Security via User Interface Design & Single Login


WELCOME TO THE MISSILE LAUNCH WEB INTERFACE!
CLICK
ENTER THE TARGET'S COORDINATES.
TYPE TYPE
ENTER YOUR EMAIL ADDRESS FOR OUR RECORDS.
TYPE TYPE
ENTER YOUR EMAIL AGAIN, TO ENSURE YOU TYPED IT CORRECTLY.

Single Login

- A single login, or single sin-on (SSO) is a method of access control that enables a user to authenticate against many systems with one login activity.
- Used to counter password fatigue (PostIts) http://en.wikipedia.org/wiki/Password_fatigue

Implementations of SSO

- LDAP (Lightweight Directory Access Protocol) http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
- Kerberos – network authentication protocol as well as an application suite http://en.wikipedia.org/wiki/Kerberos_protocol
- Windows Live ID – sites that use it are Hotmail, MSNBC, MSN, and other Microsoft sites http://en.wikipedia.org/wiki/Microsoft_account
- Google and its various services
- Client password management tools – iMacros for Firefox

Web Implementations of SSO

- As web sites and servers tend to be too varied for any one system, a web implementation of SSO becomes tricky
- One solution is to use sessions and cookies
  - Sessions are easier to manage programmatically
  - Cookies can be a challenge – domain specific
- Oauth – Open standard for authorizaion. More of an app solution than a web solution, but can be part of a web server solution. Problems within the project and the standards, but seems well used. http://en.wikipedia.org/wiki/OAuth

Security will sometimes fail

- If users need to select the security option as part of application use
- When users need to determine which encryption keys as part of a communication sequence
- Accidental configure access control systems and make their private data world readable

Non-interface solutions have limited success

- Hackers often don’t care about legal consequences; may be beyond reciprocity
  - Users may not have legal resources to go after hackers
  - Users may not be aware attack took place
- Training is always going to fail for some users
- Automation will help, but must be augmented with proper user interface design

Introduced Vulnerabilities

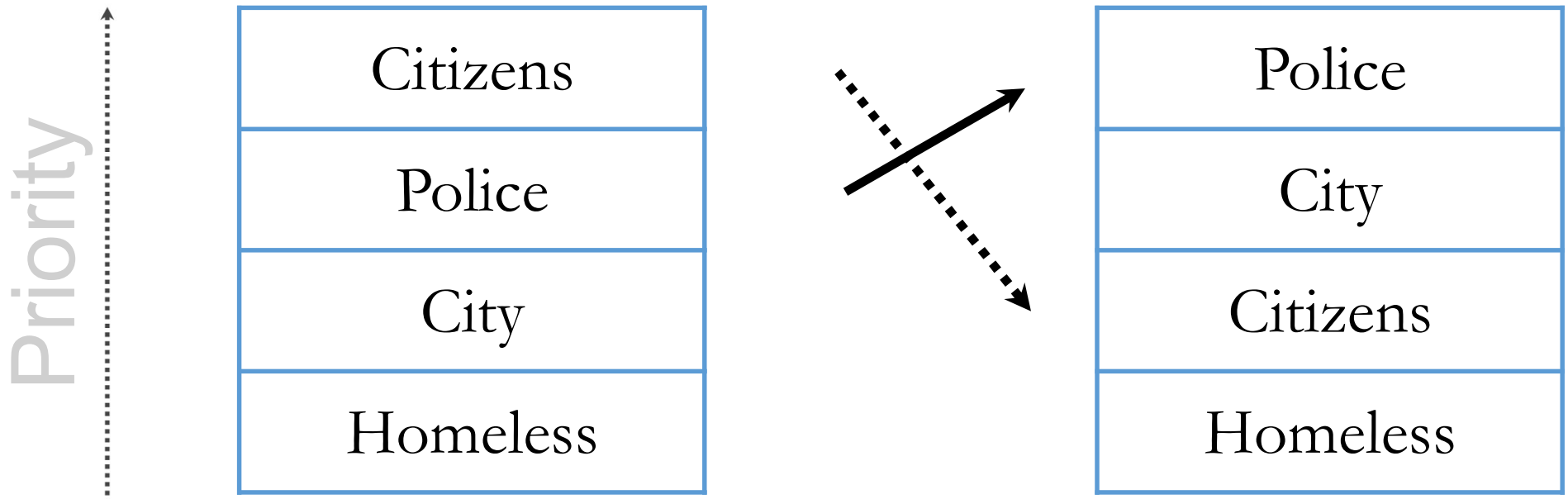
- JQuery tools can introduce vulnerabilities when not properly implemented
  - FOSS projects based on JQuery can introduce vulnerabilities as well
  - Mostly XSS and XSRF, but others as well
  - As a sample: https://www.cvedetails.com/vulnerability-list/vendor_id-6538/Jquery.html

Other libraries

- Most JS libraries/UI frameworks have vulnerabilities, check vulnerability search engines for yours, and subscribe to mailing lists.
  - Test using pentesting tools, sqlmap, w3af, etc
- Building your own might not be any better, so look for mature frameworks and subscribe to security mailinglists

Design Considerations

Design Considerations



Design

- “Design is not just what it looks like and feels like. Design is how it works.”

Steven Jobs

Design Issues as Bugs

- If it impacts how your users use the application, it follows that usability issues and interface design issues should be considered bugs
- Treat them as bugs; track them in your bug tracking system
  - Get input from your users; don't just ask about software failures, talk about interface failures as well
  - Prototype interface very early on

Prototyping Interface Layouts

- Stick figures
  - Draw body first
  - Draw head
  - Draw face
  - Draw legs
  - Draw arms

Prototyping interface design (cont)

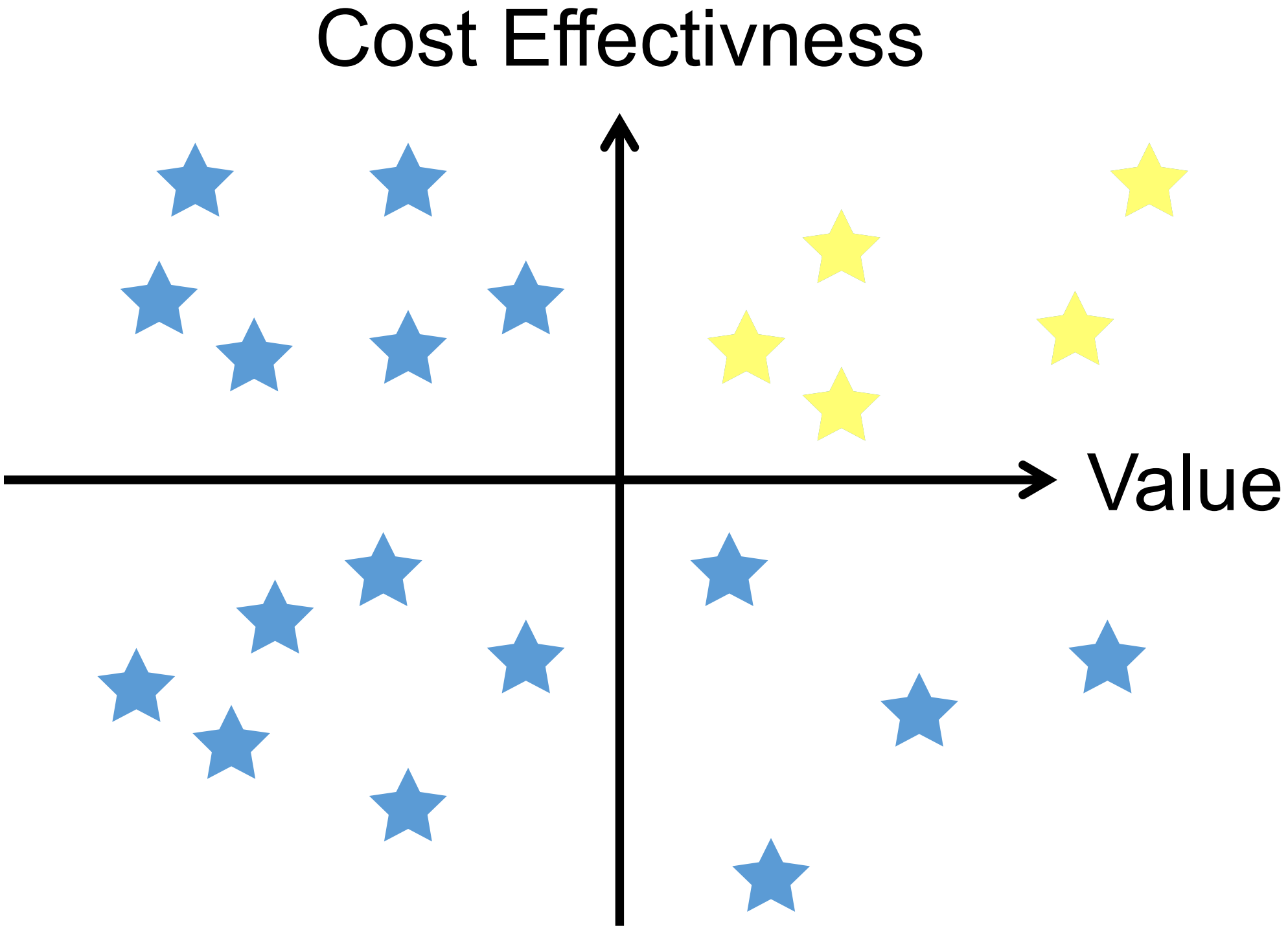
- Vet prototypes through users/potential users
- Consider showing users paper mock ups rather than highly detailed electronic versions
  - Users tend to be reluctant to criticize something that a lot of work has gone into
  - Consider prototyping interface design using layout tools until you have the interface you want, and then draw it out to vet to your users
  - Consider explaining that the layout is very easily changed.

Design Iteratively

Observe

Design

Analyze


Cost Effectivness
Value

Research design elements

- Yahoo developer network user interface library (YUI) http://yuilibrary.com/
  - Very good resource for design elements and ideas. **Unfortunately discontinued**.
- Web Analytics
  - http://en.wikipedia.org/wiki/Web_analytics
- Jquery
  - http://jquery.com/
- Wikipedia article on JS Frameworks/Libraries:
  - https://en.wikipedia.org/wiki/Comparison_of_JavaScript_frameworks