
First Workshop on the Security and Privacy of Emerging Ubiquitous Communication Systems (SPEUCS)

Marco Gruteser, Wade Trappe, Yanyong Zhang

Scope of SPEUCS

- ❑ Countermeasures to jamming and radio interference
- ❑ Secure localization
- ❑ Location privacy
- ❑ Security and privacy for RFID systems
- ❑ Sensor security and privacy, both static and mobile sensors
- ❑ Networks of embedded devices
- ❑ Vehicular networks
- ❑ Software-defined radios
- ❑ Video sensor systems
- ❑ Spatial and context-aware access control
- ❑ And many more ...

SPEUCS Program

- ❑ 9:15-10:30 keynote address
- ❑ 10:30-10:45 break
- ❑ 10:45-12:15 session 1 - Spatial/Context-Aware Access Control
- ❑ 12:15-1:30 lunch
- ❑ 1:30-2:30 Session 2 - Secure Routing and Applications
- ❑ 2:30-3:00 break
- ❑ 3:00-4:00 session 3 - Security-Enhanced Communication
- ❑ 4:00-4:15 break
- ❑ 4:15-4:45 Discussion session (interactive panel)

Discussion Question I:

1. What are the emerging technologies that constitute or will facilitate future ubiquitous communication and computational systems?
 - ❑ Low-cost computing platforms and low-cost short-ranged communication devices
 - ❖ RFID, sensor networks, Wimax, Cellular, MANET/MESH, embedded devices/scada, software radios
 - ❑ Energy efficient computing/networking algorithms
 - ❖ Area-cast
 - ❖ Semantic/location/context-aware routing
 - ❖ In-network storage/processing
 - ❑ Pervasive programming models
 - ❖ Location-oriented addressing
 - ❖ Context-aware programming
 - ❖ Opportunistic (non-deterministic) programming
 - ❑ Ubiquitous Applications
 - ❖ Mobile commerce
 - ❖ Better information sharing
 - ❖ Data collection
 - ❖ Inventory tracking

Discussion Question II:

What are the key security and privacy challenges facing ubiquitous networks in the near future?

- ❑ Defining what security and privacy mean (and metrics)?
 - ❖ Security and privacy are application specific
 - ❖ A hard problem due to unknown attacks
- ❑ Contextual privacy
 - ❖ Location, source/destination, identity, inferring information from traffic patterns
 - ❖ Should be user-controllable
- ❑ enforcement of privacy requirements
 - ❖ laws
- ❑ Denial of Service (could mean many different things)
- ❑ AAA -> who is going to make the money?
- ❑ Trust establishment and maintenance
- ❑ Key management in ubiquitous systems
- ❑ Key protection for memory-constrained devices (devices are easy to be lost or stolen)
- ❑ How to forward/process encrypted contents in a content-based network? (private information retrieval)

Discussion Question III

How are these threats unique to ubiquitous computing systems?

- ❑ Resource constraints
 - Power, memory
- ❑ Large number of nodes
 - Scalability
- ❑ Need for mobility
 - on-and-off connection
- ❑ Lack of infrastructure

Which threats can be addressed using conventional network and computer security mechanisms?

- ❑ Issues with authentication, encryption

Discussion Question IV

How can community resources have an impact on security research?

- ❑ Mount 802.11 devices on volunteer's houses
 - Construct social networks (to collect social interaction patterns)
- ❑ Collection of lightweight crypto implementations
- ❑ Usability studies
- ❑ Develop and use testbeds for security research

What are some specific experiments that should be conducted to verify the strength of proposed security/privacy solutions?

- ❑ Improve evaluation
 - Security problems that are quantifiable (worm/intrusion detection)
 - Evaluate the impact of some attacks (cost tradeoff)
- ❑ Validate the underlying security models
 - Proof, red-teaming

Discussion Question V

What are the key attributes to be used or tools to be developed in order to address these security and privacy issues? Which of these topics need investment/funding?

- ❑ Metrics + benchmarks
 - Attributes that measure privacy preserving capabilities
 - Attacking models that can be deployed in outdoor testbed
- ❑ Methods for risk assessment and tradeoff analysis

Discussion Question VI

What are the opportunities for collaboration (domestically and internationally)?

- Testbed development
- Collaboration between industry and academics
 - Industry needs to tell academics about what are the important problems
- Development of end-to-end security solutions
- Engineers and CS need to learn from each other (cross-layer)
- Sharing across nation boundaries has been hard -> how to fix?
- A lot of security can be addressed through other methods
 - Better laws, better user interfaces