OpenSSH/Putty/SSH is a program that allows encrypted communications between two untrusted hosts over an insecure network. There are a few different versions based on the operating system that a given user might have. Since I use Windows I use Putty whereas UNIX users would use OpenSSH. Essentially what it does is that it allows users to create remote sessions on a computer. So using Putty, users can connect to a UNIX system such as bluenose.cs.dal.ca and run code on it as if they were sitting in front of that UNIX system.

Putty was originally developed for Windows systems. It has since been ported to other systems such as mobile systems. It began development in 1998 and has continued to be one of the leading tools in remote connections. The current most stable release is version 0.67. Each version has long lengthy beta periods which is one of the main critiques of the software. Version 0.67 was released on March 3rd, 2016 It was created by Simon Tatham.

To begin using Putty, the software must be downloaded from the software webpage. Once downloaded and launched a small window opens call Putty Configuration. Within this window there are options on the left side and the main window in the middle. The main default window is where you input a host name or IP address to connect to. It also allows you to select the protocol that you will use to connect to the given host or IP address. It also has the option to save a session. This tab is the main window to connect, most of the time users won’t change anything else but the information in this window. Under the session tab on the left side of the GUI there is a Logging option. Under this tab there are numerous options to decide how or if you want to log the session information from your connection.

The second tab on the left has options for how the terminal works. Within it, it initially defines how the terminal behaves such as wrapping text and whether the user wants blinking text or not. There are three sub-options under the Terminal tab. The first one contains information about how the keyboard works. This allows users to change basic keyboard related information such as backspace being either CNTRL-H or CNTRL-?, and what the function keys are. The second sub-tab allows users to control the terminal bell which is essentially just a simple alert. The final tab is used to either enable or disable some of the terminals advanced features.

The next tab contains options to change Putty’s window. The main page allows for users to control the size of the window by changing how many columns and rows will be displayed by default and how it will act if the window is resized. It also allows for scrollbar options. The first sub-tab in the Window tab allows users to change things about its appearance. These are things such as how the cursor looks and what kind of font is being used. The second sub-tab is for behaviour. These are things such as warning’s for closure or using a command to full screen. The third sub-tab is for translation, it contains an option for changing the character set. The fourth sub-tab is for controlling how copy and paste works. The fifth sub-tab is for controlling the colors displayed. Using RGB values every color option such as background and font can be changed to what the user wants.

The Final tab in Putty contains connection options. The default window allows for users to set a keep alive time and change the IP version being used. The first sub-tab allows users to change data sent to the server. Options such as auto-login username and environment variables can be set on this tab. The next sub-tab is the proxy tab. This allows users to change the proxy type from none to something like telnet or HTTP. The next four sub-tabs allow users to change how their specified connection type works. There is a telnet, rlogin, SSH, and serial tabs. They all contain various options to manipulate the given connection type that you are using.

Putty is a powerful tool that allows users to use operating systems that they would otherwise not have access to. Not only does it allow users to access operating systems, but it allows users to access a grouping of systems. For bluenose, it allows users to connect to its service and make use of all of Dal’s services. Services that could be uses would be the ability to submit assignments, making use of bluenose’s program environment, and remote file storage. This can make it easy to have a grouping of people access information.

Putty could possibly be used in a malicious way as with most network analysis software. A user could feasibly connect to a system that it does not have access to. The accessed group would then be compromised and important data could be stolen. Another way that Putty could be used maliciously was from people making a fake Putty client. The fake Putty client would then give the users their credentials by spoofing an access. This would allow malicious users to then connect to the host with the stolen credentials and thus compromise the system.

Putty is one of the most used SSH clients in the world. While made initially for Windows, other versions have been made for mobile phones and other operating systems. It allows for remote access to systems, making it easy for people to work on the system from far locations. It also makes it easy to share information with a large group of people. It is fairly secure, and malicious users would have to do different strategies to take information rather than just analyze data and plan an attack like most network analyzing tools.

Kovacs, Eduard. *Attackers Use Trojanized Version of Putty to Steal SSH Credentials.* Security Week. <http://www.securityweek.com/attackers-use-trojanized-version-putty-steal-ssh-credentials>

Tatham, Simon. *Putty FAQ.* Putty.<http://www.chiark.greenend.org.uk/~sgtatham/putty/faq.html>