RESOURCE AND PATIENT MANAGEMENT SYSTEM

# Encrypt Data in Flight; Disable Telnet Access.

## Installation Guide

MARCH 2019

Office of Information Technology (OIT)

Rockville, Maryland

# Table of Contents

# 1.0 Document Overview

## 1.1 Historical Information

When computers first started being used to store medical information, there would be one central computer called a mainframe and "dumb" display terminals that interfaced with that one computer.

As computers improved to the point where it was more economical to have individual PCs on the desktop, the paradigm of 'connecting to a central server' still existed and the server software itself was still quite useful, so programs were written so these computers could emulate the display terminals of long ago to communicate with the medical server. The currently used protocol for this communication is called ***Telnet.***

Unfortunately, as computers and networks progressed, so did ways of accessing this data inappropriately, and Telnet is a protocol that sends data "in the clear" or unencrypted. Another way to state this is "easily accessed by people that shouldn't."

There are ways of encrypting network traffic so nefarious users can't access it, however, RPMS isn't currently compatible with the most used standards. So, we have to install an "invisible" workaround to encrypt the traffic. There are free programs that will create an encrypted tunnel – then all we have to do is "point" our unencrypted network traffic at the tunnel and verify it works; then once all workstations are set up with the tunnel software, disable the unencrypted connectivity via an Access Control List or firewall.

## 1.2 Project Overview

We're going to install encrypted tunneling software (called 'stunnel') on the RPMS server and workstations, test it, install the stunnel software on the workstations, verify all Telnet traffic is now encrypted, then disable the Telnet port on the server disallowing any unencrypted data transmission.

# 2.0 Acquire Software

## 2.1 Software Description

The required software is called 'stunnel' and is completely free to use in a commercial setting and open source. So, outside of the time & personnel required for the project, there won't be any capital outlay. Be sure to download the latest version of the software

## 2.2 Download Software (Windows)

The software can be downloaded here: https://www.stunnel.org/downloads.html

## 2.3 Download Software (AIX)

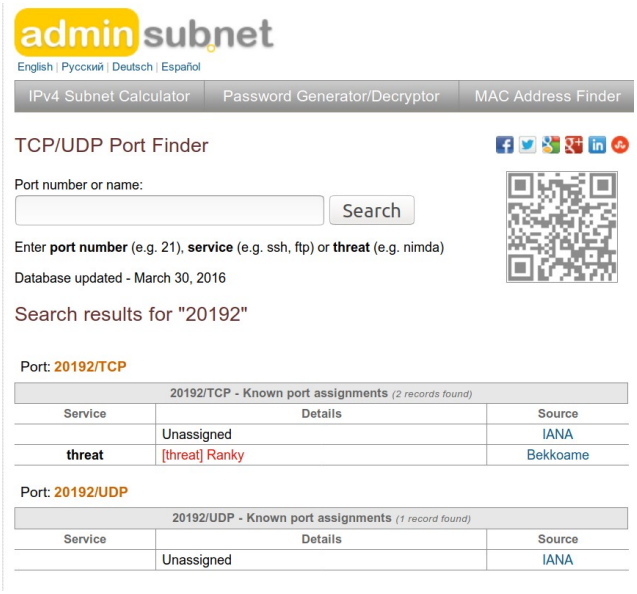
The software can be downloaded here: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.html

# 3.0 Configure and Install Server Software

## 3.1 Choose New Port

To tunnel the Telnet traffic, we need to choose a new, unused port on the server. Assigned ports are controlled by the IANA, or Internet Assigned Numbers Authority. There are many utilities on the web that can tell you if a port is assigned or not, here's one such website:

http://www.adminsub.net/tcp-udp-port-finder/




It's not a bad idea to use a port that would be easy to remember – in this case, 20190 would work fine. It's not assigned, and chances are good that it's not in use on your server, but always doublecheck!

One reason is that certain ports may have been 'hijacked' by malware – if you use these ports and open your firewall to them, that may allow a malware attack vector into your server. The most descriptive term for this is **"Bad Mojo!"** See the attached image to the right.

For the rest of this document, we're going to use the port 20190 in our examples.

## 3.2 Configure and install Software (Windows Server)

Verify you are a server administrator, as full administrative rights are required to install this software.

Locate the software installer you downloaded in section 2.2 and double-click on it. If you receive a pop-up asking to make changes to the server, click 'Yes.'

You will see several screens, you can choose the default for each screen.

Once installed, you'll need to install the service – this can either be done from the Start Menu with this icon: 

Or with this command issued in an Administrator Command Prompt:

```
"c:\Program Files (x86)\stunnel\bin\stunnel.exe" -install
```

*[[ If the command fails, try removing the underlined portion of the command above. If that still fails, try the GUI icon instead. ]]*

Now, we'll need to configure the service. Click this icon in the Start menu: 


and it will request permission to start Notepad with Administrator privileges – click "Yes." You can either remove all lines from the file and start from scratch (easier but removes documentation) or 'comment' out all of the existing lines that do not start with a semicolon - ';'. Once that's complete, at the bottom of the file add these lines *[[ again, assuming the new port will be 20190 ]]*:

```
[telnet]
accept = 20190
connect = 23
cert = stunnel.pem
```

and Save the file.