Anonymity, Usability, and Humans. Pick Two.

Runa A. Sandvik
runa@torproject.org

20 September 2011
About Runa

- Studied at the Norwegian University of Science and Technology
- Worked for the Tor Project during Google Summer of Code in 2009
- Developer, security researcher, translation coordinator
What are we talking about?

- Crash course on anonymous communications
- Quick overview of Tor
- Usability, Security, and Humans
501(c)(3) non-profit organization dedicated to the research and development of technologies for online anonymity and privacy
What is anonymity?
Anonymity isn’t cryptography

- Cryptography protects the contents in transit
- You still know who is talking to whom, how often, and how much data is sent.
Anonymity isn’t steganography

Attacker can tell Alice is talking to someone, how often, and how much data is sent.
Anonymity isn’t just wishful thinking...

- "You can’t prove it was me!"
Anonymity isn’t just wishful thinking...

- ”You can’t prove it was me!”
- ”Promise you won’t look”
Anonymity isn’t just wishful thinking...

- "You can’t prove it was me!"
- "Promise you won’t look"
- "Promise you won’t remember"
Anonymity isn’t just wishful thinking...

- "You can’t prove it was me!"
- "Promise you won’t look"
- "Promise you won’t remember"
- "Promise you won’t tell"
Anonymity isn’t just wishful thinking...

- "You can’t prove it was me!"
- "Promise you won’t look"
- "Promise you won’t remember"
- "Promise you won’t tell"
- "I didn’t write my name on it!"
Anonymity isn’t just wishful thinking...

- ”You can’t prove it was me!”
- ”Promise you won’t look”
- ”Promise you won’t remember”
- ”Promise you won’t tell”
- ”I didn’t write my name on it!”
- ”Isn’t the Internet already anonymous?”
..since “weak” isn’t anonymity.

• “You can’t prove it was me!” Proof is a very strong word. Statistical analysis allows suspicion to become certainty.
..since "weak" isn’t anonymity.

- "Promise you won’t look/remember/tell" Will other parties have the abilities and incentives to keep these promises?
..since "weak" isn’t anonymity.

- "I didn’t write my name on it!” Not what we’re talking about.
..since "weak" isn't anonymity.

- "Isn't the Internet already anonymous?" Nope!
Anonymous communication

- People have to hide in a crowd of other people (“anonymity loves company”)
- The goal of the system is to make all users look as similar as possible, to give a bigger crowd
- Hide who is communicating with whom
- Layered encryption and random delays hide correlation between input traffic and output traffic
What is Tor?

- Online anonymity software and network
What is Tor?

- Online anonymity software and network
- Open source, freely available (3-clause BSD license)
What is Tor?

- Online anonymity software and network
- Open source, freely available (3-clause BSD license)
- Active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech

Anonymity, Usability, and Humans. Pick Two. 20 September 2011 11 / 26
What is Tor?

- Online anonymity software and network
- Open source, freely available (3-clause BSD license)
- Active research environment:
  Rice, UMN, NSF, NRL, Drexel, Waterloo, Cambridge UK, Bamberg Germany, Boston Univ, Harvard, MIT, RPI, Georgia Tech
- Increasingly diverse toolset:
  Tor, Torbutton, Tor Browser Bundle, TAILS Anonymous Operating System, Tor Weather, GetTor, Thandy, Orbot, Tor Check, Arm, Torouter, Tor Cloud and more
What makes Tor different, part 1
What makes Tor different, part 1
What makes Tor different, part 1
What makes Tor different, part 2

How Tor Works: 1

Step 1: Alice’s Tor client obtains a list of Tor nodes from a directory server.

Alice

Dave

Jane

Bob

Tor node

unencrypted link

encrypted link
What makes Tor different, part 2

Step 2: Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.
Step 3: If at a later time, the user visits another site, Alice’s tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Bridges versus relays

- A step forward in the blocking resistance race
- Bridge relays (or ”bridges” for short) are Tor relays that aren’t listed in the main Tor directory
- To use a bridge, you will need to locate one first (can be done using bridges.torproject.org, email, social media etc)
- A bridge will act as the first hop in the circuit
Hidden services

- Tor makes it possible for users to hide their locations while offering various kinds of services, such as a website or an IM server.
- Using Tor’s rendezvous points, other Tor users can connect to these hidden services, each without knowing the other’s network identity.
- A hidden service will have an address that ends in .onion, e.g. http://duskgytldkxiuqc6.onion/
Who uses Tor?

- Normal people
- Law Enforcement
- Human Rights Activists
- Business Execs
- Militaries
- Abuse Victims
estimated 300k to 800k daily users
How many people use Tor daily?

Directly connecting users from all countries

The Tor Project - https://metrics.torproject.org/
Tor users in China

Directly connecting users from China

The Tor Project - https://metrics.torproject.org/
Tor users in China

Bridge users from China

The Tor Project - https://metrics.torproject.org/
Tor users in Egypt

Directly connecting users from Egypt

The Tor Project - https://metrics.torproject.org/
Tor users in Egypt

Bridge users from Egypt

The Tor Project - https://metrics.torproject.org/
Tor users in Iran

Directly connecting users from the Islamic Republic of Iran

The Tor Project - https://metrics.torproject.org/
Tor users in Iran

Bridge users from the Islamic Republic of Iran

The Tor Project - https://metrics.torproject.org/
Anonymity, Usability, and Humans

- Allow the user to fully configure Tor rather than manually searching for and opening text files.
- Let users learn about the current state of their Tor connection, and configure or find out whether any of their applications are using it.
- Make alerts and error conditions visible to the user.
- Run on Windows, Linux, and OS X, on a normal consumer-level machine.
Time for a demo

Demonstration of Tor Browser Bundle
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- The quality of translations can vary.
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- The quality of translations can vary.
- Concepts of anonymity and its threats escape most users.
  "I want my Youtube!" "I use tor to organize on facebook."

Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.

Software leaks data all over the place. Stopping these leaks leads to unexpected user experiences.

Five years since we last dabbled in Usability.
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- The quality of translations can vary.
- Concepts of anonymity and its threats escape most users. "I want my Youtube!" "I use tor to organize on facebook."
- Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- The quality of translations can vary.
- Concepts of anonymity and its threats escape most users.
  "I want my Youtube!" "I use tor to organize on facebook."
- Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.
- Software leaks data all over the place. Stopping these leaks leads to unexpected user experiences.
Experience so far

- Our web site is confusing to users and not technical enough for researchers.
- The quality of translations can vary.
- Concepts of anonymity and its threats escape most users. “I want my Youtube!” ”I use tor to organize on facebook.”
- Cultural differences and their expectations of software, usability, anonymity, privacy, and what tor provides.
- Software leaks data all over the place. Stopping these leaks leads to unexpected user experiences.
- Five years since we last dabbled in Usability.
Next steps and how you can help

- Test software.
- Provide feedback and suggest improvements.
- Help with development.
- Visit https://www.torproject.org/ for more information, links, and ideas.
who uses tor?
http://www.flickr.com/photos/mattw/2336507468/sizes/l/, Matt Westervelt, CC-BY-SA.