Breakout Participants

Nael Abu-Ghazaleh (SUNY at Binghamton)
William Adams (University of Michigan Ann Arbor)

Nicolas Christin (Carnegie-Mellon University)
Michael Clarkson (George Washington University)

Michael Gorlick (University of California Irvine)
Manimaran Govindarasu (Iowa State University)

Vern Paxson (International Computer Science Institute)
Chunyi Peng (Ohio State University)
Roberto Perdisci (University of Georgia)
Zachary Peterson (California Polytechnic State University)
Frank Pfenning (Carnegie-Mellon University)
Victor Piotrowski (National Science Foundation)
James Plusquellic (University of New Mexico)
Dmitry Ponomarev (SUNY at Binghamton)
Donald Porter (Stony Brook University)
Atul Prakash (University of Michigan Ann Arbor)
Portia Pusey
Yanjun Qi (University of Virginia)
Daji Qiao (Iowa State University)
Tal Rabin (IBM Thomas J Watson Research Center)
Mariana Raykova (SRI International)
Paul Reber (Northwestern University)
A.L. Narasimha Reddy (Texas Engineering Experiment Station)
Michael Reiter (University of North Carolina at Chapel Hill)
Kui Ren (SUNY at Buffalo)
Leonid Reyzin (Boston University)
Edward Rhyne (DHS S&T)
Golden Richard (University of New Orleans)
Heather Richter Lipford (University of North Carolina at Charlotte)
Thomas Ristenpart (University of Wisconsin-Madison)
William Robertson (Northeastern University)
Keith Ross (New York University)
Michael Rosulek (Oregon State University)
Brent Rowe (University of North Carolina at Chapel Hill)
Jerzy Rozenblit (University of Arizona)
Andrew Ruef (University of Maryland)
Norman Sadeh (Carnegie-Mellon University)
Rei Safavi-Naini (Boston University)
Jared Saia (University of New Mexico)
Lalitha Sankar (Arizona State University)
Fareena Saqib (Florida Institute of Technology)
Stefan Savage (University of California-San Diego)
Patrick Schaumont (Virginia Polytechnic Institute and State University)
Karen Schofield-Leca (Internet Society)
Dawn Schrader (Cornell University)
Stephanie Schuckers (West Virginia University Research Corporation)
Joseph Schwartz
Kathryn Seigfried-Spellar (University of Alabama Tuscaloosa)
Ramasubramanian Sekar (Stony Brook University)
Wendy Seltzer (World Wide Web Consortium-MIT)
Cyrus Shahabi (University of Southern California)
Deborah Shands (National Science Foundation)
Zhong Shao (Yale University)
Micah Sherr (Georgetown University)
Elaine Shi (University of Maryland College Park)
Zhijie Shi (University of Connecticut)
Dongwan Shin (New Mexico Institute of Mining and Technology)
Thomas Shrimpton (Portland State University)
Jordan Shropshire (University of South Alabama)

Tomas Vagoun
Jaideep Vaidya (Rutgers University Newark)
Rohit Valecha (SUNY Buffalo)
Michael Valenzuela (University of Arizona)
Jacobus Van der Merwe (University of Utah)
Kami Vaniea (Indiana University)
Eugene Vasserman (Kansas State University)
Pramode Verma (University of Oklahoma Norman Campus)
Rakesh Verma (University of Houston)
Giovanni Vigna (University of California-Santa Barbara)
Geoffrey Voelker (University of California-San Diego)
Mladen Vouk (North Carolina State University)
R Wachter (National Science Foundation)
David Walker (Princeton University)
Jesse Walker
Gang Wang (University of California-Santa Barbara)
Honggang Wang (University of Massachusetts, Dartmouth)
Hui Wang (Stevens Institute of Technology)
Jingguo Wang (University of Texas at Arlington)
Weichao Wang (University of North Carolina at Charlotte)
XiaoFeng Wang (Indiana University)
Richard Wash (Michigan State University)
Myra Washington (University of New Mexico)
Ronald Watro (BBN)
Sam Weber (Carnegie Mellon University Software Engineering Institute)
Steven Weber (Drexel University)

Joseph Kielman
Sara Kiesler (Carnegie-Mellon University)
Chris Kim (University of Minnesota-Twin Cities)
Andrew Klapper (University of Kentucky Research Foundation)
Alfred Kobsa (University of California-Irvine)
Janusz Konrad (Boston University)

Von Welch (Indiana University)
Susanne Wetzel (Stevens Institute of Technology)
Daniel Wichs (Northeastern University)
Stephen Wicker (University of California-Berkeley)
Marianne Winslett (University of Illinois at Urbana-Champaign)
Emmett Witchel (University of Texas at Austin)
Rebecca Wright (Rutgers University New Brunswick)

Craig Shue (Worcester Polytechnic Institute)
Akbar Siami Namin (Texas Tech University)
Joseph Silverman (Brown University)
Christian Skalka (University of Vermont & State Agricultural College)
Elizabeth Sklar (CUNY Brooklyn College)
Geoffrey Smith (Florida International University)
Dawn Song (University of California-Berkeley)
Anna Squicciarini (Pennsylvania State Univ University Park)
Vincent Sritapan (Department of Homeland Security)
Ankur Srivastava (University of Maryland College Park)
Christopher Stark (National Science Foundation)
David Starobinski (Boston University)
Angelos Stavrou (George Mason University)
Scott Stoller (Stony Brook University)
Koduvayur Subbalakshmi (Stevens Institute of Technology)
Gookwon Suh (Cornell University)
Kun Sun (College of William and Mary)
Yan Sun (University of Rhode Island)
Berk Sunar (Worcester Polytechnic Institute)
S. Shyam Sundar (Pennsylvania State Univ University Park)
Jakub Szefer (Yale University)
Carolyn Talcott (SRI International)

Gang Tan (Lehigh University)
Yuzhe Tang (Syracuse University)
Richard Taylor (University of California-Irvine)
Mohammad Tehranipoor (University of Connecticut)
Rahul Telang (Carnegie-Mellon University)
Stefano Tessaro (University of California-Santa Barbara)
Russell Tessier (University of Massachusetts Amherst)
Bhavani Thuraisingham (University of Texas at Dallas)
Derron Thweatt
Laura Tinnel (SRI International)
Scott Tousley (DHS S&T/CSD)
Samir Tout (Eastern Michigan University)
Ari Trachtenberg (Boston University)
Patrick Traynor (University of Florida)
Ryan Triplett
Nestan Tsiskaridze (University of Iowa)
Akhilesh Tyagi (Iowa State University)
Gary Tyson (Florida State University)
A. Selcuk Uluagac (Georgia Tech Research Corporation)
Sennur Ulukus (University of Maryland College Park)
Shambhu Upadhyaya (SUNY at Buffalo)
Salil Vadhan (Harvard University)

William Martin
Douglas Maughan (DHS S&T)
Rio Maulana
Roy Maxion (Carnegie-Mellon University)
David McClure (Duke University)
Damon McCoy (George Mason University)

Breakout 1: Cryptocurrency

Elaine Shi
University of Maryland

“The Rise and Rise of Cryptocurrency”

- Bitcoin came around in 2009.
- Today, traded at $284 per bitcoin.
- Total available bitcoins: billions of dollars.
- Cryptocurrency startups: **551**
- Average evaluation: **$3.9M**
- Numerous altcoins
  - Ethereum, dodgecoin, litecoin, …
- Large online service providers have started accepting Bitcoin payments
  - Expedia, Reddit, and Overstock.com

Usage of cryptocurrency outstrips our understanding

- Various attacks observed, e.g., Mt Gox failure
- Several altcoins flawed designs exploited
- Many research papers showing attacks
  - "Selfish mining"
  - Attacks against anonymity

Therefore, it is imperative to develop a "**science of cryptocurrency**"

What is the "**science of cryptocurrency**"?

1. What are the main scientific challenges?

2. What makes this a science?

– Jeremy Epstein

1

What are the main scientific challenges?

- What makes a cryptocurrency popular? How do we model user incentives?
- How do you design a provably secure cryptocurrency? How do you even define security?
- How do you design a cryptocurrency that accommodates inspection and legal enforcement?
- How can we design technologies to help users protect themselves, e.g., not commit money to a buggy contract?
- Can we have a theoretical characterizations of possible tasks/ applications atop a blockchain-based cryptocurrency?
- How can we formally model adversarial behavior/incentives?

2

What makes this a science?

Demonstrate the generic applicability of an approach beyond a single embodiment of cryptocurrency.

What areas of research are needed for the "science of cryptocurrency"?

- **Computer Science**
  - Cryptography/security, PL, data science, formal methods, hardware, game theory, mechanism design
- **Public policy**
- **Psychology**
- **Economics** and **finance**

How can we bring communities together to make cryptocurrencies better?

Workshops that bring together researchers and the developer community

Cryptocurrency conferences/workshops with PC members from developer communities

Message for NSF

Digital money will be the way of the future: it will enable rich smart contract applications, and enable new markets and eco-systems.

- It is imperative to develop a "science of cryptocurrency"

- Cryptocurrency in the broader form
  - Not just about Bitcoin or a single cryptocurrency.
  - Related to "why this is a science" question

Breakout 2:
Social Networks and Crowdsourcing

Ben Zhao
UC Santa Barbara

The Challenge

- Security work in social networks / crowd systems has been very focused on small set of problems
  - Detection of Sybil (fake) identities
  - Detection of forged content, e.g. Yelp/Amazon reviews
- Challenge:

  Can we formulate clear research challenges in the space for the near- and long-term

1. Leveraging/Managing the Crowd

- The crowd is a powerful resource for good…
  - Can go significantly beyond state of art ML/AI systems
  - e.g. reporting phishing sites (phishtank), Sybil profile detection
  - How to incentivize/how to separate wheat from chaff
  - Can we leverage it to solve harder security problems?
- But also powerful tool for attackers…
  - "Crowdturfing" observed in multiple countries/sites
  - Malicious crowds difficult to distinguish from normal users
    - Can generate "authentic-looking" original content
    - Can launch attacks against ML classifiers
    - Easily bypass existing tools that detect scripts/automation
  - Need to develop robust defenses (adversarial ML?)

2. The Content Curation Tussle

For user-generated content, curation is a necessity

Yet unclear how transparent providers should be in the process

e.g. server-side black box vs. user decisions on fully-transparent data

Less Transparency

- Providers have established credibility
- Leverage access to variety of data, more powerful models, robust against Sybils/Turfing
- Simpler process addresses a need to reach broader, non-technical users

More Transparency

- Complex black boxes, e.g. reputations, can be gamed
- Transparency reduces impact of "bandwagon heuristic"
- Providers have incentives mismatch
  - More content → more users → more content …

2. The Content Curation Tussle

For user-generated content, curation is a necessity

Yet unclear how transparent providers should be in the process
e.g. server-side black box vs. user decisions on fully-transparent data

Less Transparency

- Providers have established credibility
- Le… d… ro…
- Si… to reach broader, non-technical users

More Transparency

- Complex black boxes, e.g. reputations, can be gamed
- Transparency reduces impact of …
  - …ore content …

Is there a solution that addresses both need for transparency and does not exclude less-technical users? Perhaps solutions lie in the HCI space…

3. Educating Users on OSNs

- Many users still unaware of security risks on social networks, or the tools to mitigate them
- Can we develop more effective tools that leverage the social systems themselves?
  - Can we apply tools / lessons from social psychology?
    - Challenge: establishing credibility in absence of visible pedigree
  - Tap into power of first-hand stories, or folk models
  - Can we make stories about cybersecurity *go viral*?

Breakout 3: **Cryptographic Assumptions and the Real World**

Tal Malkin
Columbia University

Matching Crypto Models to the Physical World

- Side Channel Attacks
  - Theoretical leakage and tamper resilience models vs practical attacks and countermeasures
- Theoretical Modeling and Building Secure Crypto over Vulnerable Hardware (e.g., Trojans)
- Underlying Physics: How do we model/ define/ verify what we physically need / have? and what can be done with it? E.g., :
  - Physical assumptions like Wyner wiretap model, noisy key agreement, etc
  - Physical Unclonable Functions (PUF)
  - Understanding Randomness

Basic Crypto Research (for the Real World)

- Cryptographic Complexity Assumptions
  - How do we validate assumptions / avoid working with inappropriate assumptions?
- Foundations of Symmetric Cryptography
  - Better understanding of primitives like block ciphers, hash functions, ROM
  - Weaker assumptions while maintaining efficiency
- Secure MPC
  - Why isn't it used in the real world? (are we solving the wrong problems? Wrong models? Economic considerations?)
- Power-aware cryptography
  - Minimize communication complexity, though computation also relevant.

Employing Crypto in the Real World

- IoT Key Management (e.g, medical, cars,…)
  - Issue: complex usage environment (many parties / life cycle / removing and replacing and adding devices out in the field)

- Proving Security for large systems like TLS
  - Issue: complex system / many cryptographic components

New Dimensions Beyond Current Crypto

- Security problems often due to poor implementation, misuse, and other software engineering issues, not crypto
  - where is the boundary?
- Simplicity of implementation and use
  - Often more important than just efficiency

Can Crypto help? Can we design rigorous models to address these (traditionally non-crypto) issues?

- Questioning Kerckoffs' law / Asymptotic Approach
  - Security by obscurity /increased reverse engineering
  - Better concrete security models / metrics for time/work to break a system

Meta Issues

How to incentivize researchers to do the right thing?

- More interdisciplinary research
  - Help bridge the gap to the “real world”
- More long-term research
  - E.g., work on appropriate, well studied assumptions

Possible problems:

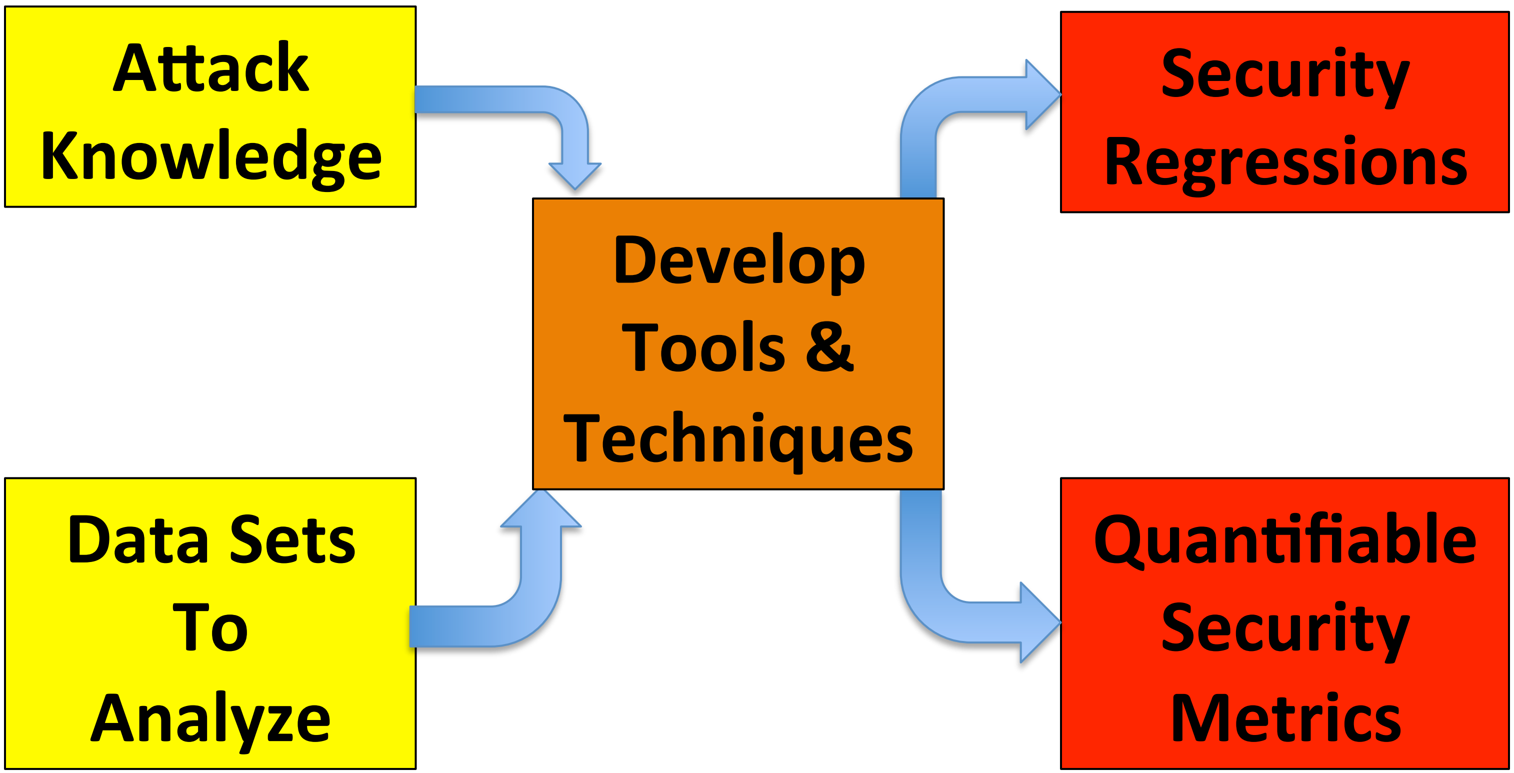
- Do we over publish? (expect fast/many publications, quality less important?)
- Interdisciplinary research difficult (e.g., find common language), may or may not be hard to publish?
  - Suggestion: submit real-world crypto proposals to AITF

- Crypto Education

Breakout 4:
Benchmarks for Security Research

Erez Zadok
Stony Brook University

Security Benchmarking Needs



Attack Knowledge

- Need:
  - Understand basic principles
  - Comprehensive list of attacks, updated
  - Companies to disclose attack details and internals
- Understand complex interactions
  - Hardware, software, networks, people

Data Sets to Analyze

- Have:
  - WINE, CAIDA, DNS/Farsight, CRAWDAD
  - Anti-Phishing Working Group (APWG)
- Problems:
  - Old, synthetic, small
  - Overly sanitized: nearly "useless"
- Need:
  - Lots of new data
  - Minimal/configurable anonymization
  - Incentives for companies to share data
    - NSF I/UCRC model?

Security Regressions

- Have:
  - "Red" teams
  - Static code analysis (e.g., Coverity)
- Need:
  - Security vulnerability tools
    - Automated
  - Domain-specific suites
    - e.g., network routing, Web, SQL, etc.
  - Comprehensive, continually updated
  - Community effort, open/free access

Quantifiable Security Metrics

- Have:
  - Metrics for performance, energy
  - Coarse security classifications/regs (EAL1-7, SOX, HIPAA, PCI, …)
- Need metrics such as:
  - TCB size; code complexity metrics, correlate with safety
  - Time needed to break security; time to recover
  - Resources needed to break security (#machines, CPUs, etc.)
  - Number of infected systems; amount of lost data
  - $cost:
    - Price of buying attacks, cost of ransomware
    - Cost of insurance, lost revenue
- Useful combination metrics (cost functions)

Develop Tools & Techniques

- Need:
  - Inventory of existing tools & techniques
  - Identify gaps
  - Timeliness of tools/techniques key
  - Rich set of tools & techniques
  - Apply or "port" existing techniques to new threats
  - Reduce false alarms
  - Collaborate with other fields
    - e.g., ML, Prog. Lang., Verification, Viz. Analytics
    - e.g., Economics, Business, Sociology, Psychology, Medicine

To Funding Agencies

- Benchmarking is bigger Broader Impact than SaTC
- Incentives to develop/release software
- More "Transition to Practice" (TTP)
- Greater access to events (e.g., Black Hat)
- Incentives for community efforts
- Encourage in GPG/CFPs
  - NSF BRAP: Benchmarks of Realistic Scientific Application Performance(?)

Breakout 5: **Cybersecurity and the Social Sciences**

Robert Axelrod
University of Michigan

Advice for Collaboration between Computer Scientists and Social Scientists

1. **Include both sides from the start.**
2. **Explicitly discuss goals and expectations** including publications and fundraising.
3. **Organize brown bags** across departments.
4. Beware that **joint PhD's have limited job prospects**.
5. Avoid **joint appointments** for Assistant Professors.

[No classified material will be shown in this breakout summary]

Breakout 6:
Responding to the NSA Revelations

Wendy Seltzer
W3C/MIT

Responding to the NSA Revelations

- Should our research change post-Snowden?
  - New or expanded topics of research
  - Changing research methods
  - Participation in public discourse

Research: Defending privacy

- Definitions and policy
- Technology and systems
- Institutions

Topics: definitions and policy

- Threat modeling: Identifying and scaling up the adversary
- Contribute to ongoing public discussion, challenge false and misleading statements
  - Demonstrate the importance of context data – it's not “just metadata”
    - Push-back on the third-party doctrine
  - Develop and publicize the more privacy-protective analytic methods we have
    - Shift the burden of proof to the information-gatherers
  - Utility-modeling
    - Small data – what we can learn from it; old-fashioned gumshoe work
- Quantifying privacy harms and risks
  - Quantifying vs. contextual?
  - Does quantifying force particular personal or policy responses? Backlash?
- Incentive alignment.
  - Not storing data might be in a business's interest
  - Industrial privacy; business trade secrecy
- User convenience, role of usability
  - Evaluation of privacy/security
  - Could there be a security label?
  - FDA (gov't) or UL (industry) model?

Topics: technology and systems

- Systems resilient against coercion/legal intervention
  - Eliminating central points of control/infiltration
    - Multi-party access control
  - "Warrant canary" transparency: "we have not yet received a request to turn over data"
    - Jurisdictional diversity?
  - Provable security
  - Secure randomness
  - Search on encrypted data
  - Exfiltration-resilient cryptography
  - Threshold crypto
  - Alternative approaches to crypto
  - Secure Multi-party computation

Topics: Institutions

- Governance: Research on norms of organizations, communication and its break-downs
  - Understanding the interactions between norms, laws, technology
  - How do new mechanisms interact with oversight?
  - Building systems to enable transparent citizen control
- Systems to enable individuals to choose/change privacy parameters (as individuals and as democratic citizens)
  - Make the costs and benefits more transparent
  - Provide meaningful choice
  - Designing good defaults

Methods

- Build in security from the beginning
  - With appropriate threat modeling, risk analysis
- Don't say “stop cryptanalysis”
- Think about protecting research subjects
  - Destroy data that's not needed
  - Secure “dark archiving” of identifying data needed for reproducible research
  - Don't expose subjects to new surveillance risks

Public involvement

- Interaction between research community and gov't agencies in setting security standards
  - Choosing experts
  - Transparent process
- Fund basic research, whatever its political valence.
  - Protection of privacy is in the national interest

Public engagement

- Public dissemination, communication, and translation of research, methodology and results
  - Demonstration of transparency best practices
  - Discussion with policy-makers
  - Interaction with tech companies
  - Participation in standards-setting
- Long-term research response