CSC 580
Cryptography and Computer Security

Overview of Research in Computer Science and Computer Security

January 11, 2018

Overview

Research will be a theme for this semester.

- Many CS students pay little attention to the "science" part of "computer science"
- Students who get involved with research often have an ad hoc introduction
- Knowing how to get started can be intimidating (it's a big field!)

All students in CSC 580 will complete a "guided research project"

- Cloud storage will be used consistently as an example
- We will discuss research standards and practices in this context
- Students will complete team projects (possible collaboration with ISM 324)
  - More info on collaborative projects on Tuesday (joint class meeting)

Graduate students:

- Take this a step farther with an independent research project
- Project topic of your choice - not discussed or "guided" in class though!

What do we mean by research?

Doing a "research paper" in a class

- Seek out information (library, etc.)
- Paper summarizes existing knowledge

"Doing research" (to a scientist)

- Identify interesting question *with unknown (to anyone!) answer*
- Seek out information on "state of knowledge" for that question
- Design a study to *advance knowledge*
- Perform study, giving insight to question (maybe not an answer!)
- Paper to share *new knowledge discovered*

Key aspect: Extending the current state of knowledge

Basic Terminology

Discipline vs Field vs Sub-Field

Disciplines	*Fields related to CS*
Biology Chemistry Computer Science Mathematics English Sociology ...	Computer Security Operating Systems Programming Languages Artificial Intelligence Theoretical Computer Science Computer Architecture …

Sub-Fields of Theoretical CS
Complexity Theory Algorithms Computational Geometry ...

Question: Where do you think cryptography belongs?

Styles of Research

Basic vs Applied (and Industry…)

Basic Research

- Curiosity-driven
- Spark is often "I wonder why…"
- *Can* have applications, just not main motivation
- Utility is in insight provided, not applications possible

Applied Research

- Driven by potential application
- Spark is often "I wonder if we could make…"
- Utility is both insight and potential application
- Often doesn't lead to a product - "applied" is motivation, not product
- Can lead to a product - *technology transfer* and *patents* relevant

Industry Research

- Can be basic or applied, and can be proprietary/private

Publication in Research

Goal of research is to create and share new knowledge

- How is it shared?
- How is quality ensured?

Sharing is via scholarly publication

- Conferences, journals, and books
- Standard practices vary by discipline and by field
  - Humanities: Books are most important!
  - Physical sciences: Journals are most important!
  - Computer Science: Conferences are most important!
    - Note: Many other fields find CS strange because of this
    - A lot of internal debate in CS about conference primacy
    - Probably not going to change...

Peer Review - Ensuring Quality

To publish a research paper:

- Author(s) send to a publisher (conference or journal)
- Publisher/editor locates experts in that field/subfield/topic
- Experts (3-5 “peers”) review manuscript and consider:
  - Does the paper make a significant contribution to field?
  - Is the science sound (correct mathematics, sound experiments, …)
  - Is the writing quality good (easy to understand, …)
- Publisher/editor makes decision based on reviews
  - Accept!
  - Accept with minor modifications
  - Decline but could be resubmitted with major modifications
  - Decline and discourage resubmission

Review by experts is critical to maintaining scientific integrity!

- Beware of self-published work (just on a web page)
- Beware of “vanity press” and “pay to play” conferences/journals

Conferences in Computer Science

Conferences are main publishing outlet for most CS fields

- Example: Security is almost entirely conferences
- Counter example: Theoretical CS has lots of journals

Top Conferences

- Top conferences are highly competitive (<15% acceptance)
- Panels of experts debate which papers to accept
- Each field has one or two “top conferences”
  - Theory: STOC and FOCS
  - Programming Languages: POPL
  - Operating Systems: SOSP
  - Architecture: ISCA
  - Databases: SIGMOD
  - Security: IEEE S&P and ACM CCS (more later!)
- Getting a paper into a top conferences can be a career-maker!

Conferences: Beyond the top-tier

Most work doesn’t go to a top-tier conference (obviously!)

Other options:

- Less selective conference for a field (e.g., CANS)
- Regional conference (e.g., ESORICS)
- Specialized sub-field conference/workshop (e.g., PKC)

How to get information on conference quality/prestige

- Ask the experts!
- Check http://conferenceranks.com (let’s try this…)

Final note: Beware of scam conferences...

Structure of a Research Paper

Typical structure (order of some parts may vary):

- Abstract - brief summary - always published openly!
- Introduction - setting the stage
- Prior/Related Work - providing context
- Definitions/Techniques/Results - the “meat” of the paper
- Discussion - putting the results in context
- Conclusion and Future Work/Open Problems

Let’s look at some examples:

- https://dl.acm.org/citation.cfm?id=2382227
- https://dl.acm.org/citation.cfm?id=3133987

Accessing Publications

Some things change, some are the same:

- Publishers used to be exclusive gateway to research
  - Required purchase of paper or subscription
  - Authors signed over copyright to publisher
  - Usually accessed at a library
- Then… welcome to the World Wide Web
  - Researchers set up personal web pages for their work
  - Publisher agreements changed to accommodate this
  - Some gray area for some publication/publishers
- Most recently: Open Access Publishing
  - No more “pay wall” - publisher distributes freely
  - But… authors have to pay for publication - shifts costs

What stays the same: Peer Review

How to Find Relevant Work

Publishers:

- ACM Digital Library (note UNCG subscription)
- IEEE Xplore Digital Library
- SpringerLink

Search/Index Services

- Google Scholar is great!
  - Previously-seen paper: https://goo.gl/ZWXJCD

“ePrint” archives

- https://arxiv.org - for Physics, Math, and CS
- https://eprint.iacr.org/ - specifically for crypto
- Warning: These are not peer reviewed!

Research in Computer Security

- ACM Computer and Communication Security (CCS)
  - https://dl.acm.org/event.cfm?id=RE182
- IEEE Security and Privacy (S&P or “Oakland”)
  - http://www.ieee-security.org/TC/SP-Index.html
- USENIX Security
  - https://www.usenix.org/conferences/byname/108
  - Note: All are open access!
- CRYPTO
  - https://www.iacr.org/meetings/crypto/

Final Bits...

You may not have thought about research much before….

Take this time/responsibility seriously and see what it’s about!