Cyber Security and Science
(A technical perspective)

Peter Weinberger
pjw@google.com

March 2, 2011

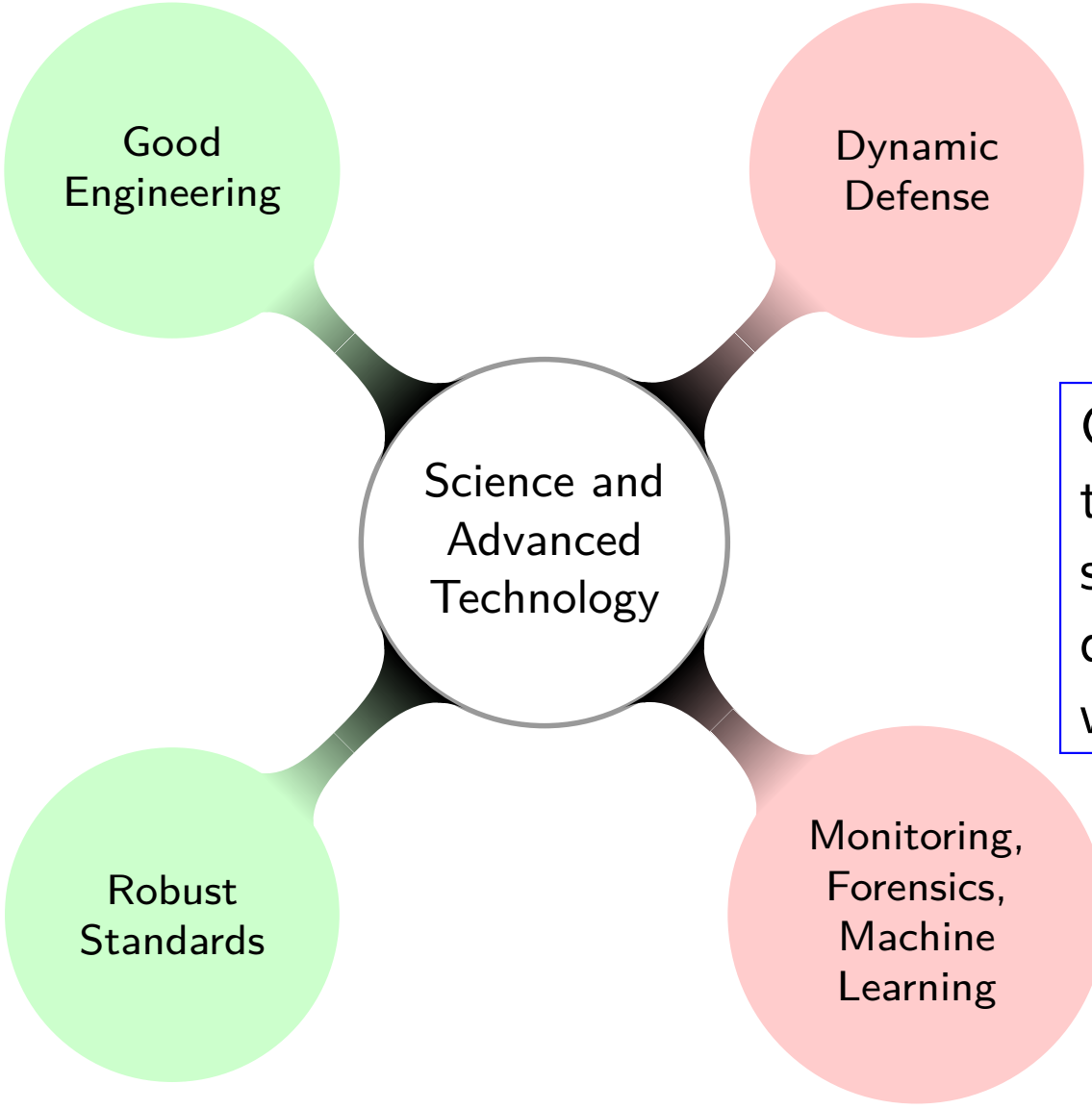
These opinions are only mine, no one else's

and even then, only today. They may change at any time.

What won't change:

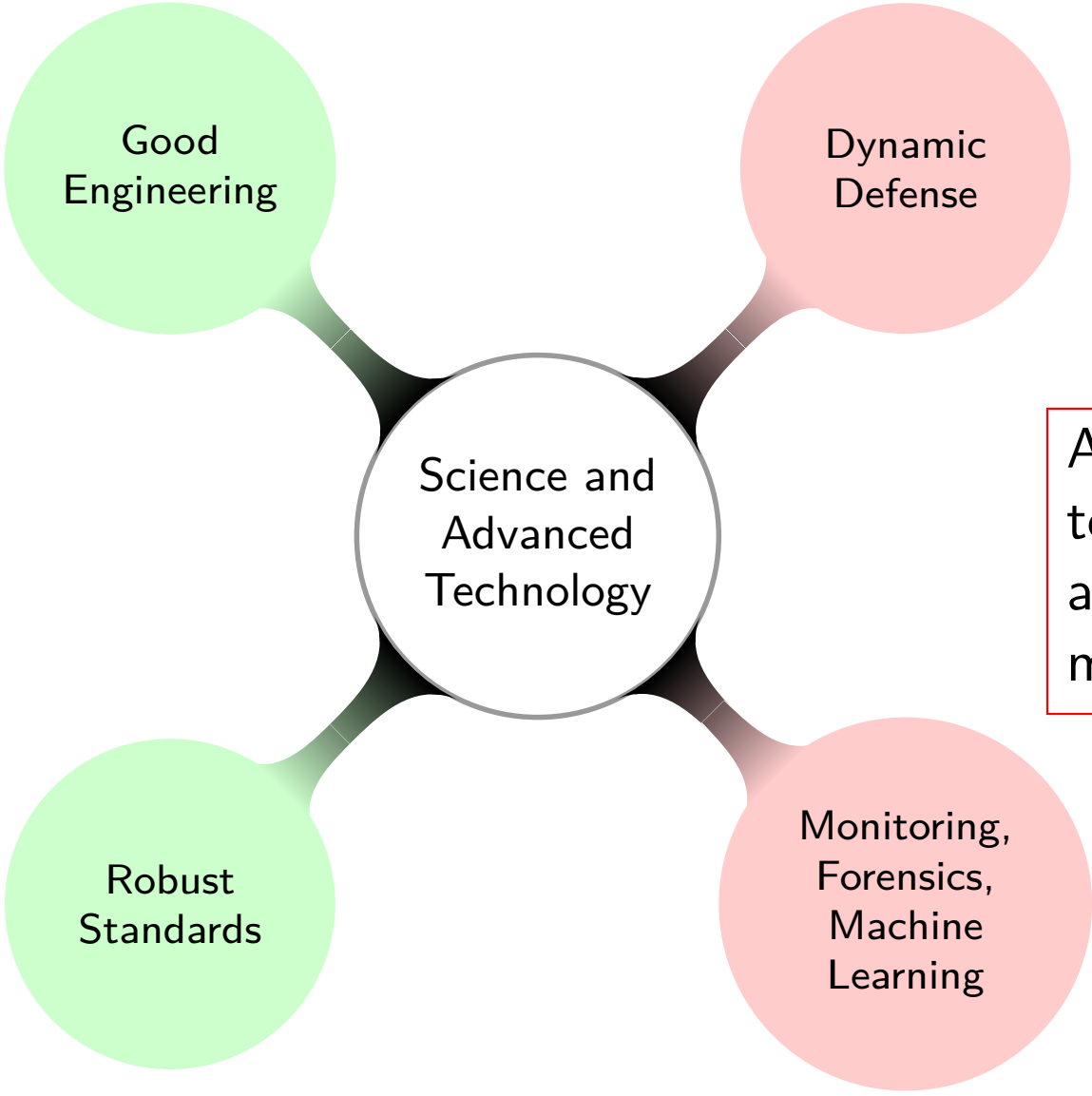
- Cyber security is a manageable problem
- There is a desperate need for a variety of fundamental work (and a lot of it)

The technical picture



Green (left) raises the general level of security. Red (right) deals with the real world.

The technical picture



And then you need to understand the adversary's business model. (goals)

As Don Knuth said:

Computer science is largely concerned with an understanding of how low-level details make it possible to achieve high-level goals.

This is certainly true for security.

‘Advanced Techology’ includes engineering

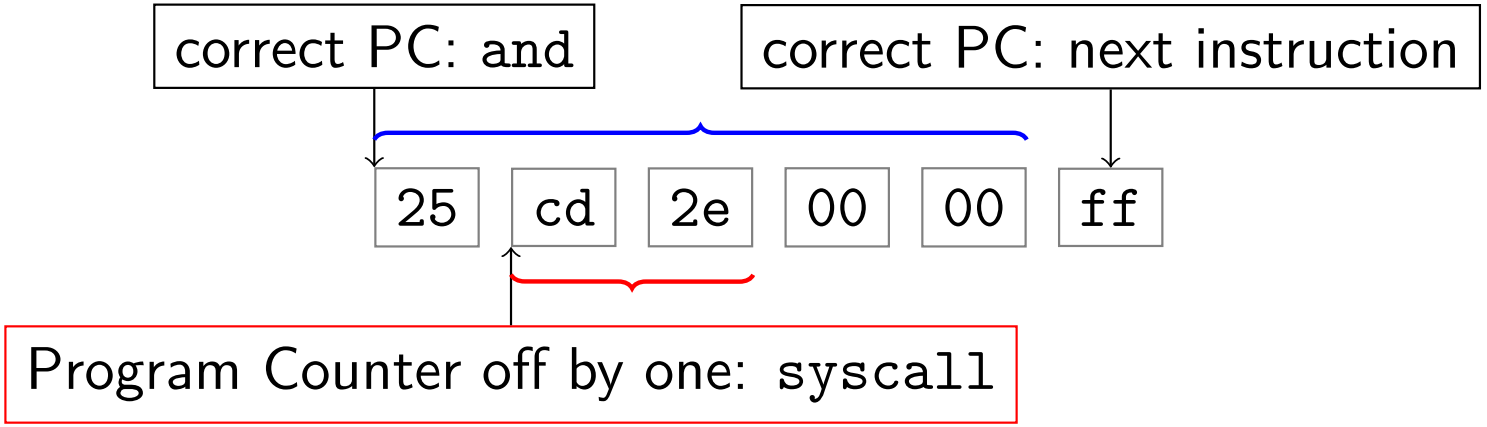
- We live in a world that requires compromises
- Consider numeric data types in programs
- Surely two numbers of the same type are either equal or not

```
class  Eq a  where
    (==), (/=) :: a -> a -> Bool

       -- Minimal complete definition:
       --      (==) or (/=)
    x /= y      =  not (x == y)
    x == y      =  not (x /= y)
```

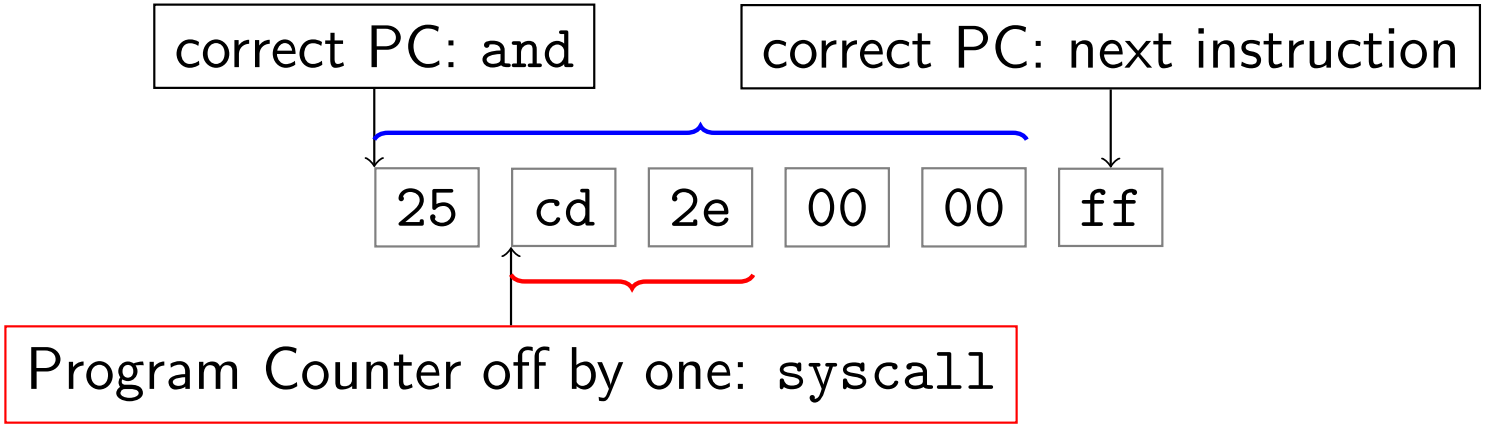
But even in Haskell, RealFloat is in Eq, but NaNs $(0.0/0.0.)$ are unequal to everything, including themselves. (And don’t even ask about C++.)

Just one bit is enough



- These attacks subvert programmer-assumed properties.
- Lots of ways of getting bad code onto machines start this way.

Just one bit is enough



- These attacks subvert programmer-assumed properties.
- Lots of ways of getting bad code onto machines start this way.
- Almost all of these attacks could be avoided by not using C.
- Researchers have many approaches, with varying practicality.
- Microsoft chose a few of these (ASLR, no-exec stack, etc).
- ASLR a kind of randomization of memory addresses.
- We're still seeing some memory corruption attacks, alas.
- And randomization is used by attackers too.

Cyber security is a peculiar problem

Generally security only gets worse over time

- ATM Skimmers
- House keys and lock bumping

Some of the issues are unique

- We don't know what 'secure' means (bad)
- The whole field is a human construct (good)
- The adversaries are adaptive and intelligent (bad)
  - Perhaps they can be deterred
- Compared to other sorts of infrastructure, change is rapid.

Cyber security is a peculiar problem

Generally security only gets worse over time

- ATM Skimmers
- House keys and lock bumping

Some of the issues are unique

- We don't know what 'secure' means (bad)
- The whole field is a human construct (good)
- The adversaries are adaptive and intelligent (bad)
  - Perhaps they can be deterred
- Compared to other sorts of infrastructure, change is rapid.

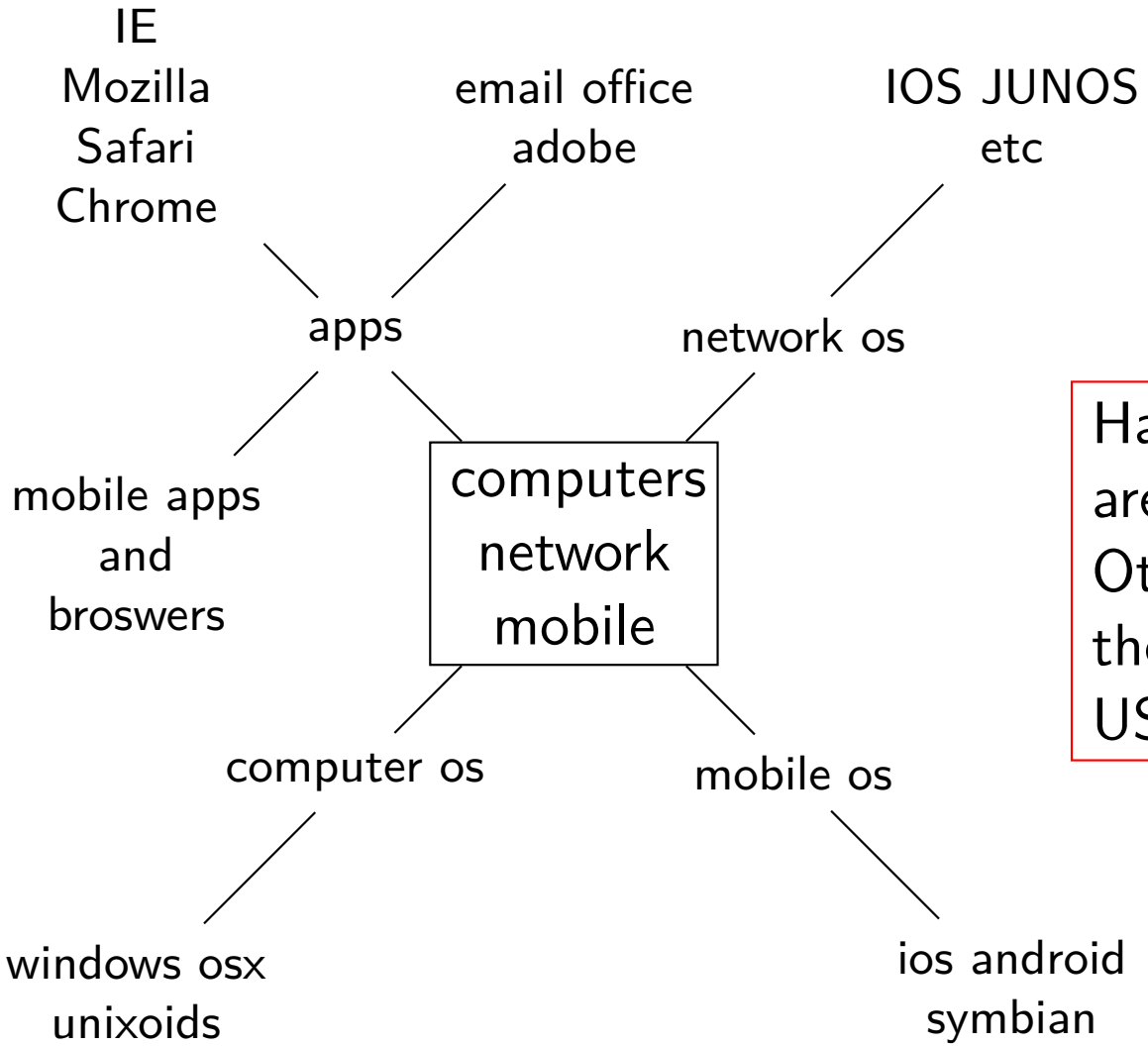
How well can we expect to do (cf health, or crime, or agriculture)?

- The bad guys are doing R&D, so we'd better.
- What are the tools of civilization?

New technologies bring new opportunities all around

- Cloud (whatever definition): churn and observation
- Browsers
  - Malleable virtual operating system (standards based, limited backwards compatibility problems)
  - Apply knowledge and techniques too radical for lower layers
- Whole new areas
  - Cell phones (e.g., malware pre-installed)
  - Wireless everywhere
  - Power meters and smart grid
  - Multi-core CPU architectures
- Complexity is not decreasing
  - Cell phones bridge WiFi and cellular network, bypassing your WiFi firewall

Who will bring us better security?



Hardware, Huawei are done overseas. Otherwise most of these companies are US.

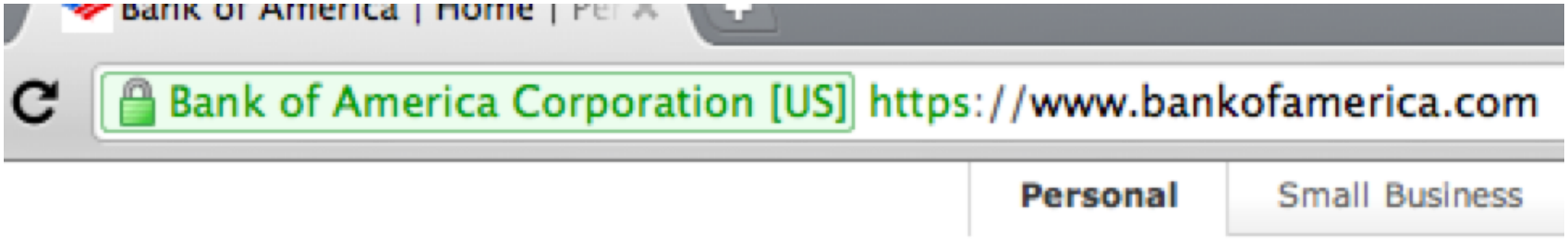
Who will bring better security?

- The general level of security is going to be improved (or not) depending on what these players do
- The security specialists will provide services that deal with day-to-day exigencies
- And big ISPs offer security services
- and what is the role of government? (precedents are uninspiring: effective regulation of new technology takes a generation or so) Funding!!!
- Anti-virus vendors make a useful thought experiment
  - Useless against sophisticated attacks.
  - Important against re-used attacks.
  - But that's not what their marketing says.

For instance, how could browsers help?

They could make sure you understand how you are connected:

They could make sure you understand who you are connected to:



- And they could warn you about sites that contain malware.
- Webmail already handles spam pretty well.
  - And law enforcement has helped (temporarily each time) with big actors
- Webmail could warn you about spear phishing. (SPF, DKIM)
- `secbrowsing.appspot.com` tells you about doubtful plugins

A sketch of some science

Improve things all around

- Clear concepts (cryptography)
- Formal methods (Bug or necessary feature?) (M won't do P)
- Model checking and bug finding (DNSSEC and HTML5, Tunisian stealing passwords)
- Game theory (801.11 ad hoc networks)
- Randomization (ASLR)

React to events

- Machine learning (epidemiology example)
- Dynamic defense (speculative)

Cryptography—Crucial to secure networking

Public key encryption game

- Challenger created key, sends public key to Adversary
- Adversary send two distinct messages X, Y to Challenger
- Challenger picks one at random, say Z,
- Challenger encrypts Z and sends it to Adversary
- Can Adversary tell if Z came from X with probability $> 1/2$?

Provide precisely quantifiable notions of security. Same framework even for quantum computers, should they ever exist.

- Homomorphic encryption

Further opportunities for research

- Systems that present a lot of uncertainty to attackers
  - Can the defense adapt faster than the attackers?
  - E.g., randomization, virtualized rapid restart, heterogeneity
- Building secure systems out of insecure components
  - E.g., multiple paths, auditing, checkpoints, virtualization
- Knowing the security state of a system by observation
  - External observations, internal observations
  - Are you doing what you claim to be?
  - Multiple observations separated in time or space

And the cyber answer is?

- It's a manageable problem because we can see almost everything, if we look (it's a lot simpler than health)
- The big players will make the most difference (d'oh)
- Substantial resources required (don't ask, I don't know)
- Intrinsically a technical field: adversaries do R&D, so must the forces of civilization
- Improve the security baseline and deal with day-to-day
- All the technology in the world won't make up for bad human factors

A recent report worth reading (after the meeting)

Search for "Reducing Systemic Cybersecurity Risk"

http://www.oecd.org/dataoecd/57/44/46889922.pdf

"We should not forget that many of the countries that are havens for cybercrime have invested billions in domestic communications monitoring to supplement an already extensive set of police tools for political control. The notion that a cybercriminal in one of these countries operates without the knowledge and thus tacit consent of the government is difficult to accept."