Strategies for Computer Security Research: Practical Strategies for Taming the Angst and Changing the World

Jeanna Matthews (Clarkson University)
jnm@clarkson.edu

The Distinguished Speakers Program is made possible by

Association for Computing Machinery

Advancing Computing as a Science & Profession

For additional information, please visit http://dsp.acm.org/

About ACM

ACM, the Association for Computing Machinery is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges.

ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence.

ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

With over 100,000 members from over 100 countries, ACM works to advance computing as a science and a profession. www.acm.org

Some of my Career Path

- Ph.D., UC Berkeley, 1994-1999
- Associate professor at Clarkson, small PhD granting university in upstate NY
- Assistant professor at Cornell for 2 years
- Sabbatical at VMware
- Work with ACM – SIGOPS chair, editor of OSR, conference chair, US-ACM, etc.

- Today I am going to share with you the best concrete advice that I can in 45 minutes
- Treat you like my students for 45 minutes
  - Lessons I share with my grad students regularly
  - How to pick a research topic
  - How to find venues to follow
  - How to recognize good work and how to criticize work
  - How to find papers to model your work after

- Picking a problem or research topic is hard!
- Important part of what it means to be a researcher
- Not only do have to solve the problem, first you have to find the problem

Lesson 1: Find venues to follow

- Being a researcher means joining a community and teaching that community something they don't already know!
  - Example of good targeted question to ask a mentor!
  - But you can also find good venues yourself

Some examples

- Some suggestions for computer security
  - USENIX Security: https://www.usenix.org/conferences/byname/108
  - IEEE SP: http://www.ieee-security.org/TC/SP-Index.html
  - Associated workshops like LEET, Woot, …
  - There are many others!
- Look on www.wikicfp.com
- Who sponsors the conference? ACM? IEEE? USENIX? Who is on the program committee?

Benefits of "venue selection"

- Choosing venues to follow is a fair amount of work
  - But its worth it
  - Read titles of papers, sessions, look at program committee
- Allow yourself to be instructed by successful publishing authors in your choice of topic
  - What are people currently publishing!
  - What has already been done
- Much better than looking for a topic without such guidance!

Lesson 2: Read, read, read

- Now that you've chosen some venues, lets choose some papers
- Read every paper in those venues for the last 5 years
  - Every one? Yes!
  - Every word in every one? No!!
- Being a researcher means being familiar with the literature in your subject
  - No substitute for reading lots of papers
  - Never stops

Reading

- You are going to be doing a lot of reading of research papers
  - This is a huge part of what it means to be a researcher!
  - Its how you know whether something is new and that is what it means to be research
  - Its how you know where to publish your ideas
- How do you become a good writer? Just writing? No! reading great writing!
- How do you become a good researcher? Just doing research? No! reading great research!

Form a reading group

- Others to help cover space – which papers worth reading more deeply
- Vet your ideas with others
- Choose similar research topics
- Support each other
- Excellence grows up together

Keys to reading papers well

- Learn how to read papers
  - Increasing levels of depth – just the abstract vs. all the related work
  - Find some paper worth reading very very deeply
  - One more level of reading deeply – repeated research
  - See pamphlet – "Efficient Reading of Papers in Science and Technology"
- Read with a purpose
  - Take focused notes – a topic I might consider, future work I could do, methods I can learn from
  - Write down questions, criticisms, ideas

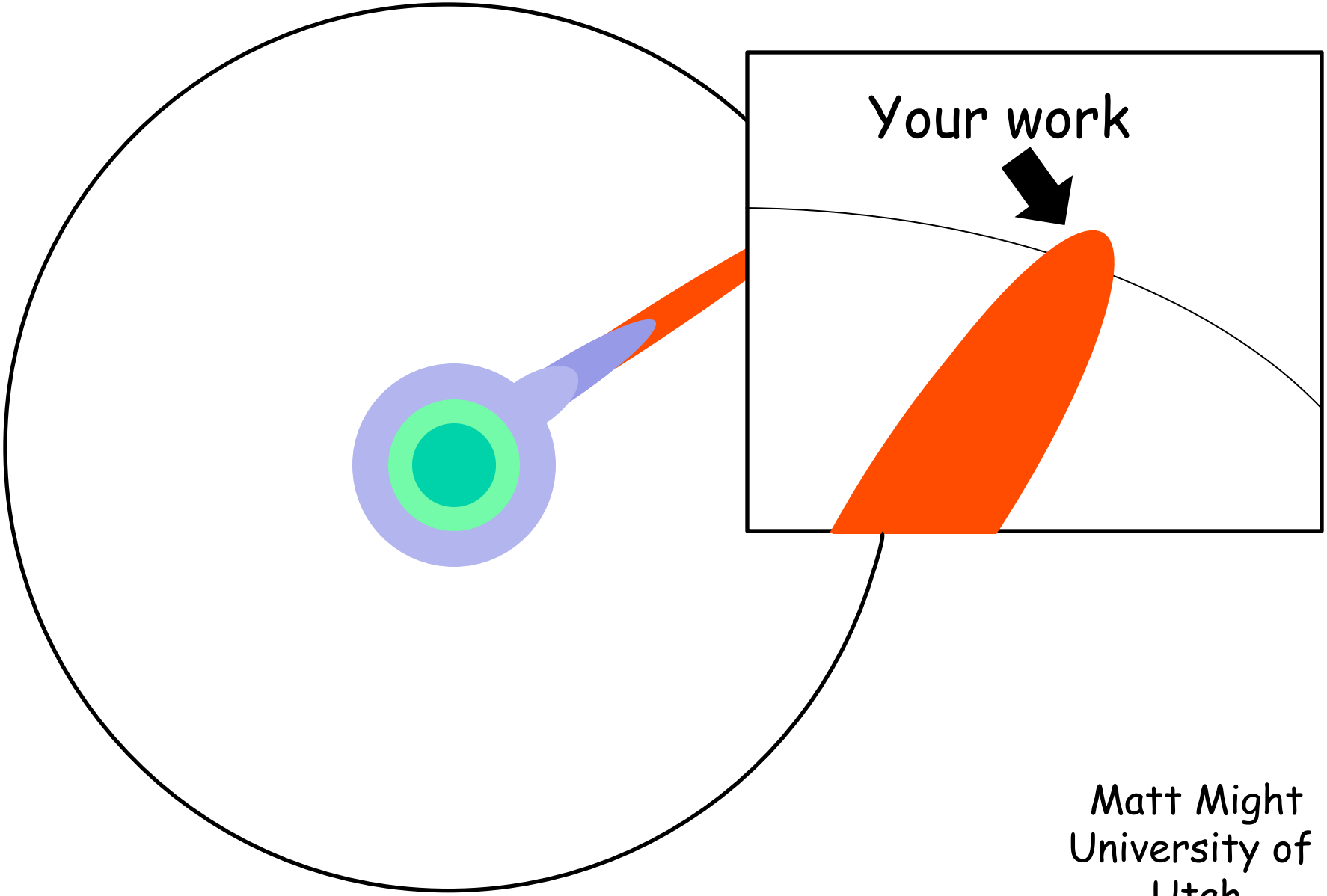
Lesson 3: Learn to criticize productively

- I have my students read "An Evaluation of the 9th SOSP Submissions"
  - http://static.usenix.org/publications/library/proceedings/dsl97/good_paper.html
- I have my students practice criticizing work they read
  - Summarizing is easy, liking something is just summarizing with some sugar added
  - Often start with more superficial criticisms
  - Pointing out things undone
  - Suggesting future work

- You can't become a researcher until you can teach a community something = must be able to see what is missing

- YOU MUST BE ABLE TO ARTICULATE:
  - The specific problem that you're solving
  - Why that problem is important
  - Why previous solutions are insufficient
  - Why your approach has the potential to succeed where others failed

What Is Research?



Matt Might
University of
Utah

Lesson 4: Repeated research model

- Puts you in perfect position for follow-on work
- Learn so much by examining each graph and asking do I understand how this was generated and what "gotchas" might be hiding
- Big fan of repeated research for MS and then build on that work for PhD

- Find a great paper you like, that you think you could have done, that inspires you, a paper for which you can see work undone
- Allow yourself to be instructed by particular papers in the art of doing research!
- If you find a paper that inspires you, see what else the same authors have done
  - Look to connect with them at a conference ☺

Lesson 5: Look for methods not just results

- When you read paper, don't just look at the results, look also at the methods
  - What data did they use
  - What systems did they use
- Ask yourself how could I use the same data or method to do other things
- Especially good thing to talk to people about at conferences!!

A few concrete examples

- Measuring the Practical Impact of DNSSEC Deployment, Lian et al., USENIX Security 2013
- PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs, McCoy et al., USENIX Security 2012
- Show Me the Money: Characterizing Spam-advertised Revenue, Kanich et al., USENIX Security 2011
- Dirty Jobs: The Role of Freelance Labor in Web Service Abuse, Motoyama et al., USENIX Security 2011
- An Analysis of Underground Forums, Motoyama et al., ACM Internet Measurement Conference

Lesson 6: Get concrete

- Do something concrete and hands-on as early as you can
  - Ask how can I gather concrete ground truth data
  - Look for open source software you can build on
  - Small groups (and smart groups) look to add targeted changes to open source systems
- You know when you are making a difference, when you have "traction" – if not, then find something you can do
  - Measure, trace, document, simulate
  - Don't exhaust yourself staring at something – say what can I do that is productive

Research is hard

- Know venues and researches in your field
- Read all the papers!
- Learn to criticize and suggest new directions
- Find data sets and partners, master techniques/systems/methodologies
- Remember if we knew the answers it wouldn't be research
  - Searching a dark space ..reporting what you find
- I can't make it easy but I can try to help you work smart…make the time you have to spend count

Outtakes

- Make what you do count
  - Insist on concrete deliverables; finish things
  - Be willing to define your contributions more broadly
  - Document efforts such as form reading group, specific papers read
  - Write a research blog
- Chose a topic that inspires you
  - More willing to do what it takes to read related work…more likely you recognize good solution when you see it
  - At least you will be satisfied at the end of the day

Good examples of things to ask a remote mentor

- Can you suggest a few publication venues related to my topic/ interests?
- Is my 3-5 sentence problem definition sufficiently focused?
- I am trying to choose between these three topics – can you comment on them?
- Ask "meta-questions" – how did you learn that? What tools do you use? What venues do you like?
- Can you suggest 3-5 recent papers you loved?
- Can you suggest courses, books etc related to my topic?
- Can you suggest a few researchers you respect in my area?