Class 16 – Internet Part 2

You can get your midterm before class if you want
Notes

• Office hours are back in EPS 348
  • Door is sometimes locked, if so, just knock (loudly) or email me

• Rough Draft Due next Thursday
  • I just need to see evidence you have been working on it.

• Recitations (Today)
  • Hands on: here – Overview of software development strategies (i.e. how teams of software engineers work together. Waterfall development vs Agile methods.
  • Discussion: Roberts 412
60 minute segment on Dark Web

https://www.youtube.com/watch?v=ONMwumOgagw
Deep Web vs Dark Web

• What is the difference?
Deep Web

- Not indexed by main search engines like Google, Bing, Yahoo, etc.
- 96% of the internet is estimated to be “deep web”.
- More than half of Deep Web content resides in topic-specific databases, such as
  - National Climatic Data Centre,
  - NASA EOSDIS
  - the National Oceanographic Data Centre,
  - etc.

Dark Web

• Collection of thousands of websites that use anonymity tools like Tor and I2P to hide their IP address (http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/)

• In other words, you need special software to access it

• ~.01% of the web

• **Uses include (but are not limited to)**
  • drugs, weapons, counterfeit documents and child pornography
  • WikiLeaks
  • Even Facebook has a dark web version for those who are on the dark web because they are concerned about
Deep Web
https://www.ted.com/talks/jamie_bartlett_how_the_mysterious_dark_net_is_going_mainstream
Silk Road

• February 2011 - launched by Ross William Ulbricht under charges of being the site's pseudonymous founder "Dread Pirate Roberts"
• October 2013 - Shut down in 2013 by FBI
• November 2013 - Silk Road 2.0 re-launched by former site’s admin
• November 2014 – Shut down by an international law enforcement operation targeting dark net and tor browsing activities called Operation Onymous
• January 2015 – Silk Road 3 Reloaded launched by Diabolus Market – a competitor trying to capitalize on the name
Tor and Tor Browser

• Came from a US Navel Research Lab project called *The Onion Router*
• “Onion” refers to the multiple layers of encryption
• Electronic Freedom Foundation (EFF) started funding the project in 2004, after the project was released and made open source

• [https://www.torproject.org/about/overview](https://www.torproject.org/about/overview)
Tor and Tor Browser

How Tor Works: 1

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

How Tor Works: 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**.
Tor and Tor Browser

• You can download the Tor Browser to start perusing the dark net: https://www.torproject.org/projects/torbrowser.html.en
• Built on top of Firefox
Tor and Linux Distro

• Next Level: Linux TAILS distro, everything is built around privacy
• Bootable USB (or disk or what have you) that does not leave a trace on the machine
• All communications MUST go through Tor
• Non-anonymous communications are blocked
• Utilizes virtual keyboard to block key loggers
Before you start your illegal paper writing scheme

• To get to a website, you must exit the Tor Network, and this exit node may be monitored and your traffic may be tracked
• 2007 a Security Researcher was able to retrieve passwords and emails from an exit node (because they were unencrypted)
• Exit nodes are also susceptible to man-in-the-middle attacks
• Plugins can leak your IP (this includes bitTorrent)
• NSA and other agencies target Tor, with some success.
• Tor users have more than doubled since Snowden, the volunteer relay nodes have not
Speaking of Snowden

Some files released relate to Tor

Slides entitled “Tor Stinks” and some excerpts:
"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,"

In a different top-secret presentation: "the king of high-secure, low-latency internet anonymity".
Questions Closing Remarks?

• **Recitations (Today)**
  • **Hands on:** here – Overview of software development strategies (i.e. how teams of software engineers work together. Waterfall development vs Agile methods.
  • **Discussion:** Roberts 412