The battle for a safer Internet

Vint Cerf

Silicon Flatirons

February 2018

Touch Points

- Safety, Privacy, Security in Cyberspace
  - These are shared responsibilities
  - Users have a key role (no pun intended)
  - The role of liability and law (think: seatbelts)
- It all starts with buggy software
  - Sneakernet: infected diskettes
  - Lousy programming tools (and languages?)

More Touchpoints

- Hardware-reinforced security
  - Project MAC (rings of protection, virtual memory)
  - X86 chipsets still have rings but unused (?)
  - Signed bootstrap checking (ESF success)
  - Trusted Computing Base/Modules
  - 2-Factor Authentication (scaling!)
  - Continuous HW Monitoring/logging/auditing?
  - We need more of this

Cloud Computing

- Consistent software environment
  - Uniformity (well, much of the time)
  - Timely and complete software updates
  - Consistent data distribution and replication
    - (this is really HARD)
- Continuous Monitoring/logging/auditing
- Serious Backup Exercises
  - Google: DiRT for a week
  - http://queue.acm.org/detail.cfm?id=2371516

About Safety

- Do we need a cyber-fire department?
  - Private sector needs somewhere to turn for help
  - Appealing metaphor but has some glitches
  - Company A calls cyber-fire department for Company B (anti-competitive scenario)
  - Fire Department can break in the roof and windows and pour water into the building even if it ruins stuff

More About Safety

- Do we need an Internet ”Driver’s License”?
- How will we deal with ”fake news” and, more generally, misinformation (deliberate or out of ignorance)?
- What is the role of critical thinking? Can we teach it?
- Can algorithms help? Much?

About Security

- Is there an irreducible level of inconvenience?
- How can we make good practices easier?
- Will a Cyber-Hotline and anti-hacking treaty really help?
- Original Internet Security Model was end/end
  - Did you know the NSA helped with this?
- How do we deal with malware and DDOS attacks?

Internet of Things/Everything

- Scaling – billions of devices
  - What happens when you move and bring 200 devices into a house with 200 existing ones?
- Software updating is vital. How?
- Big privacy issues (even temperature data!)
- Ephemeral access to personal data
  - Fire and police department examples
  - Medical emergency example

Internet of Everything - 2

- Strong Authentication is necessary
  - Devices only talk to authorized and authenticated sources/sinks
  - Users want to grant/revoke controlled third-party access
  - Anonymity is sometimes good but sometimes you really need to KNOW who/what you are talking to.

Things that still worry me

- Security Practices Recommendations
  - Often overly high level
  - Very hard to measure effectiveness
  - Reward for good documentation of possibly poor practices
- Assumptions
  - Every time I screw up it is because I made a bad assumption
  - Take nothing for granted

Roundup

- We all have to get our security act together
- Private sector needs better tools and incentives
- Cyber-insurance doesn’t fix vulnerabilities
- Liability and consequences for bad practices