forward

http://www.ict-forward.eu/

http://www.vu.nl

Future Threats

MOBILE PERSONAL DEVICES

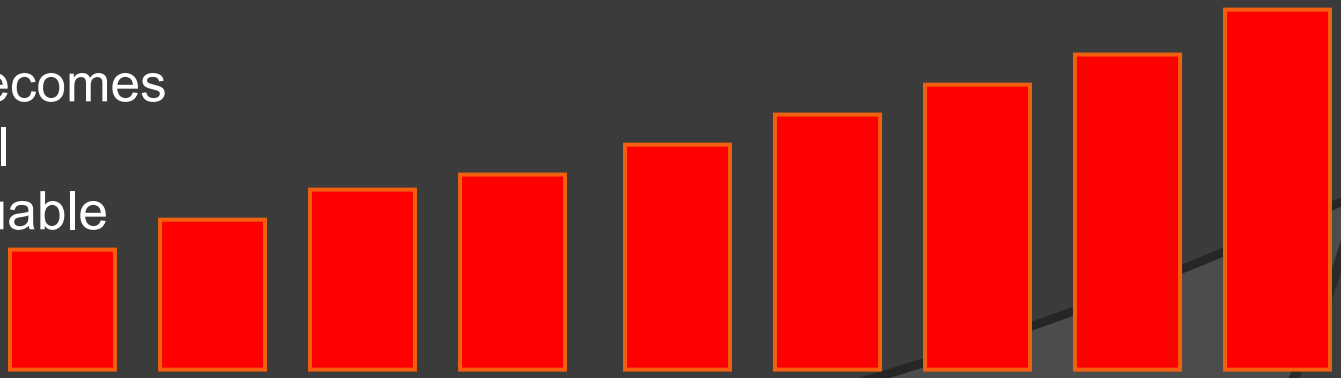
Personal Computing

Scientific data

Work related data

Work & personal data

Information becomes more personal and more valuable



Critical data you keep on your phone

- Text messages
  - E-mail, SMS
- Multimedia content
  - Photos, videos, audio recordings
- Critical saved information
  - PIN, Credit card numbers, passwords
- Money
  - Pay for parking, metro, groceries

Critical data your phone keeps on you

- Location
  - Not a provider privilege anymore
  - Directly provided by GPS
  - Think of a different twitter
    - *John is at the red light district*
    - *John is at the bulldog coffeeshop*
    - *John is at home with his wife*
- Call history

Threats: What could someone do with your phone

- Steal information
  - Saved information, messages
- Spy
  - Listen in
- Place calls
  - Back from the past, calling 0900 numbers in Australia can make a profit
- Ask for ransom
  - Pay me 10$ or your phone is toast

What does the future hold?

- More Internet enabled devices
  - “Is my fridge running up-to-date software?”
- Smart-phones may become a global remote control
  - “Well, I always carry it with me”
- More powerful devices
  - Uses always want to do more, but so do attackers

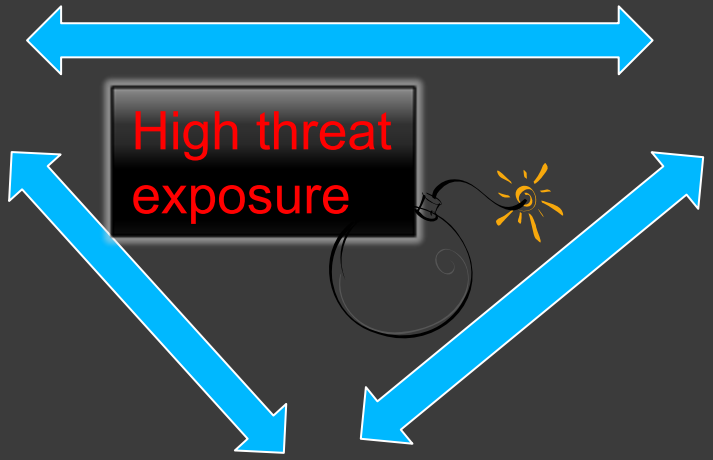
Security Challenges

Mobility

Device Differences

High mobility

HOME



OFFICE

ROAD

Device differences

- Limited resources
  - RAM
  - CPU
  - Battery
- Architecture differences
- Face more dangers from physical environment

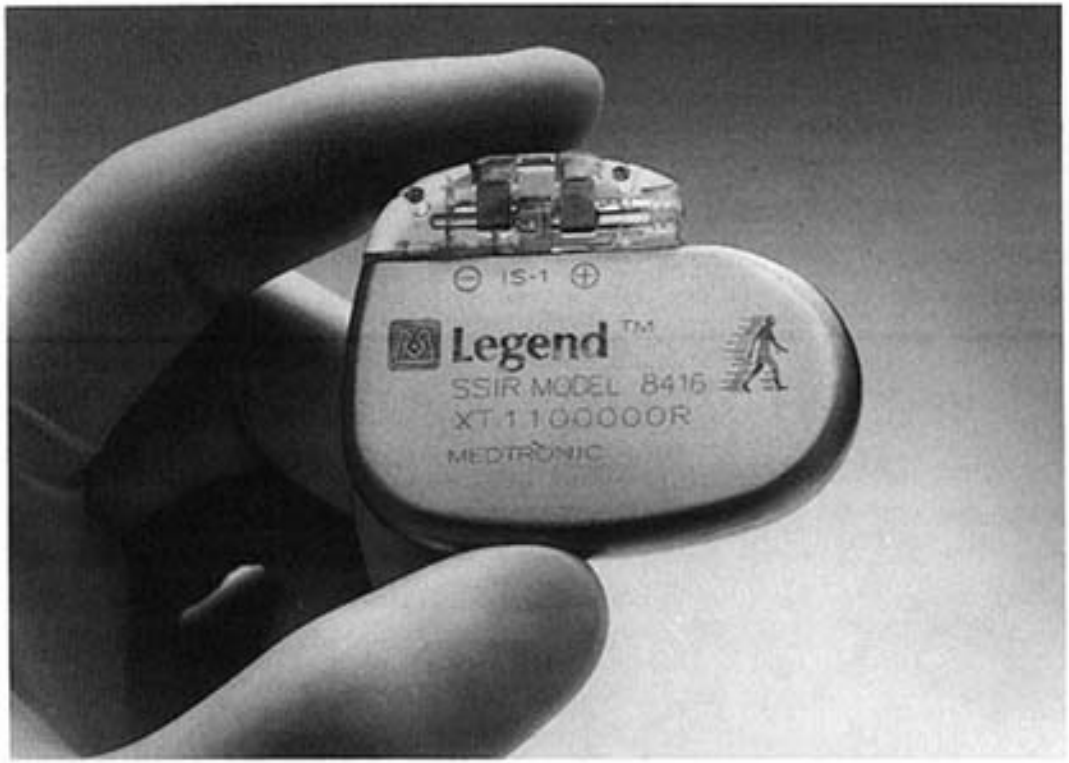
Sci-fi or reality

- *“23 minutes ago, her cyber-brain was hacked via telephone connection”*

  – Ghost in the shell
- *Are we going to add more hardware in humans?*
  - *Pace makers, visual aids, …*
- A group of researchers demonstrated how they could switch off a pace maker over wifi

Defcon: Excuse me while I turn off your pacemaker

DEAN TAKAHASHI | AUGUST 8TH, 2008



The Defcon conference is the wild and woolly version of Black Hat for the unwashed masses of hackers. It always has its share of unusual hacks. The oddest so far is a collaborative academic effort where medical device security researchers have figured out how to turn off someone's pacemaker via remote control. They previously disclosed the paper at a conference in May. But the larger point of the vulnerability of all wirelessly-controlled medical devices remains a hot topic here at the show in Las Vegas.

Let's not have a collective heart attack, at least not yet. The people on the right side of the security fence are the ones who have figured this out so far. But this has very serious implications for the 2.6 million people who had pacemakers installed from 1990 to 2002 (the