ESCORT: a Decentralized and Localized Access Control System for Mobile Wireless Access to Secured Domains

ACM Wireless Security WiSe 2003
September 19, 2003
San Diego, California, USA

James Jiejun Kong, Shirshanka Das, Edward Tsai, Mario Gerla

Wireless-Adaptive-Mobility Laboratory
Department of Computer Science
University of California, Los Angeles

Outline

✓ Problem Statement
✓ Design objectives
✓ Design
✓ Discussions & Evaluations
✓ Conclusion and future work
Context: Secured Wireless LAN

- **Case I.**
  - Prof. Smith of Univ. S invites Prof. Taylor of Univ. T for a two-hour talk, how to grant Prof. Taylor an instant and secure access at Univ. S?

- **Case II.**
  - Transient access for interns and visitors in private enterprise X
  - Security demand high
  - Permanent account not preferred

- **Case III.**
  - Replace wired connection with indestructible wireless connection, but WLAN can only support and secure a single wireless hop

Adversary Model

- **External adversary**
  - Wireless link eavesdroppers and traffic analysts
  - Cannot invert one-way functions (or differentiate cryptographically strong pseudorandom numbers CSPRN from truly random numbers)

- **Internal adversary**
  - Compromised nodes inside wireless LAN
  - In extreme cases, tamper-resistant boxes can also be compromised
- Problem Statement
- **Design objectives**
- Design
- **Discussions & Evaluations**
- **Conclusion and future work**

### Objectives

- **Simplified trust model**
  - Pre-established guest-escort acquaintance
    - Do not have one, then get one
  - At the time of mobile access, escort is guest’s trust anchor in local domain

- **For mobile guests**
  - *Instant* network access for escorted guests
  - Protect such guests’ *mobile privacy*
    - Confidentiality, anonymity

- **For secured wireless LAN**
  - Reject network access to other guests and malicious nodes (e.g., illegitimate and misbehaving escorts)
  - Backward compatible, *zero* IP protocol stack change (except on escorts)
Mobile Privacy

✓ Privacy in mobile networks has different semantics from the traditional notion for banking systems and fixed Internet
  - E.g., three aspects identified by [Cooper and Birman, 1995]: content, participant identity, participant location

  - Our efforts focus on localized control paradigm, communication efficiency, and minimal protocol stack change

Related Work

✓ Mobile access control
  - Dominant paradigm: centralized control (e.g., Kerberos, 802.1x, RADIUS, InSite, NetBar, SPINACH) must present at the time of mobile access
  - Not scalable in many aspects
  - Less tolerant to faults, single point of failure of the entire system exists
  - So far no anonymity support

✓ Mobile Privacy in last-hop wireless networks
  - Some efforts in the context of mobile IP [Samfat et al., Mobicom 1995], [Ateniese et al., 1999]
  - Require non-trivial changes in IP protocol stack
Design aspects

- Localized security model
  - Localized → decentralized

- Mobile privacy
  - Confidentiality, anonymity

- Backward compatibility
  - Immediately deployable
  - Compatible with existing WLAN access and security solutions
  - 802.11 WEP, TKIP/Michael, AES/CCMP, 802.1x, Kerberos, RADIUS, DHCP, etc.
Localized Security for *Wireless* Communication

- Has been extensively used in ad hoc networks
  - Watchdog [Marti et al., MOBICOM’00]
  - Packet leash/TK [Hu et al., INFOCOM’03]
  - Distributed consensus [Zhang & Lee, MOBICOM’00; Yang et al., WiSe’02]
  - Ubiquitous authorization & access control [Kong et al., ICNP’01; Luo et al., ISCC’02]

- Advantages (in Wireless LAN)
  - Decentralized and localized access control
  - Localized intrusion detection
  - Suitable for providing *mobile privacy support* in wireless LAN (“the ring argument”)

- Disadvantage
  - Extra deployment cost

“The Ring Argument” for mobile anonymity design in WLAN

- Decentralized and localized solution vs. *Centralized* solution
- Less vulnerable points
- 1-hop minimal communication overhead
Our Proposal: Localized ESCORTs

✓ Case I:
  - A permanent member of LAN, say Prof. Smith’s laptop, serves as Prof. Taylor’s escort
  - T can access those S can access & S can control/filter

✓ Case II:
  - Access control is objectified on an authorized & easy-to-manage object
  - Grant/recycle the object → grant/recycle access
  - Instant access grant/denial, no permanent resource leftover (e.g., ghost account)

✓ Case III:
  - A wireless access point can be upgraded to be an escort (for local roaming nodes), multi-hop enabled

Essential properties of an escort box

1. Already a permanent or semi-permanent member of local domain

2. Trusted by both local domain and mobile guest

3. Forwarding packets between local domain and mobile guest

4. Mobile and tamper-resistant implementation
   - Roam with mobile guest (without being compromised)

✓ Existing authorities and gateways do not possess all four essential properties
Guest-Escort Acquaintance: Pre-registration

- Leave the job to application layer
  - Why overload the mobile device’s network layer?
  - Lots of off-the-shelf applications available
- Guest-Escort acquaintance
  - Physical contact (bioinformatic)
  - PGP recommendation (Web-of-trust)
  - Online E-commerce transaction paid by credit card
  - et cetera......
- To get: an anonymous 128-bit token index
  - Easy to carry and use
  - Keep it in safe place: escort will serve the first mobile node who presents the token in its one-hop neighborhood
  - On escort, shared security parameters are stored under the unique index

Escort serving single guest

- Escort: Network Address Translation (NAT)
- Guest: a single node in an ad-hoc network
  - No protocol stack change on guest and WLAN
Escort serving multiple guests
- Escort & Guests: a 1-hop MANET
- Software encryption on escort
- Scalability

Escort serving anonymous guests
- No protocol stack change in WLAN and minimal protocol stack change on guest
  - Use anonymous pseudonyms in data forwarding
  - Also minimal computation/communication overheads

Anonymity by pseudorandom packet stamping
Pseudorandom Packet Stamp

✓ “Unpredictable in polynomial time”
  - In secular term, *looks truly random* to third parties
  - Hardcore functions needed in generating provably-secure cryptographically strong pseudorandom numbers (CSPRN)
  - For unicast traffic, PRN# also a proof of data origin

<table>
<thead>
<tr>
<th>shared seed</th>
<th>1</th>
<th>sender's PRN#</th>
<th>receiver's PRN#</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEQ# as index</td>
<td>2</td>
<td>56a35d537fe</td>
<td>56a35d537fe</td>
</tr>
<tr>
<td>(for synchronization in lossy channel)</td>
<td>3</td>
<td>198573f8d5b</td>
<td>198573f8d5b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e53410957fa</td>
<td>e53410957fa</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

✓ Problem Statement
✓ Design objectives
✓ Design
✓ Discussions & Evaluations
✓ Conclusion and future work
Localized Detection & Recovery

- Legitimate and illegitimate escorts
  - AP can block illegitimate escorts
  - Avoid insecure configuration on legitimate escorts

- Watchdog: intrusion detection agent
  - Low-cost: a radio receiving interface in RFMON mode

- Authorized escrow detection server
  - "Big brother" authorized to know keys on guest-escort & escort-AP hop
  - Monitor all traffic via watchdog agents
  - Notify AP to block escort/guest on any misuse and anomaly (e.g., undecipherable traffic)

Once one-hop away, an (stolen) escort box is useless and harmless

Once an (stolen) escort box is within one-hop, legitimate side can detect it
Towards Ideal Implementation

- Five low-cost and energy-efficient components
  1. Mobile processor
  2. Accessories like memory and battery
  3. Wireless interface to infrastructure
  4. Wireless interface to guest
  5. Tamper-resistant shell

Impact of Encryption on Throughput

- no-wep
- hardware-wep
- software-wep
Impact of NAT on Throughput

- Real world scenarios
  - Single guest
  - Multiple guests

Impact of NAT: single guests

No NAT

A - Single Guest downloading from Escort.

B - Multiple Guests downloading from Escort.

C - Single Guest downloading from department FTP server.

D - Multiple Guests downloading from department FTP server.
Conclusion and Future Work

- Decentralized and localized mobile access control is feasible and efficient
- Localized security model is suitable to ensure mobile privacy
- More implementation and tests
  - Improve escort’s portability, energy, and communication efficiency
  - Local intrusion detection agents and escrow server
  - Compare efficiency between ESCORT and other anonymity solutions
- Pre-registration phase
  - Ensure a secure acquaintance between the guest and its escort
  - Real-time cross-domain roaming: micro-/macro-mobility