How to Look for Ideas in Computer Science Research

Zhiyun Qian

University of California, Riverside

Outline

- Getting started
  - Advisor / group
  - Research taste
  - Breaking down a research area
- Idea pattern
- Process and habits

Getting Started - Advsior / Group

- Junior vs. Senior professor
- Hands-on vs. Hands-off
- Small vs. Large group

Getting Started – Research Taste

- Paper reading
  - Class: 3 – 4 papers each week / class
  - Talks/reading groups: participate as much as you can
- Pay attention to the ideas
  - What type of papers stick with you?
  - What makes you appreciate the paper?
  - How did the authors come up with the idea?

Getting Started – Breaking Down Cybersecurity

- Domains
  - System: OS, software, binary
  - Network: Different layers of protocols
  - Hardware/architecture, Web, Crypto, etc.
  - Social / human
- Style
  - Attacks, Defenses, Analysis, Measurement, System building, etc.
- Techniques
  - Manual analysis, program analysis, formal methods, design, data-driven approaches (ML/AI).

Outline

- Getting started
  - Advisor / group
  - Research taste
  - Breaking down a research area
- Idea pattern
- Process and habits

Idea Pattern #1 – Fill in the blank

Domain\Techniques	Static analysis	Dynamic analysis
Use-after-free		✓
Out-of-bounds access	✓	✓

- Common dimensions
  - Assumptions
  - Domains
  - Guarantees/properties
  - Methodology/techniques
  - Datasets
- Examples
  - AML on images -> AML on other domains (malware, NIDS)
  - Static analysis vs. dynamic analysis
- Key is to map out the dimensions

Idea Pattern #2 – Expansion

- Many smaller dimensions are visible only if you work in the space
- Example
  - TCP side channel (Oakland 2012, CCS 2012, USENIX Security 16 and 18)
    - [Requirements: Firewall + Malware | Malware | Non]
    - [Shared resources: Software | Network | Hardware (to-be-done)]
  - DNS cache poisoning attack (CCS 2020)
    - [Protocol: TCP | UDP]

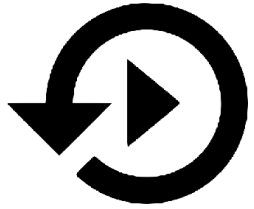
Idea Pattern #3 – Build a hammer and find nails

- Any unique expertise, technique, system, or even dataset
- Examples
  - Expertise: Virtual machine
  - Expertise: Network side channels
  - Technique: GAN / AML
  - System: Angr
  - Dataset: CAIDA

Idea Pattern #4 – Start small, then generalize

- Signs to look for
  - Initial observation is intriguing / surprising
  - Not easily explained by well-known concepts
  - Unlikely one-off
- Example
  - Strange network traffic -> TCP sequence number checking firewall -> Off-Path TCP sequence number inference (Oakland 2012)
  - Unzeroed pages returned to user space -> Android ION memory allocator analysis (CCS 2016)

Idea Pattern #5 – Reproduction of prior work



- How to make small observations in the first place?
  - Answer: one way is to reproduce prior work
- What can you see?
  - Different results than what were shown
  - Limitations when applying it to a different problem
  - Side discoveries

Idea Pattern #6 – External sources: from industry, news feed, etc.

- Industry
  - Build connections and learn their pain points
  - Great sources of research problems
    - Industry often not interested in investing in risky solutions
  - Example: Android Patching
- News & things happening around you
  - Something you can relate to
  - Example: Adblock and anti-adblock
  - Example: Uniqueness in Chinese markets, e.g., Android one-click root apps

Other Idea Patterns

- Adversarial research
  - Attack -> Defense
  - Defense -> Attack

- Automating a process
  - Reverse engineering
  - Vulnerability discovery
  - Bug triage
  - Exploitation (recent example: evasion of NIDS)
  - Patch presence test / Patch generation

Outline

- Getting started
  - Advisor / group
  - Research taste
  - Breaking down a research area
- Idea pattern
- Process and habits

Process and Habits

- Realize the difference between idea formulation vs. idea execution
  - Many students focus on execution alone

- Make time to practice idea formulation
  - Be curious and ask questions often
  - Participating in meetings/talks (preparation for questions)
  - Paper reading for classes and outside of classes
  - Paper reviews
  - Talk to your labmates

Article Version

- Zhihu
  - https://zhuanlan.zhihu.com/p/341685279
- Medium
  - https://medium.com/digital-diplomacy/how-to-look-for-ideas-in-computer-science-research-7a3fa6f4696f