UPCOMING SECURITY ISSUES IN THE UBICOMP/MOBILE DOMAIN

Rene Mayrhofer, FH Hagenberg

VISION: CONVERGENCE INTO MOBILE DEVICES

RESEARCH ISSUES: DEVICES

- Security of mobile/smart/pervasive devices is hard to achieve:
  - wireless networking
  - Security architectures immature
  - proliferation of platforms
- Small is beautiful, but:
  - easy to pocket → easy to forget, easy to steal
  - malicious wireless nodes nearly impossible to find
- **Approach**:
  - apply known techniques and give it some more time

RESEARCH ISSUES: SECURE CHANNELS

- Assumption: devices can be made secure (or at least some parts)

- Components need to communicate among each other
  - secure virtual guest and applet
  - virtual guest and/or applet with infrastructure
- Components need to communicate with user
  - e.g. financial transaction details,
    PIN code to unlock smart card applet,
    OK for reading virtual passport, etc.

- **Approach**: ???

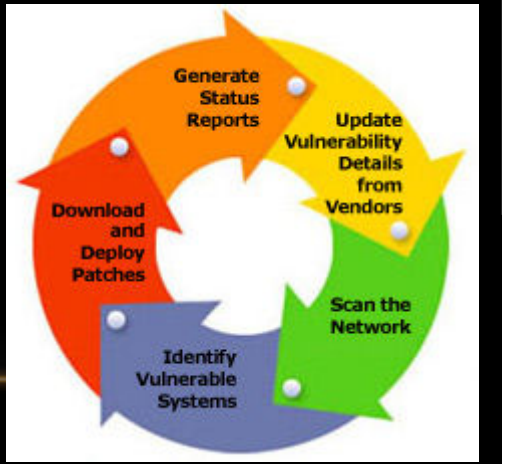
RESEARCH ISSUES: USABILITY

- Users are often the weakest link in the security chain
- Obtrusive security measures are either disabled or circumvented
- Constant information overload
  → security cannot add any additional burden

- **Approach**: security measures must be
  unobtrusive, but not invisible
  - e.g. biometric user authentication
  - e.g. integrate device authentication with main user interaction
  - e.g. visualize trust/reputation scores

EXPECTED IMPACT: EXTRAPOLATING THE PAST

1. No revenue can be generated by improving security or privacy for end-users or for infrastructure services
2. Security and privacy will be ignored for as long as possible
3. Bugs, exploits, insider documentation, first (benign) proof-of-concept code
4. Security-critical applications are being created (e.g. financial transactions, identity documents, remote control of critical infrastructure)
5. Financial interest for exploiting security issues becomes evident
6. First large-scale exploits/malware hit the mainstream media
7. Reputation of some systems/platforms/companies suffers sufficiently
8. Security and privacy measures are bolted onto existing systems, patch-cycles start



EXPECTED IMPACT: DOING BETTER

1. No revenue can be generated by improving security or privacy for end-users or for infrastructure services
2. Security and privacy will be ignored for as long as possible
3. Bugs, exploits, insider documentation, first (benign) proof-of-concept code
4. Security-critical applications are being created (e.g. financial transactions, identity documents, remote control of critical infrastructure)
5. Design, develop, and evaluate new security architectures and concepts with end-users
6. **Security measures disappear into the background and no longer need to be applied consciously (and incorrectly) – systems are secure by default and users are free to concentrate on applications and interactions.**