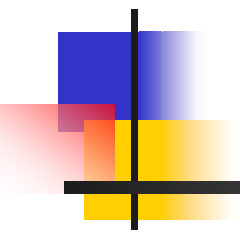
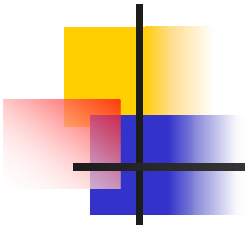


# Pervasive Computing

## Sensors Galore, Information Warfare and Death in IKEA

John A Clark
Dept. of Computer Science
University of York, UK
jac@cs.york.ac.uk

06.08.02

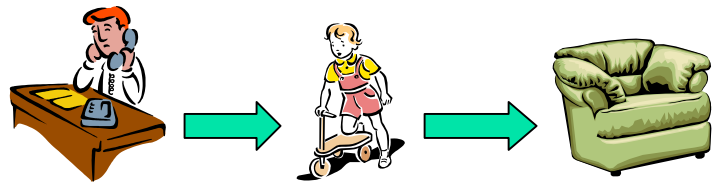


# Pervasive Computation

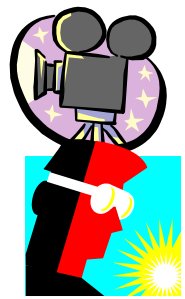
- What is Pervasive Computing?
  - **"Convenient access, through a new class of applications, to relevant information with the ability to easily take action on it when and where you need to" – IBM**
- Weisner's initial vision:
  - **Ubiquity.**
  - **Invisibility.**
- I am going to take a *slightly* non-standard view.
  - **Talk later is about requirements.**
  - **I will take a lower level view but highlight some issues such as security**

# Examples

- Integrated social environments:
  - **Smart workspaces**
  - **Smart kindergartens!**
  - **House of the future.**
  - **Retirement homes.**



- Wearable computers:
  - **Can be used as significant data collection capability.**
  - **Test beds for more integrated living and working.**



- Structural and environmental management systems
  - **Aircraft skins**
  - **Instrumented building structures**
  - **Environmental monitoring and controls systems**
  - **Medical monitoring systems.**

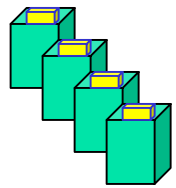
# Systems Challenges I

- **Immense Scale**:
  - Vast numbers of devices.
  - Dense instrumentation will require devices to scale down
  - In 5-10 years complete systems with storage computation, communications, sensing and energy storage could be as small as $1mm^3$.
- *Fidelity and availability will come from the quantity of partially redundant measurements and their correlation, not the indivuidual component's quality and precision.*
- As vastness increases, configuration becomes an issue (i.e. Do-It-Yourself)

**Source: Estrin, Culler, Pister and Sukhatme**

# Resources- Energy

- Energy
  - Batteries still primary resource.
    - Fuel based alternatives under research.
    - Fabrication of 1mm$^3$ lead acid batteries.

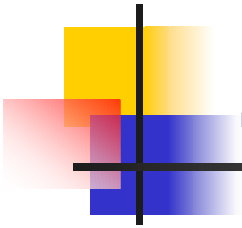


  - Harvesting is an option:
    - Can allow potentially arbitrary lifetimes but limited action per unit time.
    - Solar

    - Manual, e.g. piezo-electric generation as shoe structure is distorted (by walking)
    - Fluid flow, variants on windmills if you like
      - **Bloodmills?**

# Sensor Technology

- Sensor Technology (Micro-electromechanical systems – MEMS) is making huge progress
  - Millimetre scale accelerometers
  - Pressure sensors etc.
  - Loads testing on aircraft structures etc.
  - Standoff chemical sensors.
  - Smart detonators.
  - Harsh environment MEMS.



# Systems Challenges II

- **Limited Access**:
  - Embedded devices may be in locations that are expensive to reach with wires, difficult to maintain etc.
  - Much communication will be wireless (this has failure implications itself)
  - If cannot repair then need for self-organisation to allow flexible and resilient behaviour. 'Partial failure is the norm'.
  - Energy must be harvested from the environment in many cases.

**Source: Estrin, Culler, Pister and Sukhatme**

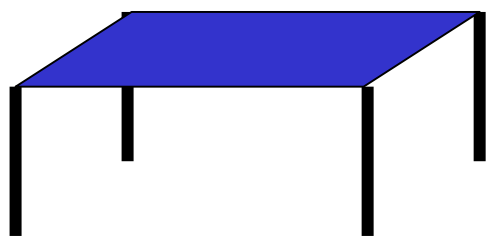
# Systems Challenges III

- **Extreme dynamics**
  - Environmental factors can affect low power RF propagation
  - Demand variation. Most of the time nothing happens.
    - Passive vigilance is punctuated by bursts of concurrency?
      - Is this an old fashioned view?
  - Systems governed by internal control loops in which components continuously adapt their individual and joint behaviour to resource and stimulus availability.

**Source: Estrin, Culler, Pister and Sukhatme**

# Resilience to the Environment

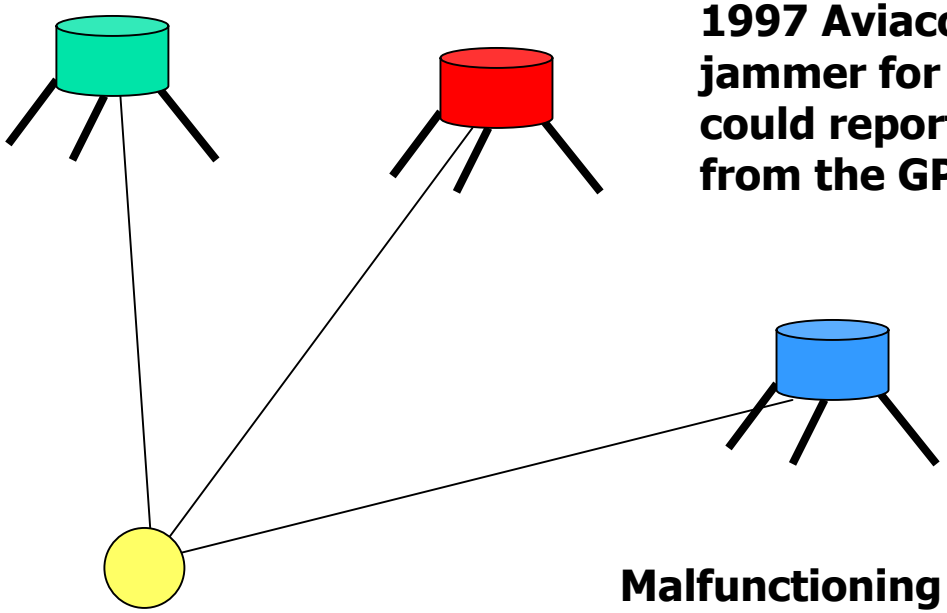
- Will need to cope with occasionally unhelpful behaviour from the environment:
  - **"There was a flash of lightning and my table dropped dead on its feet"**
  - **May need to cope with occasional jamming or disruption of operation for a while.**
  - **Older household equipment does this already**
    - **Hoover near the TV**
- Far-fetched?



**Source**: **Information Warfare *and* Security** by Dorothy Denning.

# Resilience to the Environment

Global Positioning System (GPS)

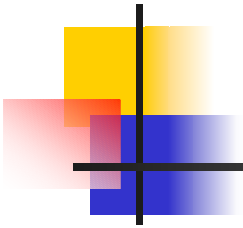


**1997 Aviaconversia announced a 4-Watt jammer for less than $4000 that could reportedly jam the microwave signals from the GPS over a 200km radius.**

**Various uses of GPs ranging from in-car auto-route through to aircraft navigation.**

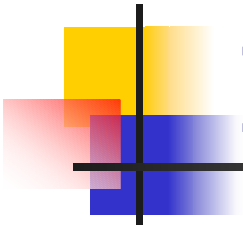
**Malfunctioning 5-Watt air force transmitter disrupted GPS over upstate New York for two weeks.**

**Source**: **Information Warfare *and* Security** by Dorothy Denning.



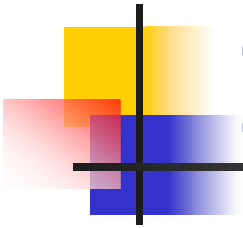
# Resilience to the Environment

- More generally failure will be the norm. This differs from the usual distributed systems philosophy.
  - Has impact for protocol development.
- Systems will need to simply accept partial failures and adapt
  - Self-organisation again.



# Invasive Computing

- **Large scale**
  - **UAV used to give back real-time feedback for the military (and satellite TV subscribers)**
- **Mid-scale**
  - **Smaller, e.g. six inch experimental equipment flying with cameras:**
    - **Military and civilian uses.**
    - **"Fast, Cheap, and Out of Control" (Rodney A. Brooks and Anita M. Flynn.)**
- **Small scale:**
  - **Rather tedious (hidden cameras).**
  - **Unhygienic. In 1997 experiments with micro-cameras surgically implanted in cockroaches.**
  - **Research projects investigating 2 inch flyers with cameras powered by microwave beam.**

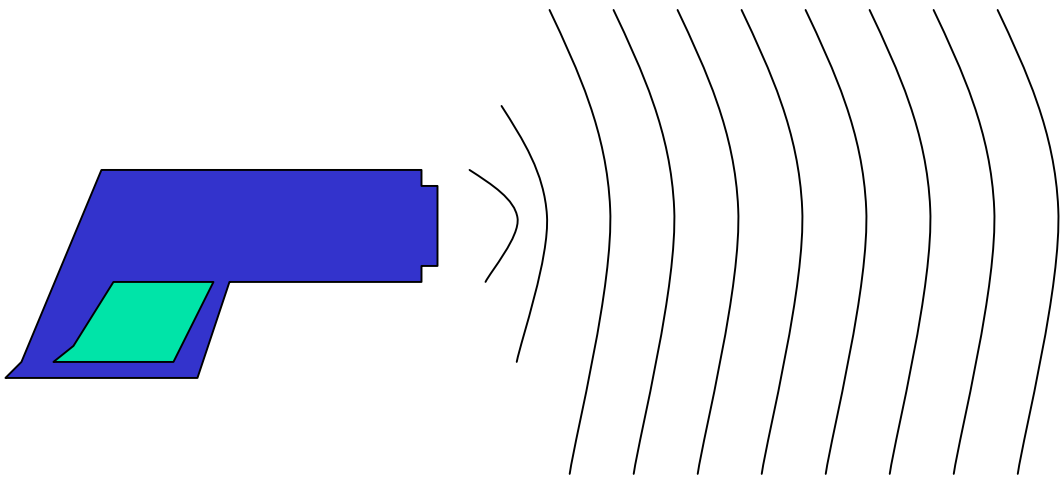


# Invasive Computing

- Invasive computing is already with us
  - Barium meals
- Materials
  - Ultrasonic
  - NMR/MRI Scanning.
- But can imagine micro-devices
  - Typical cited example is cholesterol devouring nanites in the arteries
    - See earlier bloodmills comment.
  - General instrumentation capabilities will radically increase our knowledge.

# Radio Frequency Weapons

- **Emit electromagnetic radiation somewhere in the radio spectrum.**



- **Drive by RF-shootings? Far fetched?**

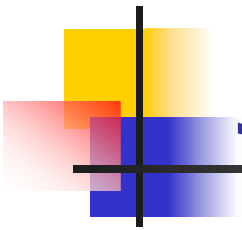
# Radio Frequency Weapons

- **Broadband: produce a sharp, pulsed electro-magnetic transient field.**
  - **High voltage spike or ringing on exposed cables and wiring – can damage or destroy semi-conductor circuits**
    - **Nuclear EMP (worst)**
    - **Flux Generator EMP**
    - **Spark Gap devices**
    - **Swedish army tests – created EMP guns from openly available materials that could permanently damage cars at 30 metres and stop their engines at 90m.**
- **Narrowband: Produce a carrier wave within a relatively narrow band. VHF, UHF or microwave.**
  - **Couple into electrical wiring or directly through gaps in chassis to set up high-voltage standing waves that can damage semiconductor circuitry**
    - **High Power Microwave (HPM) (1-35 gigahertz generating RF field strengths of tens of kilovolts per metre at distances of hundreds of metres or more)**

**Source**: **Information Warfare *and* Security** by Dorothy Denning.

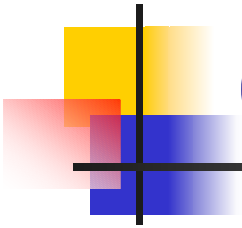
# Inbreeding Shows

- There may well be a trend to reprogrammable reusable building block technologies.
  - **We know from standard digital world that homogeneous systems are susceptible to attack.**
    - **IBM Christmas Tree virus**
  - **Heterogeneous systems may demonstrate natural partial immunity**
  - **Will standardisation lead to susceptibility to biologically-inspired attacks?**
- With the potential for global connectivity the ability for viruses to wreak havoc.
  - **IKEA virus?**
  - **Chintz cushions attack (more popular).**
  - **BMW, Mercedes-Benz, Ford car viruses?**
    - **Or more likely, exploitation of some protocol security weakness**
  - **Can fridges catch colds?**



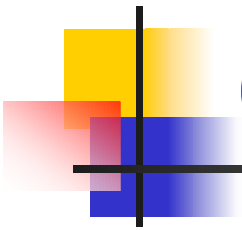
# Jabbers

- Bugs in the System:
  - Business these days may well choose to sweep offices used for important meetings.
  - When the whole environment is a sensing and broadcasting fabric this is likely to prove more troublesome.



# Other Security Issues

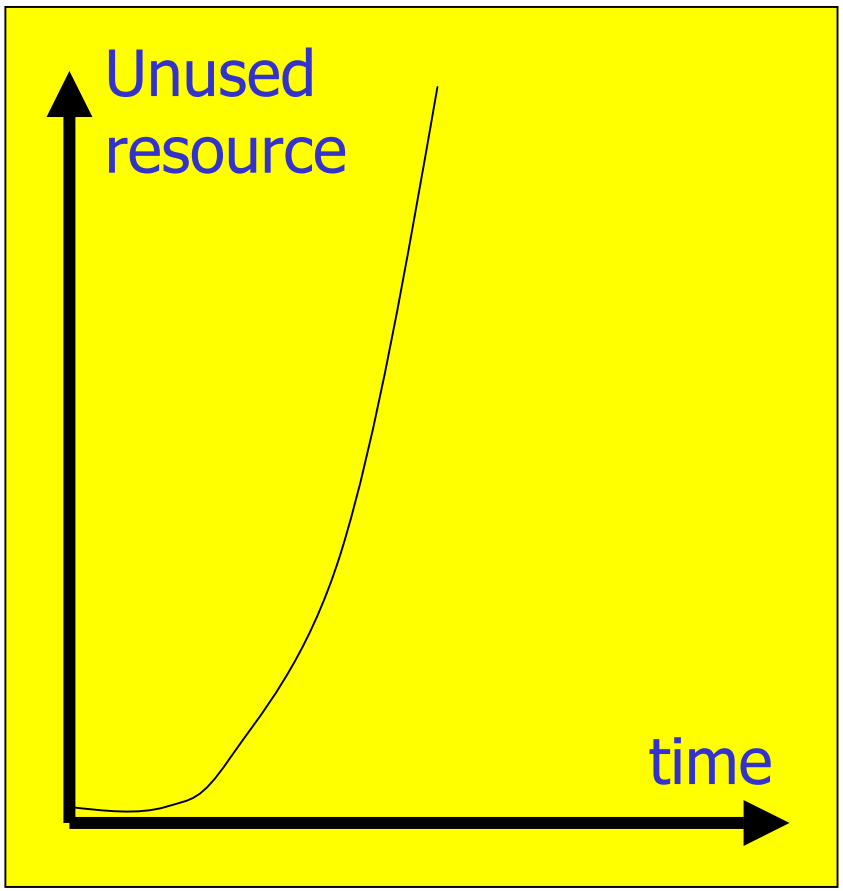
- If we ever get widely available nano-programming environments we are heading for some trouble.
  - Use of a technology=> you approve of it
  - Abuse of a technology=> you don't approve of it
- Have emphasised more info-war types of security issue. But you don't have to go that far:
  - Much security is based on old-fashioned model where you identify everyone in advance and typical enforce subject-access-object models (leads to ACLs etc.)
  - New systems will spontaneously interact and you will need to decide how to cope with this.
- Crucial here is the notion of trust.
  - What is it?
  - How is it gained and regained?
  - Role based access controls will become higher profile than present.



# Other Security Issues

- There is the notion of confidentiality which will come under increasing threat.
  - Obvious worries about broadcast media.
  - Things are pinned down anymore
    - In more IT, pervasive computing in the workplace applications, elements containing confidential data may be lost, e.g. PDAs.
    - Could be lots of information flying about generally
    - Legal issues emerging as very important in the US regarding medical data (HIPAA).
    - Stalking or aggressive location?
  - Charging!!!!!!

# Pervasive Non-computing

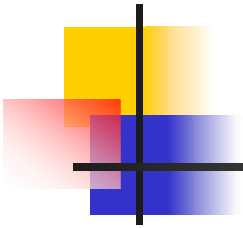



We know about Moore's Law but there would appear to be potential for a "**Idleness Law**" which details the growth of unused resources?

Pervasive computing will for the most part essentially become pervasive non-computing.

Can we do anything about this?

Never mind **The Grid** what about the **Micro-Mesh** **(nano-mesh, picomesh etc)?**



# Finally

- Perhaps a slightly eccentric take on pervasive computing.
- Challenges to deliver appropriate functionality.
- Challenges to stop others stopping you doing it.
- Have not addressed a good number of issues:
  - **What is it that you actually want these systems to do?**
    - **QoS? Utility? Degrees of approximation and tradeoffs? Who or what does what?**
  - **How can you measure/test that.**
  - **Are current systems engineering approaches appropriate?**
    - **How do you specify, design and refine a pervasive system?**
- **Oh, and if you think pervasive computing is out of this world…**
  - **It is!**
  - **And 'pico-satellites' have already been launched and tested.**