How to do Research

This is as much discussion as presentation so please interrupt!
Roadmap

Choosing and Refining Ideas
Finding/Reading Academic Papers
Project Scale and Prior Work
Collaboration
Please don’t make us go to court
Meet with staff next week
Choosing Project Ideas

- What do you ❤️?
  - Hobbies? Your favorite class?
  - Security is *everywhere*
Choosing Project Ideas

- What do you love?  
  - Hobbies? Your favorite class?  
  - Security is everywhere

- What do you use?  
  - Do you understand how the devices around you work?  
    - How does your computer know what time it is?  
    - Caller ID???
    - The unlock button on a car remote?
Choosing Project Ideas

● What do you ♥️?
  ○ Hobbies? Your favorite class?
  ○ Security is *everywhere*

● What do you use?
  ○ Do you understand how the devices around you work?
    ■ How does your computer know what time it is?
    ■ Caller ID???
    ■ The unlock button on a car remote?

● What is exciting?
  ○ If you aren’t excited about your project, no one else will be either
Choosing Project Ideas

● What do you ❤️?
  ○ Hobbies? Your favorite class?
  ○ Security is everywhere

● What do you use?
  ○ Do you understand how the devices around you work?
    ■ How does your computer know what time it is?
    ■ Caller ID???
    ■ The unlock button on a car remote?

● What is exciting?
  ○ If you aren’t excited about your project, no one else will be either

● Do you enjoy the type of work you’re about to sign up for?
  ○ When you consider a topic, think about how you’ll reach your result, not just about the result itself! Programming? Reverse engineering?
Refining your Topic

What problem are you solving?

Why is this an important problem?

What other work exists in the area?

What are the limitations of your approach?
How to Find Papers

scholar.google.com
How to Find Papers

Google Scholar

anonymous communication

Articles   Case law
How to Find Papers

Cited by

- Generally corresponds to “influence”
- Look at works citing a paper to find similar followup works!
An anonymous communication technique using dummies for location-based services
H Kido, Y Yanagisawa, T Satoh - ICPS'05, Proceedings ..., 2005 - ieeexplore.ieee.org

A protocol for anonymous communication over the internet
C Shields, B.N. Loving - Proceedings of the 7th ACM Conference on ..., 2000 - dl.acm.org

A survey of anonymous communication channels
G Danezis, C Diaz - 2008 - hostmaster.freehaven.net

P5: A protocol for scalable anonymous communication
R Sherwood, B Bhattacharjee - Journal of Computer ..., 2005 - content.iospress.com
A protocol for anonymous communication over the internet

Anonymous usage of location-based services through spatial and temporal cloaking
M Gruteser, D Grunwald - ... of the 1st international conference on Mobile ..., 2003 - dl.acm.org
Advances in sensing and tracking technology enable location-based applications but they also create significant privacy risks. Anonymity can provide a high degree of privacy, save service users from dealing with service providers' privacy policies, and reduce the service ...

Peer-to-peer computing
DS Milojcic, Y Kalogeraki, R Lukose, K Nagaraja... - 2002 - cs.kau.se
The term "peer-to-peer"(P2P) refers to a class of systems and applications that employ distributed resources to perform a function in a decentralized manner. With the pervasive deployment of computers, P2P is increasingly receiving attention in research, product ...

ANORD: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks
J Kong, X Hong - Proceedings of the 4th ACM international symposium ..., 2003 - dl.acm.org
In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a ...

Statistical identification of encrypted web browsing traffic
Q Sun, DR Simon, YM Wang, W Russell... - ... IEEE Symposium on ..., 2002 - ieeexplore.ieee.org
Encryption is often proposed as a tool for protecting the privacy of World Wide Web browsing. However, encryption-particularly as typically implemented in, or in concert with popular Web browsers-does not hide all information about the encrypted plaintext ...
How to Find Papers

Year

- Old =/= bad, but newer papers will give a better view of the current state of the area
- It can be helpful to start with new and work back
Privacy-aware secure anonymous communication protocol in CPSS cloud computing
F Li, C Cui, D Wang, Z Liu, N Eminrah, Y Wang... - IEEE, 2020 - ieeexplore.ieee.org
This mechanism achieves a novel anonymous communication protocol to protect the identity... an anonymous communication link establishment method and an anonymous communication... to anonymous communication packet encapsulation format and anonymous communication...

Anonymous communication via anonymous identity-based encryption and its application in IoT
L Jiang, T Li, X Li, M Atiquzzaman, H Ahmed... - Mobile Computing, 2018 - hindawi.com
To solve this problem, we propose an anonymous communication system based on anonymous IBE. Our scheme has significant advantage in efficiency compared with previous work and can also offer strong anonymity. In the future, we will consider the user...

On privacy notions in anonymous communication
C Kuhn, M Beck, S Schiffer, E Jorswieck... - Proceedings on Privacy,... - 2019 - sciendo.com
On Privacy Notions in Anonymous Communication Abstract: Many anonymous communication networks (ACNs) with different privacy goals ... To protect metadata from state and industrial surveillance, a broad variety of anonymous communication networks (ACNs) has emerged;...
How to Find Papers

Conference tier

- Top tier conferences are pickier about what they accept
  - USENIX, S&P, CCS, NDSS, RWC
  - Crypto, TCC, EUROCRYPT
  - OSDI, SOSP, NSDI
An anonymous communication technique using dummies for location-based services

... We propose a new anonymous communication technique to protect the location privacy of people using LBSS. In our proposed technique, a user sends true position data. To apply our anonymous communication technique in LBSS, we discuss the following two important issues:...

A protocol for anonymous communication over the internet
C Shields, B.N Levine - Proceedings of the 7th ACM Conference on ..., 2000 - dl.acm.org

... In this paper, we present a new protocol for providing anonymous communication on the Internet. Hordes achieves these reductions by making use of multicast communication, and is the first method of comparing the anonymity provided by anonymous protocols. In Section 4, we ...

A survey of anonymous communication channels
G Danezis, C Diaz - 2008 - hostmaster.freehaven.net

... anonymous communication systems. In this survey we look at the definition of anonymous communications and the major anonymous communication protocols. Data communication networks use addresses to perform routing which are, as a rule, visible to anyone observing the network...

P5: A protocol for scalable anonymous communication
R Sherwood, B Bhattacharjee... - Journal of Computer Security ..., 2005 - content.iop.org

... We present a protocol for anonymous communication over the Internet. Our protocol, called P5 (communication efficiency, and hence can be used to scalably implement large anonymous groups. We present a description of P5, an analysis of its anonymity and communication efficiency...

[PDF] psu.edu
[PDF] acm.org
[PDF] freehaven.net
[PDF] mtu.edu
How to Find Papers

Terminology

- Google Scholar is very picky about your word choices
  - (this is a feature not a bug)
  - You need to try many different search queries when searching for papers
How to Find Papers

Terminology

● Google Scholar is very picky about your word choices
   ○ (this is a feature not a bug)
   ○ You need to try many different search queries when searching for papers

Where was Tor is my anonymous communication searches? (not there)
Usability of anonymous web browsing: an examination of Tor interfaces and deployability
J Clarke, PC Van Oorschot, C Adams - in the 3rd symposium on Usable ...., 2007 - dl.acm.org
... Tor is an important privacy tool that provides anonymous web browsing capabilities by
sending users' traffic through a network of specialized nodes. In Section 2, we review the
preliminaries of anonymous communication and onion routing, and examine the relevant
threat models.

How to make personalized web browsing simple, secure, and anonymous
E Gabber, PB Gibbons, Y Matias - International Conference on ...., 1997 - Springer
... The work closest in spirit to our goal of anonymous personalized web browsing
is the visionary paper of Chaum [C85] on digital pseudonyms. Chaum presented a general
framework in which users maintain distinct pseudonyms for different organizations, such
that pseudonyms are unique and are not reusable.

Predicted packet padding for anonymous web browsing against traffic analysis
attacks
S Yu, G Zhao, W Dou, S James - IEEE Transactions on ...., 2012 - ieeexplore.ieee.org
... In this paper, we focused on reducing the delay and bandwidth waste of anonymous
web browsing systems in order to make anonymous web browsing applicable for web viewers.
We proposed the predicted packet padding strategy to achieve this goal. A simple
mathematical ...

Anonymous connections and onion routing
PF Swanson, DM Goldschlag... - Proceedings. 1997 IEEE ...., 1997 - ieeexplore.ieee.org
... In this paper, we will focus on the HTTP proxy for Web browsing, in the basic
configuration where a firewall lies between a trusted and untrusted network. The onion
router and its proxies live on the firewall. There are two classes of proxies: one that brige
connections from...
How to Read Papers

Don’t read the whole thing top to bottom as soon as you find it!!!

1. Read the abstract
   a. Does it still seem relevant?
How to Read Papers

Don’t read the whole thing top to bottom as soon as you find it!!!

1. Read the abstract
   a. Does it still seem relevant?

2. Read the introduction
   a. This will be a summary of the paper’s contributions along with its motivation
   b. Does the paper still seem relevant?
How to Read Papers

Don’t read the whole thing top to bottom as soon as you find it!!!

1. Read the abstract
   a. Does it still seem relevant?

2. Read the introduction
   a. This will be a summary of the paper’s contributions along with its motivation
   b. Does the paper still seem relevant?

3. Read the related works
   a. This is where you find other papers in the area (and why this paper thinks they didn’t solve the problem)
   b. Find papers that cite this paper in their related works to see what might have been missed
How to Read Papers

Don’t read the whole thing top to bottom as soon as you find it!!!

1. Read the abstract
   a. Does it still seem relevant?

2. Read the introduction
   a. This will be a summary of the paper’s contributions along with its motivation
   b. Does the paper still seem relevant?

3. Read the related works
   a. This is where you find other papers in the area (and why this paper thinks they didn’t solve the problem)
   b. Find papers that cite this paper in their related works to see what might have been missed

4. Read the rest of the paper (optional)
   a. You should be reading full papers for works closely related to yours
Refining your Topic

What problem are you solving?

Anonymous communication is pretty slow
Refining your Topic

What problem are you solving?

*Anonymous communication is pretty slow*

Why is this an important problem?

*People won’t use it if it’s slow*
Refining your Topic

What problem are you solving?

*Anonymous communication is pretty slow*

Why is this an important problem?

*People won’t use it if it’s slow*

What other work exists in the area?

*Tor: more usable than academic works, but not as strong anonymity*
Refining your Topic

What problem are you solving?

*Anonymous communication is pretty slow*

Why is this an important problem?

*People won’t use it if it’s slow*

What other work exists in the area?

*Tor: more usable than academic works, but not as strong anonymity*

What are the limitations of your approach?

*Better performance often means worse security*
Read Papers

Refine Your Topic
Roadblocks

Novelty: So you found a paper that looks like it already solved your problem

- Are there missing pieces to their solution?
  - See related work or, if present, “limitations”
- Is there a related problem that seems open?
Roadblocks

Novelty: So you found a paper that looks like it already solved your problem

- Are there missing pieces to their solution?
  - See related work or, if present, “limitations”
- Is there a related problem that seems open?

Scope: Your project is out of scope for a course project

- Any bite sized pieces you can break off?
Roadblocks

Novelty: So you found a paper that looks like it already solved your problem

- Are there missing pieces to their solution?
  - See related work or, if present, “limitations”
- Is there a related problem that seems open?

Scope: Your project is out of scope for a course project

- Any bite sized pieces you can break off?

Binary Projects: Your problem is either “solved” or “unsolved” with no middle ground

- You want steps along the way
  - Checkpoints along the way should be meaningful in their own right
  - Move the goalposts
  - See: Papers with titles of the format “Towards….”
Read Papers

Refine Your Topic
Finding papers (redux)

Cite related work!

- Important for your own understanding of the topic
- Credit where credit is due

It’s okay if you miss some papers initially

- Or even over time. (course staff can help here)
- Very important to do your best
- Repeat your searches as your understanding grows
Collaboration

Research is best with friends

This is how you will refine your ideas and find bugs

It’s easy to get into the weeds and lose sight of the big picture.

A fresh brain will catch things you missed.

Can I help?

Your classmates >> a rubber duck
Ethics

- This guy (Andy Sellars) is part of the CyberLaw Clinic
  - Go to the BU Cyberlaw Clinic with legal questions!
- Absolutely no breaking of things without permission
  - Don't even look at things without permission
- Law is confusing - do not make assumptions
  - Ask for help if ever unsure
Ethics

- This guy (Andy Sellars) is part of the CyberLaw Clinic
  - Go to the BU Cyberlaw Clinic with legal questions!
- Absolutely no breaking of things without permission
  - Don't even look at things without permission
- Law is confusing - do not make assumptions
  - Ask for help if ever unsure

Bug bounties: some companies have a policy about security research involving them.

Responsible disclosure: if you find a problem you MUST let the organization know BEFORE you make it public
Next week: come talk to us!

- Kelsey  M10-11  32-G9
- Andrea  M2:30-3:30  32-G9
- Henry    M3-4    32-G970
- Kyle     W10-11  32-G9
- Simon    W3-4    32-G9
- Alex     Th4-5   32-G9
- Yael     (by appointment)
Write up your results into a snazzy paper!