

Are we asking the right questions?



Great science needs to relate to today's problems...

Susan Appleby, CESG, UK

or does it?

“Basic” research

“Basic research leads to new knowledge. It provides scientific capital. It creates the fund from which the practical applications of knowledge must be drawn ... Basic research is the pacemaker of technological progress... A nation that depends on others for its new basic scientific knowledge will be slow in its industrial progress and weak in its competitive position in world trade.”

Science the Endless Frontier by Vannevar Bush; report to President Truman, 1945



“Applied” research

“University professors who are opposed to organising, planning and directing research after the manner of industrial laboratories ... have something to think about now. A most important piece of research [the atomic bomb] was conducted on behalf of the Army in precisely the means adopted in industrial laboratories. End results: an invention was given to the world in three years, which would have taken perhaps half-a-century to develop if we had to rely on prima donna research scientists who work alone”

New York Times, 7th August 1945



An old debate

a new topic

Science of Security

Basic
Blue skies
Fundamental
"More inspired and
creative"



Problem driven
Useful
Shorter term?
Narrower scope?

Basic vs applied research:
what should the balance be?

"Can we *afford* blue skies research in cybersecurity? In a field where the landscape alters beyond recognition every 3-5 years?"

Hm... papers are hard to categorise

Not a member? Click here to register! Forgot username or password?

3RD ANNUAL Best Scientific Cybersecurity Paper Competition

CPS-VO » SCIENCE OF SECURITY VO » BEST SCIENTIFIC CYBERSECURITY PAPER COMPETITION » 1ST ANNUAL COMPETITION

1st Annual Competition

- Home
- Review Team
- 2nd Annual Competition
- 1st Annual Competition →
- Submit Paper
- Files

SUBGROUPS

MEMBER INFO

1st Annual Best Scientific Cybersecurity Paper Competition

The first NSA Competition for Best Scientific Cybersecurity Paper invited nominations of papers published in fiscal year 2012 (Oct. 1, 2011 - Sept. 30, 2012) that show an outstanding contribution to cybersecurity science.

Winning Paper



This winner of the *1st Annual Best Scientific Cybersecurity Paper Competition* is **Joseph Bonneau** for his paper "**The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords.**" This paper, which offered careful and rigorous measurements of password use in practice and theoretical contributions to how to measure and model password strength, reflected many dimensions of good science: it was well grounded in past work, yet clearly differentiated itself from that work; it uses appropriate mathematics and articulates a new entropy measure that can be used to enhance the work in other investigations; it is a strong example of evidenced-based security research, grounded in a data set of sufficient size and diversity; it clearly exposed the author's data collection method; the methodology described was designed with ethical considerations in mind and it offered external validation of the author's results. It effectively drew on and contributed to the community of security researchers, and ought to have impact beyond the particular problem discussed in the paper.

Dr. Bonneau is a software engineer with Google in New York City. He holds B.S. (2006) and MS (2007) degrees from Stanford University in Computer Science. He worked for Cryptography Research, Inc. for a year before moving on to graduate studies at Cambridge University as the recipient of a Gates Fellowship in 2008. He received his PhD from Cambridge in 2012, working under Prof. Ross Anderson. The award paper documents work reported in the dissertation, entitled "Guessing Human Chosen Secrets". His dissertation acknowledges Profs. Ilya Mironov, John Mitchell, and Dan Boneh of Stanford (along with many

Not a member? Click here to register! Forgot username or password?

2nd Annual Best Scientific Cybersecurity Paper Competition

SCIENTIFIC CYBERSECURITY PAPER COMPETITION » 2ND ANNUAL COMPETITION

2nd Annual Best Scientific Cybersecurity Paper Competition

The NSA Competition for Best Scientific Cybersecurity Paper invited nominations of papers published between October 1, 2012 and October 31, 2013. Nominated papers must show an outstanding contribution to cybersecurity science.

Winning Paper

The annual paper competition winning paper, "**Memory Trace Oblivious Program Execution**," was originally presented at the Computer Security Foundation by **Chang Liu**, **Dr. Michael Hicks**, and **Dr. Elaine Shi**. Their research centered on the use of a scientific foundation for the use of Oblivious RAM (ORAM) in programs. Two aspects of this work were especially notable to the reviewers: First, it builds a bridge between cryptographic research and information flow research, and shows how the two can be applied together to solve a long-standing problem in a principled and secure manner. Second, it establishes a scientific foundation for the use of ORAM in programs and provides a valuable and exciting direction toward making ORAM practical.

Chang Liu is a second year doctoral student at the University of Maryland in the Department of Computer Science.

Dr. Michael Hicks is a professor in the Computer Science Department and University of Maryland Institute for Advanced Computer Studies (UMIACS) at the University of Maryland, College Park.

Dr. Elaine Shi is an assistant professor in the Computer Science Department at University of Maryland, College Park.

Honorable Mention

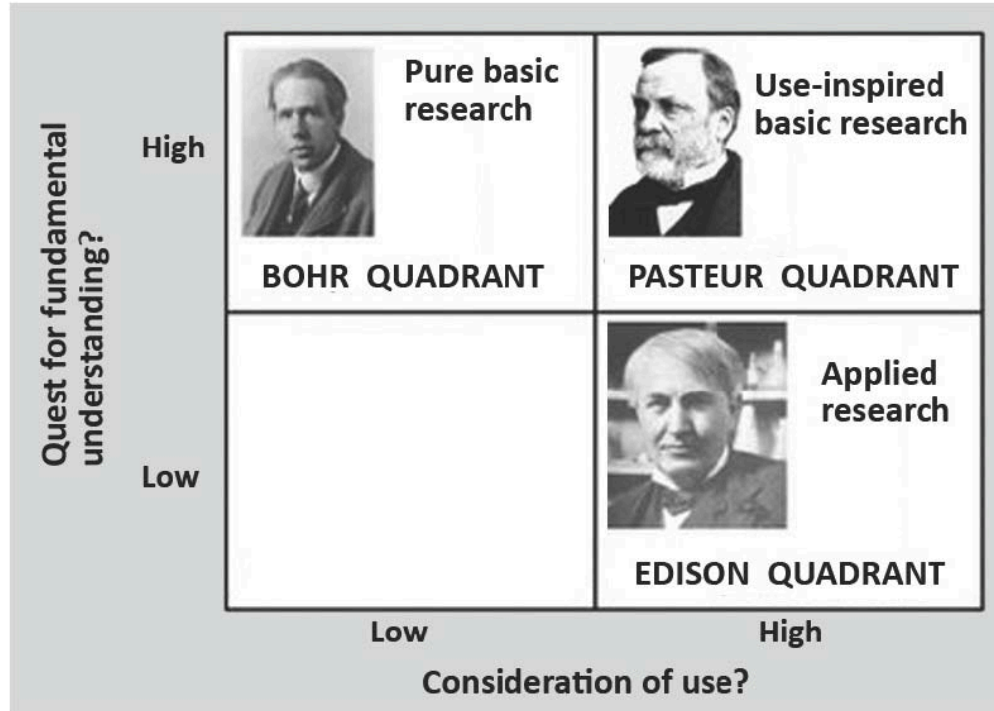
Of the 35 papers nominated one received honorable mention in this year's competition - "**Rethinking SSL Development in an Affiliated World**" by Sascha Fahl, Marian Harbach, Henning Perl, Markus Koetter, and Dr. Matthew Smith from the Distributed Computing and

Files

SUBGROUPS

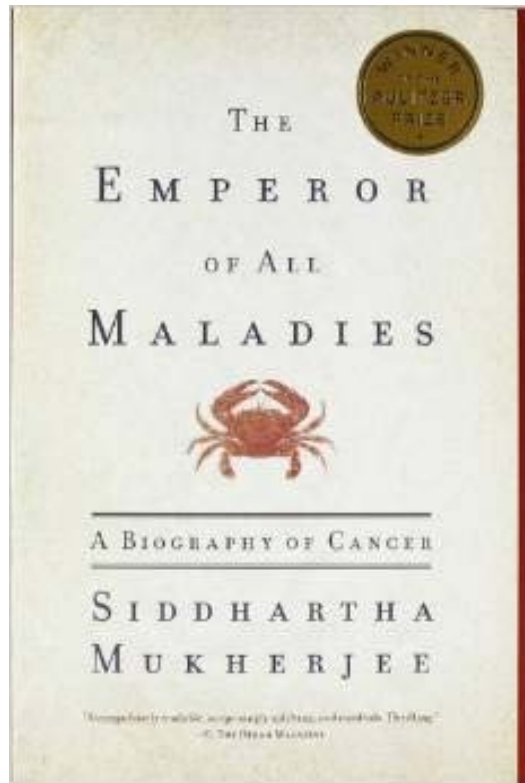
MEMBER INFO

Stokes proposed an alternative (1997)



Research can simultaneously be driven by considerations of use and by a quest for fundamental understanding

Remember those 1945 quotes? I stole them from this book



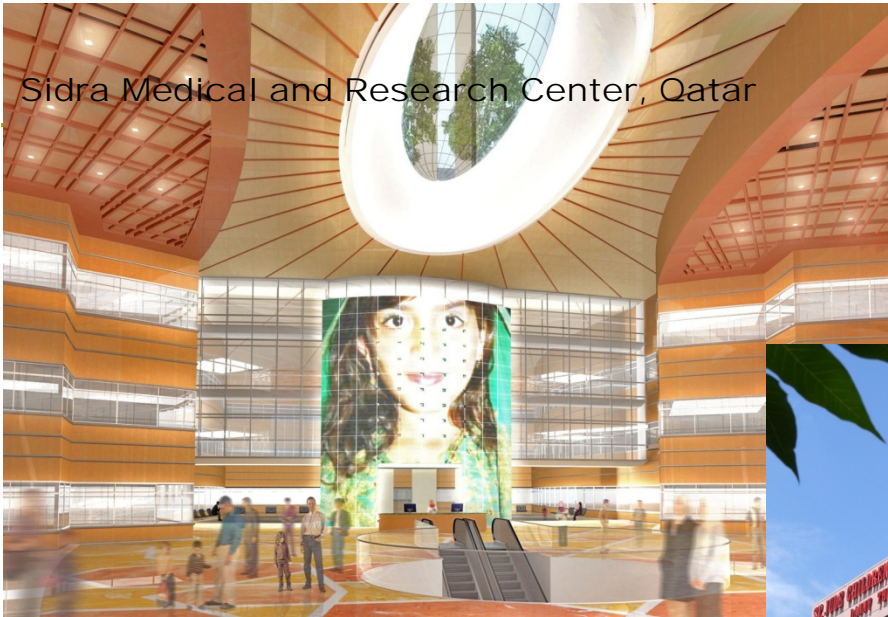
About the Author

Siddhartha Mukherjee M.D., Ph.D., is a cancer physician and researcher. He is an assistant professor of medicine at Columbia University and a cancer physician at the CU/NYU Presbyterian Hospital. A Rhodes Scholar, he graduated from Stanford University, University of Oxford, and from Harvard Medical School and was a Fellow at the Dana Farber Cancer Institute and an attending physician at the Massachusetts General Hospital and Harvard Medical School.

a CV flitting between research and practice

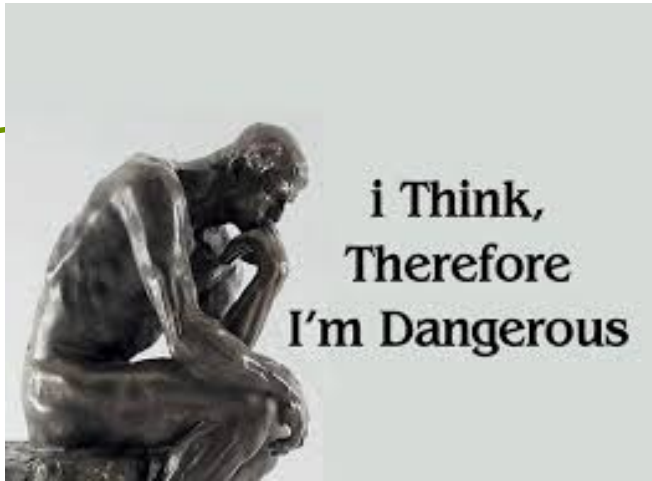


Sidra Medical and Research Center, Qatar



in a field where research and practice are intertwined

Whereas, back in cybersecurity...



**..The
Great
Divide?**



Research

Practice

Vox Pop

"Apparently it's quite common for research proposals to get a kicking from reviewers because they don't show any appreciation of the realities of life in the healthcare sector. I don't think this is true of cyber ones."

RCUK worker – personal correspondence

"We've just done a big piece of work on anonymising a massive scale public record database – so it can't be de-anonymised. We looked at what was out there – academic stuff – well, let's just say we decided not to use it."

Commercial IT research worker

"We don't really bother looking at academia. We did take a look once, but there wasn't anything relevant there. We didn't bother again."

Government security researcher

Is this why there are gaps in our capability?

Research Area	Number of UK Academic Centres of Excellence covering area (2013 data)
Cryptography, key management & related protocols	2
Information Risk Management	0
Systems Engineering & security analysis	6
Information Assurance Methodologies	1
Operational Assurance Techniques	0
Strategic technologies and Products	2
Science of Cyber Security	1
Building Trusted and Trustworthy Systems	3

Some examples from my perspective

□ System security architecting

- Extremely skilled work
- But many repeatable/mechanistic elements
- Design principles not defined
- ... But researchers lack insight into this world/access to practitioners

□ Human context switching

- Audio/visual interfaces across different trust domains
- How does security behaviour change with rapid context switching?
- How does design affect mistakes? decisions?
 - Eg – Multi domain telephony/VTC
 - Eg – browse down solutions
 - Eg – BYOD

Barriers to collaboration

- ❑ Commercial (IPR protection, pressure to deliver, 'firefighting' climate)
- ❑ Cultural (language, skillsets, mismatched incentives)
- ❑ Ethical (data privacy)
- ❑ Logistical (red tape, inflexible funding mechanisms, national security)
- ❑ Difficulty of working across disciplines



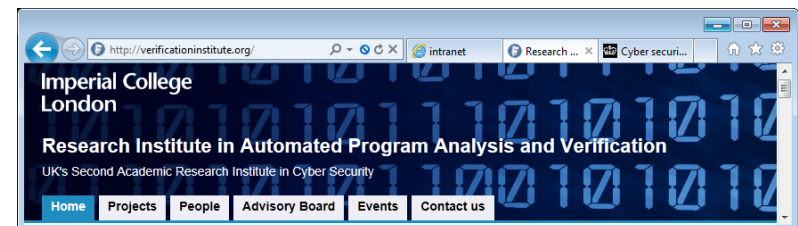
Some UK initiatives to help

- ❑ Academic Centres of Excellence in Cyber Security Research
 - Recognising centres with breadth and depth of expertise
 - 11 UK Universities now recognised as ACE-CSRs
 - Community build



□ Research Institutes

- Funded research, building strategic capability
- RI – *Science of Cyber Security*
- RI – *Automated Program Analysis & Verification*
- RI – *Trustworthy Industrial Control Systems*
- Platforms for dialogue & collaboration



An attempt at a conclusion

□ I assert:

- We need more “use-inspired research”
- We need greater entwinement between practitioners and researchers
 - Researchers need more exposure to problem owners
 - Problem owners need to divert more resource away from firefighting into research

□ I ask:

- Is co-location (part of) the answer??
- How do we break down the barriers to collaboration?

DISCUSS!!...