How did we get into this mess, and how will we get out?

Putting the *science* in computer science/security

January 24th, 2015

Sami Saydjari (Cyber Defense Agency)
Shing-hon Lau (Carnegie Mellon University)

Let’s talk science

- Two perspectives:
  - How did funding agencies end up this way?
  - How did academia end up this way?

  - What can we do to get out?

A program manager's perspective

How did funding agencies end up this way?

What can funding agencies do to get out of this mess?

Why don't funding agencies do something?

- Are under extreme pressure to show short-term results due to:
  - Gravity of risks
  - Shortness of their tour (3 years)
- Unique challenge of right engineering-science mix in studying synthetic cyberspace [Susan]
- Are not accountable to do science
- Made up of academics and research engineers
  - Use academia and research engineers on panels to decide funding

Changing Research Investment Environment

1960s	1970s	1980s	1990s	2000s
• Space Race • Avoid Tech Surprise	• 10yr invest • Internet • Stealth	• VLSI • VHSIC • $ Surge • Cyberspace Forms	• Shorter term • Military focus • Cyberspace commerce • Dot Com • Desert Storm	• Bombs & Bullets displace research $ • Afghan • Iraq • Terror

Confusing Landscape

- Cyberspace is purely synthetic [John]
- Must construct artifacts to study
  - Science Requires Engineering!
- Sometimes artifacts are large and complex, requiring sophisticated engineering [Vern]
  - Supercomputing
  - Internet
  - Cyber Ranges
  - SCADA
- Confusion amongst sponsors on who to fund—who leads, who follows?

Accountability

- Yet to experience *catastrophic* cyberspace failures
- When failures happen, who is blamed
  - Not the engineers that built on shaky ground
  - Not the funding agencies that did not invest properly
  - Not academia who was complicitous
- "Systems are so complex, nobody can understand them"...so why try?
- Who is accountable for an devastating attack on a known-vulnerable infrastructure
  - None of us??.....All of us!!!

Culture Parallels

- NASA
  - Shifted from “safety first” to “better, faster, cheaper”
  - The second displaced the first
  - Root cause of both shuttle accidents
- DARPA
  - Era of the quad chart and 18-month “mid-terms”
  - Decisions constantly second-guessed
  - Pressure to award to big companies with solns in hand
  - Decade of short-term expediency
  - Culture takes a long time to change—at least 6 years
  - Created a PI community optimized for that investment environment

An academic's perspective

How did academia get this way?

What can academia do to get out of this mess?

Academia is like a contest

- The objective is to improve your CV
  - This opens up doors and produces opportunities
- How do you improve your CV?
  - Get appointed to prestigious positions
  - Get funding
  - **Publish papers**
- **It is in our rational self-interest to spend the least amount of effort to publish the most papers.**

Misguided incentives

- We are incentivized to:
  - Publish as much as possible
  - To do the bare minimum to get a paper accepted
    - The minimum is set by reviewers based on personal opinion and the guidance they receive from the venue
  - To **AVOID** fundamental and infrastructure work
    - More difficult and more time-consuming
    - Requires heavy investment of time and “academic capital”
    - Harder to get funded
  - To dispense with everything not related to publishing papers with minimal effort

Heard in the hallway…

- “Conference X is in a month; let’s start working on something so that we can publish it there.”
- “If we shop this paper around, we should be able to get it published.”
- “Let’s just take the shotgun approach and send out as many papers to as many conferences as we can.”
- “Let’s pick all the low-hanging fruit here and leave the rest for somebody else.”

Why is this all a problem?

- The bare minimum standards contain nothing about doing good science (or even bad science)
- We waste time and money building off of flawed work (e.g., Lincoln Labs [John])
- Much harder to discredit bad literature than to stop it from appearing in the first place [Phil]
- Fundamental and infrastructure work are critical to long-term success
- Weakening of peer review

“Peer” review

- So many authors trying to publish so many papers has lead to venue expansion
- Finding competent reviewers is harder
  - Editors/PC may not know appropriate reviewers
  - Reviewers are being asked to do more reviews
  - Busy reviewers produce lower-quality reviews
  - Tendency to be hyper-critical to dispense with a review quickly
  - **Peer review is often not done by “peers”**
- Faced with unfair reviews, we re-submit to the next available venue, starting the cycle over

Raising the bar

- **We need fewer, higher quality publications**

- We need to raise standards so that the bare minimum involves doing good science
- If the quality is in doubt, reject
- High standards are a necessary counterweight to the pressure to go fast
- Right now, we are out of balance!

Why isn’t science in the standard?

- Lack of education
  - Science is not on the curriculum in grad school
  - Generational problem: the teachers don’t know how to do good science so their students will never learn
- Reviewer culture
  - Too many hypercritical reviewers out to find flaws to sink a paper instead of offering constructive feedback
  - Review forms and instructions are rarely detailed and usually do not ask reviewers to look for good science
- No written guidelines
  - Nothing to point to when people ask how to do science
- Nobody is making us
  - No external pressure from funding agencies to change

But what can I do?

Action items – Reviewers

- Take the time to do a good review (2-3 hours per review) and encourage colleagues to do the same
- Use LASER criteria in your reviews starting now [Roy]
- Avoid hypercritical reviews – make at least 1 suggestion for every 2 criticisms you make
- Don’t do reviews that you are not qualified to do
- Give less importance to “cool” and more importance to whether the work makes a scientific contribution

Action items – Authors

- Write structured papers with structured abstracts [Roy]
- Clearly and concisely state the research question being addressed
- Provide enough information for replication work [Victoria]
- Share data and code when your work is published [Victoria]
- Perform replication work
- Undertake fundamental and infrastructure work

Action items – Conference organizers and journal editors

- Insist on structured abstracts and structured papers [Roy]
- Revise review forms/instructions to reviewers
- Make review criteria available to authors at the same time as the call for papers
- Strongly encourage, if not mandate, sharing of data and code [Victoria]
- Offer a prize/award for the most scientific paper
- Offer prizes/awards to encourage good reviews (e.g., “Best reviewer award”)
- Education workshops to teach good scientific practice to both students and professionals

Action items – Long term goals

- Put science on the curriculum (Dept. heads, funding agencies)
- Written best practices for experimental papers (IFIP?, Funding agencies)
- Implement a standard review form across all security venues (IEEE, ACM, Usenix)
- Reduce variance in reviewer results (IEEE, ACM, Usenix, Conference organizers, journal editors)
- Improve the existing publication model (IEEE, ACM, Usenix)
- “Look back from the future” – mock congressional hearing about who is responsible for gaps that lead to a devastating cybersecurity attack (Congress)
- Empower a government organization to ensure science is done (Congress, funding agencies)
- Change the funding model to reduce time spent on pursuing funding (Congress, funding agencies)