Low Layers Threat Model ALIEN BoF

draft-haddad-momipriv-threat-model-00

Wassim Haddad et al.
Wassim.Haddad@ericsson.com

IETF, August 2005

Locations and Goals of the Attacker

- The malicious node can be located "at" or "near" the source of information. In this case, the malicious node tries to learn the target's IPv6 address and other parameters related to the IP layer.

→ using temporary IPv6 addresses may be enough.

- The malicious node can be located near the target itself, for example within the same DS in 802.11. In such scenario, the malicious node tries to correlate the MAC and IPv6 addresses => more opportunities!

Threat Model Applied to Privacy in a Momipriv Environment(1)

- Threat Model applied to the MAC and IP layers only
- Three main threats against privacy are:

  - Identifying
  - Locating
  - Tracing

And prior information...

→ Note that the above order is not strict.

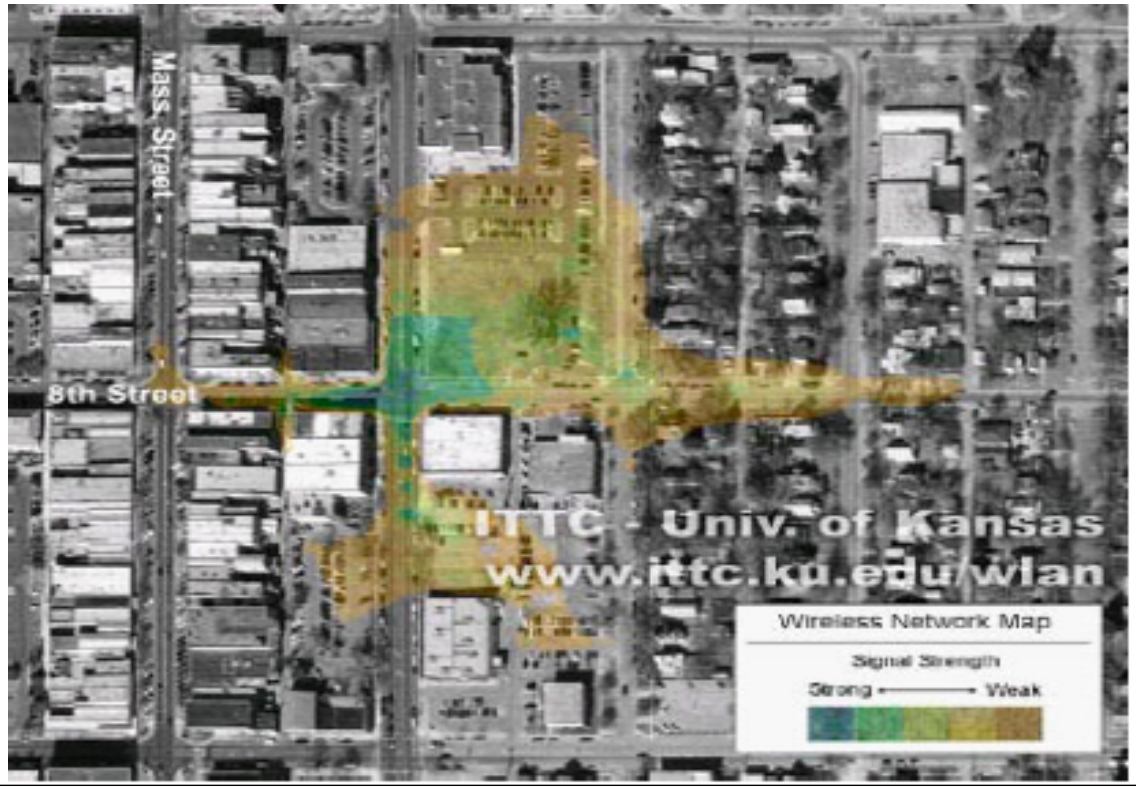
Threat Model Applied to Privacy in a Momipriv Environment(2)

- In a typical scenario, the malicious node tries first to identifying its target.
- After identification, the target is pinpointed.
- The third phase consists on tracing the target (possibly in real time).
- A successful three steps allow the malicious node to gradually increase its knowledge about the target, build a profile...
- Data gathered may include higher layer identifiers, pseudonyms, location and/or temporal information, mobility patterns...

Threat Model Applied to MAC Layer

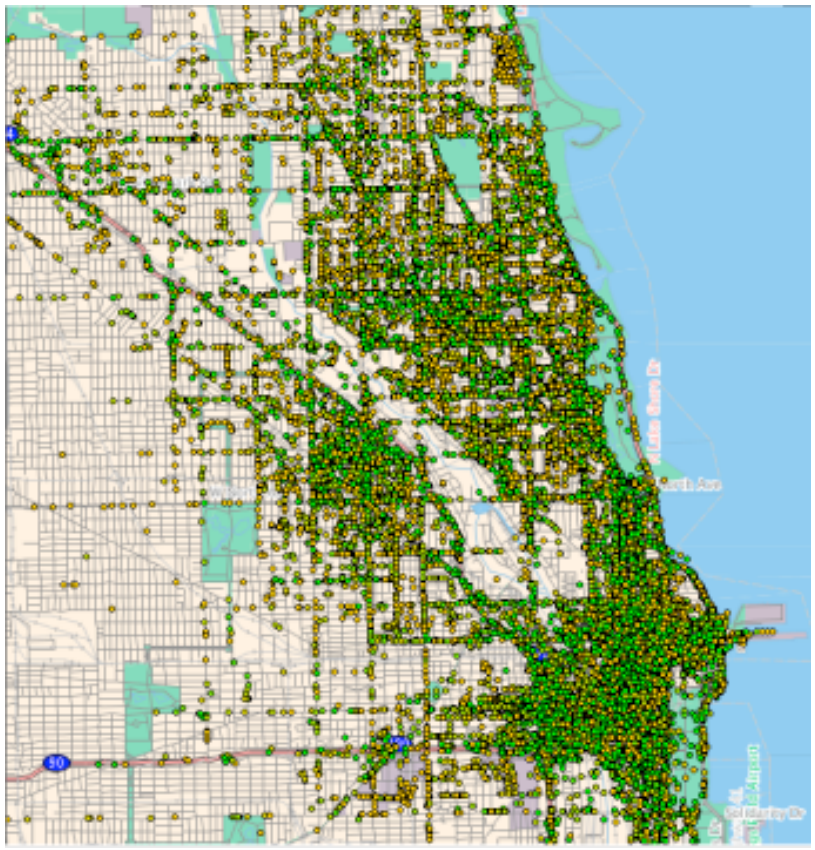
Malicious node's location(s)

In order to monitor traffic and perform traffic analysis, the malicious node should normally be located on the same link or within the ESS. However, this may be much easier in reality due to "signal leakage" as shown below.



Threat Model Applied to MAC Layer (1)

Threats from various malicious nodes



Many malicious nodes can be deployed in several locations and join their efforts to cover large areas.

Threat Model Applied to IP Layer (1)

Threats against Privacy in MIPv6 BT mode:

- In the BT mode, the CN is unaware about the MN mobility.

- MN needs to update its HA each time it switches to a new link.

- Depending on the malicious node's location, Identifying, locating and tracing are possible via the MAC address or by looking into the data packets headers. Note that the tunnel may be protected with ESP.

Threat Model Applied to IP Layer (2)

Threats against Privacy in MIPv6 RO mode :

- A malicious CN which has already learned the MN's HoA, can establish a session with the MN, and push the target to switch to the RO mode and disclose its CoA.

- A malicious node can position itself between the MN and the CN, identify the MN's HoA and current CoA, and trace the MN's in real time by looking into the data packets and/ or binding update messages.

- When identification is not possible, the malicious node can trace movements by tracking the sequence number in the BU messages by relying on prior information, e.g., identifying the MAC address, time, current location...

Threat Model Applied to Static Multi-homed Node(1)

- Multi-homed node can be described as being attached to multiple ISPs. Consequently, all addresses are pre-defined and known in advance in most cases.

- HBA provides a secure binding between multiple addresses with different prefixes available to a host within a multi-homed site.

- Main privacy concern is the ability to identify the multi-homed node by an untrusted party and to discover its available addresses.

- Untrusted party may be the CN or a third party located somewhere between the multi-homed node and the CN.

Threat Model Applied to Static Multi-homed Node(2)

- A malicious node can identify the multi-homed node via its MAC address then try to learn part or all of the available locators (requires geographical location of the target).

- A malicious CN can establish a session with the target by using a pre-identified locator. The CN can later stop replying in order to "push" the target to switch to a new locator by not replying to packets sent with the initial locator...

- Malicious node located near a particular CN, can correlate between different locators used by the targeted node or sniff context establishment to learn available locators.

Thank You!