CSCI 6900

Computer Network Attacks and Defenses

A few tips on how to write a conference-style paper

Instructor: Prof. Roberto Perdisci

Fundamental Components

- **Hot topic**
- **Well written**
- **New** ideas
- **New** methodology
- Lots of **real data**
- **Realistic** experimental setup
- **Good results**
- Honest **limitations** section

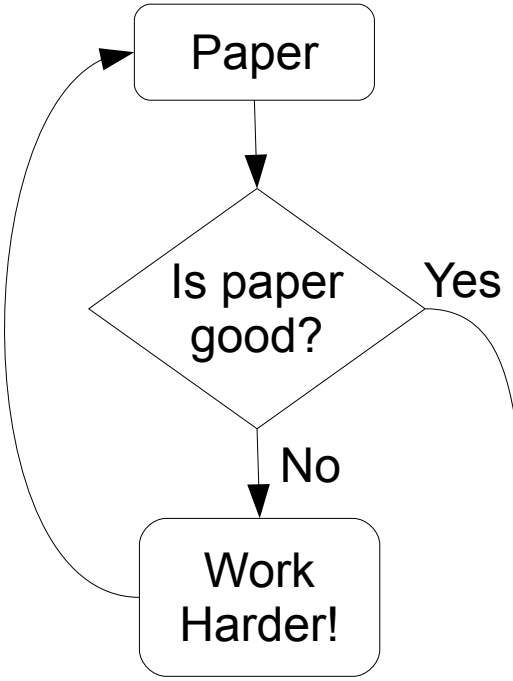
Fundamental Components

- **Hot topic**
- **Well written**
- **New** ideas
- **New** methodology
- Lots of **real data**
- **Realistic** experimental setup
- **Good results**
- Honest **limitations** section

Congrats!
You now have *50% chance* of being accepted!!!

Why only 50%

- Well... I was talking about top-tier security conferences
  - IEEE S&P, USENIX Security, ACM CCS, NDSS
- Others are a little easier to get into (still hard, though...)
  - ESORICS, RAID, ACSAC, DSN, ASIA CCS, DIMVA,...



- This **DOES NOT** mean "give up!"
- Instead, **work** towards perfecting your paper
- The smaller the *attack surface* for the reviewer, the higher your chances of being **accepted**!

Paper Organization

- A **well-organized** paper is the first step in the right direction!
  - Abstract
  - Introduction
  - Threat model
  - Related work
  - Your approach/methodology
    - use subsections to organize the description of a multi-components system
  - Evaluation
    - Experimental setup
    - Experimental results
  - Discussion/Limitations
  - Conclusion

Typical Paper Structure

- Threat model
  - not always a separate section
  - may be embedded in Intro
  - may be "implicit"
- Related work
  - may be replaced by a background section
    - info needed to understand the paper
    - previous work in the area
  - may be at the end, before conclusion

Abstract

- not more than 2-3 short paragraphs
- what is the problem you are trying to address?
- why is it important, why is it challenging?
- how do you propose to solve it?
  - "In this paper, we present..."
- summary of main results
  - be very concise and direct
  - don't be too shy, brag about good results
  - but don't exaggerate! your work very likely has many limitations...

Introduction

- First sentence: what is the problem?
  - e.g., "Botnets are considered one of the most serious threats to Internet security..."
- why is the problem challenging?
- what is the specific (sub)problem you are trying to address?
- brief summary of current attempted solutions (both academic and commercial)
- **motivate your work!**
  - why are the current solutions not effective?
  - you need to convince the reader that we cannot solve the problem with incremental improvements on existing solutions! we need your work!

Introduction

- what do you propose to solve the problem
  - summarize the approach
  - briefly describe the methodology
- summary of main results
  - e.g., "we can detect bot-compromised machines with 98% detection rate and 0.01% false positives"
- spell-out your contributions, for example:
  - "To the best or our knowledge, we are the first to address this problem ..."
  - "We implemented a POC and performed experiments on large real sets of data ..."
  - "The experimental results indicate that our approach is effective/promising ..."

Related Work

- It's not just a list of previous papers on the same topic!!!
- It has to be useful!
- Group previous papers that have a similar goal or use a similar approach
- For each (group of) paper, briefly describe their approach and in what way your work differs from them
- Indicate what work is the closest to yours, and what are the differences between them

Threat Model

- Clearly describes the attack scenarios you consider/want to defend from
- List your assumptions clearly
- Say why the assumptions are reasonable
- Mention whether the proposed solution could be generalized to a broader threat model
  - actual details usually go in the Discussion section

Approach/Methodology

- This is the main part of the paper
- Different styles for different kinds of papers, no real standard way to write it
- Well-organized subsections can help a lot!
  - System overview
  - Summary of notation/terminology helps when using heavy formalism
  - Details of each module
  - Algorithms in pseudo-code help clarify the description

Evaluation

- Experimental setup
  - Data collection process
  - Datasets used for evaluation
  - Description of the POC system
    - (LOC, libraries, etc.)
  - Equipment used for experiments
- Experimental results
  - detection results, false positives, successful attacks, ...
  - performance measurements
  - use standard benchmarks whenever possible
- Ideally, evaluation should be reproducible

Discussion/Limitations

- Discuss the assumption on which your work is based
  - What happens if the assumptions do not hold?
  - Sometimes used to comment on the experimental results...
- Limitations are always there
  - Corner cases you cannot currently handle?
  - Sophisticated attacks that may “break” your defense system?
  - Scenarios in which FPs may increase?
  - Propose potential ways of overcoming the limitations (future work?)

Conclusion

- 2-3 paragraphs
  - In a way similar to abstract, but no need to introduce the problem again...
  - “In this paper we presented...”
  - Briefly say what problem you solved
  - Mention the high-level approach you followed
  - Remind the reviewer of the results you obtained

Disclaimer!

- These are only high-level guidelines
  - Each paper follows a different presentation style, depending on the type of paper itself
  - no rule written in stone, although a number of things are always there and follow a fairly standard format
    - Abstract, Intro, Related Work, Conclusion