

System Security for Cyborgs

Ross Anderson
Cambridge

Security for Cyborgs

- Within 20 years, people might have 50 - 100 worn or embedded devices
- Some will be tools, like phones and iPods
- Others will be medical devices, like pacemakers
- Others will cross the boundary - e.g. the heart-rate monitor that mutes your mobile phone while you're cycling
- Human beings will become the ultimate 'embedded systems'

Safety and Interaction

- If a medical device is based on Windows, and Bill ships a security patch, do you apply it and lose certification, or not patch and become vulnerable to malware?
- All infrastructure slowly becomes critical. If we lose the phone system, how many more people should be in hospital?
- If schoolteachers can't get petrol, nurses can't go to work

Are there any precedents?

- RFID - tags being added to products to monitor them in the supply chain. Problems: privacy backlash, supply chain control
- Smart dust - RF motes organize own network for environment / military monitoring
- Digital home - appliances will talk via 802.11, Bluetooth, IR, UWB. Problems: DRM, privacy...
- But the single environment that's closest to the 'ubiquitous computing' ideal of computers embedded invisibly everywhere is the car

Electronic security in cars

- Expensive cars have 40-50 CPUs, CANBUS, bluetooth, GPRS, remote firmware upgrade...
- Growing problem of feature interaction - multiple administrators / 'owners'
- Separation between safety and infotainment systems is progressively eroding
- Worries grow about platform vulnerability
- Privacy too - the combination of GSM, GPS, logging, road pricing and DRM destroys customer control of personal data



The Privacy Dilemma

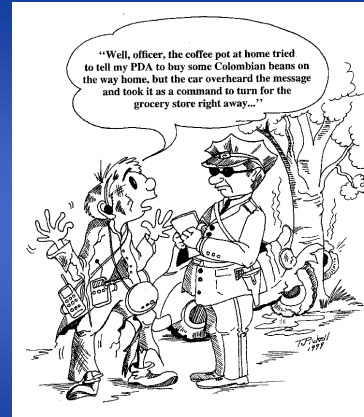
- Price discrimination is efficient in general! (e.g. if Barclays will pay 8K and Lloyds 4K for writing a report that costs me 10K)
- Technological progress deepens both the incentive and the opportunity for this
- People say that they value privacy, but behave differently (why no riots about the NPfIT?)
- Some partial explanations now available, e.g. type of goods, nature of discounting...
- Economics of privacy now a rapidly developing discipline

Odlyzko's warning

- The future home environment is likely to be more complex than today's office environment
- Home users are generally less knowledgeable
- We will need to outsource the setup and maintenance of home appliances to experts
- We will get varying levels of control, depending on skills and 'trustworthiness'
- We can already see this beginning in mobile-phone and car-electronics markets

Ubicomp and Usability

- U-Vision - embedded devices will be easy to use, thus eliminating the PC's frustrations
- More realistic view - the trade-off between flexibility and ease of use is different for different users (and same user at different times/tasks)
- 'We will still be frustrated, but at a higher level of functionality, and there will be more of us willing to be frustrated'
- Implications for safety / privacy?



Market demand for usability?

- 'Microsoft has triumphed because it has given us what we asked for: constant novelty coupled with acceptable stability, rather than the other way around. ... People talk simplicity but buy features and pay the consequences. Complex features multiply hidden costs and erode both efficiency and simplicity.' (E Tenner, 'The Microsoft We Deserve')

Usability and incentives

- User sees his phone banking app not as a Vodafone thing but a NatWest thing
- If it works, Natwest gets the credit
- If it doesn't, Vodafone gets the blame
- Incentives aren't right for the app vendor or the platform vendor
- Worse - there are half-a-dozen stages in the supply chain. Who'll do the work?

The big security challenges - usability and maintainability

- Computer scientists have spent the last 50 years building tools that help developers get further up the complexity mountain
- But the complexity that now matters is not from the CPU's viewpoint but the brain's
- Also, up till now we fixed security problems by replacement or upgrade
- But this is costly with many embedded systems - from air conditioners through electricity meters to pacemakers

Policy challenges

- As we get CPUs and communications into more and more devices, more and more industries will come to resemble the software industry
- We'll get the good (flexibility), the bad (frustration) and the ugly (monopolies)
- What will be the effects on medical ethics?
- 'Is this a safety system that helps me, or a control system that restricts me?'

Conclusion

- As humans acquire - and then become - embedded systems, there will be interesting technical challenges
- Usability and maintainability are the most obvious ones now
- There are serious policy issues too. Many incentives are misaligned; everything from privacy to competition is at stake
- Security economics will matter too