Why Johnnys' Network got Owned by Evil Hackers Bent on World Domination and Johnny was Helpless to Stop It: A Study on Project Usability from a Cyber-Security Professionals Perspective

John Paul Dunning

Rajesh Gangam

Agenda

- Problem
- Motivation
- Related Work
- Usability Study
- Analysis
- Usability Attributes
- Application of Usability Attributes
- Conclusion and Future Work

Problem

- Security Professionals are in need of usable security tools and applications.
- Why?
  - Security is the primary functionality.
  - Dynamic Environment: Security Tools and App's always have upgrades and patches.
  - Collaborative Tools.
- What do you Gain?
  - Better Security. Better Support. Faster Solutions.

Motivation

- Little research has been done on usable security applications for security professionals on a broad scale.
- Administrators design, configure, troubleshoot, and maintain complex computer system comprised of a multitude of components.

Related Work

- User End Usability
  - Kazaa
  - Johnny
  - Johnny 2
- Problems faced by System Administrators.
  - Field Studies of Computer System Administrators
  - I Know My Network: Collaboration and Expertise in Intrusion Detection

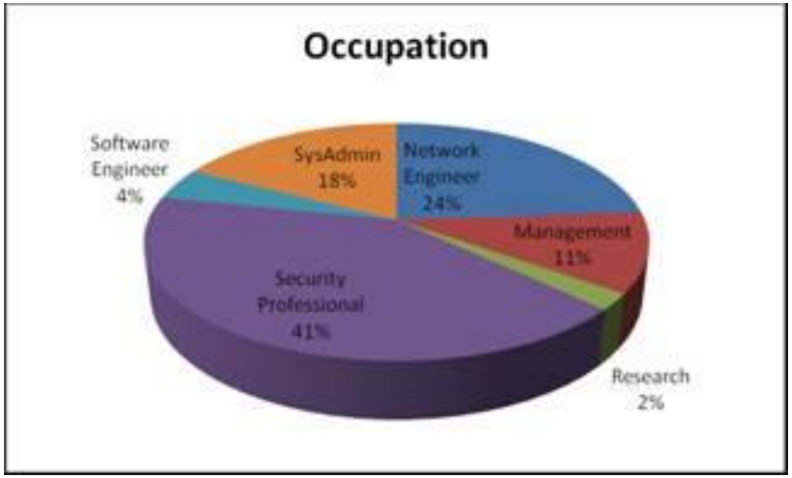
Definitions:

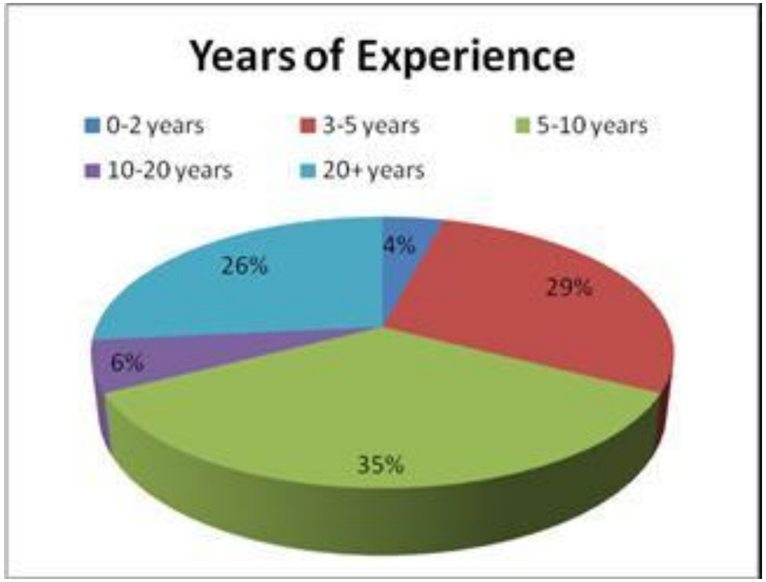
- Administrators
  - Individuals who are responsible for the well being of systems on a large scale.
- Project Vs Application Usability.
  - Usability concerns at a project level where application is only a part.
    - Contains Product Support, Access to Source Code, Environment, Cost , Scale, Target.

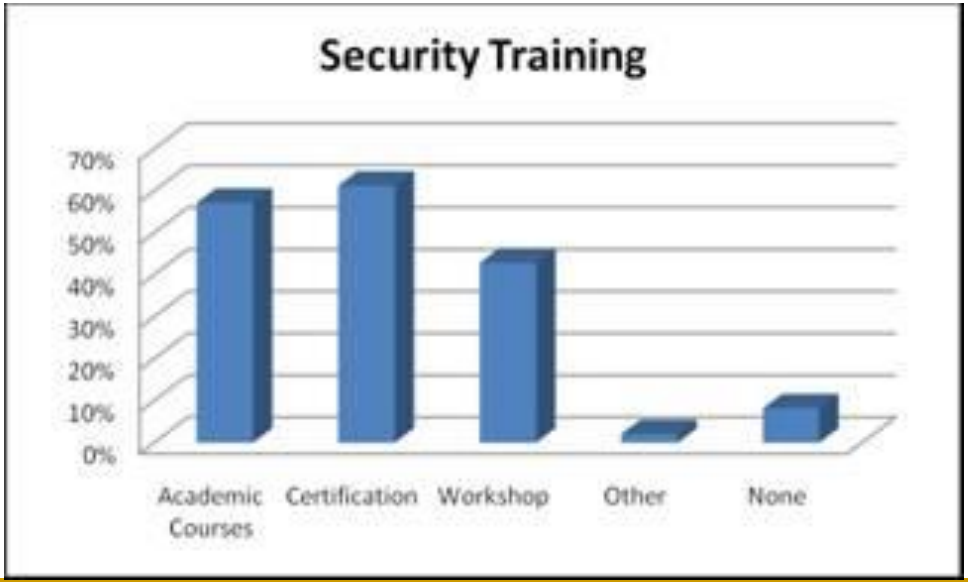
Usability Study

- We have surveyed **50** Administrators.
- The Participants belonged to
  - Virginia Tech Technical Listserv
  - The Army Network Engineering Listserv
  - University Security Operations Group Listserv of SANS.

Usability Study





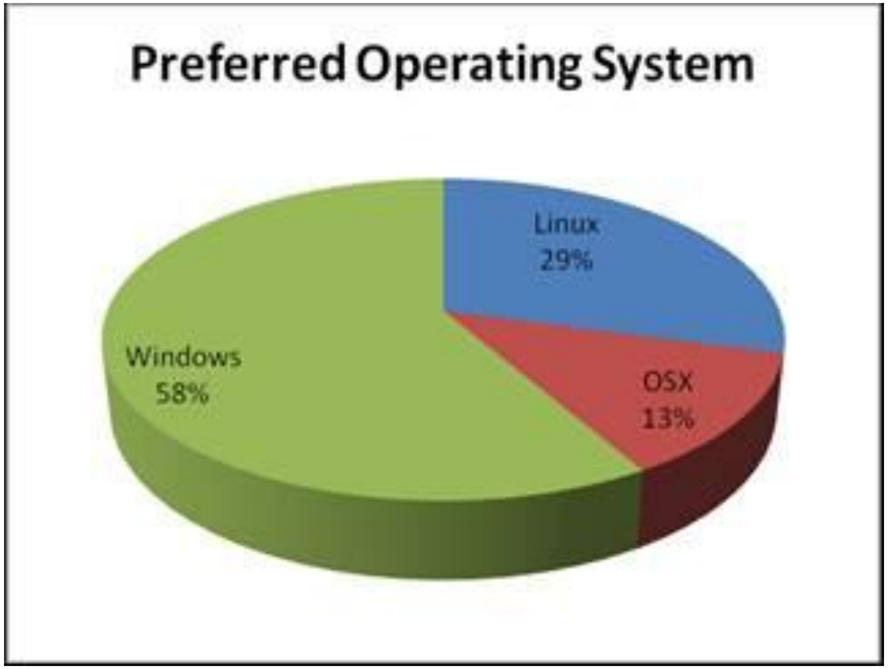


Findings From the Survey

- Popular Security Tools
  - Nmap
    - A Network Scanner which tries to identify the services and machine configurations on the network.
  - Nessus
    - A Network Vulnerability Scanner.
  - Wireshark
    - Network Packet Analyzer used for network troubleshooting.
  - Snort
    - A Network Intrusion Prevention and Detection System,
  - TcpDump
    - Network Packet Analyzer.

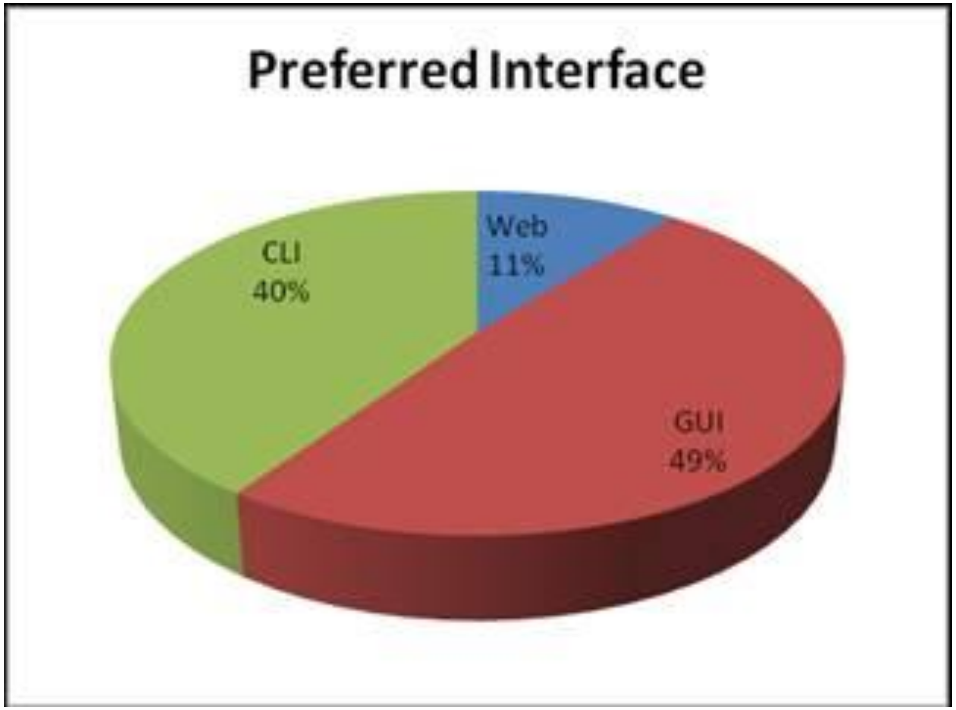
Observations:

- Preferred Operating System.
  - The Host Environment of the application.
  - Windows is the Most Preferred..
  - It is recognized as the primary attribute.



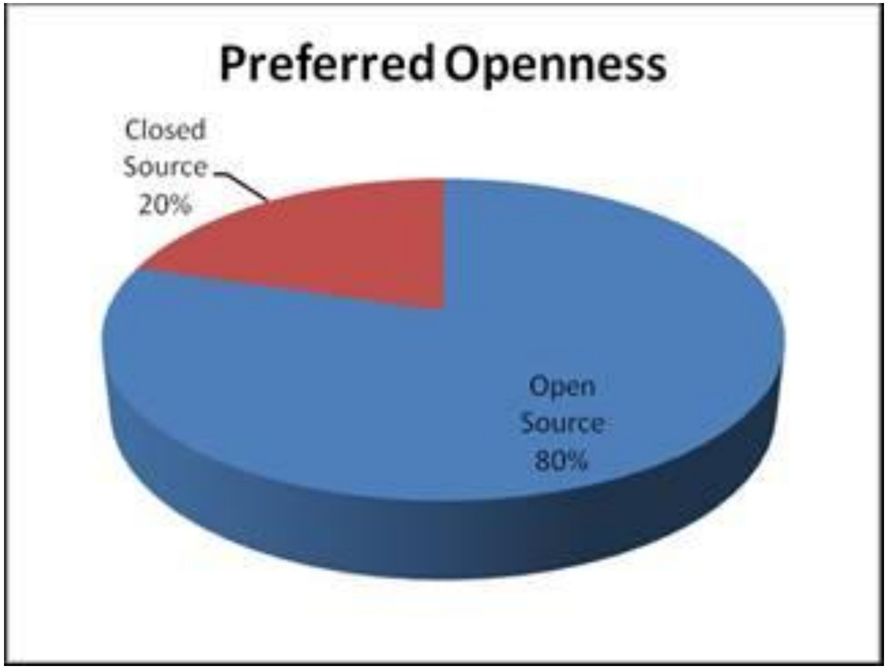
Observations:

- Preferred Interface
  - Identify the popular user interface.
  - Graphical User Interface and CLI.
  - Recognized as primary attribute.



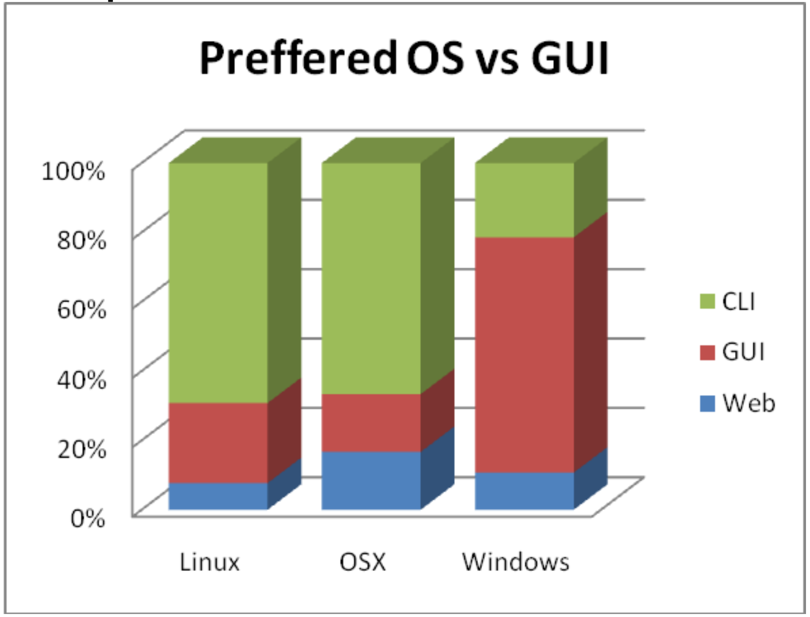
Observations:

- Preferred Openness
  - Offers Customization to the tools.`
  - Open Source is Most preferred.
  - Recognized as primary attribute.



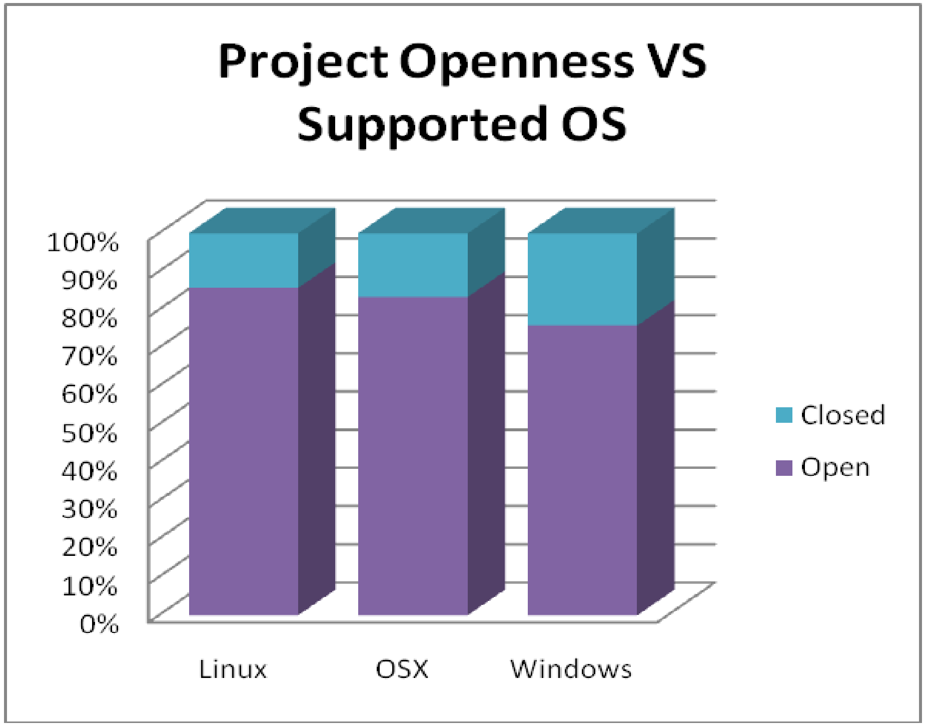
Observations:

- Preferred OS and UI
  - Users Preferred Command Line Interface on both Linux and OSX.
  - Similarly Windows Users would need GUI.
  - Developers are recommended to provide both GUI and CLI interfaces interchangebly.



Observations:

- Project Openness vs Supported OS
  - Availability of Open Projects on all the Operating Systems.
  - A Higher Range of Openness is expected only in Linux.



Usability Attributes

- Attribute
- Primary Attributes Check List
  - Operating System
  - User Interface
  - Community Involvement
  - Target System

PUA CheckList

Attribute	*Option 1*	*Option 2*	*Option 3*
Operating System	[ ] Windows	[ ] OSX	[ ] Linux
User Interface	[ ] GUI	[ ] Web Browser	[ ] Command Line
Community Involvement	[ ] Open	[ ] Closed	
Target System	[ ] End User System	[ ] Administrator System	

Secondary Attributes

- Secondary attributes in the area of interest to administrators.
- We found 18 distinct attributes from the survey results.

Secondary Attributes

- *Documentation*
- *Customer Support*
- *Customizable*
- *Development Practices*
- *Cost*
- *Scale of Developed*
- *Maintenance*
- *Complexity*
- *Installation and Setup*
- *System Resources*
- *Default Settings*
- *Code Availability*
- *Platform*
- *Unique*
- *Effectiveness*
- *Scope*
- *Feedback*
- *Demographic*

SUA Framework

- *Documentation*: Is the project well documented? This includes information on the purpose of the project, the functionality of the project, instructions on project use, etc?
- *Customer Support*: Is project support provided? Does the support come directly from the project developing entity or is it supported by a third party, like a community forum?
- *Customizable*: Does the project allow for customization or is it static? Can users change settings, add/remove components, etc?
- *Development Practices*: Where adequate coding development enforced during application development to ensure code security, test for correct functionality, minimize side effects, document code, etc?
- *Cost*: Is the price reasonable for the intended customer base?

Application to Project

- Pwntooth is a fully automated "search and destroy" project designed to automate Bluetooth pen-testing.
- Applying the PUA CheckList.
- Applying the SUA Framework.

Applying the PUA CheckList

Attribute	***Option 1***	***Option 2***	***Option 3***
Operating System	[ ] Windows	[ ] OSX	[x] Linux
User Interface	[ ] GUI	[ ] Web Browser	[ ] Command Line
Community Involvement	[ ] Open	[ ] Closed	
Target System	[ ] End User System	[x] Administrator System	

Applying the PUA CheckList

Attribute	***Option 1***	***Option 2***	***Option 3***
Operating System	[ ] Windows	[ ] OSX	[x] Linux
User Interface	[ ] GUI	[ ] Web Browser	[x] Command Line
Community Involvement	[x] Open	[ ] Closed	
Target System	[ ] End User System	[x] Administ-rator System	

Applying SUA Framework

Attribute	Description
Documentation	Documentation is provided through execution of the application with the -h flag. The documentation includes a brief description of the tool as well as a description the functionality availably thought invoking various flags. The project is also accompanied by a changelog and installation instructions.
Customer Support	Customer support is mainly by the developer, but also through the user community.
Customizable	Users can customize which exploits are conducted and in what manner. The project is also customizable through the addition and removal of other Bluetooth auditing command line projects.
Development Practices	The project testing was done on a small scale by a single individual. Testing was expected of the community.
Cost	Free of charge.

Conclusions and Future Work

- We have Identify Primary and Secondary attributes of a Security Project and Application.
- We Have applied this Attributes to the Security Application (PwnTooth).
- One-on-One Guided Interview.
- More Study on Day-to-Day issues.

- Thank You!