Why Johnny Can't Blow the Whistle:

Identifying and Reducing Usability Issues in Anonymity Systems

Greg Norcie
Jim Blythe
Kelly Caine
L Jean Camp

February 23rd, 2014, NDSS Workshop on Usable Security

Outline

- Tor
  - What is Tor?
  - What is the Tor Browser Bundle (TBB)?
  - Why usability is important for the TBB?
- Study 1: Identifying usability issues
- Study 2: Reducing usability issues
- Discussion of results
- Conclusions / Future work

Q: What is Tor and how does it work?

- Anonymity service utilizing onion routing technology
- 3 hops between Alice and Bob per circuit
- Encrypted in transit, but enters/exits in plaintext.

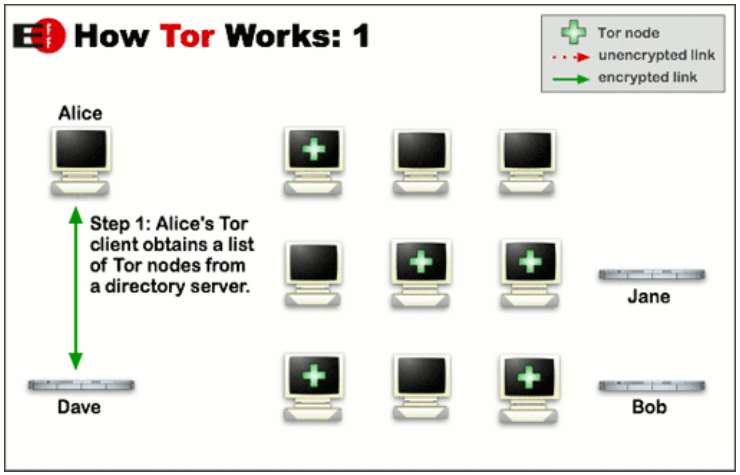


Illustration courtesy Tor Project.org

Q: What is Tor and how does it work?

- Anonymity service utilizing onion routing technology
- 3 hops between Alice and Bob per circuit
- Encrypted in transit, but enters/exits in plaintext.

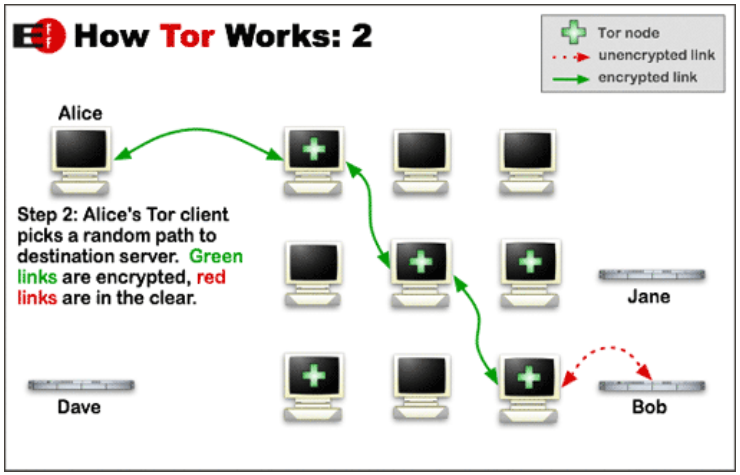


Illustration courtesy Tor Project.org

Q: What is Tor and how does it work?

- Anonymity service utilizing onion routing technology
- 3 hops between Alice and Bob per circuit
- Encrypted in transit, but enters/exits in plaintext.

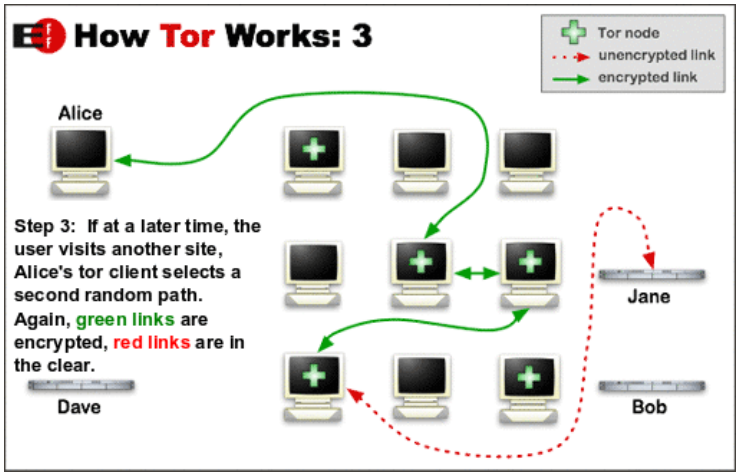


Illustration courtesy Tor Project.org

Q: What is the Tor Browser Bundle?

- TBB presented previously disparate tools in one simple GUI.
  - Firefox (browser) + Vidalia (Proxy managment) + Tor
- Additional security features/changes to system defaults to prevent information leakage.
  - Redirecting to DuckDuckGo
  - NoScript blocks certain attacks
  - No Flash
- As of TBB 3.0, Vidalia has been dropped
  - See **http://tinyurl.com/noVidalia**

** https://blog.torproject.org/blog/announcing-tor-browser-bundle-30alpha1*

Q: Why a Browser Bundle?

- Integrated solutions tend to be more usable. [1]
- TBB presents previously disparate, command line tools in one relatively simple GUI.
- Additional security features/changes to system defaults to prevent information leakage in usable manner.
  - Too many settings to toggle manually

[1] J. Clark, P. Van Oorschot, and C. Adams. Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability. In Proceedings of the 3rd Symposium on Usable Privacy and Security, pages 41–51. ACM, 2007.

Q: Why does usability matter?

- "Anonymity Loves Company"[1]
- More users = higher anonymity
- Thus, increasing # of users increases anonymity
- Thus, increasing usability increases anonymity.

[1] R. Dingledine and N. Mathewson. Anonymity Loves Company: Usability and the Network Effect. In Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006), Cambridge, UK, June, 2006.

Study 1 Goals:

- Improve TBB usability – find specific solutions
- Derive general design heuristics

Laboratory Think Aloud Study

- 25 students downloaded, installed Tor Browser Bundle **2.2.35-7.1** for Windows

  -22/25 male, 20/25 in 18-25 bracket
- Instructed to write down any “stop points” as they occur + prompted afterwards to elaborate on their exit survey.
- Responses used to create a list of specific usability issues (and solutions)
- From specific issues, derives general heuristics

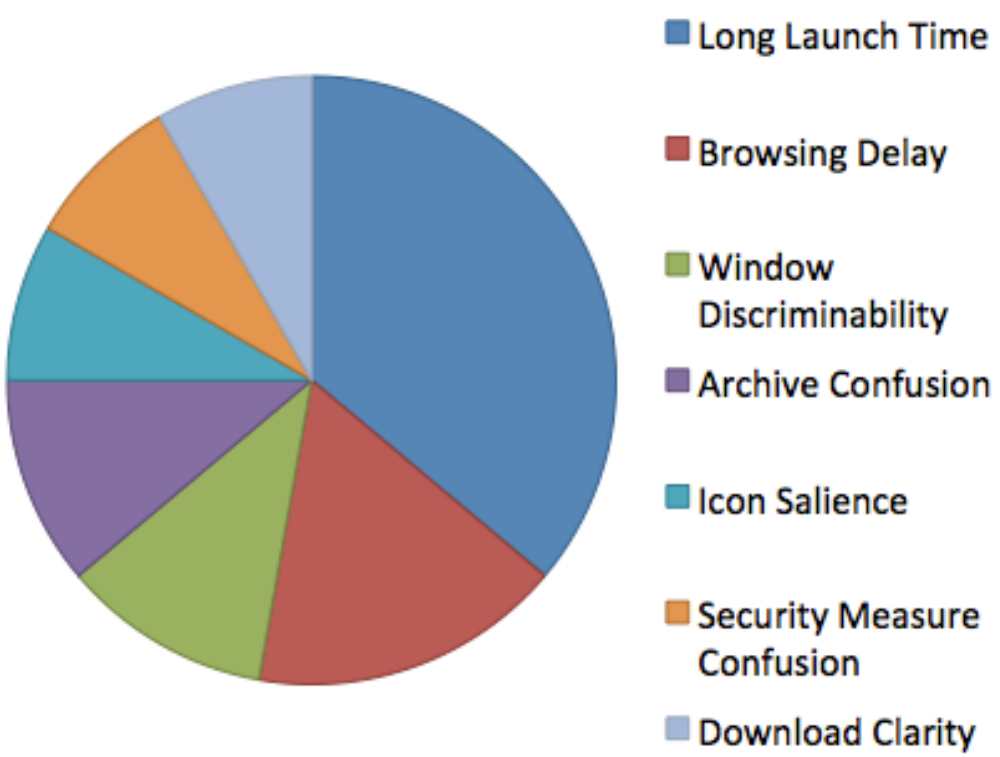
Analysis Process

1. Sort free responses into individual issues.
2. Generate list of mutually exclusive categories.
3. Two coders independently categorize.[1]
4. Derive set of Tor specific Issues.
5. Derive set of general heuristics.

[1] J. L. Fleiss and J. Cohen. The Equivalence of Weighted Kappa and the Intraclass Correlation Coefficient as Measures of Reliability. Educational and Psychological Measurement, 33(3):613–619, 1973.

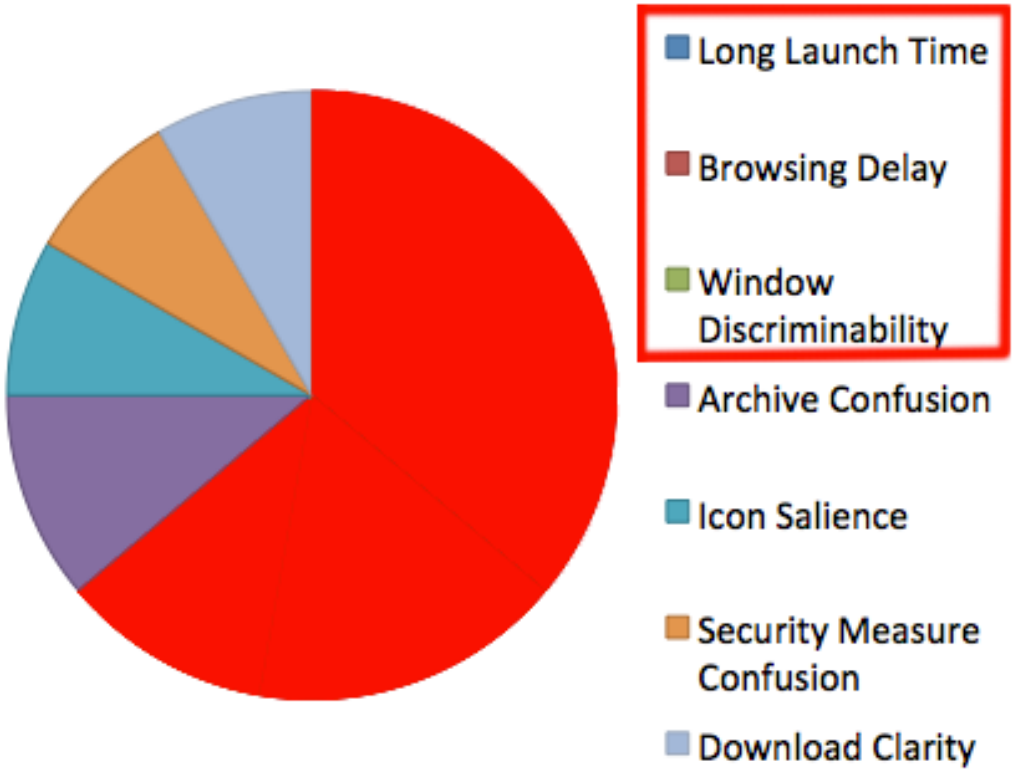
Initial Results - Categories

Category	N	%
Long Launch Time	13	40.6
Browsing Delay	6	18.8
Window Discriminability	4	12.5
Archive Confusion	4	12.5
Icon Salience	3	9.4
Security Measure Confusion	3	9.4
Download Clarity	3	9.4
TOTAL	36	



Initial Results - Categories

Category	N	%
Long Launch Time	13	40.6
Browsing Delay	6	18.8
Window Discriminability	4	12.5
Archive Confusion	4	12.5
Icon Salience	3	9.4
Security Measure Confusion	3	9.4
Download Clarity	3	9.4
TOTAL	36	

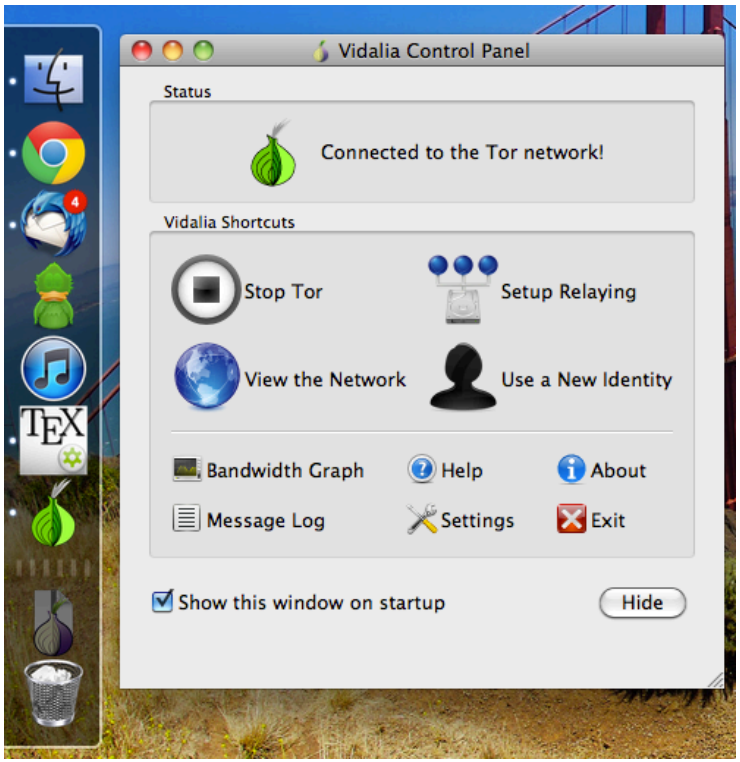


Discussion of Study 1 results

- We found that “long launch time”, “window discriminability”, and “browsing delay” made up a majority (**56%) of reported issues**.
- Moving on we will spend a few slides detailing these issues
  - (along with out proposed solutions)
- For discussion of other issues, see full paper.

Issue: Long Launch Time

- *"The user noticed a lag between clicking the icon to start the Tor Browser Bundle, and the TBB window opening."*
- Proposed Solution: Alter Vidalia so lag between two is shorter



Issue: Window Discriminability

- *"User wasn't sure which window was TBB and which was a normal browser."*
- Solution 1: Custom logo.
- Solution 2: Alter Firefox chrome via theme
- (Solution 2 later scrapped per Roger's suggestion since it could out users)

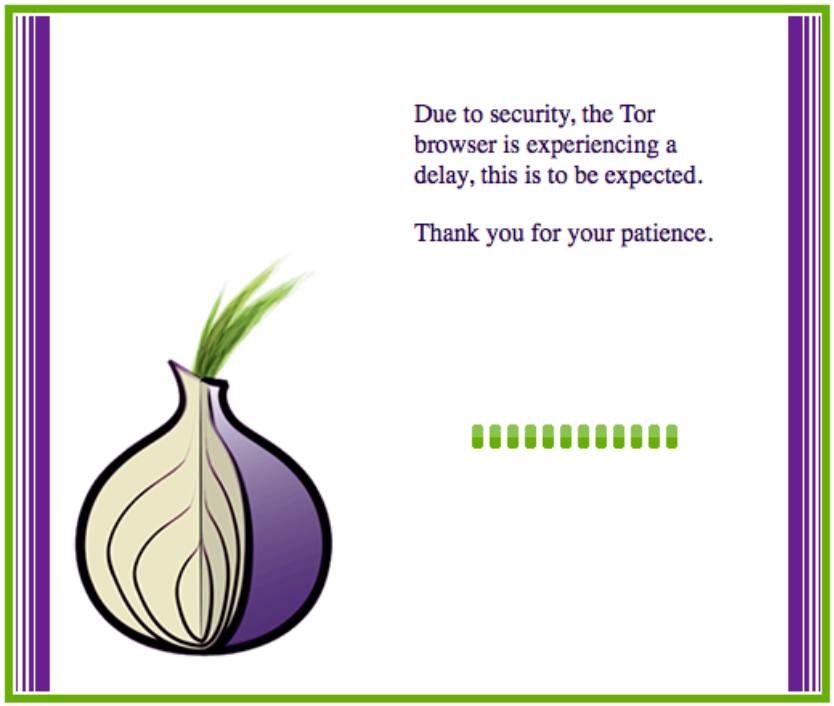
Issue: Browsing Delay

- *"Browsing through the TBB had a noticable lag."*
- Since security is a primary task, TBB users may be willing to tolerate latency if informed
- Ex: Users in coffeeshops don't expect the same speeds as at home.
- Explain to users that delays are normal, and they can adjust expectations.

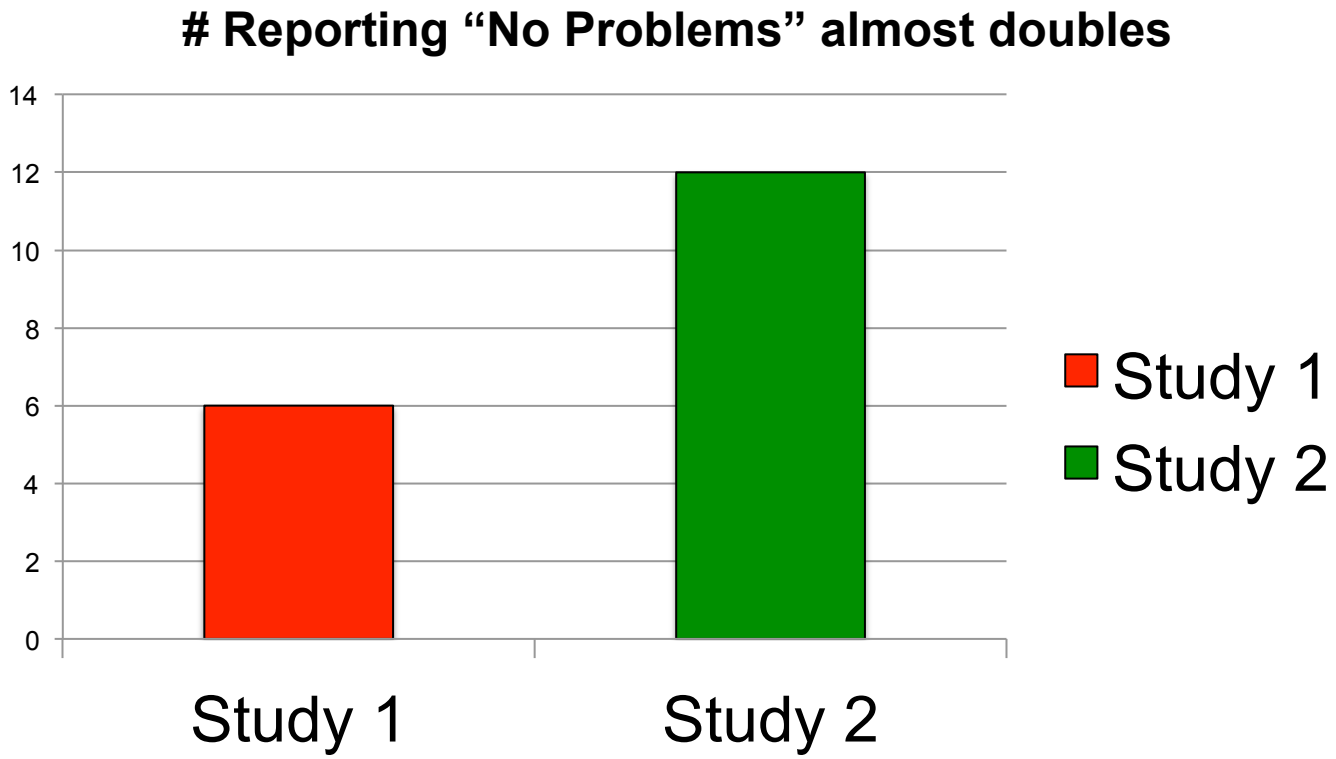
  -Perhaps via message in installer

Changes made for 2nd Study

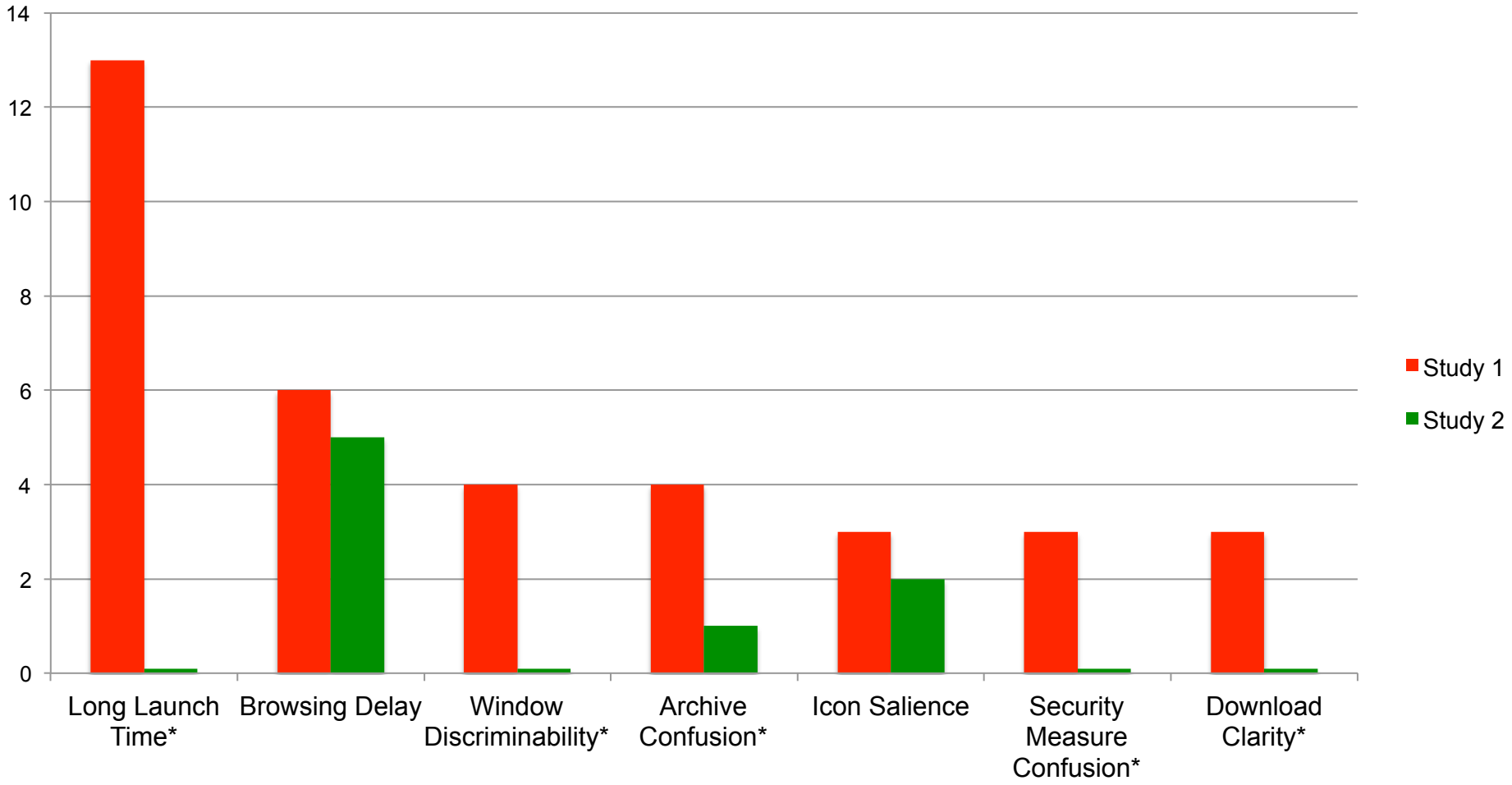
- TBB now has it's own custom icon
- Lag between Vidalia launch and TBB opening has been greatly reduced
- Custom coded extension warns users that delays are to be expected when lag >10s occurs



Results of Changes – Big Picture



Results of Changes – Detailed Look



Summary of change results:

- Long Launch Time, Window Discriminability dramatically reduced reduced ($p < .001$)
- Browsing delay reduced 5% (From 24% to 19%) but this was not statistically significant
- Usability issues in extension could have hampered experiment.
  - 44% of users complained about excessive popups

Heuristics for anonymity systems

1. Installation precedes operation.
2. Ensure users are aware of trade offs.
3. Say why, not how.

Installation Precedes Operation

- Again, anonymity loves company.
- If the user gets confused during installation, then the usability of our user interface is irrelevant.
- We can’t control the OS, but we can make our download page and installer as clear as possible.

Say Why, Not How

- Explain why a security measure was taken.
- Provide jargon free explanations
- Allow experts to drill down to detailed information

Ensure Users are Aware of Trade Offs

- User's expectations are a bigger issue than Tor's speed
  - Most users don't try to watch Netflix at an internet café
- When using Tor, security is a primary task
- Set reasonable expectations, users will be happy.

Summary

- Contributions
  - Described a set of specific Tor issues
  - Described design heuristics for all 1/N anonymity systems
- Potential future work
  - Determine best parameters for Delay Detector – how long is too long?
  - Focus more on how to design warnings in browser (Ex: unencrypted warning)

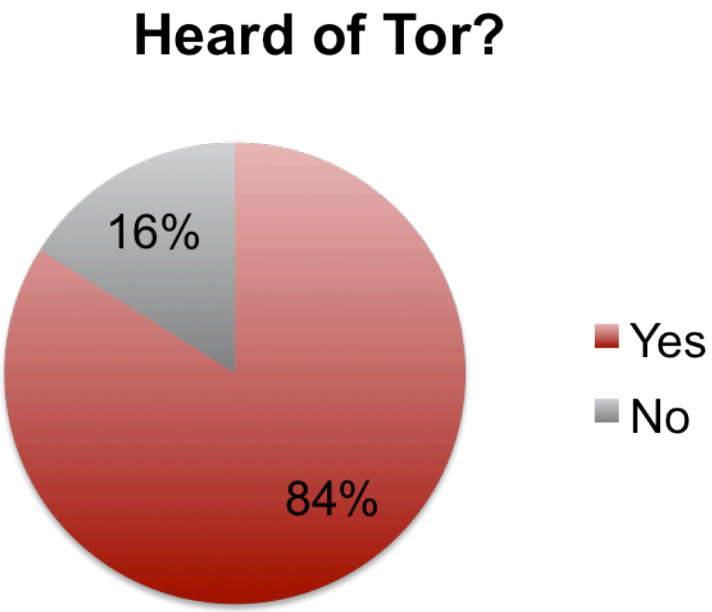
Acknowledgements:

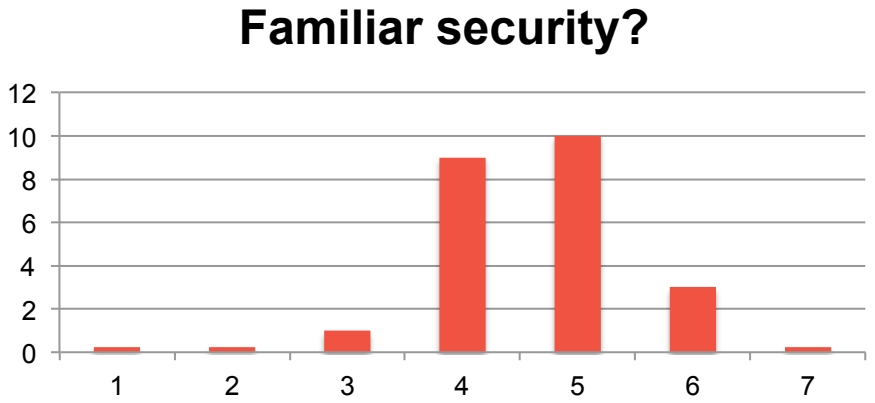
- Coauthors
- Reviewers
- Department of Homeland Security under contract number N66001-12-C-0137
- Also many thanks to the Tor Project, including (but not limited to):
  - Roger Dingledine
  - Mike Perry
  - Tom Lowenthal

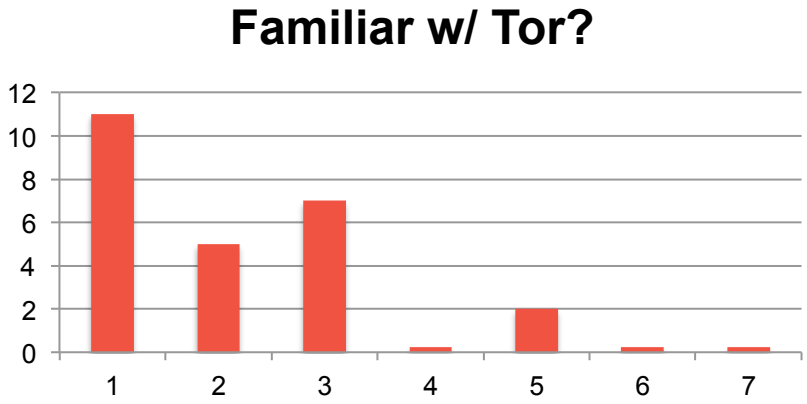
Results of Changes

Category	Exp 1 N	Exp 1 %	Exp 2 N	Exp 2 %
No problems*	**6**	**24%**	**12**	**44.4%**
Long Launch Time*	13	40.6%	0	0%
Browsing Delay	6	18.8%	5	18.5%
Window Discriminability*	4	12.5%	0	0%
Archive Confusion*	4	12.5%	1	3.7%
Icon Salience	3	9.4%	2	7.4%
Security Measure Confusion*	3	9.4%	0	0%
Download Clarity*	3	9.4%	0	0%
Popup Peeves	N/A	N/A	12	44%

Methodology – Participant Characteristics







“But can’t the NSA break Tor?!”

- “Tor Stinks” - internal NSA presentation
  - *“We will never be able to de-anonymize all Tor users all the time…”*
  - *“…with manual analysis we can de-anonymize a very small fraction of Tor users”*
- http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption