A Science of Security Course

Daniel Bosk Sonja Buchegger

KTH EECS, dbosk@kth.se

28th May 2020

'Sure, I know the methods I've used in my papers, but I don't feel particularly like a scientist.' [**Anonymous**]

What makes my work scientific?

C. Herley and P. C. v. Oorschot. 'SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit'. In: *2017 IEEE Symposium on Security and Privacy (SP)*. May 2017, pp. 99–120. DOI: 10.1109/SP.2017.38

'[C]laims of necessary conditions for real-world security are unfalsifiable. Claims of necessary conditions for formally-defined security are tautological restatements of the assumptions' [HO17, §IV].

Note: This is a problem

- The community itself is in disagreement on the Science of Security [HO17].
- This will be very confusing when entering the field.

Example (According to some)

- Cryptography isn't science.
- But provable security is.

Note: This is a problem

- The community itself is in disagreement on the Science of Security [HO17].
- This will be very confusing when entering the field.

Example (According to some)

- Cryptography isn't science.
- But provable security is.

The goal

- Give a holistic view of Science of Security.
- Where are the disputes and why?

The goal

- Give a holistic view of Science of Security.
- Where are the disputes and why?

Example ('Provable security')

- A uniformly random string of length n is the most secure password.
- We can prove it will take millions of years to guess it.

Note

- Attackers still get in, strange.

Example ('Provable security')

- A uniformly random string of length n is the most secure password.
- We can prove it will take millions of years to guess it.

Note

- Attackers still get in, strange.

Example (Usability)

- Turns out people can't handle uniformly random passwords.
- With a unique such password for every service.

Contents, part I

Note: What to focus

- What makes a method scientific?
- How do these play together? (The holistic aspect.)
- Emphasize the deduction/induction divide [HO17].

Contents, part I

1. Philosophy of Science of Security
2. Purely deductive methods

⋮

n. Purely inductive methods

Note: What to focus

- What makes a method scientific?
- How do these play together? (The holistic aspect.)
- Emphasize the deduction/induction divide [HO17].

Example (Philosophy of Science of Security)

- Start with a discussion of 'SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit'[1].
- What is Science of Security?
- Does that even exist at the moment?
- Shall we work according to the hypothetico-deductive model?
- What are the problems?

[1] C. Herley and P. C. v. Oorschot. 'SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit'. In: *2017 IEEE Symposium on Security and Privacy (SP)*. May 2017, pp. 99–120. DOI: 10.1109/SP.2017.38.

Example (Deductive inquiry)

- What are the limitations?
- Can this be science on its own?
- Or does it require a combination of application and further study to form something scientific?

Contents, part II

- General introductions to various subfields.
- Which methods are used and why?
- Some exemplary papers?
- How does a subfield fit into the holistic picture of Security?

Note

- All above was top down: faculty[2] present their view on
  - the methodologies,
  - the practices,
  - the adversary models,
  - the assumptions,
  - the relation to scientific approach in their respective subfield.

[2] From different subfields.

Bottom up

- Course participants review the scientific merits of papers[3] from top conferences in the subfield.
- They identify/reverse engineer methodology and components of evaluation.
- They value why this is scientific and how and what knowledge it contributes.

[3] Chosen by subfield designer, not participants.

Learning objectives

Should be able to

- choose an appropriate method of inquiry to answer a given research question in the field of Security.
- assess how a paper contributes to the advancement of the field of Security.
- evaluate the choice of methodology in a given paper.

Assessment

- Apply subfield methodology from bottom-up and top-down insights to own paper.
- Reflect on how this paper fits in the big picture of Security as a science.
- Discussion/reflection on limits of how scientific security research can be; e.g., provability versus complexity of actual systems, engineering versus science.
- Peer-review (among course participants) these individual papers[4] to identify gaps in the scientific approach that could be filled.

[4] Or a paper in progress or already published paper.

Idea

- Develop material jointly.
- Design as MOOC.
- This allows us to
  - each run the course locally when we have new students, or
  - run it jointly in relation to the SWITS seminar, and
  - reuse parts of the material in other courses too.

Teaching material

- Develop material jointly (video lectures, exercises etc.).
- Each research group is specialized on a part of the Science of Security methodology.
- Use tools that bridge the social aspects over time and space: e.g., Perusall.

Giving the course

1. Give the course in relation to SWITS every year.
2. Each faculty member can do assessment of their students locally, i.e., give it any time.

Note: Administration

1. One host institution, others do credit transfer?
2. Each institution has their own syllabus, course code etc.?
3. Split into small modules, different institutions responsible for each?

Giving the course

1. Give the course in relation to SWITS every year.
2. Each faculty member can do assessment of their students locally, i.e., give it any time.

Note: Administration

1. One host institution, others do credit transfer?
2. Each institution has their own syllabus, course code etc.?
3. Split into small modules, different institutions responsible for each?

Comments, questions, other thoughts?

[HO17] C. Herley and P. C. v. Oorschot. 'SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit'. In: *2017 IEEE Symposium on Security and Privacy (SP)*. May 2017, pp. 99–120. DOI: 10.1109/SP.2017.38.