We are losing this battle

Vint Cerf
Google
October 2015
Touchpoints

• 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)
  – Google ATAP VAULT chipset
  – 2-Factor Authentication
  – 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
Cloud Computing - 2

• Virtual Machines and Containers
  – Increased isolation of user processes
  – Portability across Clouds (redundancy)
  – Preservation of old operating systems/apps
    • RANT: Digital Dark Age and Bit Rot
    • OLIVE project (CMU)
    • This rant could go on for a while...
About Safety

• Do we need a cyber-fire department?
  – 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
  – Private sector needs somewhere to turn for help
About Security

• Is there an irreducible level of inconvenience?
• How can we make good practices easier?
• Will TLA+ and COQ help with SW specs?
• Will a Cyber-Hotline and anti-hacking treaty really help?
• Certificate Authority compromise. (DANE?)
• Original Internet Security Model was end/end
  – Did you know the NSA helped with this?
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.
Practices that seem important

- Religious about post-mortems
- Continuous Monitoring
- Audit trails
- Protection of user information confidentiality (firing offenses)
- Ease of ability to invoke security features (e.g. SSL)
- 2-Factor and other Strong Authentication
- Reward for bug finding/reporting
- Open Source Scrutiny
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