Interface Design for Hacking Tools

Greg Conti
Disclaimer

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense or the U.S. Government.
Outline

• Introduction
• Command Line vs. GUI's
• Task, User, & Technology
• Principles of Design
• GUI Components
• Critique of Tools
• Pointers
• Q&A
What is an Interface?

“The point of interaction or communication between a computer and any other entity, such as a printer or human operator.”
What is an Interface?

“The way that you accomplish tasks with a product and how it responds – that’s the interface.”

The Humane Interface by Jef Raskin, p2
Command Line vs. GUI

- Flexibility
- Time
- Ease of use
- Best for heavy users

image: http://helpdesk.princeton.edu/images/ping.gif
source: http://www.jpeek.com/talks/svlug_19991103/020.html
Crack in One Line of Perl

perl -nle 'setpwent;crypt($_,$c)eq$c&&print"$u $_
while($u,$c)=getpwent'
Several Lines of Perl Can Crack DVD Encryption

#!/usr/bin/perl
# 472-byte qrpff, Keith Winstein and Marc Horowitz <sipb-iap-dvd@mit.edu>
# MPEG 2 PS VOB file -> descrambled output on stdout.
# usage: perl -I <k1>:<k2>:<k3>:<k4>:<k5> qrpff
# where k1..k5 are the title key bytes in least to most-significant order

s'$/=\2048;while(<>){$G=29;R=142;if(@a=unqT="C",_)[20]&48){D=89;_=unqb24,qT, @}b=map{ord qB8,unqb8,qT,_^$a[--D]}@INC;s/...$/1$&/;Q=unqV,qb25,_;H=73;O=$b[4]<<9 |256|$b[3];Q=Q>>8^P=(E=255)&(Q>>12^Q>>4^Q/8^Q))<<17,0=O>>8^P=(E=(S=0>>14&7^0) ^S/8^S<<6))<<9,_=(map{U=_%16orE^R^=110&(S=(unqT,"\xb\ntd\xbz\x14d")[_/16%8])[_/16%8]};E ^=72,0z=(64,72,G^=12*(U-2?0:S&17)),H=_%64?12:0,0z)[_%8]}(16..271))[_]^((D>>>8 )+=P+(-F&E))for@a[128..$#a]}print+qT,@a'};

Authors: Keith Winstein and Marc Horowitz
Original source: http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/qrpff.pl
*Note that code above is not complete
Foundations...

- Tasks
- Users
- Technology
Understanding Tasks

What tasks are your users trying to accomplish?

image: http://www.pvtmurphy.com, used with permission
Who are your users?
Your Users may be Beginners...

“Ok I know i'm very slow, stupid too maybe....I can't see a damn thing execpt the poster's e-mail address .... I am new to computers and am trying to learn what I can so please be gentle.”

- alt.2600.hackersz
Advanced…

“From your questions, it seems you are over-simplifying just what a disassembler can do for you. If you are not an experienced assembly language programmer then the disassembled file will look like Greek”

- alt.2600.hackersz
Some System Scan options are not selected

System Scan is not set to use all of its scan options. This might allow some viruses to go undetected.

VShield is not selected, which could be a mistake.

Your need for protection may require you to select the appropriate options.

McAfee VirusScan can be found at www.mcafee.com
Enabling Technology

Analyze the task and your users first. The proper technology follows.
Principles of Design

• Cognitive Science
• Design for Clarity
• Navigation
• Color
• Fonts
• Metaphor
• Consistency
• Feedback
• Testing
• Information Display and Visualization
Cognitive Science

- Fitt’s Law
- Invisible structures
- Mental Models
- Modes
Design for Clarity

- Intuitive
- Allow Exploration
- Always allow a way out
- Consistency
Navigation

- Beware too many features at top level
- Go where users expect
Color

- People need contrast
- Less is more
- Color Blindness
- White or pale backgrounds are preferred
- Use of colors to draw attention

http://www.geocities.com/webtekrocks/
Client Testimonials
Proof positive that WebTek can work for you!

http://www.geocities.com/webtekrocks/html/services.html

useit.com: Jakob Nielsen’s Website
Permanent Content
Alertbox
Jakob’s column on Web usability
Usability For $200 (June 2)
How can a small company’s website benefit from usability activities despite a

News
User Experience 2003
> Chicago: September 21-25
> London: October 6-10

Our biggest conference ever with 28 full-day tutorials

http://www.useit.com
http://www.google.com
Metaphor use can map easily from people’s experience with other concepts

- Don’t force it
- Some are overdone…
  - “The Town”
  - “The Library”
WINAMP can be found at www.winamp.com

Consistency

Build on prior knowledge of other applications

• Placement of controls
• Keyboard shortcuts
• Within program, environment and related tools
Feedback

- Timely feedback
- Busy indicator
- Progress indicator
- Visual and audible
Testing

• Try it out on users, get feedback and fix
• You may be surprised
• Allow time to fix your project
• Value of Testing
• Iterative design
• How to conduct testing
Information Visualization

tracert from the command line

tracert downloads.com

Tracing route to downloads.com [216.200.247.148] over a maximum of 30 hops:

1 10 ms 100 ms 10 ms ad78-17.magix.com.sg [165.21.78.17]
2 <10 ms 10 ms 10 ms 203.112.21.247
3 <10 ms 10 ms 10 ms 192.168.2.6
4 10 ms 10 ms 10 ms ATM-4-0-0-access2.ix.singtel.com [203.127.108.16]
5 10 ms 10 ms 10 ms POS1-2.tp-core1.ix.singtel.com [202.160.250.13]
6 230 ms 441 ms 220 ms 203.208.154.26
7 290 ms 220 ms 231 ms 203.208.154.6
8 230 ms 230 ms 301 ms main1-main2-ge.col06.sjc2.above.net [208.185.237
9 220 ms 350 ms 221 ms sjc2-gige-core6.sjc2.above.net [208.185.156.34]
10 230 ms 220 ms 221 ms core2-core6-oc48.sjc2.above.net [208.185.156.69]
11 331 ms 230 ms 230 ms sjc2-gige-main1.col01.sjc2.above.net [208.184.1
12 220 ms 230 ms 451 ms cnet-abovenet.1.above.net [216.200.254.106]
13 220 ms 231 ms 240 ms abv-sjc2-redirect.cnet.com [216.200.247.148]

Trace complete.

I:/>ping downloads.com

Pinging downloads.com [216.200.247.148] with 32 bytes of data:

Reply from 216.200.247.148: bytes=32 time=221ms TTL=242
Reply from 216.200.247.148: bytes=32 time=220ms TTL=242
Reply from 216.200.247.148: bytes=32 time=221ms TTL=242
Reply from 216.200.247.148: bytes=32 time=310ms TTL=242

Ping statistics for 216.200.247.148:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
     Minimum = 220ms, Maximum = 310ms, Average = 243ms

I:/>
Xtraceroute
Neotracer visualization

Xtraceroute by Björn Augustsson is available at http://www.dtek.chalmers.se/~d3august/xt/
See also the excellent Atlas of Cyberspaces at http://www.cybergeography.org/atlas/routes.html
Network Traffic Dataset
Network Traffic Viewed in Ethereal

The Ethereal Network Analyzer

<table>
<thead>
<tr>
<th>No</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>00:80:c8:11:b4:e1</td>
<td>ff:ff:ff:ff:ff:ff</td>
<td>ARP</td>
<td>Who has 192.168.1.2? Tell 192.168.1.1</td>
</tr>
<tr>
<td>2</td>
<td>0.000400</td>
<td>00:80:c8:33:1e:56</td>
<td>00:80:c8:11:b4:e1</td>
<td>ARP</td>
<td>192.168.1.2 is at 00:80:c8:33:1e:56</td>
</tr>
<tr>
<td>3</td>
<td>0.000444</td>
<td>uranus.beaupeyrat.com</td>
<td>192.168.1.2</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>4</td>
<td>0.000936</td>
<td>192.168.1.2</td>
<td>uranus.beaupeyrat.com</td>
<td>ICMP</td>
<td>Echo (ping) reply</td>
</tr>
<tr>
<td>5</td>
<td>0.001676</td>
<td>uranus.beaupeyrat.com</td>
<td>192.168.1.2</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>6</td>
<td>0.004175</td>
<td>uranus.beaupeyrat.com</td>
<td>192.168.1.2</td>
<td>ICMP</td>
<td>Echo (ping) reply</td>
</tr>
<tr>
<td>7</td>
<td>0.017292</td>
<td>192.168.1.2</td>
<td>192.168.1.2</td>
<td>SMB</td>
<td>SMBtrans Response</td>
</tr>
<tr>
<td>8</td>
<td>0.024093</td>
<td>192.168.1.2</td>
<td>192.168.1.2</td>
<td>SMB</td>
<td>SMBtrans Response</td>
</tr>
</tbody>
</table>

Ethereal by Gerald Combs can be found at http://www.etherreal.com/
image: http://www.linux-france.org/prj/edu/archinet/AMSI/index/images/etherreal.gif
Network Traffic as Viewed in EtherApe

EtherApe by Juan Toledo can be found at http://etherape.sourceforge.net/
screenshot:  http://www.solaris4you.dk/sniffersSS.html
GUI Components

- Radio Buttons
- Check Boxes
- Dialog Boxes
- Menus
- Labels
- Text Fields
- Toolbars
- Forms
- Splash Screens
- Push Buttons List Boxes
- Spinners
- Sliders
- and more…
Radio Buttons

- 1 to Many Control
- Try to limit to 6 items
- Set Default
- Not a check box
- Never use just one
Radio Buttons

Proper Use

Background Color
- Blue
- Black
- White
- Yellow

- Blue
- Black
- White
- Yellow

- Python
- Perl
- C++
- Ada
- Java
- C
- C#
- JavaScript
- ECMA Script
- Assembler
- LISP
- FORTRAN
- FORTH
- APL
- COBOL
- Prolog
- QBASIC
- Visual Basic
Check Boxes

- Used for single on/off settings
- Max 12 per group
- Don’t confuse with radio buttons
Checkbox

Proper Use

Would you like to receive...

- News mailings
- Our email newsletter
- Phone calls from our sales department
- Free samples

Proper Use

What tools do you use

- Ethereal
- TCPDump
- DSniff
- Ettercap
- Nmap
- Superscan
- traceroute
- ping
- telnet
- whois

Background

- Yellow
- White
- Blue

Your homestate...

- New York
- Georgia
- Arizona
- Florida

Choice 1
Choice 2
Choice 3
Choice 4
Choice 5
Choice 6
Choice 7
Choice 8
Choice 9
Choice 10
Choice 11
Choice 12
Choice 13
Choice 14
Choice 15
Choice 16
Choice 17
Choice 18
Choice 19
Choice 20
Choice 21
Choice 22
Choice 23
Choice 24
Choice 25
Dialog Boxes

- Modal (immediate task)
- Modeless (on going task)
- Beware too many levels
- Cancel doesn’t cancel

images: PCMark2002, MS Word, Win XP
PCMark2002 by Futuremark Corp can be found at http://futuremark.com/products/pcmark2002/
Menus

- Menu length
- Confusing menu items
- Keyboard shortcuts
Menus

Dynamic interfaces are generally considered bad.
• Keep text clear
• Place labels close to setting
• Consistent terminology, writing

• Avoid ambiguity
• Concepts must be distinct
Text Fields

- Defaults
- Make them large enough
- Highlighted current data
- Font size
- Alignment

Ethereal by Gerald Combs can be found at http://www.ethereal.com/
image: http://www.ethereal.com/docs/user-guide/ch03capturestart.html#CH03CAPPREF
Toolbars/Icons

- Consistency
- Test your images
- Sometimes text just works better
- Don’t Overdo It
Four Criteria

- Dominant reading order
- Frequency of use
- Relationship to other controls
- User Expectations

Other Issues

- Resizable
- Background Images
- Logical Grouping
- Line things up

1. GUI Blooper by Jeff Johnson, p.143
2. OTP can be found at www.rumint.com
Let’s Tear Apart My Own Projects

• Frequency Counter
• Advanced Frequency Counter

http://www.uk-anime.net/gallery/images/tenchi3.jpg
# Frequency Counter

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Count</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0735</td>
<td>26224</td>
<td>C:\Documents and Settings\RUMINT\Desktop\samplefile.txt</td>
</tr>
<tr>
<td>0.015</td>
<td>5352</td>
<td></td>
</tr>
<tr>
<td>0.0214</td>
<td>7623</td>
<td></td>
</tr>
<tr>
<td>0.0469</td>
<td>16755</td>
<td></td>
</tr>
<tr>
<td>0.1197</td>
<td>42730</td>
<td></td>
</tr>
<tr>
<td>0.0244</td>
<td>8710</td>
<td></td>
</tr>
<tr>
<td>0.0215</td>
<td>7670</td>
<td></td>
</tr>
<tr>
<td>0.0697</td>
<td>24882</td>
<td></td>
</tr>
<tr>
<td>0.0676</td>
<td>24139</td>
<td></td>
</tr>
<tr>
<td>0.0013</td>
<td>459</td>
<td></td>
</tr>
<tr>
<td>0.0055</td>
<td>1961</td>
<td></td>
</tr>
<tr>
<td>0.0427</td>
<td>15249</td>
<td></td>
</tr>
<tr>
<td>0.0249</td>
<td>8871</td>
<td></td>
</tr>
<tr>
<td>0.0696</td>
<td>24851</td>
<td></td>
</tr>
<tr>
<td>0.0763</td>
<td>27245</td>
<td></td>
</tr>
<tr>
<td>0.0172</td>
<td>6133</td>
<td></td>
</tr>
<tr>
<td>0.0007</td>
<td>252</td>
<td></td>
</tr>
<tr>
<td>0.0647</td>
<td>23094</td>
<td></td>
</tr>
<tr>
<td>0.0672</td>
<td>23998</td>
<td></td>
</tr>
<tr>
<td>0.0903</td>
<td>32213</td>
<td></td>
</tr>
<tr>
<td>0.0305</td>
<td>10900</td>
<td></td>
</tr>
<tr>
<td>0.0109</td>
<td>3886</td>
<td></td>
</tr>
<tr>
<td>0.0242</td>
<td>8650</td>
<td></td>
</tr>
<tr>
<td>0.0013</td>
<td>456</td>
<td></td>
</tr>
<tr>
<td>0.0124</td>
<td>4415</td>
<td></td>
</tr>
<tr>
<td>0.0005</td>
<td>176</td>
<td></td>
</tr>
</tbody>
</table>

**Total Characters:** 356894

Frequency Counter can be found at [www.rumint.com](http://www.rumint.com)
Advanced Frequency Counter

Advanced Frequency Counter can be found at www.rumint.com
Critique of tools
Respect to Authors

Your Kung Fu is Very Good
NetBus

Image source: http://members.tripod.com/~gineco/NET-BUS
Netbus is by Carl Fredrik Neikter
Nmap by Fyodor is available at http://www.insecure.org/
The Nmapwin front end by Jens Vogt is available at http://www.nmapwin.org/

### Output from: nmap \(-sS\) \(-O\) \(-D\) antionline.com xanadu vectra playground

**Interesting ports on vectra.yuma.net (192.168.0.5):**

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Protocol</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>open</td>
<td>tcp</td>
<td>daytime</td>
</tr>
<tr>
<td>21</td>
<td>open</td>
<td>tcp</td>
<td>ftp</td>
</tr>
<tr>
<td>22</td>
<td>open</td>
<td>tcp</td>
<td>ssh</td>
</tr>
<tr>
<td>23</td>
<td>open</td>
<td>tcp</td>
<td>telnet</td>
</tr>
<tr>
<td>37</td>
<td>open</td>
<td>tcp</td>
<td>time</td>
</tr>
<tr>
<td>79</td>
<td>open</td>
<td>tcp</td>
<td>finger</td>
</tr>
<tr>
<td>111</td>
<td>open</td>
<td>tcp</td>
<td>sunrpc</td>
</tr>
<tr>
<td>113</td>
<td>open</td>
<td>tcp</td>
<td>auth</td>
</tr>
<tr>
<td>513</td>
<td>open</td>
<td>tcp</td>
<td>login</td>
</tr>
<tr>
<td>514</td>
<td>open</td>
<td>tcp</td>
<td>shell</td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=14943 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

**Interesting ports on playground.yuma.net (192.168.0.1):**

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Protocol</th>
<th>Service</th>
</tr>
</thead>
</table>
SubSeven

Image source: http://www.zdnet.co.jp/help/howto/security/j04/images/sub7.gif
SubSeven is by mobman. The official site is http://www.subseven.ws/
SubSeven

• Connection
• Keys / messages
• Advanced
• Miscellaneous
• Fun manager
• Extra fun
• Local Options
Zone Alarm

Welcome
You're protected by ZoneAlarm!

Overview
No further setup is necessary — ZoneAlarm will alert you if you need to make any adjustments.
See how ZoneAlarm is protecting you by viewing the security statistics to the right.

Blocked Intrusions
53 Intrusions have been blocked since installation.
6 of those have been high rated.

Inbound Protection
The firewall has blocked 0 access attempts.

Outbound Protection
53 program(s) secured for Internet access.

Email Protection
MailSafe is currently active.
0 suspect email attachments quarantined.

Zone Alarm is by ZoneLabs and can be found at http://www.zonelabs.com/
<table>
<thead>
<tr>
<th>Keys</th>
<th>Validity</th>
<th>Trust</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ann Campi <a href="mailto:acampi@nai.com">acampi@nai.com</a></td>
<td></td>
<td></td>
<td>2048/1024</td>
<td>DH/DSS public</td>
</tr>
<tr>
<td>Bill Blanke <a href="mailto:wjb@pgp.com">wjb@pgp.com</a></td>
<td></td>
<td></td>
<td>4096/1024</td>
<td>DH/DSS public</td>
</tr>
<tr>
<td>Chanda Groom <a href="mailto:chanda_groom@nai.com">chanda_groom@nai.com</a></td>
<td></td>
<td></td>
<td>2048/1024</td>
<td>DH/DSS public</td>
</tr>
<tr>
<td>Damon Gallaty <a href="mailto:dgall@pgp.com">dgall@pgp.com</a></td>
<td></td>
<td></td>
<td>3072/1024</td>
<td>DH/DSS public</td>
</tr>
<tr>
<td>Jason Bobier <a href="mailto:jason@pgp.com">jason@pgp.com</a></td>
<td></td>
<td></td>
<td>2059/1024</td>
<td>DH/DSS public</td>
</tr>
<tr>
<td>Julien JAY <a href="mailto:JAY_Julien@wanadoo.fr">JAY_Julien@wanadoo.fr</a></td>
<td></td>
<td></td>
<td>2048/1024</td>
<td>DH/DSS key p.</td>
</tr>
<tr>
<td>Katherine Massucci Pettit <a href="mailto:kmp@pgp.com">kmp@pgp.com</a></td>
<td></td>
<td></td>
<td>2048/1024</td>
<td>DH/DSS public</td>
</tr>
<tr>
<td>Marc Duksterhouse <a href="mailto:marcd@pgp.com">marcd@pgp.com</a></td>
<td></td>
<td></td>
<td>2048/1024</td>
<td>DH/DSS public</td>
</tr>
</tbody>
</table>
Norton Antivirus by Symantec Corp can be found at http://www.symantec.com/
Example Redesigns

image: http://www.noderunner.net/~sparks/art/render/nasako-gym-anime.gif by Rachel Blackman, used with permission
Win Nuke V95

WinNuke V95
(c)1997 BurntBogus of the Den
Greets to Hound Dog

NUKE IP ADDRESS
127.0.0.1

NUKE WITH MESSAGE
Dies ist ein Test!

Exit
WinNuke 95 Redesign
GUI Bloopers by Jeff Johnson
The Design of Everyday Things by Donald Norman
The Humane Interface by Jef Raskin
Envisioning Information by Tufte
The Visual Display of Quantitative Information by Tufte
Visual Explanations by Tufte

See also the Tufte road show, details at www.edwardtufte.com
Web Pages That Suck by Flanders and Willis
Designing Web Usability & Homepage Usability by Nielsen (www.useit.com)
Non-Designers Design Book by Robin Williams
Designing the User Interface by Ben Shneiderman

Association for Computing Machinery
Special Interest Group for Computer Human Interaction (SIGCHI)
www.acm.org/sigchi
There are 10 types of people who understand interface design: those that do and those that don’t…

Your Questions???