Paper Presentation Assignments

- Go over papers and dates
- Email me *3 top bids* by Friday
- I will pick *one*

Mock PC on HotCRP

Security Research Methods II

Why write a paper?

- There are many reasons to write a paper:
  - Articulate a new idea, thought, or observation ...
  - Document your research ...
  - Talk about new (observed) phenomenon ....
  - Advance your career ...
  - Because you have to ...

- *Reality*: publication is the coin of the realm in science, failure to do this successfully will lead to failure. You have to be effective at this to be a good (a) graduate student, (b) faculty member, or [sometimes] (c) researcher in professional research laboratory (IBM/AT&T/MS)

Paper evaluation

- A paper is evaluated on
  - Novelty
  - Correctness
  - Impact
  - Presentation
  - Relevance
  - "hotness"

Parts of a paper

- Parts of paper (vast generalization)

1. Abstract
2. Introduction
3. Related Work/Background
4. Solution/Problem
5. Evaluation/Analysis/Experiment
6. Discussion (often, but not always)
7. Conclusions

Abstract

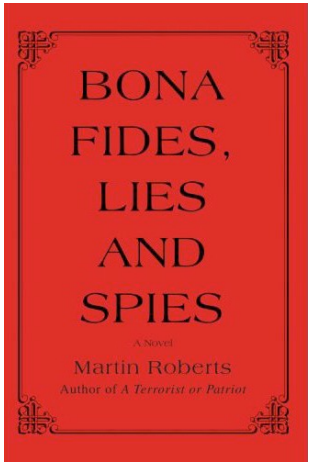
- One sentence each for:
  - Area
    - Topic of work
  - Problem
    - What's the issue?
  - Solution
    - How do you propose to address the problem?
  - Methodology
    - What's the experiment?
  - Results
    - What did you find?
  - Take Away: Lesson

Introduction

- One paragraph each on:
- Area
  - More elaborate
- Problem
  - Scenario
- Why is problem not solved
  - Brief of related work or the challenge
- Proposed insight ("In this paper, ...")
  - What is the experiment?
- Contributions -- What will the reader learn?
- Boilerplate outline (?)

Related work

- This is a statement of the work that led to this one.
  - who this work relies on
  - who has done work in the area
  - areas that inspired this work (not just technology)
  - Not a laundry list
- There are several reasons for related work section:
  - Motivate the current work
  - Differentiate from past work
  - Establish "bona fides"



Motivation, Background

- **Motivation**
  - Why is this a problem?
  - Motivating Example: Alice…
  - Why isn't the problem solved?
    - Forward/backward reference to the related work.
- **Problem, assumptions**: Problem statement, threat model, TCB.
- **Background:** What all does the reader need to know to understand your approach?
    - Already known material related to the solution
    - Tip: You can always move text from the design to the background, to focus on the *novel contributions in the design*.

System Architecture and Design

- How do you solve the problem?
- General Architecture / Overview
- What are the
  - Design Goals?
  - Challenges?
  - Contributions of your design (i.e., the design decisions) that help overcome the design challenges, hence achieving the design goals?

Experiment

- Experiment
  - Means of showing truth
  - Big Insight -- Hypothesis -- Claim
    - Show why it is interesting
  - Expected Results
    - Informal proof/argument that is true
- Experiment types
  - *Empirical* - measure some aspect of the solution
  - *Analytical* - prove something about solution
  - *Observational* - show something about solution

Implementation

- Experimental Platform
  - Exact specification of platform
  - Design may have more than implementation -- what did you implement?
  - How are key design features/mechanisms implemented?
  - *Not the design*: Separating the novel design contributions/decisions from their implementation is often a challenge)

Results vs Findings

- Results
  - Summarize -- what do the results mean?
  - Specific experiments
    - We did X, saw Y
  - What do the experiments prove
  - What other experiments would you want to do based on these results?
- Key Findings
  - What do the results mean?
  - What are the lessons?
  - Lead to the takeaway.

Conclusion

- Like the abstract in past tense
- Problem
  - What was the problem?
- Solution
  - What was the insight and why was it expected to work?
- Method and Results
  - What did you find?
- Take away: Lesson
- Future work

Hint

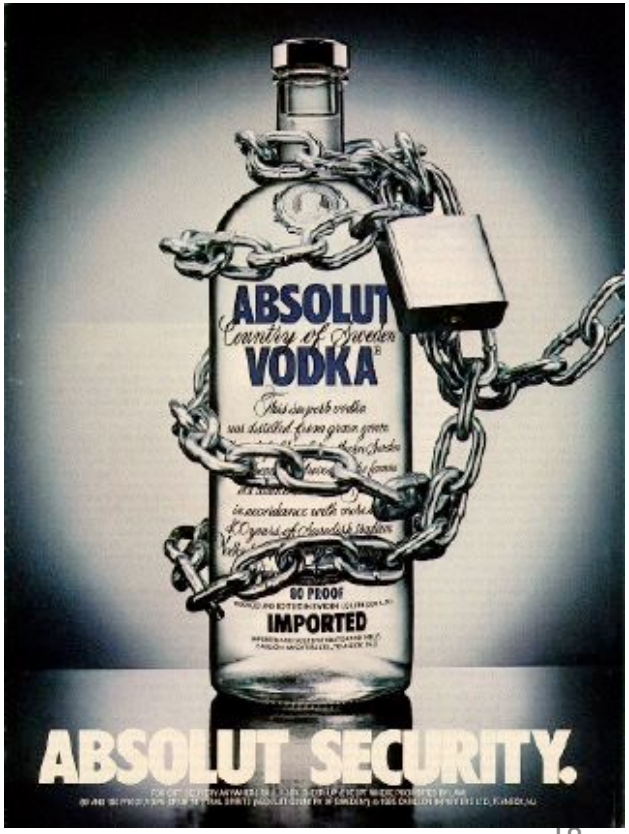
- Intro: tell them what you are going to tell them
- Body: tell them
- Conclusion: tell them what you told them.

Why is there so much bad research?

- Most papers (90%+) I encounter are ***bad*** --- for one or more of the following reasons. The authors …
- … don't formulate the problem well (or at all).
- … don't motivate the problem well (or at all).
- … address an unimportant or moot problem.
- … are not familiar with the breadth or depth of the area.
- … do not discuss important related work.
- … don't realize the problem has been solved (or at least better addressed).
- … don't have a coherent solution or it does not solve the problem.
- … don't have a coherent or appropriate methodology.
- … don't apply the methodology well.
- … don't draw the correct conclusions from the results.
- … don't present the work well enough to be understandable.
- … don't articulate the take away.
- Any paper failing to do any of these things is a failure.

Security Research

- Almost as diverse as computer science itself
  - Systems design
  - Formal analysis
  - Programming languages
  - Hardware design
  - Software engineering
  - Human computer interfaces
  - Networking, …
- Some are specific to security
  - Cryptography
  - Security protocol design
  - Security Policy, …



Note on Security Evaluation

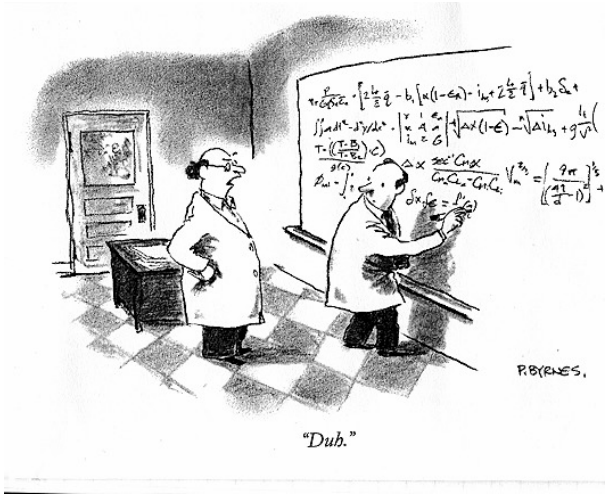
- Important for most papers
- Can be
  - Formal - Prove formal guarantees
  - Design arguments. Often at the end of each design choice.
    - Arguments considering the security model
  - Empirical, Observational.
  - State **threats to validity**

What is research?

- Which activities are research?
  - Designing a new protocol?
  - Building an implementation of a protocol?
  - Measuring the cost of the protocol?
  - Formally evaluating the correctness of a protocol?
  - Developing methods of implementing, evaluation a protocol?

What is not research?

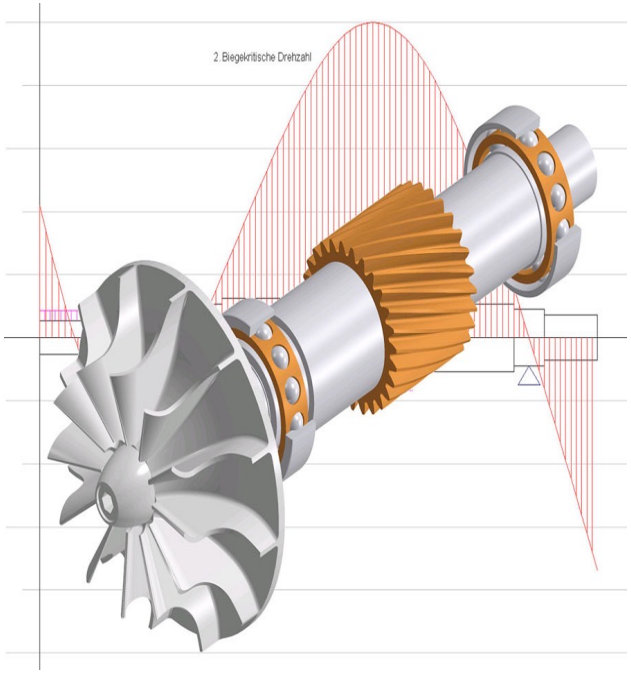
- Arguing the quality of a protocol?
- Arguing the appropriateness of a protocol?
- Surveying a field?
- Illustrating a limitation of a common practice or system?



"Duh."

Research vs. engineering

- Novelty …
- Importance … (sort of)
- Discovering a new fact or idea

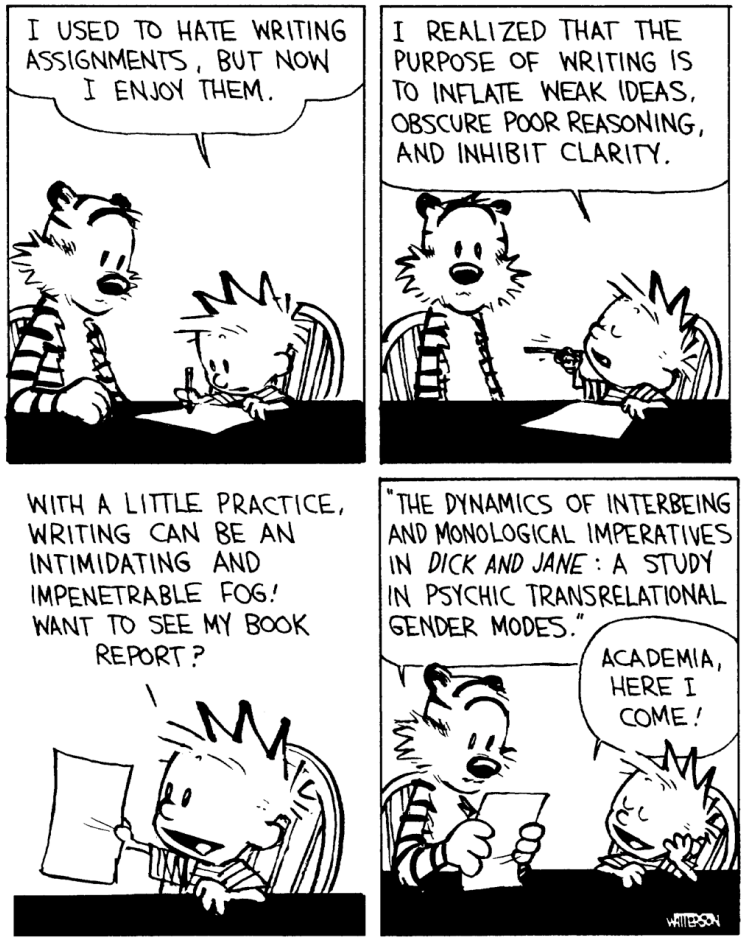


- Engineering is often harder than research
- One must be careful to understand the difference

Research vs. Opinion

- Arguing a position is not research unless it uncovers some *new thought* or *new methodological device*
  - Difference is subtle
- Experts will often produce manifesto about an area
  - E.g., Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure. C. Ellison and B. Schneier Computer Security Journal, v 16, n 1, 2000, pp. 1-7.
  - The key here is that they are *experts* and have the bona fides to make some an argument
  - This is **not research**

Writing a paper



Course Project

- End Result: *Research* Paper (8-10 page conference-style paper)
  - Motivation for an Experiment
  - Background
  - Related Work
  - Experimental Approach
  - Experimental Evaluation
- Start with an Existing System/Approach
  - Break It
- Improve It
  - Aim for a Research-Quality Result
- Reproduce prior results

Course Project

- The course project requires the student execute some limited research in security.
  - Demonstrate applied knowledge
  - Be realistic and practical about what can be accomplished in a single semester.
    - Don't try to learn some new *non-security field* *(e.g., if you do not know NLP, then…)*
    - Don't rely on external resources you don't have *(devices, servers, data)*
  - However, the work should reflect real thought and effort.
- The grade will be based on the following factors: *novelty*, *depth*, *correctness*, *clarity of presentation*, and ***effort***.
- Talk to me if you want to do something related to your research

Project Choice

- *Create a Project Proposal and submit it to Blackboard (**Deadline:** September 21st*
  - Ordered list of projects
  - Propose at least five unique projects in order of interest
  - Choose groups of 1, 2 (or 3 with approval)
  - A list of 2-3 meeting slots to meet with me to finalize the project *(Office Hours + by appointment)*
    - *Meeting with me prior to the deadline is recommended*
- I have the end say on your project and group
  - Hopefully, I can resolve the constraints implied
  - One functional group per project

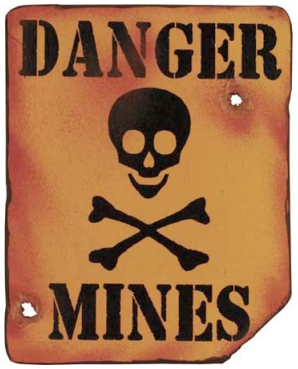
Topic Examples

- Mobile or IoT Systems
  - Design and build an Android security extension.
  - Evaluate the security of a specific *class of Android apps* via systematic analysis (e.g., IoT managers)
- *Defenses for attacks seen elsewhere (Slashdot, BlackHat, DefCon, …)*
- ***Reproducibility study**: Reproduce the results of a recent top conf paper **(only if the source+dependencies are available).***
- Note: picking a topic is very important, and should almost certainly involve an area that you know well

Project Speed Dating

- 09/14
- Look over past proceedings
- Find preliminary ideas to discuss
- I will organize groups in class so we can brainstorm and help each other

Bad Ideas



- An encryption library for IM/SMS.
  - Done... to death...
- Firewall rule checkers
- Steganographic schemes
- Anything that requires massive amounts of data that you can't get your hands on...
  - Online Game trends that require snapshots of all users...
- Anything that requires source code access to proprietary software