Defense Strategies & Mechanisms

Defense Strategies & Mechanisms

Attack Strategies & Mechanisms

Attack & Defense

- Properties: physical, cyber, and human factor (+ social & environmental)
  - E.g., model-based design?
- Dependency & Interference
- Objectives of Attack and Defense
  - E.g., attack-tree, vulnerability analysis
- Strategies and Mechanisms
  - E.g., prevention, detection, response, recovery, deception, diversity…
- Security Management
  - E.g., virus updates (➔DoS), firewall configuration (➔punch holes)

Research Problems

- Paradigms
  - A different/disruptive security approach for TCPS?
  - E.g., "Built-in" Security Strength
- Scale/Complexity/Unexpected
  - Model/Abstraction/Priority/Critical Properties
  - Control vs. "Management"
- "Cyber meets Physical"
  - E.g., interface for security has been very poor!
- Validation/Verification, Testing, Evaluation
  - for both attack and defense + human

Research Problems – Notes from Discussion

- **What does cybersecurity cover in TCPS**?
  - Device-centric; different from enterprise security
  - Paradigm shift: Clean-Slate program
  - Bring communities together!
  - Transfer into practice

Research Problems

- We have all problems from purely cyber systems, but add to that mobility
- Consequences can be much more severe than, e.g., loss of data – stakes are higher
- Level of trust about attacks you can have: spoofing sensor may not be a rational attack?
- What are reasonable (physical) attacks that can be imagined

Research Problems

- **Consider security from the start, and integral throughout entire lifecycle process**
  - Internet: As each attack has been recognized, methods to deal with it have been developed. Fix is the only thing you can do.
- HACMS DARPA program
  - Design principles that create safe behaviors even in the presence of attacks
- IT attacks are not real time. In addition, the human interface element is different (less tech savvy than computer user?)

Research Problems – Notes from Discussion

- Build/design secure systems for *known* attacks, but what about **unknown attacks**?
  - How can you detect them?
  - How can you deal with them?

Research Problems

- What can we test and what can we check?
  - Case study: unintended acceleration
  - How does driver deal with it?
- Detect, prevent, respond
  - We must look at all 3 mechanisms
  - Response: do something safe (domain dependent)
  - What does the *detect* side look like?

Research Problems

- Education at the UG level in EE&CS will be important
- It will be in the hands of everyone (like smart phones)
- Cost to include security into the design process, not just cost of attacks

Research Problems

- Which attacks are not purely physical (e.g., we trust our mechanic)
- The above determines the defense strategies
- Knowing when system is attacked/ compromised
- What observables can I use from the *physical* system
- Driver/pilot is not a system administrator
  - Very low false positive (b/c leads to recall – economic impact)

Research Problems

- **Role of (robust) control theory**: Are there defense strategies that rely on the fact that we are dealing with a control system
  - Use that information to tell the health of my system: intrusion detection
  - Design principles that are different from pure IT systems
  - In car: powertain element and software bug element: they need to be handled differently
  - Systems are complex and interconnected
  - Intrusion-tolerance

Research Problems

- **Privacy is a huge issue**
  - How to detect, how to mitigate
  - In case of attack on your car, how to do safe degradation? Who will do it?
  - Consent, authority
- Attacks that make “small” changes in each car, but lead to globally unsafe behavior
- Difference between aircraft and automobile domains
  - Many suppliers: what is in each box?