Cyber Security and Science

Peter Weinberger
pjw@google.com

Feb 9, 2011

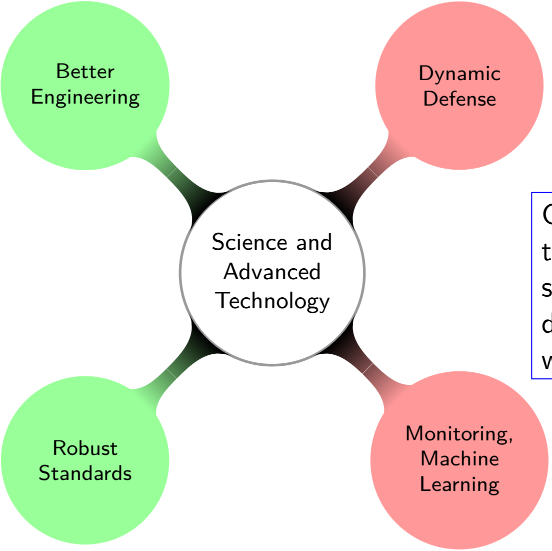
These opinions are only mine, no one else's

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

Protecting intellectual property requires securing access

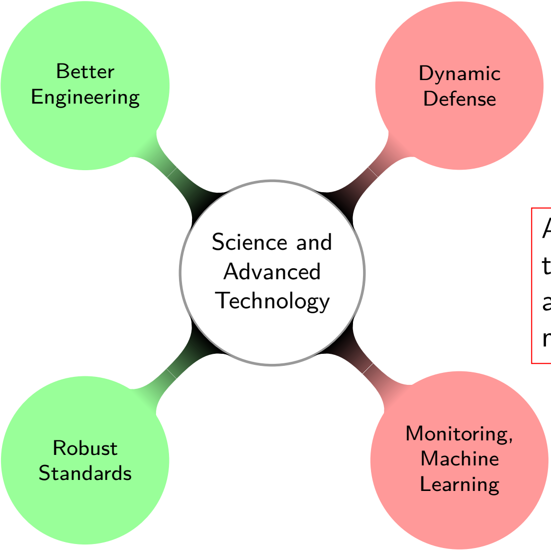
- How were HTTPS passwords being stolen in Tunisia? Why?
- Changed threat: it's not simple passwords but reused ones
- Passwords are not enough. Need:
- 2nd factor
- Time-limited credential generated
- Generated credential bound to one machine
- Internal firewalls and checks
- and a sound methodology for vetting the security of all this

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)

Cyber security is a peculiar problem

Generally security only gets worse over time

- ATM Skimmers
- House keys and lock bumping (look it up)

Some of the cyber 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

A useful metaphor is human health

- Sanitation, building codes, food regulations
- Vaccination, public health, mosquito abatement
- Doctors, drugs, hospitals, nurses
- Darwinian adversaries, large research budgets
- Limited goals
- Personnel issues in education and training
- and seat belts, smoking regulation, and many more

The Chinese View

(王晨: 关于我国互联网发展和管 April 29, 2010)

On the development and management of the internet in our country
http://www.ce.cn/xwzx/gnsz/gdxw/201006/08/t20100608_21493632.shtm
(or hric.org)

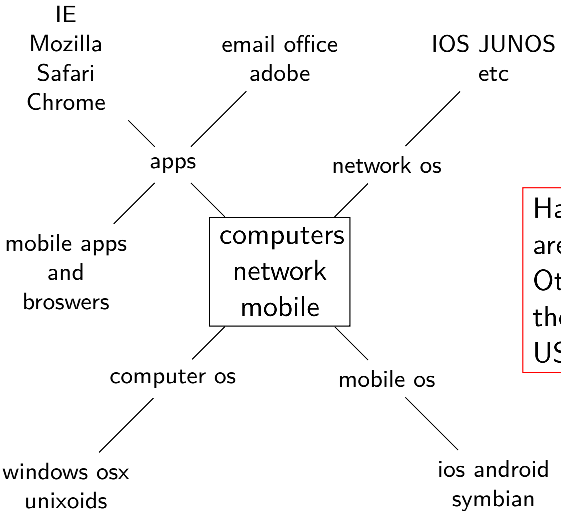
"Internet security problems are becoming more conspicuous with each passing day. Online information such as pornography and obscenities are seriously harming the physical and mental health of minors. Criminal activities such as online fraud and theft are seriously harming public security. Computer viruses and hacker attacks are posing serious threats to the security of the operation of the Internet. Leaking of secrets via the Internet is posing serious threats to national security and interests"

William Lynn's view

"On the other hand, I don't know how any of these things work, and I pretty much left off the technical side when I couldn't learn to program my VCR. So the technical side of this is not going to be my strength. But I want to talk a bit about the attributes of the thr co t the t. And in the article – and I'll start here, too – I started with an incident which was a seminal moment for cybersecurity in the Pentagon. It was an intrusion in 2008 into our networks, and that intrusion extended to our classified networks. And we did not think our classified networks could be penetrated to that point. So it was – it was a fairly shocking development. It happened with a thumb drive transferring data from the unclassified networks to the classified networks, happened in the Middle East."

THIS ATTACK WOULD NOT HAVE SUCCEEDED IF THOSE SYSTEMS HAD BEEN PATCHED

Who can bring better security?



IE
Mozilla
Safari
Chrome

email office
adobe

IOS JUNOS
etc

apps

network os

mobile apps
and
broswers

computers
network
mobile

computer os

mobile os

windows osx
unixoids

ios android
symbian

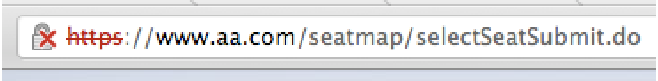
Hardware, Huawei are done overseas. Otherwise most of these companies are US.

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)
- Anti-virus vendors make a useful thought experiment

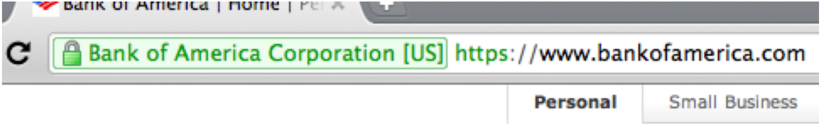
For instance, browsers could help

They could make sure you understand how you are connected:



~~https~~://www.aa.com/seatmap/selectSeatSubmit.do

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



Bank of America | Home | Pe

Bank of America Corporation [US] https://www.bankofamerica.com

- 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

New technologies bring new opportunities for users and adversaries (and defenders)

- 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

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)
- 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 depending on the public key algorithm and the computational capabilities of the Adversary

- Proxy re-encryption
- Homomorphic encryption

Experiments?

- The goal of experiments ought to be generalizable knowledge
- There are non-experimental sciences (astronomy, epidemiology)
- There are non-quantitative sciences too (medicine)
- Sure it's complicated, but so is the world of biology
- Security metrics will be an adapting field (or useless)
- What can be learned from a series of test ranges? (possibly of increasing size)

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