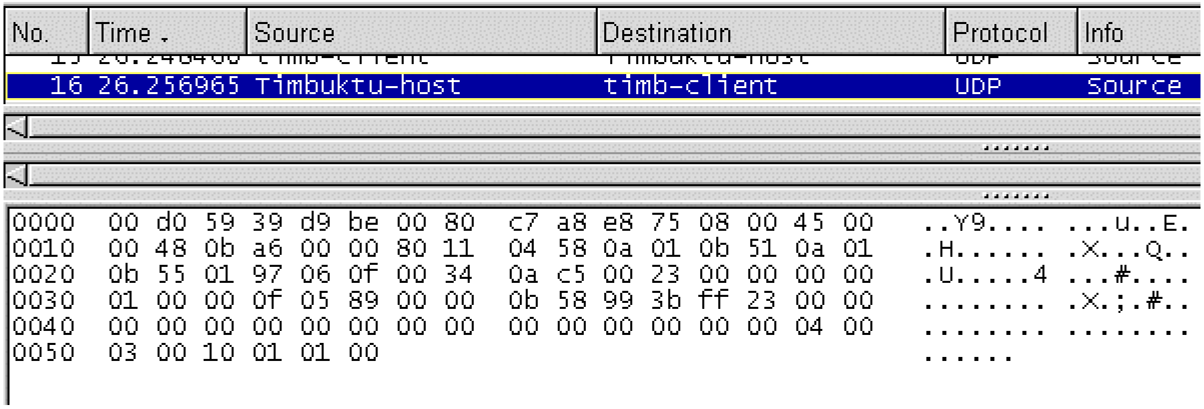


```
No.  Time       Source         Destination     Protocol  Info
  15 26.248460  timb-client    Timbuktu-host   UDP       Source p
```

```
0000  00 80 c7 a8 e8 75 00 d0  59 39 d9 be 08 00 45 00   .....u.. Y9....E.
0010  00 cc b6 f4 00 00 80 11  58 85 0a 01 0b 55 0a 01   ........ X....U..
0020  0b 51 06 0f 01 97 00 b8  f1 25 00 23 07 22 03 00   .Q...... .%.#."..
0030  90 0f bb 55 00 41 94 82  61 af 21 45 8b a7 d1 57   ...U.A.. a.!E...W
0040  02 01 1a 61 62 63 64 65  66 67 68 69 6a 6b 6c 6d   ...abcde fghijklm
0050  6e 6f 70 71 72 73 74 75  76 77 78 79 7a 00 00 00   nopqrstu vwxyz...
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 0e 43 6c 69   ........ .....Cli
0080  65 6e 74 2d 6d 61 63 68  69 6e 65 00 00 00 00 00   ent-mach ine.....
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 01 00   ........ ........
00c0  00 0f 34 4e 30 3b 00 00  00 00 00 00 00 00 00 00   ..4N0;.. ........
00d0  00 00 00 00 00 00 00 00  00 00                     ........ ..
```

Here we can clearly see two pieces of valuable information. At hex offset 0x0043 we can see the Timbuktu user name. The name is unusual in that it is "abcdefghijklmnopqrstuvwxyz", but I wanted to use an obvious character string. Also, at hex offset 0x007D, we can see the name of the Timbuktu client workstation. The name is "Client-machine." Now the attacker has two more pieces of information.; a valid user name and the name of Timbuktu machine that a valid client may come from.

Here is Frame 16:



```
No.  Time       Source         Destination     Protocol  Info
  16 26.256965  Timbuktu-host  timb-client     UDP       Source
```

```
0000  00 d0 59 39 d9 be 00 80  c7 a8 e8 75 08 00 45 00   ..Y9.... ...u..E.
0010  00 48 0b a6 00 00 80 11  04 58 0a 01 0b 51 0a 01   .H...... .X...Q..
0020  0b 55 01 97 06 0f 00 34  0a c5 00 23 00 00 00 00   .U.....4 ...#....
0030  01 00 00 0f 05 89 00 00  0b 58 99 3b ff 23 00 00   ........ .X.;.#..
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 04 00   ........ ........
0050  03 00 10 01 01 00                                  ......
```

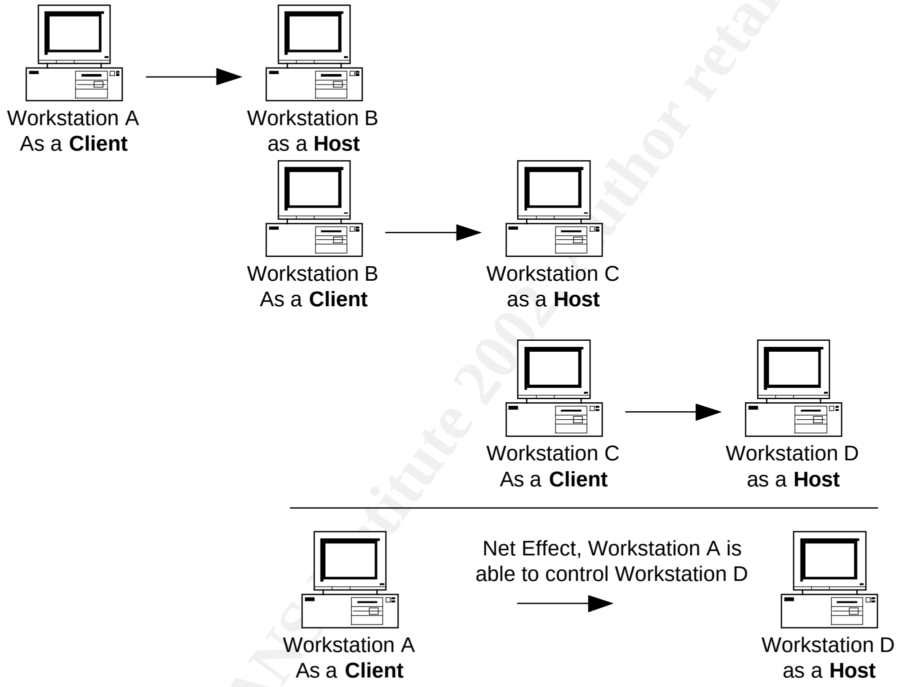
No obviously useful information here other than what an acknowledgement of valid credentials looks like.

It is important to note that during this exchange, the password was not sent in clear text. Also, the encoded password was not sent in clear text. It is my belief that the client software re-encodes the password prior to sending it from the client to the host.

Security risks Associated with Remote Control Software:

An important feature of Timbuktu is that a device can function as both a Timbuktu host and client simultaneously. For example, Workstation A can connect as a client to Workstation B. Workstation B can then (while under the control of Workstation A) initiate a connection to Workstation C .

While not unique to Timbuktu, the ability to leapfrog functional control from machine to machine can lead to unanticipated security vulnerabilities and exposures.



In the example above, workstation A controls workstation D, even with firewall(s) separating the two machines.

To avoid problems of this type, organizations should follow the principle of least privilege access.
Remote access functionality should not be allowed to span borders of autonomous groups, nor should non-secured devices be allowed to control high secured, highly sensitive servers.

Defense in Depth Response to the challenges posed by Timbuktu and Remote access tools in General.

1. Understand and mitigate the risks
   - Recognize that the use of Remote control software effectively extends the network perimeter to include the Remote clients.
   - Avoid software/technical solutions where one device can simultaneously function as a Remote host and a client.

2. Develop Policy to address the risks
   - Prohibit the use of remote control software implementations that have not been reviewed and approved by the Information Technology Security Department.
   - Educate Help Desk staff and other support personnel of their obligation to obtain consent and inform individuals when their workstations are being accessed or controlled remotely.
   - Prohibit remote control/remote observation software from loading automatically on standard end-user desktops. If help desk or support personnel require remote access to an end-user workstation, require the end-user to start the host software.
   - Educate all employees that any attempt to escalate privileges through the use of remote control software or other means is expressly prohibited, and that individuals found to engage in such activities are subject to termination and potential civil litigation.
   - Develop corporate policy to establish minimum password requirements.
   - Audit remote control passwords to verify that they comply with established corporate policy.
   - Establish policy concerning administrative boundaries or domains for workstations and servers. Prohibit unsecured devices from controlling critical or sensitive devices.
   - Prohibit external hosts from controlling or connecting to internal workstations over the Internet.
   - Develop a Computer Incident Response Team to respond to computer security breaches/incidents.

3. Identify Appropriate Remote Access/Remote Control Technology
   - Use solutions that employ strong encryption for communications.
   - Use solutions that employ strong encryption for locally saved configuration files.
   - Use solutions that employ two-factor authentication.
   - Secure critical configuration files that may be stored on workstations with appropriate access control lists.

4. Monitor The Infrastructure
   - Monitor critical configuration files that may be stored on workstations/servers with Tripwire or other tools to be made aware of unauthorized changes.
   - Use secure, centralized logging for remote access events. Be able to document who was accessing what remote computer when.

- Use network and host based intrusion detection systems to be alerted of abnormal remote access attempts.
- Perform pro-active network scans on a periodic basis to identify rogue or unauthorized remote control software installations

5. Provide Appropriate Training
   - Educate administrators about the risks associated with remote access tools.
   - Provide training to all computer users, but System Administrators in particular about steps to take in the event they believe security has been breached.
   - Train all computer users on need to maintain strong passwords.

References:

1. Blue Boar (BlueBoar@THIEVCO.COM) Vulnerability Development mailing list web archive Timbuktu32
   October 04 1999 URL:
   http://lists.insecure.org/vuln-dev/1999/Oct/0010.html (1 October 2002)

2. “Netopia Timbuktu Help File”
   Timbuktu Pro 2000 (Version 2.0 Build 815 Es) URL:
   C:\Program Files\Timbuktu Pro\Help\1.htm

3. “Kerberos Password Policy For MHPCC” URL:
   http://www.mhpcc.edu/accounts/password_policy.html (1 October 2002)

4. Netopia FAQ “How to connect to a system behind a router running NAT” URL:
   http://www.netopia.com/en-us/support/howtodocs/win/nat.html (25 September 2002)

5. Australian National University URL:
   http://escience.anu.edu.au/lecture/ivr/networkProtocols/index.en.html (30 September 2002)

6. Levier, Laurent. “Timbuktu Pro Denial of Service”
   Security Administrator Posting Dated 14 February 2000. URL:
   http://www.secadministrator.com/Articles/Index.cfm?ArticleID=9494 (1 October 2002)

7. DR.Timbuktu.Database.Insecurity Posting
   ”Netopia Timbuktu Remote Access Software Lets Users Without Administrator Privileges Modify User Account Restrictions”
   February 2002 URL:
   http://www.securitytracker.com/alerts/2002/Feb/1003637.html (25 September 2002)

8. Wilson, Rich Security Focus “Re: Remote control of NTs”
   May, 2001 URL:
   http://online.securityfocus.com/archive/88/186226/2001-05-30/2001-06-05/2 (1 October 2002)

9. Skoll, David F. archives.postgresql.org Posting
   ”Re: OT: password encryption (salt theory)”
   August, 2002
   http://archives.postgresql.org/pgsql-admin/2002-08/msg00251.php (1 October 2002)

10. Krishna, Arvind. “Five Steps for Keeping Hackers at Bay”
    Ziff Davis Net Commentary
    18 September 2002 URL:
    http://zdnet.com.com/2100-1107-958397.html (1 October 2002)

Other Helpful Reference Information

- Konigsberg, Bob. “Auditing Inside the Enterprise via Port Scanning & Related Tools” SANS Information Security Reading Room. 18 January 2002. URL: http://rr.sans.org/audit/inside.php (1 October 2002)

- Plensdorf, Christopher. “VNC – Is it the Answer to Your Remote Control Needs?” SANS Information Security Reading Room. 25 June 2001. URL: http://rr.sans.org/win/VNC2.php (1 October 2002)

- Taylor, Laura. “Seven Elements of Highly Effective Security Policies” Ziff Davis Net Commentary. 16 February 2001. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2687089,00.html (1 October 2002)

- Boston, Terry. “The Insider Threat” SANS Information Security Reading Room. 24 October 2000. URL: http://rr.sans.org/securitybasics/insider_threat2.php (1 October 2002)

- Verton, Dan. “Survey Reveals Unexpected Drop in Insider Attack” Computerworld. 22 April 2002. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,70353,00.html (1 October 2002)

Last Updated: January 29th, 2015

Upcoming SANS Training

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

Cyber Threat Intelligence Summit & Training	**Washington, DCUS**	**Feb 02, 2015 - Feb 09, 2015**	**Live Event**
SANS Scottsdale 2015	**Scottsdale, AZUS**	**Feb 16, 2015 - Feb 21, 2015**	**Live Event**
10th Annual ICS Security Summit	**Orlando, FLUS**	**Feb 22, 2015 - Mar 02, 2015**	**Live Event**
SANS Munich 2015	**Munich, DE**	**Feb 23, 2015 - Mar 07, 2015**	**Live Event**
SANS DFIR Monterey 2015	**Monterey, CAUS**	**Feb 23, 2015 - Feb 28, 2015**	**Live Event**
SANS Cyber Guardian Baltimore 2015	**Baltimore, MDUS**	**Mar 02, 2015 - Mar 07, 2015**	**Live Event**
SANS Northern Virginia 2015	**Reston, VAUS**	**Mar 09, 2015 - Mar 14, 2015**	**Live Event**
SANS Secure Singapore 2015	**Singapore, SG**	**Mar 09, 2015 - Mar 21, 2015**	**Live Event**
SANS Abu Dhabi 2015	**Abu Dhabi, AE**	**Mar 14, 2015 - Mar 19, 2015**	**Live Event**
SANS Secure Canberra 2015	**Canberra, AU**	**Mar 16, 2015 - Mar 28, 2015**	**Live Event**
SANS Houston 2015	**Houston, TXUS**	**Mar 23, 2015 - Mar 28, 2015**	**Live Event**
SANS Stockholm 2015	**Stockholm, SE**	**Mar 23, 2015 - Mar 28, 2015**	**Live Event**
SANS Oslo 2015	**Oslo, NO**	**Mar 23, 2015 - Mar 28, 2015**	**Live Event**
SANS 2015	**Orlando, FLUS**	**Apr 11, 2015 - Apr 18, 2015**	**Live Event**
RSA Conference 2015	**San Francisco, CAUS**	**Apr 19, 2015 - Apr 20, 2015**	**Live Event**
Security Operations Center Summit & Training	**Washington, DCUS**	**Apr 24, 2015 - May 01, 2015**	**Live Event**
SANS ICS London 2015	**London, GB**	**Apr 27, 2015 - May 02, 2015**	**Live Event**
SANS Dubai 2015	**OnlineAE**	**Jan 31, 2015 - Feb 05, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**