CS 5410 - Computer and Network Security: Research Methods II

Professor Patrick Traynor
Fall 2017
Reminders

• Assignment #2 - Due on Monday
  • You should have at least 50% completed by now.
• Project Ideas due on September 13th.
  • This lecture should help you further along the path to success.
• Emails need to be prepended with [CNT 5410].
Why Publish?

- Lots of reasons to publish
  - Advancement
  - Dissemination of ideas
  - Fame
  - Travel (location oriented research...)
- This is the “coin of the realm” in academic and research communities.
  - You can not survive without them.
  - The frequency and quality of your publications determines your future.
- Ok, we get it, it’s important...
When to Publish?

• *Novelty* (or lack thereof) is the determinant of value
  • An *incremental* paper is one without a great deal of novelty
  • Nothing wrong, just viewed as less valuable

• How do you fit on this scale of publishing style?
  • Frequent small publications
  • Infrequent highly novel publications
  • Some fields tend toward infrequent (OS) or frequent (bioinformatics) publication.

• Know the expectations of your field, your institution and most importantly, your advisor...
Publications

- Technical Reports (not peer reviewed)
- Workshop Papers
- Conference Papers
- Journal Papers
- Books (careful what you wish for)

- Workshop, conference and journal papers are peer reviewed, which means that they have been judged by others and accepted or rejected based on that valuation.
Technical Reports

• Non-peer reviewed papers issued by an organization as an internal publication

• Most often used to time-stamp work
  • Time-stamping: Important to avoid intellectual property and academic misconduct problems (i.e., who came up with idea first)

• TRs can be resubmitted verbatim to a conference or journal

• You should TR all papers you complete as practice

• Often good filler for a vita, and demonstrates that you are working hard even when publications are not out yet.
Workshop Papers

- Workshops are intended to be informal gatherings of people working in a particular area
  - Mostly immature works in progress
  - Good for public time-stamping work
- Publication at these are valuable for
  - Exchanging idea/getting feedback
  - Building a reputation
  - Introducing a new body of work
- Publications are less valued, with notable exceptions
• For most computer scientists, advancement is almost entirely dependent on performance in conferences.

  • *Computer science is unlike most engineering, pure and social sciences*, where conferences are generally non-competitive and the important publications are made in journals.

• Conferences are typically 2-3 day meetings where researchers present their papers.

  • Every paper is given a 20-30 minute slot in which to present the contribution of the work
  • The *hallway track* is where you go to meet other researchers and *network*.
  • Conferences are deemed *tier 1*, *tier 2* and *tier 3*. Publish *regularly* in tier 1 if you want to be at the top of your field.
Publication Tiers

• Not all publication venues are valued the same. Publication “tiers” tell the story

• 1st tier - IEEE S&P, USENIX Sec, CCS, NDSS, TISSEC, JCS

• 2nd tier - ACSAC, ACNS, ESORICS, CSF, RAID, TOIT, DSN, Infocom, WiSec

• 3rd tier - SecureComm, ICISS
Beware of conferences that accept far too many papers, have little or no quality control, and often are set to make money for organizers. Such publications on a CV can often raise red-flags with employers or promotion committees. Always understand the quality of a conference before you submit. Remember, your publication acts as an implicit endorsement of a venue. For this reason, people who regularly publish at these venues are almost certainly going to be judged harshly.

- IASTED, HICS, The “World Multiconferences on Systemics, Cybernetics and Informatics”
Conference Evaluation

- Submissions received by hard but often malleable deadline
- Papers (abstracts) are bid on by program committee
  - Know the committee going in (and who will read your paper)
- At least 3 reviewers are assigned to each paper
  - Each give a it a numeric rating based on differing scales
- The PC meeting
  - Submitted papers are reduced to twice the program size
  - Each paper is reviewed and a verdict given (accept/reject)
  - Iterates for a long time, leading to the list of accepted papers
  - You can be conditionally accepted with directed edits (shepherding)
Journal Papers

- Archival works, taking years to publish
  - Generally speaking, work should be extremely mature
  - All work complete, presentation as close to flawless as possible
  - Appears in a physical journal subscribed to by many
  - Some fields value journals more
  - Be safe and publish a few of these

- When you become senior, you must become an associate editor or editor-in-chief to establish your bone fides in your field.
Journal Evaluation

- Unsolicited manuscripts sent to journal editor
- Generally reassigned to associate editor.
- 3 reviewers are chosen
  - **Accept** - publish paper without (more) modification
  - **Minor revision** - make minor changes to paper (edits and clarification)
  - **Major revision** - make major modifications (new experiments, reorganization)
  - **Reject** - do not consider this paper further
- Ratings lead to recommendation from associate editor
  - *accept, reject, minor* or *major revision*
- Authors are given an opportunity to modify paper (if minor/major)
- Updated paper given back to reviewers for further evaluation
- Lather, rinse, repeat...
Books

- Books represent the largest and most prestigious kind of publication
  - Not *really* necessary for advancement, but nice to have
  - A **MASSIVE** undertaking in most cases, so don't enter into this lightly

- Kinds of books
  - Topic Book: a book on a specific subject (single/few authors)
  - Dissertation: like topic, but based on dissertation
  - Edited Collection: solicited chapters in topic area
  - Encyclopedia: many short articles in a specific area
    - Nice to have entries on vita
Your ultimate goal is to communicate with the reader.

Being good at this is not limited to spelling and grammar.

Masking what you are doing in complex and flower language is bad!

Things to avoid: “utilize”, “zeal”, contractions, colloquialisms.

By “avoid” I mean “like the plague”
Sections of a Paper

• Most systems papers have the following general sections:
  • Abstract
  • Introduction
  • Related Work
  • Architecture
  • Experiment
  • Discussion
  • Conclusion

• Let’s focus on Related Work and getting this done correctly.
Why talk about related work?

• Noble Answers:
  • Demonstrate *knowledge* of other solutions and the wider issue.
  • Understand the *failure* of those solutions to solve the problem (or how you can do it better).
  • *Build* upon the knowledge of your peers.
  • *Motivate* the rest of your research.

• Pragmatic Answers:
  • People love to see their name in your bibliography.
  • Many people do read this section for precisely this reason.
Where Does This Section Go?

• Related Work sections can go in one of two locations.
  • The second section of the paper (immediately after the Introduction)
  • The second to last section (right before the conclusion).

• Placement has everything to do with the impact of your paper.
  • If you are doing *something fundamentally* new or *exploring a new area*, let the reader get to the content as fast as possible.
  • If you are working in an established space (most of us do), you need to convince the reader you know about everything in that space.

• Examples:
  • Original SMS paper put the related work section at the end.
  • Mitigation paper put it after the intro.
Every good paper has what’s known as a “narrative arch”.

This is the thread that runs through all the components.

It connects the introduction to the conclusion with a story.

More critically, it gives the reader reason to read and understand every section.

Think about the best novels you have read. If you can skip large portions of the middle because they do not develop the character or the plot, *is it really a good book?*

A Related Work section typically plays the role of “informant”

“Before our story begins...”

...and should end setting up your idea... (or “the scene”)

What Should It NOT Be?

• A Laundry List
  • Person A did work X [1]. Person B followed with work Y, which increased performance[2]. Person C tried technique Z[3].

• This is the lazy way to do a Related Work section. It fails to:
  • ... use an opportunity to show why your solution is the right one to pursue.
  • ... keep the reader’s attention.
  • ... demonstrate deep knowledge of other work in the field and the implication of these approaches.

• This is one way to convince a reviewer that you do not know what you are talking about.
  • ... and certainly invites room for willful-misinterpretation.
What Do You Need To Do?

• When you start writing, figure out where to begin and end.
  • Duh... a little help please?

• By knowing where you are and have to go, you can begin to create your narrative arc.

• By the end of this section, your arch should have convinced the reader that your approach is the necessary next step in solving the problem.
So let's see one...

- Two related work sections walk into a bar...

- [http://www.cise.ufl.edu/class/cnt5410fa17/relwork.pdf](http://www.cise.ufl.edu/class/cnt5410fa17/relwork.pdf)
What Else?

• Go and *read papers* in the area related to your project.
  • Practice, Practice, Practice...

• Ask yourself if their related work moves the story forward and motivates their work...
  • ...and recognize when they have just used their space poorly.

• Remember, don’t do any section because you think you have to. Use every opportunity to win over the reader!
  • ...or the reviewer!
Why do we have abstracts?

• Abstracts help readers understand the topic and scope of a paper.
  • Titles are not always enough.
    • Are cellular networks about biology of communications?
  • Optimistically: Inform and excite the reader about the rest of your paper.
  • Pessimistically: Help the reader figure out whether or not they should read your paper.
  • Worst Case: Turn the reader away (when you should be attracting them).

• This is your chance to entice a potential reader.
  • If you fail here, nobody will ever get to see all the work you actually did...
What should an abstract say?

• Everything...
  • ...and yet not everything.

• You need to make a reader:
  • ...aware of the area
  • ...care about the problem
  • ...aware of your solution...
  • ...understand your methodology
  • ...appreciate your results
  • ...care!
There is just one problem...

- An abstract should not be a section.
  - It must be brief...
  - It must be direct...
  - It must be unambiguous...
- You do not have the space to say everything here
  - That’s what the rest of the paper is for anyhow...
- So what should it look like?
  - And more importantly, what should it say?
There’s a formula...

- Abstracts for 99% of all papers can and should be written in 6-8 sentences.

- They are:
  - Area
  - Problem
  - Solution
  - Methodology
  - Results
  - Take Away
What area are we talking about?

- **Cellular networks** are a critical component of the economic and social infrastructures in which we live.
- **Telephone wiretap** and **dialed number recording systems** are used by law enforcement and national security agencies to collect investigative intelligence and legal evidence.

In one sentence, help the reader figure out the high-level subject of the paper:

• “Something is rotten in the state of Denmark”

• Tell your reader the problem facing that area (at least the one you are going to address).

• While such investigations have explored the impact of specific vulnerabilities, they neglect to address a larger issue - how the architecture of cellular networks makes these systems susceptible to denial of service attacks.

• However, current dynamic analysis techniques suffer from significant performance overheads, making them infeasible in practice.
Solution

• How can we solve the problem we just mentioned?
  • In this paper, we show that it is possible for clients to prove both the presence and proper functioning of security infrastructure without allowing unrestricted access to their system.

• This paper presents Xen, an x86 virtual machine monitor which allows multiple commodity operating systems to share conventional hardware in a safe and resource managed fashion, but without sacrificing either performance or functionality.

• This is your “In this paper” sentence.
Methodology

• Tell the reader how you tackled the problem.

• We show through *empirical study* that costs of ABE make its direct application inappropriate, but present constructions that mitigate its incumbent costs.

• ...we use a combination of *modeling* and *simulation* to demonstrate the feasibility of targeted text messaging attacks.

• Be clear about how you are solving the problem.
Results

• Convince your reader that your methodology was effective in solving the problem.
• Under realistic network conditions, we show that adversaries can achieve blocking rates of more than 70% with only limited resources.
• Our analyses show that this system provides an accurate (within 3 feet) and efficient means of incorporating unforgeable location information.
• It helps to put numbers/percentages, but it is not necessary.
Take Away

• Potentially the most important sentence in the paper.

• You must tell the reader what you learned/proved and why they should care!

• Our analysis demonstrates that these techniques can eliminate or extensively mitigate even the most intense targeted text messaging attacks.

• It is through these experiments that we expose the viability of not only ABE-based content delivery, but applicability of ABE systems to large-scale distributed systems.
“Secure Attribute-Based Systems”

- **Area:** Attributes define, classify, or annotate the datum to which they are assigned.

- **Problem:** However, traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments.

- **Solution:** In this paper, we introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives. A policy system that meets the needs of complex policies is defined and illustrated.

- **Methodology:** Based on the needs of those policies, we propose cryptographic optimizations that vastly improve enforcement efficiency. We further explore the use of such policies in two example applications: a HIPAA compliant distributed file system and a social network.
Example (cont)

• **Results**: A performance analysis of our ABE system and example applications demonstrates the ability to reduce cryptographic costs by as much as 98% over previously proposed constructions.

• **Take Away**: Through this, we demonstrate that our attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems.