Ethics, Computer Science and the Internet of Things

Vint Cerf

UVA

May 2019

From the User's Point of View

- Users expect products to just work

- They expect intuitive user interfaces (but don't always get them)

- They expect commonality among our products and interworking of our IOT offerings

- They want: Safety, Reliability, Privacy, Security, Ease of Use, and autonomy (ie, house works even if Internet is disconnected)

- They don't want a debate with an AI bot about which light to turn on

- Proposal: let's evaluate product offerings as users see them, not as engineers thinking "this is cool"

Avoid oversimplified models (Einstein…)

- User, Mobile, App, Internet, Device, Done….
- Must treat entire ecosystem
- Ensembles of devices (multiple brands?)
- Device discovery (add to system? Ignore? Forget?)
- Software updates – integrity? Validity (source?)
- Continued interoperability after updates? Rollback?
- Instrumentation for remote diagnostics, performance metrics
- Hubs/Firewalls for access control, defense against attack

More Desirable Properties

- Installation, configuration must scale (100s – 1000s of devices)
- Differentiation among users
  - Parents, kids, guests, emergency responders
  - What authorities are granted? For how long? How to rescind?
  - Note emergency responder episodic access scenarios
- What is required to add a new "user"? Drop one?
- What happens when devices are transferred to a new owner?
- What happens when a new owner takes possession of a house/office?

Security

- Paranoid operating systems
- Firewalls and filtering hubs (for defenseless devices)
- Strong authentication during commissioning, remote control, inter-device interaction (Challenge/Response Digital Handshake)
- Cryptography to protect confidentiality
- Recovery procedures/"factory resets"/Cached Configuration data

Example Ethical Commitments

- Software and hardware maintenance over expected lifetime of device
- Best efforts to avoid creating/distributing vulnerable software
  - Regression testing in realistic environments before release
- Resistance to external attacks
- Protection of privacy
- Ease of use (accessibility, usability)
- Source code escrow?

The Role of Standards

- Ontology/glossary of known actions
  - Cf. Schema.org
- Common protocols for communication, actions, etc.
- Instrumentation for evaluating performance, operational status
- Facilitation of interoperation among devices, controllers/hubs
- Common security models

Bottom Line

- We're going to put billions of these devices to work
- Some of them will get inadequate or no support after installation
- Some of them will not meet reliability, privacy and safety expectations
- Roles for regulation, industry standards/norms, consumer training
- New jobs: IOT installer, maintainer, remote diagnostician…
- This new trend could herald a utopian future or usher in a new nightmare.
- It is a shared responsibility to try for the former and avoid the latter.