Blindsided by Security
O hai there

- Britta
  - Adaptive technology consultant, RNZFB

- Solve hardware, software and information based technology issues

- Laura
  - Security Consultant, Lateral Security

- Web application penetration tester and former software developer
Disclaimer

• The examples and organisations referenced in this presentation are representative of the issues.
• This talk isn’t really about them though
• This isn’t a witch hunt – focus on the lessons not the companies.
Before we get into it, let’s sort out some foundations

INTERNET FOR THE BLIND 101
Blind people I work with

- Parkinsons, control of eyelids gone
- Victims of violent crime
- Cancer, optic nerves
- Autoimmune conditions affecting eyes
- Car accidents
- Hereditary and age related eye conditions
- Diabetes related vision loss
- ...

...
Technology Options

- Use screen reading and zooming software
  - Computers
  - Mobile Phones
  - Refreshable braille displays/notetakers
- Use keyboard, voice, gestures
- Don’t generally use a mouse
  audio mouse and screen coordinates tracking is available in some, not all, screen readers
Screen reading software

- **Linux**
  - ORCA, speakup, Adriane Knoppix with SBL, Vinux project...

- **Mac and iOS**
  - Voiceover (free) (iOS triple click Home, Mac Cmd+F5 on/off)

- **Windows**
  - NVDA (free, open source), JAWS, Window Eyes, System Access to Go, Supernova...

- **Android**
  - Talkback (free, open source), Mobile accessibility (paid)
Accessibility APIs

- Linux AT-SPI 2
- Windows/Linux IAccessible 2
- Windows MSAA
- **Windows UIA** (UIA on Linux, Mono accessibility project)
- Mac OS Ax/uiA
- iOS UIAccessibility Protocol Reference
- Android Accessibility API
- Java Access Bridge
Scripting Screen Readers

• Screen readers can be scripted
  – NVDA using Python
  – JAWS using Proprietary pseudo language, has a function library
  – Window Eyes using VBScript or Jscript
  – Supernova using Lua
  – Orca using Python

A Screen reader script, only fixes a Web issue locally
To fix a Web issue globally, access to HTML and addition of **ARIA roles, states, properties** needed
Something you know, Something you have, Something you are

MULTI FACTOR AUTHENTICATION
Hardware Tokens
User Response:

• “I have got around the problem and I have even owned up to the bank what I have done to circumvent it.”

• “Why they can't text me (like Fastnet Classic) I have no idea. Explaining why they can't, appears to be a security breach in itself.”

• “Yes, I have complained, so far to no avail.”
Solution: Multifactor Auth Hardware

- OCR cellphone app can be used, but ...

- Time factor 60 seconds
  - Need to detect numbers changing and signal user

- Control light conditions
Can’t be done on a PC, without vision:

- How many required letters, where in the word?
- Am I done entering required letters yet?
Solution: Kiwibank

KeepSafe Challenge

• Can be made useable – Demo

Attempt 1 of 3

Q: What did the Hedgehog say to the Pickle?

A

Attempt 1 of 3

Q

The Security question is: What did the Hedgehog say to the Pickle? There are 9 letters in your answer. The letter you currently have to input is at position 5. Tab to the letter and press enter, to input the required letter.

A
Solution: Kiwibank

KeepSafe Challenge

- Can be made useable:
  - Tell user what number letter in the word is currently required to be input
  - Tell user when they are finished
  - Tell user what to activate next, when finished
  - Ability to go back and correct mistakes
  - The help text does not have to appear visually

- Issues with my solution:
  Added Info = less secure app for the user?
Does this look suspicious to you?

VISUAL SECURITY CLUES
Web security Indicators

• “You’ll see that your address bar has turned green. This is called extended validation”
  
  BNZ

• “You'll also see the address bar is green when you visit our internet banking login page. We've done this to clearly show you're visiting Kiwibank's website, and not a fake.”
  
  Kiwibank

• “Ensure that there is a padlock symbol in the bottom right corner of your browser.”
  
  ANZ
Dividing man from machine, one auto generated image at a time

CAPTCHA
Web AIM screen reader user survey

May 2012

<table>
<thead>
<tr>
<th>Response</th>
<th># of Respondents</th>
<th>% of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very difficult</td>
<td>1179</td>
<td>69.1%</td>
</tr>
<tr>
<td>Somewhat difficult</td>
<td>367</td>
<td>21.5%</td>
</tr>
<tr>
<td>Not very difficult</td>
<td>71</td>
<td>4.2%</td>
</tr>
<tr>
<td>Not at all difficult</td>
<td>23</td>
<td>1.3%</td>
</tr>
<tr>
<td>I don't know</td>
<td>65</td>
<td>3.8%</td>
</tr>
</tbody>
</table>

90.6 % Find CAPTCHA difficult
CAPTCHA

Audio reCaptcha since June 2012

HACK A DAY

Stiltwalker beat audio reCAPTCHA
posted Jun 15th 2012 9:01am by Mike Szczys
filed under: security hacks

• Even our best, Human, RNZFB audio Captcha solver now has difficulties
Parliament

Make a Submission Webpage

Select committees
Make a submission

Companies and Limited Partnerships Amendment Bill

Public submissions are now being invited on the Companies and Limited Partnerships Amendment Bill. Submissions can be made by clicking on the link at the bottom of this page.

The closing date for submissions is Thursday, 6 September 2012

Verification

Make an online submission
CAPTCHA

Air New Zealand
Make a Bank transfer to pay for flights
But User already Logged In to Air NZ

Select your bank

Please enter the string of characters you see in the image above.
This is required to verify the authenticity of this request.

Total to pay: NZD $198.00

POLi

POLi is an online payment option you can use to safely pay for your flights directly from your bank account.
“My point to Air New Zealand however is that if you do identify yourself as a customer by logging in with your airpoints number and password, then at that point they do know who you are and there should be no CAPTCHA.”

“the only purpose of the CAPTCHA in that case is to save the time of a human who doesn't want to sift through bogus (Parliament) submissions. I think this is unreasonable”
Contributing to an electronics site:

Prove you are human by reading this resistor:

Match the sliders on the left to each color band on the resistor.

Click Here for a new resistor image.

New to electronics? Click here to learn how to read resistor values.

Submit Comment
Solution

Resistor CAPTCHA Demo

• Can be made useable:
  – Ability to sample colour of each resistor band
  – Ability to jump to sliders and emulate mouse
  – Tell user how many down arrows to press

• Issues with my solution:
  – Lot of instructions to listen to
  – Haven’t programmed ability to correct mistakes
Solution

Web Visum Text Captcha Cracking

- Firefox plugin
- Need invite or go through vetting process
- 10 Captcha a day limit
- Does reCAPTCHA well, averages 33 seconds to solve, 6 out of 28 wrong
Sometimes it takes the human touch

- CAPTCHA cracking services
- Pay humans to do it for you
- Cheap and fast
- Ethically dubious but effective
- May breach T&Cs
- If we are resorting to this – we have done something very wrong
Learning to stay safe online, one error message at a time

INSTRUCTIONS AND ERROR MESSAGES
Signalling a problem

- UI or Web app change
- Notifies screen reader
- Queries accessibility object to present to the user

Screen shots of some Silent Notifications

- avast! Information
- ESET Smart Security - Personal Firewall
- Attempt 2 of 3
  Q: Explain why Tuesdays are depressing?
  A: Whoops! Please use the onscreen keyboard below.
Web Security Advice

There’s a lot of good info out there

Secure Your Wireless
Simple steps to keep unwanted guests from using your bandwidth

Cyber crime cost New Zealanders an estimated

Ecommerce: buying securely online
Email security: phishing and spam
File sharing and downloading
Firewall basics
Installing and using security software
Getting rid of old technology
Network security and Wi-Fi
Online scams and hoaxes
Passwords: creating strong and unique passphrases
Recovery: backing up your data and devices
Smartphones and mobile internet
Updates: patching your operating system
Updates: using the latest software
... for Mouse users

- Home Internet User, Smartphone advice got to know the info is available, to Search for the text

- Mouseified Menus and Widgets can be activated by screen readers, but got to Know it’s a Menu not just a link, to action it - Chicken and Egg scenario.
Solution 1. CSS Hack

CSS Hack for screen readers

```css
.nav li ul {
    position: absolute;
    left: -999em;  // (before was display: none;)
    overflow: hidden;
}
.nav li:hover ul, .nav li:hover ul ul ul, .nav li:hover ul ul ul ul {
    display: none;
    overflow: hidden;
}
    left: auto;  // (before was display: block;)
    overflow: visible;
}
```
Solution 2. Less Hacky

Keyboard equivalent event handlers

• onmouseover also has onfocus
• onmouseout also has onfocusout/onblur
• deal with the onhover and onclick on non focusable elements
Solution 3. **ARIA**

- **ARIA**, for a web developer, means never having to say, “I’m sorry, but I don’t have time to study all those accessibility APIs”.

  ```html
  role="menuitem" aria-haspopup="true" aria-expanded="false"
  ```

  Browser interprets ARIA roles to Accessibility APIs for screen reader to consume properly

- **ARIA**, for a web developer, means having your current Web design cake, and screen readers being able to consume it, too.
Balancing requirements

SECURITY DESIGN CONSIDERATIONS
The Developer Challenge

Requirements

Resources
Security Product Decisions

When a Security Product is implemented:

100% useable by a certain type of user.

% useable for someone without vision.

Example – RNZFB new VPN app
Security Product Decisions

No keyboard access – hacky screen reader script.

```plaintext
Script RnzfbVPNAccess () ;Control+Alt+V
var
string sWindowName,
int iXCoord, int iYCoord, int iXOffset, int iYOffset, int iXVPNWindow, int iYVPNWindow

let sWindowName = GetWindowName (GetFocus())
if (sWindowName=="Shrew Soft VPN Access Manager")
;Get Coordinates of the Shrewsoft Window
   let iXVPNWindow=GetWindowLeft (GetFocus())
   let iYVPNWindow=GetWindowTop (GetFocus())
   SaveCursor()
   JAWSCursor()
;Add the never changing offset, for emulated mouse to jump on the RNZFB vpn connect button.
   let iXCoord=iXVPNWindow+25
   let iYCoord=iYVPNWindow+110
   MoveTo(iXCoord,iYCoord)
;Double Click the RNZFB vpn connect button
   LeftMouseButton()
   LeftMouseButton()
   RestoreCursor()
   SayString("Rnzfb Username and password required.")
else
   SayString("You are not focussed on the VPN Window.")
Endif
EndScript
```
Security Features

Chrome Multiprocess Browser

- Browser Process and Renderer Processes separate

Renderer processes have:
- the webpage DOM and accessibility info
- don’t interact directly with OS
- can’t send or receive events

= Screen reader can’t talk. “No UI”
Security Features

Chrome Multiprocess Browser

Solution 1 : Chrome Vox
• lots of support calls because ...
Default Chrome Vox navigation commands, Control+Alt+arrow keys, on Windows, Flips users Screens instead

Solution 2 : Security Feature limbo dance
• Chrome web browser handles comms between DOM and screen reader.
Summary

• Web applications can be challenging for those users with visual impairments.
• Simple implementation choices can make the difference between an inclusive and enjoyable and complete exclusion
• Catering to the needs of the blind however, need not be difficult, expensive or at the cost of innovation
Whitepaper

https://www.lateralsecurity.com/resources/presentations.html#BlindsidedbySecurity

Available as:

• PDF
• Screen Reader Friendly Word Document
Any Questions?