Breakout Participants

Nicolas Christin (Carnegie-Mello
Michael Clarkson (George Wash
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 Car
Thomas Ristenpart (University of Wisconsin-Ma
William Robertson (Northeastern University)
Keith Ross (New York University)
Michael Rosulek (Oregon State University)
Brent Rowe (University of North Carolina at Cha
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 Dieg
Patrick Schaumont (Virginia Polytechnic Institut
Karen Schofield-Leca (Internet Society)
Dawn Schrader (Cornell University)
Stephanie Schuckers (West Virginia University R
Joseph Schwartz
Kathryn Seigfried-Spellar (University of Alabama
Ramasubramanian Sekar (Stony Brook Universit
Wendy Seltzer (World Wide Web Consortium-M
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)

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

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 Norma
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
Steven Weber (Drexel University)

Joseph Kielman
Sara Kiesler (Carnegie-Mellon University)
Chris Kim (University of M
Andrew Klapper (Universit
Alfred Kobsa (University of
Janusz Konrad (Boston Un
David Ko
Farinaz K
Shriram
Ram Kris
Marwan
Brenden
Sandeep
Sandip K
Stephan
Brent La
Carl Lan
Catherin
Sarah La
Gary Lea

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)

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)

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 (Worce
Douglas Maughan (DHS
Rio Maulana (Syracuse
Roy Maxion (Carnegie
David McClure (Duke
Damon McCoy (George Mason University)

Breakout 7:

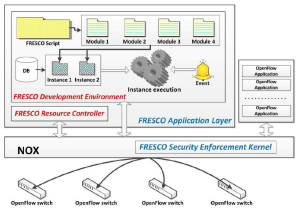
Cybersecurity Experimentation of the Future: Supporting Research for the Real World

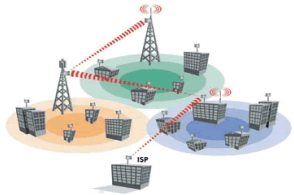
David Balenson (SRI International)
Terry Benzel (University of Southern California)
Laura Tinnel (SRI International)

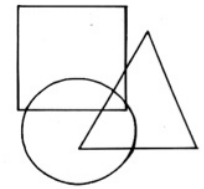
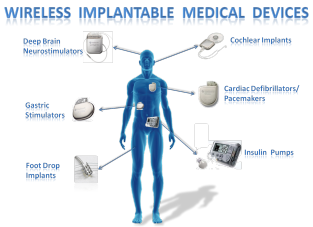
Tomorrow's Cybersecurity Challenges

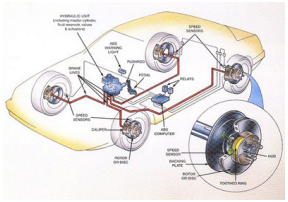
- Cyberspace is rapidly evolving with nearly every aspect of society moving toward pervasive computing and networking
- Need to move quickly to meet tomorrow's needs
  - Highly specialized cyber-physical systems (CPS)
  - Interdisciplinary experimentation
  - Modeling and reasoning about human behavior
  - Advanced networking architectures (e.g., SDN
- CEF is community-based effort to study current and expected cybersecurity experimentation infrastructure, and to produce a strategic plan and roadmap for developing infrastructure that supports tomorrow's research










Cybersecurity Experimentation of the Future

Future Experimentation Infrastructure Objectives

- Catalyze and support research
- Advanced experimental research tools, technologies, methodologies and infrastructures
- Broadly available national resources
- Beyond today's state of the art:
  - Multi-discipline, complex, and extreme scale experimentation
  - Emerging research areas specialized cyber-physical systems and cybersecurity-relevant human behavior
- Advances in scientific methodologies, experimental processes, and education
- Strategies for dynamic and flexible experimentation across user communities and infrastructure facilities

Breakout Discussion Highlights

- Experiment metrics, including those mapped to defender objectives
- Support for internal vs. external validity of experiments, context matters – ecological validity
- Capabilities to support reproducibility
- Sharing of data collection and analysis algorithms, benchmarked datasets
- Special considerations for cyber security research
- Can't just provide tools when people don't know how to use them effectively
  - Need to couple with methodologies and education
  - Need case studies to show how the RI can be used

General RI Discussion

- Caveat: can't foresee everything needed in the future
- RI should include benchmarked data
- Can't just provide tools when people don't know how to use them effectively
  - Need to couple with methodologies and education
  - Need case studies to show how the RI can be used
- Support for experiment metrics that are mapped to defender objectives
- Recognize and support for internal vs. external validity of experiments, context matters – ecological validity

Experiment Reproducibility

- How do we describe everything needed in order to reproduce an experiment, especially in complex and/or large scale experiments?
- What level of fidelity must be captured for an experiment to be reproducible?
  - What does and doesn't matter is a research topic itself.
- When documenting an experiment that uses a complex range, need ability to point to location where the detailed info is kept.
- Bundle: data + code + environment

Sharing of Common Algorithms, Data

- Data validity can be impacted by faulty data collection methods
  - Share validated collection methods, algorithms and tools
- Shared datasets are needed to perform apples to apples comparisons between approaches
  - Share datasets for specific research areas (e.g., keystroke dynamics)
- Common analysis algorithms/tools are needed to perform apples to apples comparisons between approaches
  - Share vetted analysis algorithms/tools

Characteristics of Cyber Security

- How is RI for cyber security different from other cyber problems?
  - Must take adaptive adversaries into account – models & ability to automatically generate and validate models
  - Intent (purposeful vs. accidental) may not matter when a failure occurs until we see the behavior change

Conclusion

- Science-based experimentation infrastructure is critical to enabling future cybersecurity research
- Need for revolutionary capabilities for advancing multi-discipline, complex and extreme scale experimentation for emergent cybersecurity research areas
- Lively and helpful discussion that reinforces CEF study outputs and provides guidance on what to highlight and expound upon

- Consider: How would ***you*** contribute to a collaborative effort to build and share this infrastructure?

Breakout 8:

Developing a Principled Security Curriculum

Rebecca Wright
Rutgers University

Guiding Questions

What should a security curriculum cover?

How can we improve how security principles are taught?

Who are you teaching and **what** do they need to learn?

- Need different kinds of programs – different audiences coming in, different pathways going out.
  - Concentrations or tracks in different majors (CS, IS, etc.), stand-alone cybersecurity major
- Potential interest in different kinds of career paths.
- Different principles suitable for different groups.
- Some philosophical questions still unresolved:
  - Is practicing offense necessary for understanding defense, or is offense its own specialized skill?
- Pragmatic concerns and constraints
  - Overfilled curricula, long pre-requisite sequences, students of varying backgrounds, etc.

Many Existing Useful Resources

- **NIST NICE Framework**
- National Academies Report: *Professionalizing the Nation's Cybersecurity Workforce*
- **NSA/DHS Academic Centers of Excellence:** now divided to cyber defense and cyber operations (smaller program, specialized on offense). Includes existing knowledge units.
- Military academies developing **"Cyber Science"** as a starting point separate from CS.
  - Working group of about 60 people (mostly in cybersecurity) working with ABET to develop an ABET-accredited program.
- Various courses, including some with materials or entire course available freely online.
- Many more…

Principles, **Practice**, and **Mindset**

- **Scientific** principles, **engineering** principles, and **social science** principles, among others.
- Effective to combine principles with **practical activities** and **examples** that illustrate the principles, build interest, and encourage engagement.
- In the context of a broad education (vs. training for specific skills), focus in a discipline can serve as a way to **develop a mindset**, a **culture**, and a **body of shared knowledge**. (Should also ensure teaching of problem solving, communication, and critical thinking.)
- We could do a better job of explaining the differences between different kinds of programs to potential students: what background do you need to succeed in this programs? what kinds of career or further educational pathways are natural from this program? what kinds of interests are a good fit for this program? [But beware being too narrow and scaring people off.]

Breakout 9:

User Authentication

Nicolas Christin
Carnegie Mellon University

Passwords & authentication

- Simple, cross-platform, one-size-fits-all for human-to-machine authentication
  - We'll probably still talk about passwords in a few years
- Historically, poor usability of alternatives (e.g., biometrics)

- **This may be changing**
  - Commoditization of usable biometric systems (e.g., iPhone touch ID)
  - Increased importance of machine-to-machine authentication (Internet of Things)
    - RFIDs/NFC tokens are now extremely cheap to produce and are increasingly deployed (you're using one to open your room)
  - Single-sign on systems (e.g., Google/FB accounts) are increasingly used for credential delegation
  - Multi-factor authentication

Future research directions in user authentication (1/2)

- **Privacy-preserving** authentication
  - Group signatures / pseudo-identities for large systems (e.g., transportation networks)
    - Research question example: how to scale group signatures (expensive to verify) so that they can accommodate very large networks (e.g., automobile networks)
    - Potential communication overhead to disseminate pseudo-identities
- **Reconciling threat models** with deployed primitives
  - e.g., "authenticating" to the newspaper
  - Segmentation of authentication primitives
- Potential **arms race**
  - Well known in biometrics (research on spoofing)
  - Is there an end to this arms race – can it be proven?

Future research directions in user authentication (2/2)

- Incentives to **decouple identification** from **authentication**
  - Identity providers/SSO systems – avoiding core root of trust (multiparty computation?)
  - How to decouple? Preserving privacy vs. long-term "reputation"
  - How much trust are users willing to give to authentication providers?
    - E.g., failure to accept the German National ID card
- **Metrics** to evaluate authentication
  - Going beyond false negative/false positive rates
  - Scope of the threat model, adoption rate, usability / lightweight, cost, failure implications
- Deployment of **forward secrecy**
  - Technology probably already exists but needs to be deployed to a much larger extent

Breakout 10:

An End to (Silly) Vulnerabilities

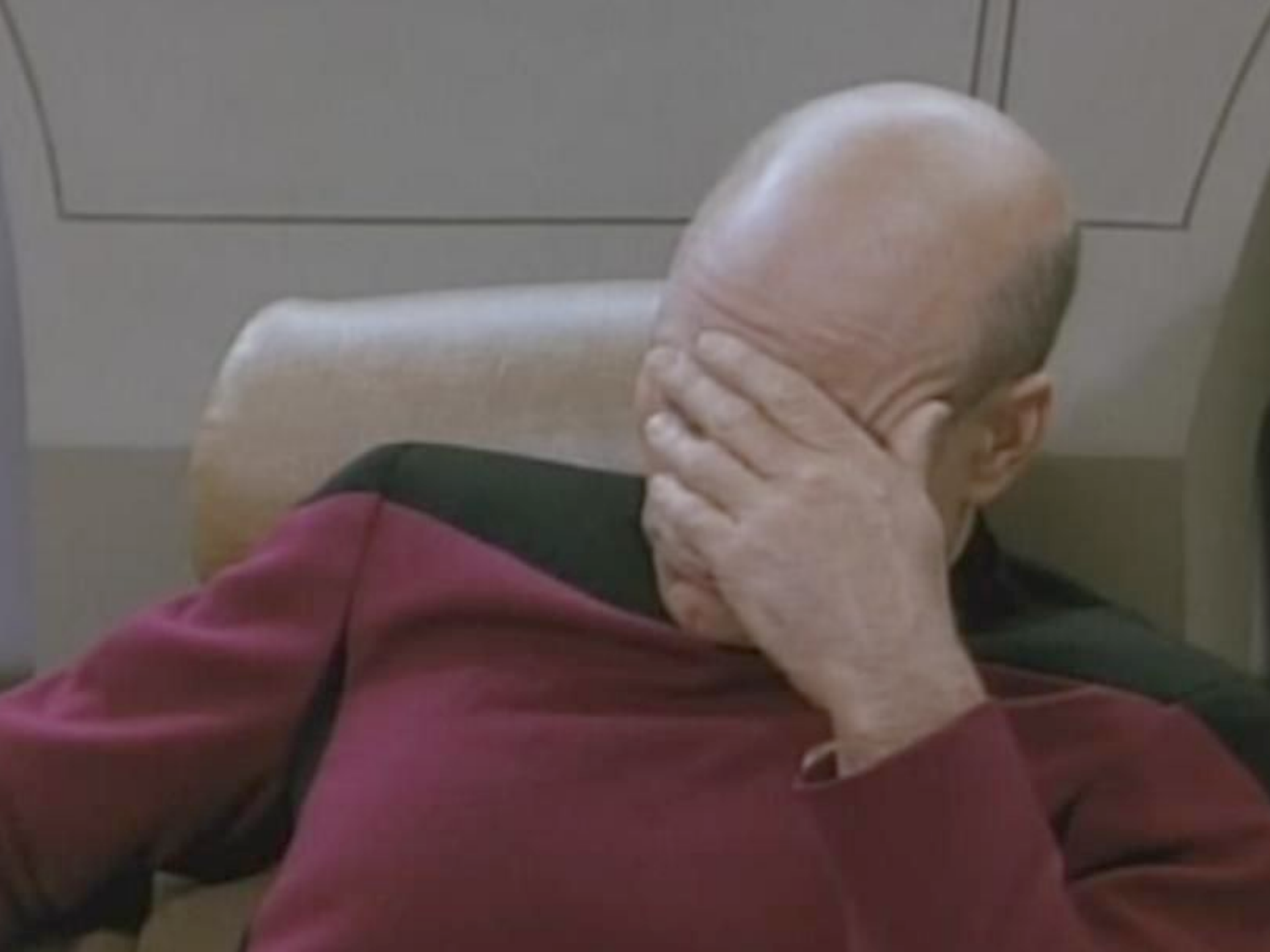
Matthew Might
University of Utah
matt.might.net
@mattmight

Research

Education

Incentives

silly vulnerability. *n*.

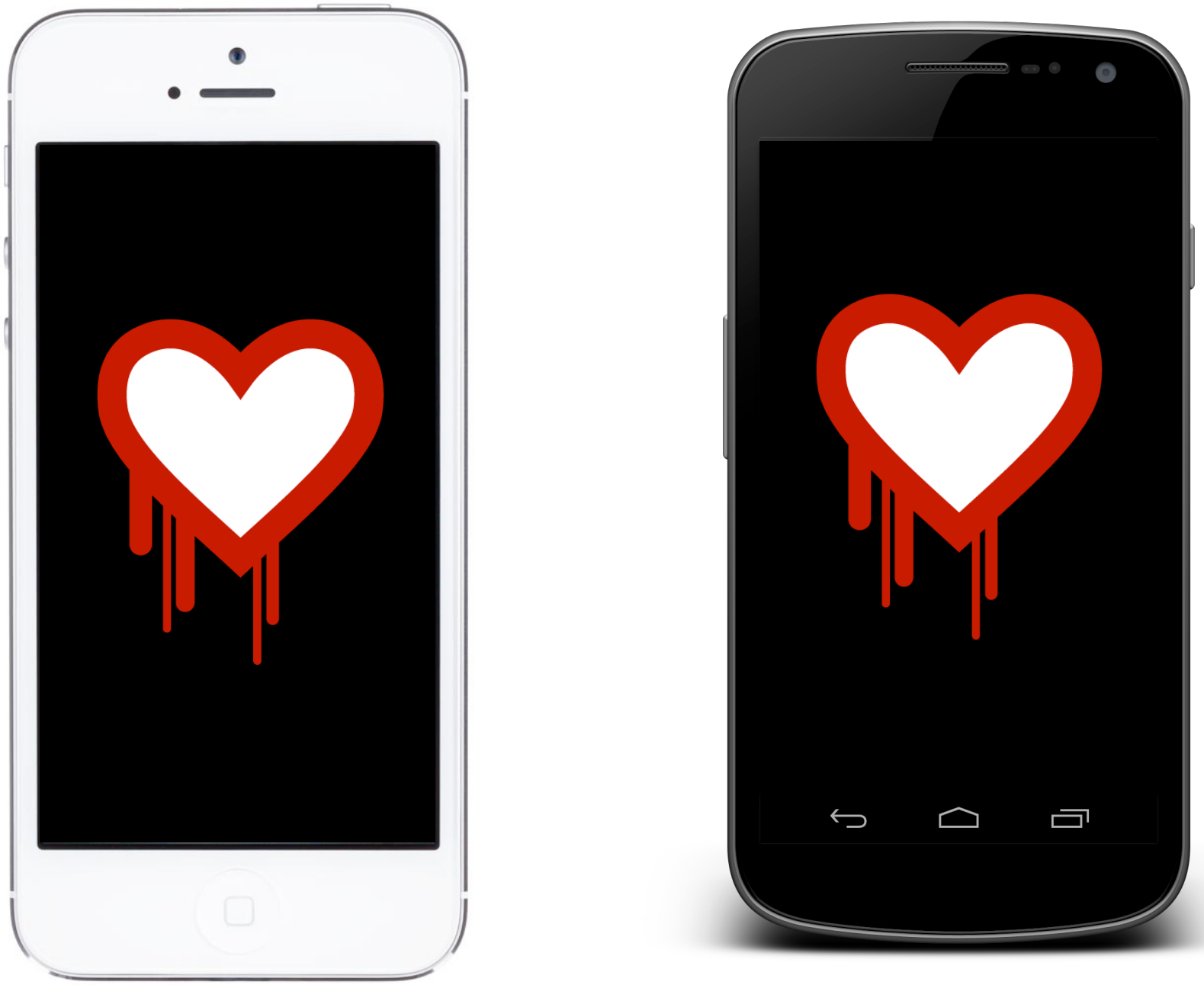


All vulnerabilities are silly!

2014


KEEP
CALM
AND
goto fail;
goto fail;


{ ; } ;




bash
Shellshock


goto fail;
goto fail;


I
SSL

$1 billion

Proposed Resolution

No further advances in research and education are necessary.

It's up to you, industry.

No further advances in research and education are necessary.

It's up to you, users.

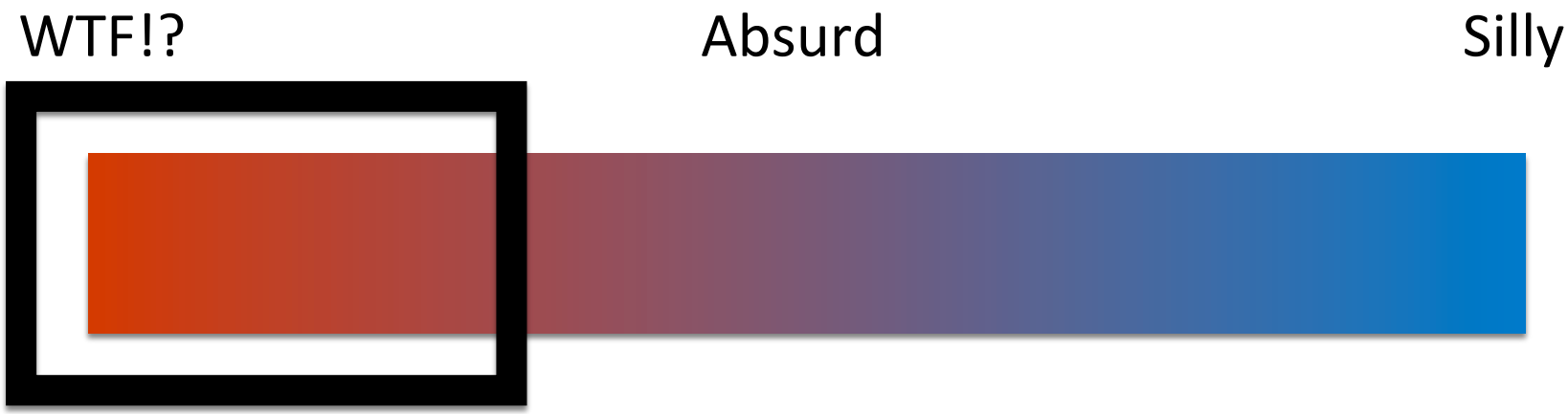
ΔResearch

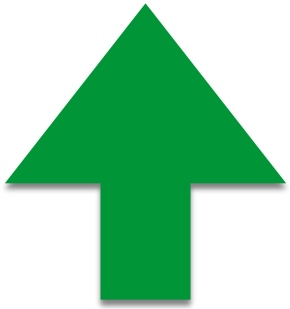
Static analysis

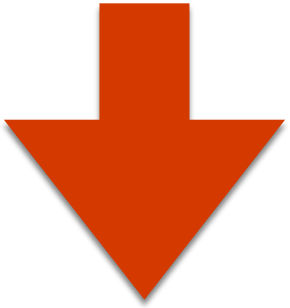
Spectrum of silliness

WTF!? Absurd Silly

Spectrum of silliness







Usability

False neg.

Scalability

False pos.


coverity®


FORTIFY
SOFTWARE

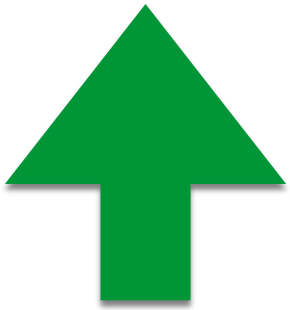

VERACODE

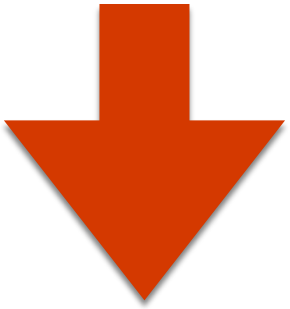

PARASOFT®


GRAMMATECH


klocwork®

Formal methods



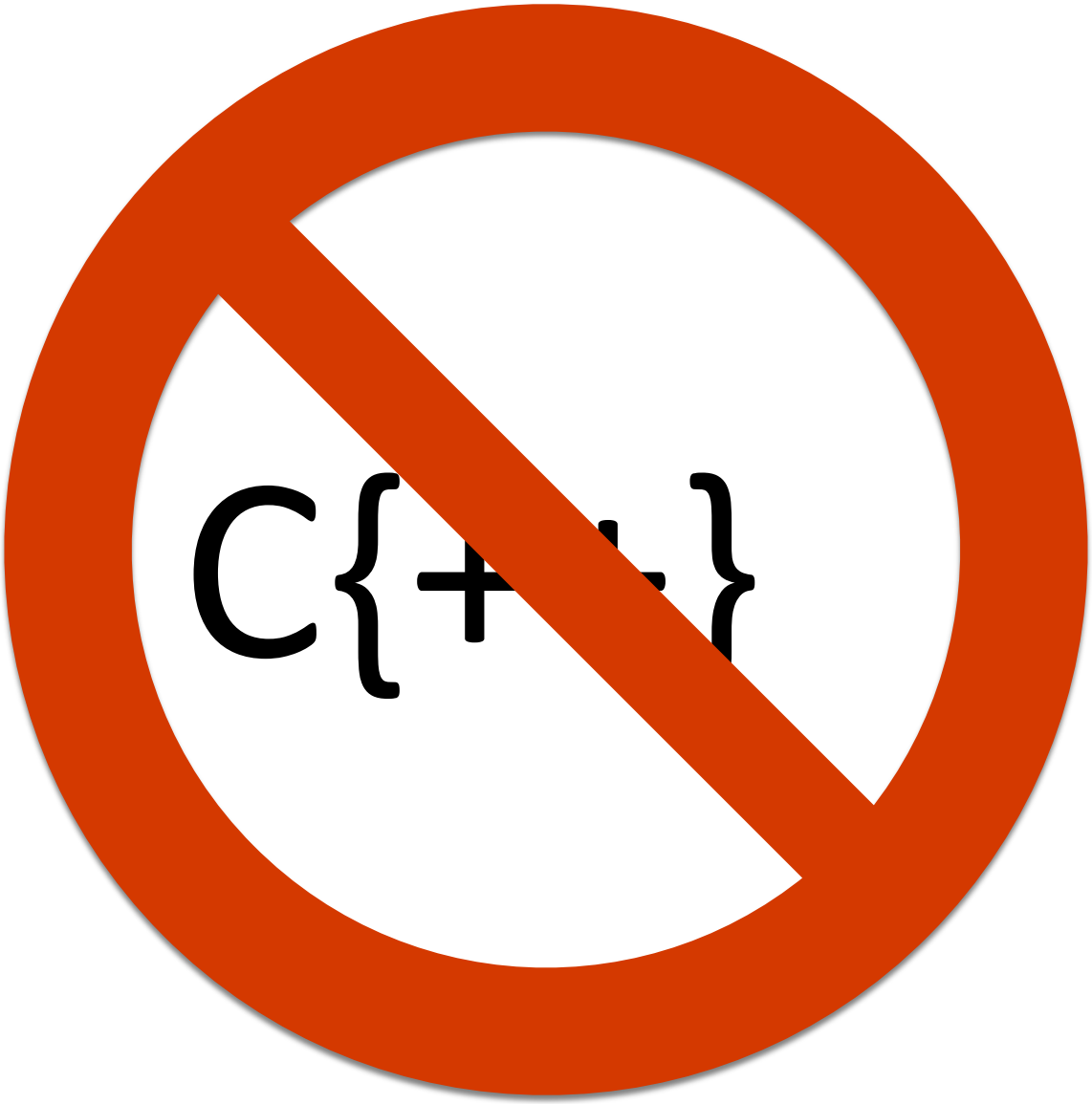


Scalability

Domain expert

Cost

Languages

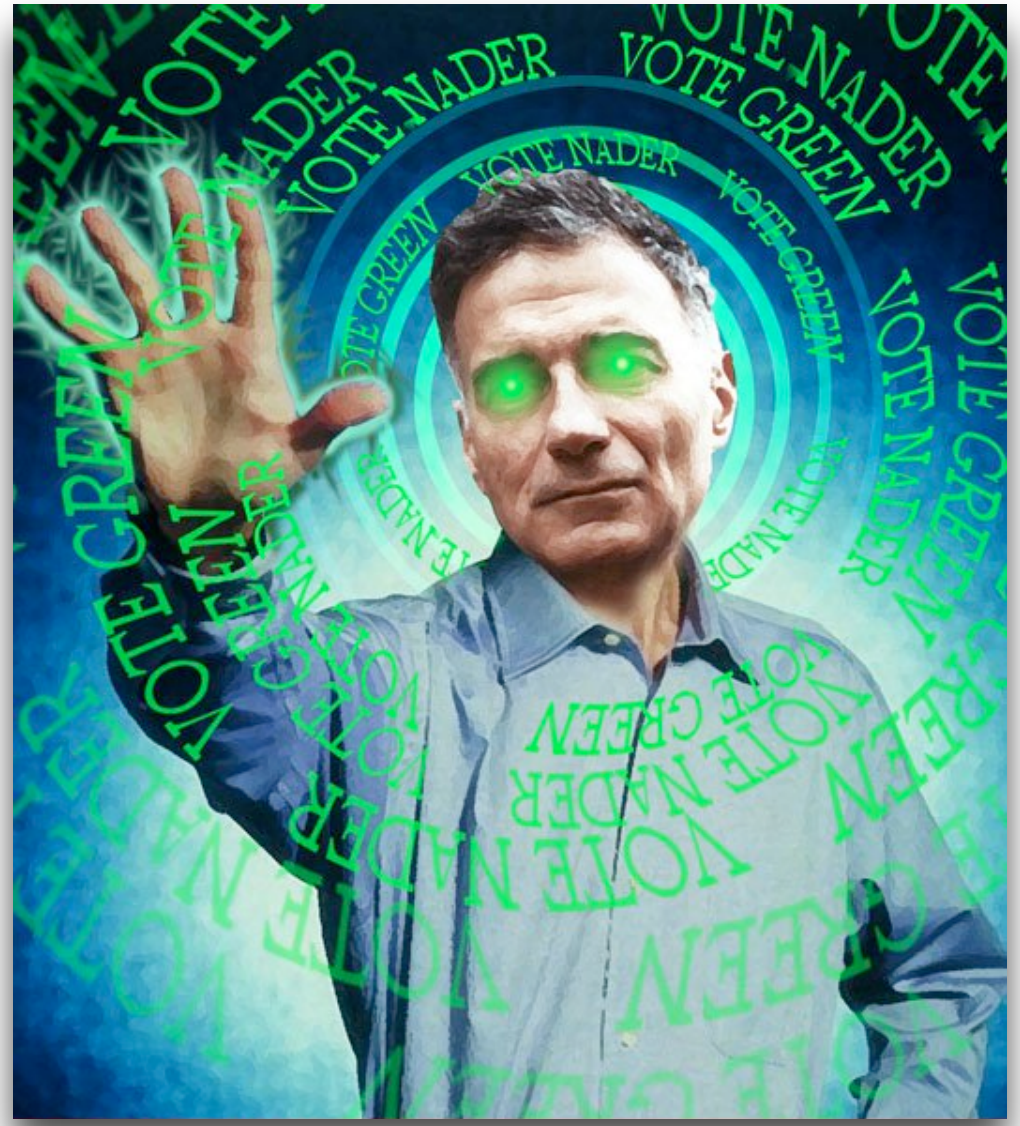

C{++}

ΔEducation

Cross-cutting & Standalone

Security from the start

ΔIncentives



Cyber Ralph Nader

Civil liability for software

Much less vulnerabilities.

Much less software.

Thanks!

Breakout 11:
Human Factors

Damon McCoy
George Mason University

Cyber Insurance

- Deal with security problem by purchasing insurance
- Problem is there is insufficient data to model risk
- “actuary tables” for cyber security would be useful
- Understanding distribution of payouts

Incentivizing Users

- Maybe we could pay users $5 dollars to do X and improve their security
- Problem is we don't know what X should be
- Need better understanding of what effects security outcomes

Teachable Moments

- Warning notices that explain why purchasing from spam is harmful
  - Display at the moment the user is about to visit merchant site
- Does notification work encourage remediation
  - What can be done to improve the effectiveness?

Breakout 12:
Architecture

Ruby Lee (Princeton University)
Gookwon (Ed) Suh (Cornell University)

Starting questions

1) What are the best opportunities today for architecture-focused security research?
2) What problems in hardware, software and network security can best be addressed by architectural changes or new architecture?
3) How should smartphone, IoT and cloud computing servers be designed to improve cyber security?
4) How should researchers in different domains collaborate with architecture researchers on security problems?
5) What are the application domains where "architecture support for security" can make the most impact?
6) What are the challenges and opportunities in designing and building hardware architecture that we can trust?

Discussion Topic and Direction

- What are the best opportunities for architecture-focused security research?
- The term "architecture" was broadly defined
  - HW, SW, network architecture
- The discussion was focused more on opportunities for *hardware* architecture to enhance security
- HW has both strengths and weaknesses
  - Strengths: 1) real-time, 2) difficult to bypass, 3) difficult to tamper with, 4) performance, energy efficiency
  - Weaknesses: 1) sematic gap, 2) difficult to fix
  - What are the right set of hardware security primitives?

Architecture Research Needs

- Hardware to guarantee critical security and privacy properties even when software layers are compromised, especially for safety-critical applications
- Threat models and security requirements for emerging application spaces such as smartphone, cloud, IoT, CPS, etc.
  - Rethink existing hardware security architecture
- Hardware design methodology and assurance
  - Improve both security and performance
  - Tools and metrics to verify the security of hardware-software designs
  - Tools and platform support to build custom secure architecture
- Facilitate tight interdisciplinary collaborations
  - HW architecture and security communities
- Common infrastructure for security architecture research
  - Open-source SoC HW, security benchmarks, and attack suites

More Research Directions

- How to secure complex heterogeneous SoCs?
  - Many processing elements, untrusted IPs
- How to provide end-to-end security including humans and communications
  - Secure I/O and user interfaces
- How to leverage parallel resources in many-core processors for security?
- What's the implications of emerging nanotechnologies for security? How do we leverage them for security?
- How to authenticate hardware?