Thoughts on Embedded Security

Philip Koopman

koopman@cmu.edu

http://www.ece.cmu.edu/~koopman

Carnegie Mellon

Electrical & Computer ENGINEERING

Small Computers Rule The Marketplace

- **Everything here has a computer – but no Pentiums**

Must We Worry About Security?

- **Consider the lowly thermostat**
  - Koopman, P., "Embedded System Security,“ *IEEE Computer*, July 2004.
- **Trends:**
  - Internet-enabled
  - Connection to utility companies for grid load management
- **Proliphix makes an Internet Thermostat**
  - (But it we’re not saying that system has these vulnerabilities!)

Waste Energy Attack

- **"I'm coming home" function**
  - Ability to tell thermostat to warm up/cool down house if you come home early from work, or return from a trip
  - Save energy when you're gone; have a comfy house when you return
  - Implement via web interface or SMS gateway

- **Attack: send a false "coming home" message**
  - Causes increase in utility bill for house owner
  - If a widespread attack, causes increased US energy usage/cause grid failure
  - Easily countered(?) – if designers think to do it!
    - Note that playback attack is possible – more than just encryption of an unchanging message is required!

Discomfort Attack

- **Remotely activated energy saver function**
  - Remotely activated energy reduction to avoid grid overload
  - Tell house “I’ll be home late”
  - Saves energy / prevents grid overload when house empty

- **Attack: send a false “energy saver” command**
  - Will designers think of this one?
  - Some utilities broadcast energy saver commands via radio
    - In some cases, air conditioning is completely disabled
    - Is it secure??
  - Consequences higher for individual than for waste energy attack
    - Possibly broken pipes from freezing in winter
    - Possibly injured/dead pets from overheating in summer

Energy Auction Scenario

- **What if power company optimizes energy use?**
  - Slightly adjust duty cycles to smooth load (pre-cool/pre-heat in anticipation of hottest/coldest daily temperatures)
  - Offer everyone the chance to save money if they volunteer for slight cutbacks during peak times of day
  - Avoid brownouts by implementing heat/cool duty cycle limits for everyone

- **You could even do real time energy auctions**
  - Set thermostat by “dollars per day” instead of by temperature
    - More dollars gives more comfort
  - Power company adjusts energy cost continuously throughout day
  - Thermostats manage house as a thermal reservoir

Direct Energy Auction Attacks

- **What if someone broke into all the thermostats?**
  - Set dollar per day value to maximum, ignoring user settings
    - Surprise! Next utility bill will be unpleasant
  - Turn on all thermostats to maximum
    - Could overload power grid
  - Pulse all thermostats in a synchronized way
    - Could synchronized transients destabilize the power grid?

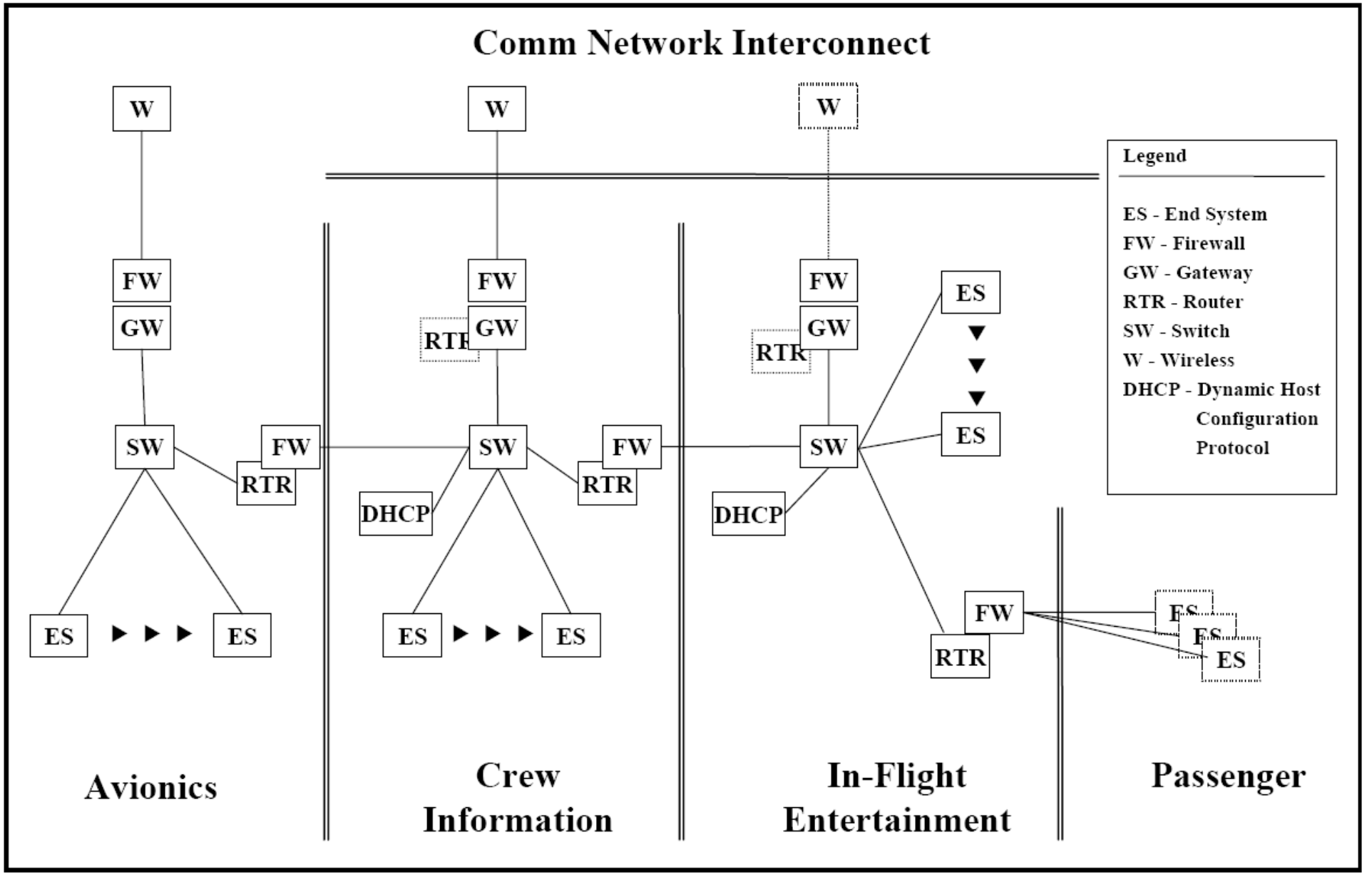
Indirect Energy Auction Attack

- **What if someone just broke into the auction server?**
  - If you set energy cost to nearly-free, everyone turns on at once to grab the cheap power
  - Guess what – enterprise computer could have indirect control of thousands of embedded systems!
    - A key point is the computer's authority over release of energy
  - Someday soon, almost "everything" will be "embedded," at least indirectly

Could There Be Safety Critical Stuff Like This?

- **Medtronic pacemaker**
  - July 1, 2001 – VP Dick Cheney gets an Internet Pacemaker (Medtronic GEM® III DR)
  - Uses phone link to connect to secure web-based monitoring system, available to patient, physician, nurses, etc.
  - "Medtronic has taken significant measures to protect the confidentiality and security of patients' healthcare information. The company has partnered with technology experts to build a secure system that employs multiple levels of security and encryption technology. The system is designed to address healthcare privacy and security laws and regulations. Access for clinicians and patients requires registration and is password protected so that only registered users will have access to patient information."
    http://www.medtronic.com/newsroom/news_20020102.html

Vice President Dick Cheney looks relatively chipper after having a Medtronic defibrillator/pacemaker implanted in his shoulder.



Wargo & Chas, 2003, proposed Airbus A-380 architecture