

Performance from Experience

Will Pervasive Computing be Manageable?

IEEE/IFIP Integrated Management Symposium Seattle May 17, 2001

> Richard F. Graveman +1 973 829 2532 rfg@acm.org

An SAIC Company

Questions to the Panel: #7 How will personal-privacy be affected by constant monitoring and location tracking? Information technology has already been a bonanza for "data collectors." The general public doesn't think about this much. The public sector either doesn't get it or doesn't want it to be gotten. The private sector wants data for targeted marketing, price discrimination, and bundling. →Example: Airplane tickets We have lots of choices, almost daily.



Will current security and management mechanisms scale to cater for millions of mobile computers interacting with a pervasive computing environment?

- -With proper design, the local complexity grows at most logarithmically in the size of the system.
- -There is a problem deploying security
 - •I don't think it's scaling.
 - Maybe it's "fear of scaling."



Vendors' Issues with Security

- Isn't it too much overhead to check the integrity of every packet (message, command)?
- Security is included in 2.0. Or was it 2.5?
- Key management is left to the user.
- ...



Personal IT Security and Privacy

• What can we learn from history?

-Cell phones and cordless phones

-CATV decoder boxes

- -Web browser plug-in viewer
- -ActiveX attack on Quicken

-Port scans on cable modems

-IR garage door openers

→ Everything worth hacking gets hacked.



User Acceptability Issues for Security

- Costs and expectations
- Usability
 - -Human authentication factors
 - -What users *really need to know* about security
 - -System setup and default security stance:
 - Out of the box behavior: "plug and pray"
 - -Questions, problems, errors, and help desks
 - -Gratuitous functionality



Cryptography, Software, and Hardware

- Cryptography
 - Strength, performance, exportability, implementation pitfalls, snake oil
 - -Neglected services:
 - Integrity and 2-way authentication
 - -Book: Pervasive Computing
 - Chapter on Security: 14 pages, all on crypto
- Software bugs, holes, Easter eggs, and upgrades
 - -Vendors don't know what they are shipping
- Smart cards and similar technology
 - -Giving users a good reason to attack their own cards
 - -Dealing with the "terminal problem"



Non-Technical and Partially Technical Issues

- Warrantee, liability, inspection, insurance, and disclaimer
- Copyrights, trade secrets, and reverse engineering
- Inhibitors to security
 - -Import, export, and usage restrictions
 - –UCITA and DMCA
 - -Security by obscurity



Privacy Policy

- Notification
 - -We tell you what information we keep
- Choice
 - -You can opt out without undue disadvantage
- Minimization
 - -We keep only what we have a use for
- Use
 - -We tell you all the ways it is used
- Security
 - -Here's how we protect it



Summary on Security and Privacy

- Necessary security technology exists.
- Growing acceptance that it's needed in this area.
- Still tend to be many poor designs.
- Special interests stifle progress.

→ First targets:

- -Network side: Internet and wireless
- -Content side: Money and entertainment
- Privacy is in much worse shape.
- Almost all active forces are working against it.



Will communication facilities be able to cope with the required bandwidth and give guaranteed quality of service for future mobile, multi-media traffic?

-Wireless is the issue.

- -Distinguish "short range private" from "public" networks.
- -Current US spectrum allocation needs attention.

–If we get everything else right, guaranteed QoS is not likely to be the answer.



Questions to the Panel: #2

Can we develop intelligent context-aware systems which can determine our activity and react appropriately, e.g., to distinguish a heart problem from exertion due to running for a bus?

-Progress will be surprisingly slow and surprising.



How do mobile computers locate the required services from the local environment to form *ad hoc* collaborative groups?

-This is a chance for the private sector to benefit from government research.



Questions to the Panel: #4

How can we develop self-organizing hardware and software architectures for pervasive computing?

- -This is the second question. The first question is what we need.
- -May be virtue in limiting amount of interaction.



Is there a distinction between management and normal functionality for adaptive and self-organizing systems?

-There's little intrinsic difference between management and other applications.



Questions to the Panel: #6

Will interaction techniques based on biological organisms be an appropriate solution for coherent behavior from vast numbers of unreliable sensors, actuators, and communication devices?

-That's frighteningly possible.

