Towards a Mobile Security & Privacy Simulator

Using Simulation to Evaluate Mobile Security and Privacy Threats as well as possible Countermeasures

2011 IEEE Conference on Open Systems (ICOS2011)

M. Sc. Benjamin Henne

Motivation

- Today: beginning of new era of mobile computing
  - Proliferation and capabilities of mobile networked devices rapidly increases
  - Mobile phones and tablets become central digital hub in the life of more and more people
    - multimedia, (mobile) social networks, online banking, location-aware services, endless apps
  - Lots of security and privacy implications come along with it
    - adopters of these technology accept implications

Motivation

- Threats grow ever more critical as number of users increase
  - Absolut number of user rise
  - Fraction of incautious and unknowing people rises

- Mobile threats has to be more intensively addressed
  - Still in research, but also
  - Usable real-world implementations are needed

Research – Up to now

- Approaches used to evaluate mobile security & privacy
  - Pure theoretical
    - e.g. mathematical epidemiology like SI-model
    - assume an average person – no personality types
    - ! limited parameters, e.g. no spatial dynamics, battery consumption, or complex infect routines
  - Field studies
    - representative people (selection and scale)
    - expensive devices
    - ! costly, time consuming and difficult to arrange

Research – Up to now

- Approaches used to evaluate mobile security & privacy
  - Simple non-interactive movement models
    - infection/privacy evaluation on top of modeled movement
    - ! interaction cannot change (movement) behavior
    - not tailored for security and privacy research
  - Real-world movement data
    - using anonym user location traces of cellular networks
    - ! unsuitable location accuracy (= cell size)
    - legal issues and hard to obtain in most countries

Why we chose to use simulation?

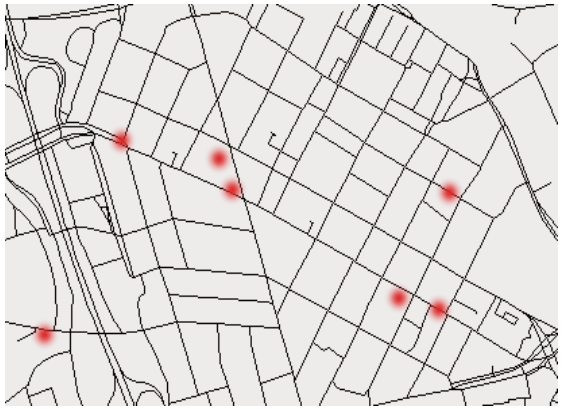
1. Modeling threats for simulation helps to understand parameters
   - technical, personal and social ones
2. Security enhancing and privacy preserving techniques can be tested against modeled threats to study their effectiveness
   - Changing different parameters can be tested
3. Any simulation parameter can be observed, also those not covered by other approaches
   - “Who infected whom when, how and why?”
   - Lots of parameters can be visualized for understanding
     - also for laymen

Mobile Security & Privacy Simulator

MOSP Simulator – Basic Features

Mobile Security & Privacy Simulator

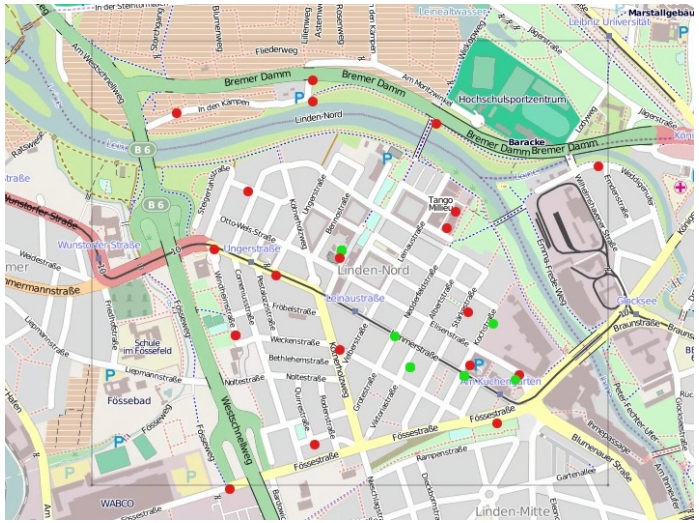
- Modeling the world
  - Maps from osm.org for realistic environment
  - Road network for movement
  - Points of interest and other geo-spatial data can be used
    - cafe/bar/pub, residential area, road width



```
<node id='42'>
  <tag k='amenity' v='cafe'>
  <tag k='name' v='Notre Dame'>
  <tag k="addr:street"
       v="Limmerstraße"/>
</node>
```

Mobile Security & Privacy Simulator

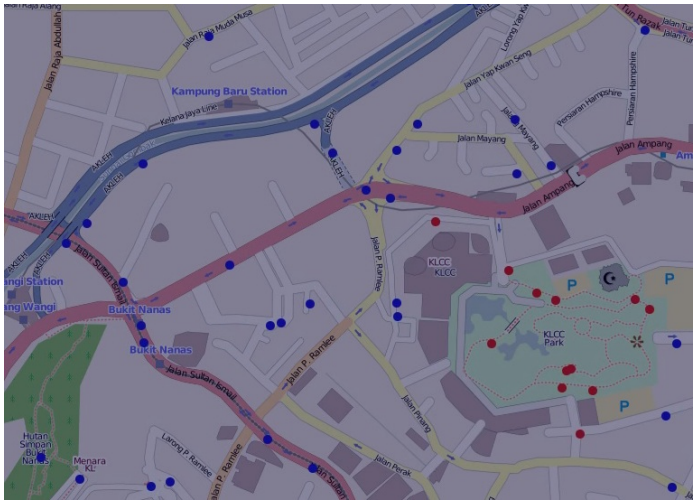
- Modeling people
  - Types/groups (*café visitor*, *walker*, …)
  - Personal parameters (*internet usage*, *speed*, *like drinking*, …)
  - Behavior may change
    - Actions, movement pattern
      - end of video: drunken one does not find his home
- Movement
  - Random movement on map
  - Routed movement from a to b
  - Stop anywhere
  - Enter modeled locations, do something at map border



live visualization: people go to work, red ones go drinking and all go home.

Mobile Security & Privacy Simulator

- Action, Interaction and perception
  - Actions
    - being an infectious zombie
    - “Who is in my vicinity?”
      - infect them all!
  - Interaction
    - taking a photo of others
    - Upload photo to a service
    - complex infection routines

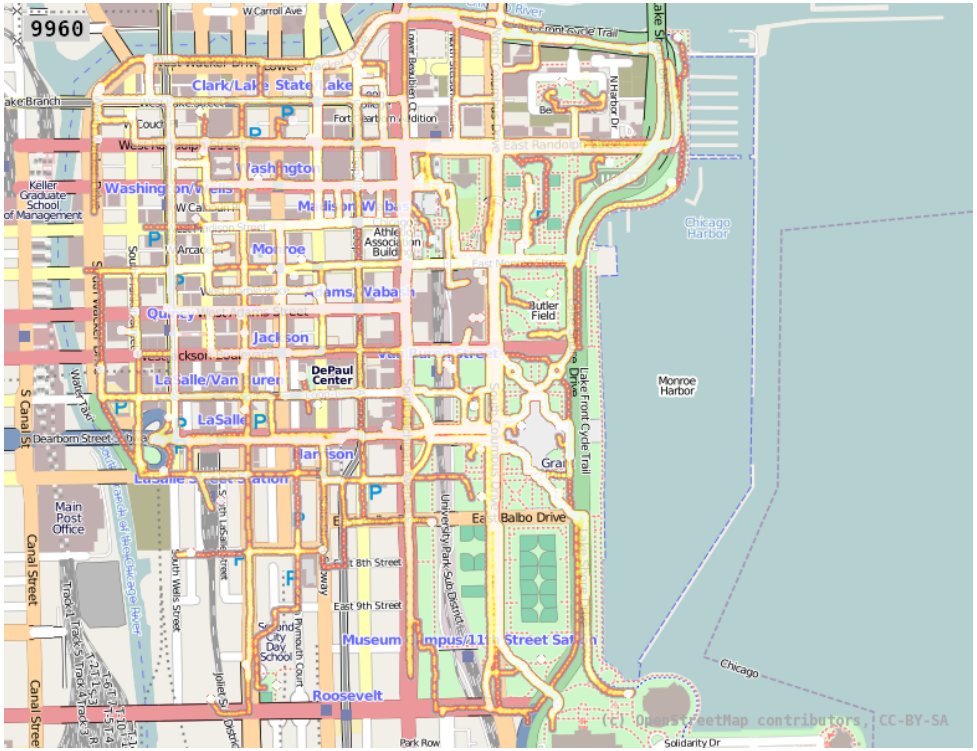


live visualization of zombie infect

MoSP: more complex infection routine

Wireless network based infection

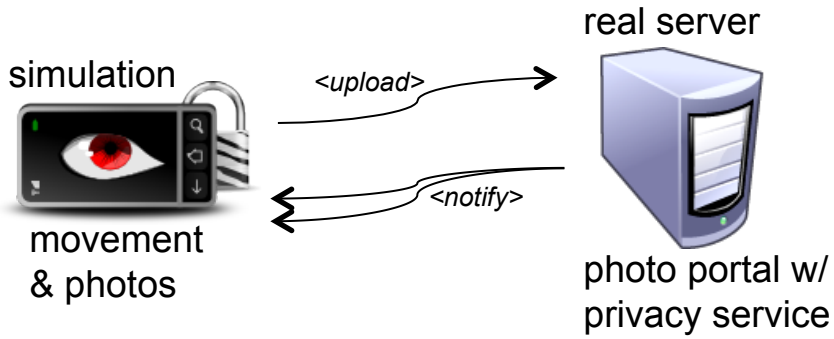
- Infection if being in range of infected in distance up to 8 meters for minimal 8 seconds and requesting connection
- Finally also becoming an infectious hotspot



heatmap of infectious area formed by moving infected devices

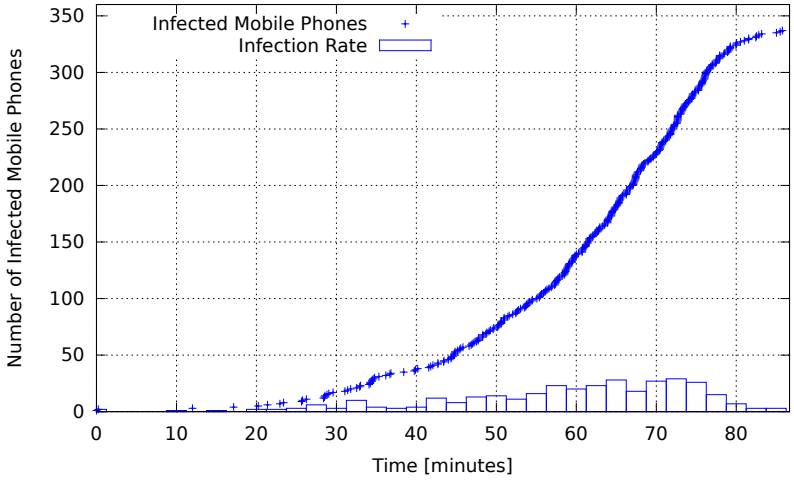
MoSP: simulation connecting real service

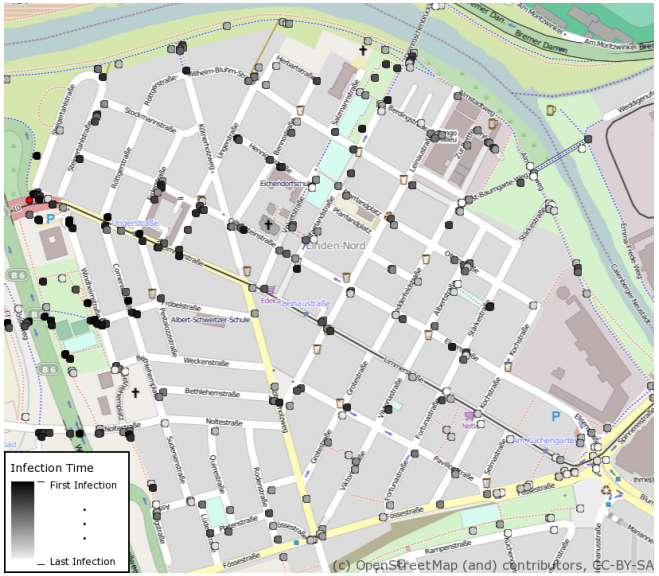
- Evaluating a photo web portal with privacy service to test privacy preserving techniques
  - Simulation of people moving around and taking snapshots
  - People upload photos to online service (real system)
  - Service may inform other people having been snapped



Mobile Security & Privacy Simulator

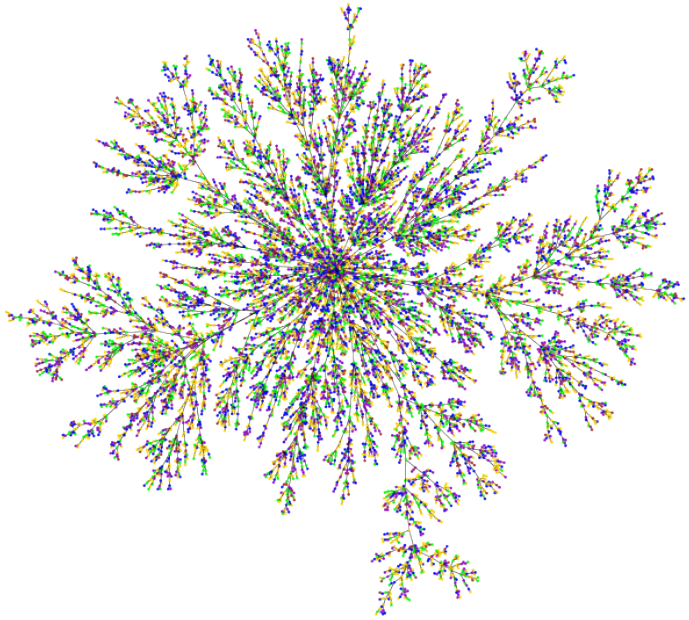
- Visualization of results
  - Plotting numbers
  - Map visualization





Mobile Security & Privacy Simulator

- Visualization of results
  - Net graph: Who infects whom?
  - Heatmap: infectious areas



Future Work

- User modeling
  - Different user/agent modeling approaches
- Non-direct/alternative routing
  - If routing, also use alternative ways to the shortest path
- Connecting simulator and real system
  - Wrapper vs. Integration of real network stack
- Connecting simulators
  - Partition simulation: partition map, indoor simulation

- Extend the software framework, add more building blocks
  - http://www.dcsec.uni-hannover.de/mosp-sim.html