Challenges to Ubiquitous Computing

Eswaran Subrahmanian
Carnegie Mellon and NIST
April 9, 2014
Virtual IOT workshop
Five aspects of Ubiquitous computing

• Definition
• Autonomous Behavior
• Technical aspects
• Privacy and security
• Economics
Ubiquitous computing

• Mark Wiser:
  • “[Devices] that weave themselves into the fabric of everyday life until they are indistinguishable from it.”
  • Computing that is available on demand, anywhere, anytime and any place without even being conscious of it.
Autonomous Behavior

• Transfer of agency
• Emergent behavior
• Electronic Transactions
• Fail safe operation – Transfer of agency
• Need for regulatory issues of limits of autonomy and liability
• IPv6: Is critical, and will require new regulations for ubiquity
Technical Challenges

• IPv6 – Encouraging widespread adoption
• Inter-operability of systems and Data
• Management and Discovery of services
• Identity management across devices/services (one could F6-USPS)
• Performance measurements and metrics for evaluation of services
Privacy and Security

- Assurance of privacy across the services and devices.
- Privacy policies can be in conflict with profile data collected by services for advertising.
- Secure communications across devices (today’s news SSL has the “heart bug”)
- The problem will get worse.
- No trust in Government and lack of complete trust of service providers also
- Regulatory and legal issues of privacy security
- Organizational information security versus individual privacy issues.
Economics

• Model of services and payment does not reflect the cost of services.
• Users give away data for free while the services are monetizing the free information by aggregation.
• There does not seem to be balance in benefits for the customers and service providers.
• Will the underlying network a private good or a public good. (net neutrality issues)
• Micropayment models will have to be explored.
Summary

• The challenges of ubiquitous computing span economics, legal, technical and agency issues.
• It is important to examine the possible consequences and challenges.
  – New legal models – looking agency and autonomy
  – New economic/business models
  – New methods for designing security into the systems instead of retrofit
  – Technology issues of compatibility/inter-operability (data and systems)