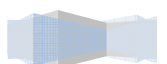


System Design



TABLE OF CONTENT

3.1. Abbreviations	1
3.2. Objective and overview	1
3.3. Preliminary User Interface	2-5
3.3.1. Main Menu	2-4
3.3.2. About Us	5
Reference	6
Bibliography	7



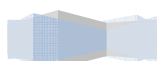
ABBREVIATIONS

- WEP: Wired Equivalent Privacy.
- IP Address: Internet Protocol Address.
- MAC: Media Access Control.
- WiFi: Wireless Fidelity.

1.1. OBJECTIVE AND OVERVIEW

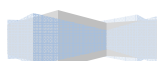
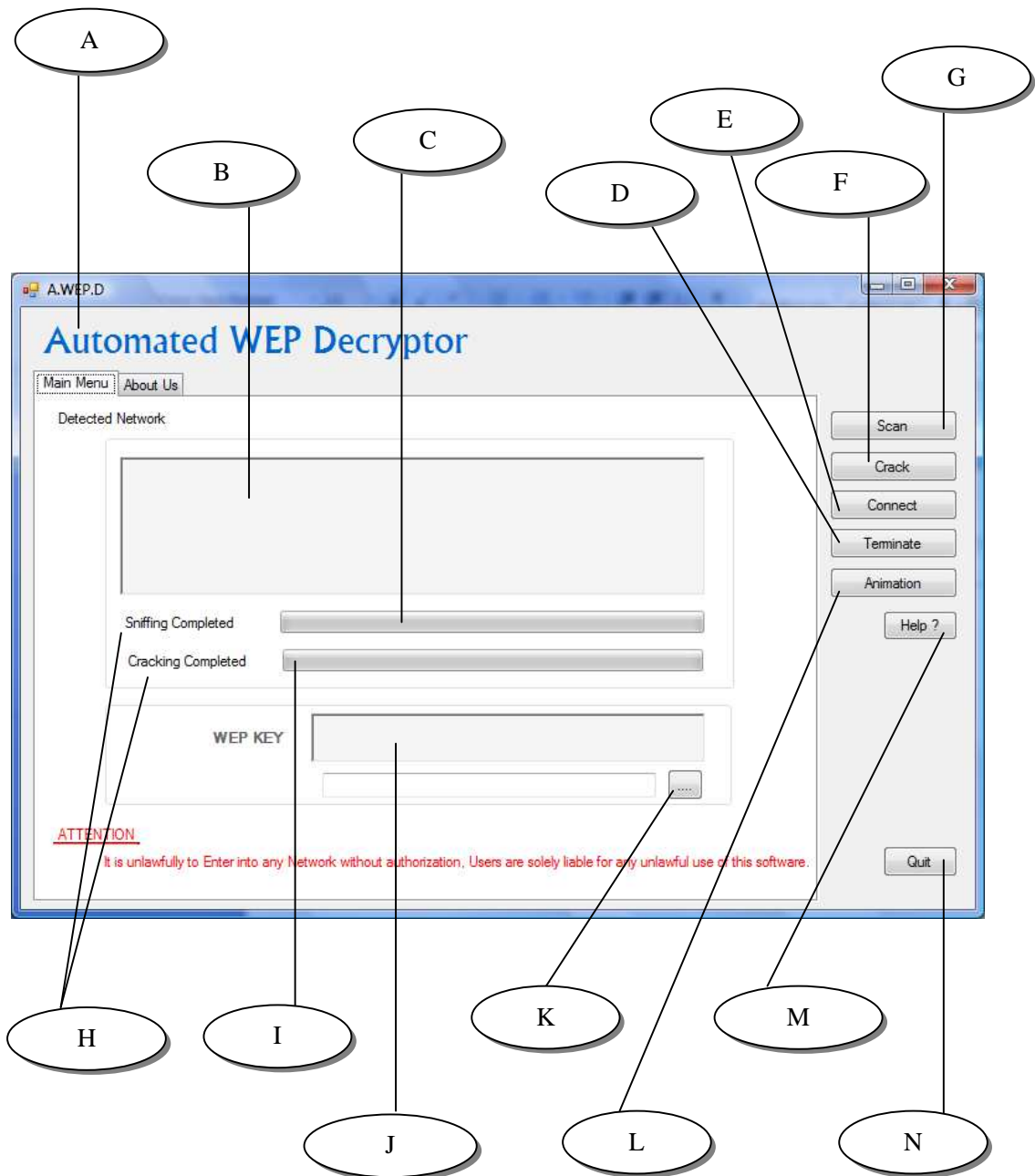
This document illustrates the feasible functions in the system and also portrays the preliminary user interface of the proposed system.

Labeled Screen shots of the preliminary User interface were used to explain the functions in the system.



1.2. USER INTERFACE

1.2.1. MAIN MENU



LABEL A (main menu): provides an interface which enables the user to interact with the system.

The Main Menu contains buttons which are used to interact with the system and text area which are display output such as WEP key and Available Network to the User.

LABEL C (process bar) it display the progression of the Sniffing mode.

LABEL D (terminate button): This function enables the user exit the Current function at any time.

LABEL E (connect button): This function enables the user to connect to the desired network. Once this button is clicked the WEP key is read from the packet information file, and then sends a connection request to the wireless router, if the WEP key matches with the routers WEP key, an acknowledgement will be sent back to the user and connection is established otherwise an error message will be sent back to the user. WEP key is also displayed at label J after this process.

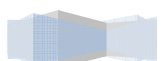
LABEL F (crack button): This function enables a user to decrypt the captured packets from the selected network (Label B).

This function sniffs for packets from the selected network. During packet sniffing the captured packets are converted into binary data, then decoded into human readable form, there after it undergoes protocol analysis. After packet sniffing is completed, the captured packets are stored in packet information file. The Cracking algorithm is executed which in turn reads the stored packets and generates the key after execution of the cracking process. The status of the sniffing and cracking progress could be monitored at label C and I.

LABEL G (scan button):

This function enables the user to scan for available networks.

Prior to detection of available wireless networks, WiFi status is checked, and then wireless signals within range are detected, afterwards the packet sniffing process executes. During packet sniffing the captured packets are converted into binary data, then decoded into human readable



form, there after it undergoes protocol analysis. Post packet sniffing, IP and MAC addresses of the router transmitting the signals are read and displayed in form of the Network Name.

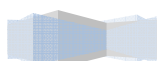
LABEL I (process bar) indicates cracking progress, it display the progression of the cracking mode. When the key is cracked successfully, user will be able to connect to the cracked network.

LABEL K (browse button) enables the user to view Captured packets and Key file.

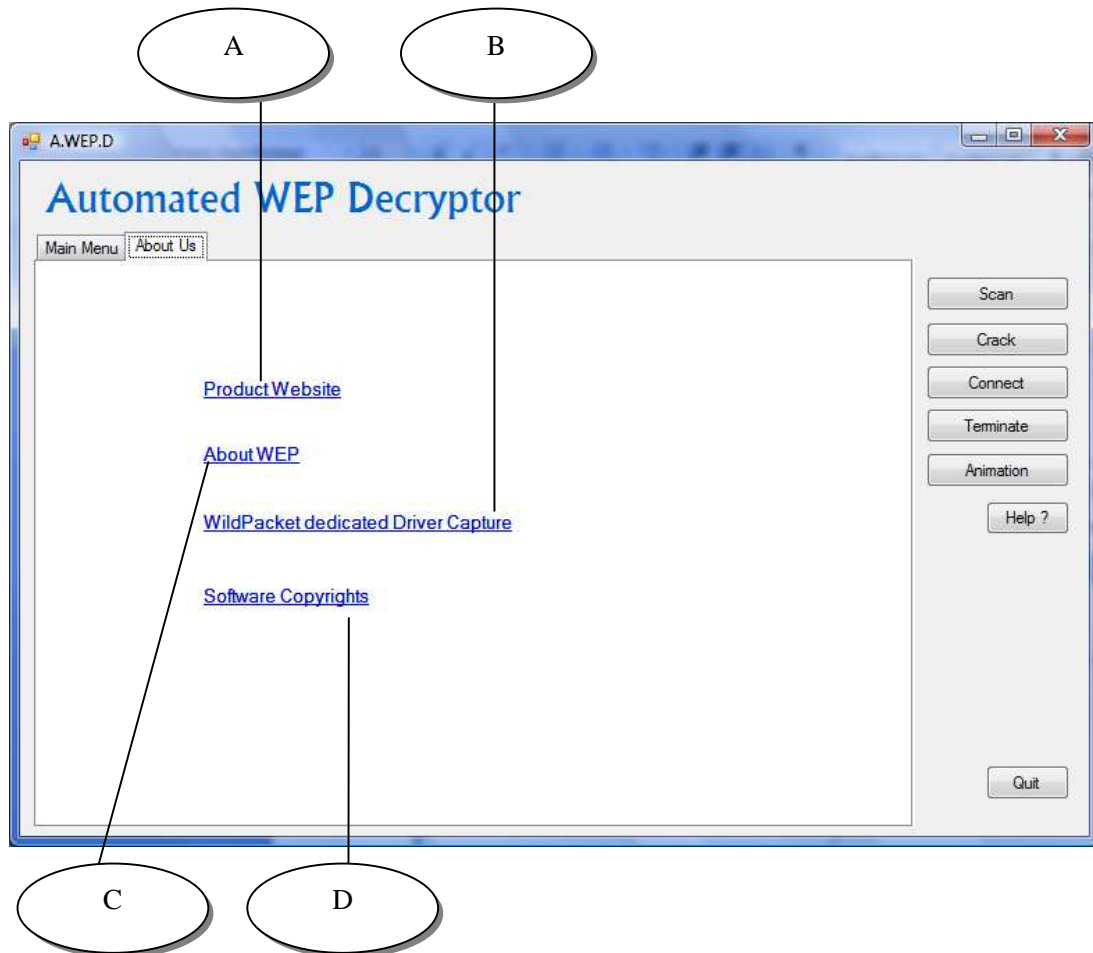
LABEL L (animation button): This function enables the user to view software demo.

LABEL M (help button) provides the user with context-sensitive help, through activation of the Help button, a window appears with the default top-level topic. While help mode is active, information about functions on the screen can be obtained.

LABEL N (quit button) closes the application.



1.2.2. ABOUT US

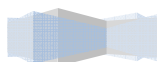


Label A: links to the project website.

Label B: links to websites which clearly explains WEP.

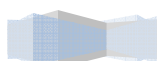
Label C: links to the download site of WildPacket drivers.

Label D: when clicked opens the copyright law related to the software.



LIST OF REFERENCES

1. Sun Microsystems Inc, 2004. Designing the Logical Architecture. [Online]
Available at: http://docs.sun.com/source/817-5759/log_architect.html [Accessed 4th June 2009].
2. Robert, G., 2002. Sniffing (network wiretap, sniffer) FAQ. [Online]
Available at: http://www.windowsecurity.com/whitepapers/Sniffing_network_wiretap_sniffer_FAQ.html [Accessed 14th May 2009].
3. The Network Monitoring Company. 2009. Packet Sniffing in LANs and WLANs.
[Online] Available at: <http://www.paessler.com/prtg/infographic/#sniffing> [Accessed 2nd June 2009].
4. Anglia Ruskin University. 2009. Harvard System of Referencing Guide. [Online] (Last Updated 26th May 2009)
Available at: http://libweb.anglia.ac.uk/referencing/harvard.htm?harvard_id=66#66
[Accessed 16th June 2009].
5. Owen, A., 2008. Logical Architecture Model for SharePoint. [Online] (Last Updated 13th April 2008) Available at: <http://www.psspug.org/blog/Lists/Posts/Post.aspx?ID=17>
[Accessed 12th July 2009].
6. Surakshan, M., 2005. Protocol decoding and surveillance. [Online]
Available at: <http://www.surasoft.com/articles/packetsniffing.php> [Accessed 20th July 2009].



LIST OF BIBLIOGRAPHYS

7. Dieter, G., 2005. Computer Security. 2nd Edition. Glasgow, Scotland: Wiley.
8. Charlie, K. Radia, P. & Mike, S., 2007. Network Security. 2nd Edition. New Jersey: Prentice Hall.

