Some Issues in WSN, MANET and Cellular Security (Position Paper)

Gene Tsudik[1]

ABSTRACT

In this position paper, we address some current limitations and challenges as well as emerging directions in three related areas of secure communication: (1) security in Wireless Sensor Networks – WSNs, (2) security in Mobile Ad Hoc Networks – MANETs, and, (3) security in Cellular Phone Networks.

WSN Security

Survivability and Intrusion Resilience: Sensors that obtain information by sensing the environment might not be able to propagate in real time. One basic reason is that, a batch of deployed sensors could form not a network *per se*, but, a collection of devices each responsible for its own sensed data. Some sensor settings do not involve sensors "talking" to each other; instead, a sensor waits for a mobile collector/sink to pass by in order to off-load sensed data. Such an environment obviates certain network security issues but opens others. Notably, a sensor needs to minimize the amount of overall collected information while preserving its security. At the same time, it needs to cope with the risk of compromise. Neither issue comes up in typical WSNs considered in the literature. We envisage a need for new techniques that combine the cryptographic features of cryptographic *forward security* with *aggregation* (of MACs and signatures) in order to satisfy security requirements of such "disconnected" sensor networks.

Secure Initialization: sensors are typically mass-produced and deployed simultaneously in batches. Unlike personal ubiquitous devices (such as cell-phones), sensors are not usually "personal" and lack traditional means of input and output. (In particular, since a sensor is not a *computer*, in a traditional sense, it lacks an HCI.) A collection of sensors that needs to be deployed may need to be initialized to share a common secret key. Much work has been done in developing a plethora of key (pre-)distribution techniques, based on both public key and/or conventional cryptography. However, all such techniques are inapplicable in scenarios where sensors are not obtained in well-defined groups that can be initialized by the manufacturer.
If no secret keys are pre-distributed, security initialization must be done in an ad hoc fashion. It cannot be done via some wireless broadcast medium since doing so would be subject to trivial eavesdropping. Doing it with wires or other direct physical connection is awkward and unscalable. Consequently, new techniques are needed that address both security and scalability. One recent proposal called "Shake-Them-Up" addresses the security issue to an extent, however, scalability remains to be tackled.

MANET Security

Anonymous Routing: we consider hostile MANET scenarios where network topology undergoes constant changes and current topology represents sensitive information which must be kept confidential even from MANET nodes themselves. (Troops on the battlefield is one prominent example.) In such cases, existing routing protocols are unsuitable and new packet forwarding methods must be developed.

Location-Based Addressing: in a MANET environments where nodes are mutually suspicious (e.g., because capture/compromise are possible) addressing and packet forwarding based on long-term identities is unsafe. This is because identities tend to reveal current locations of nodes and allow tracking of nodes as the network topology changes. At the same addressing based on location only (without knowing whether anyone is there) is not optimal since a picked location might be empty and effort expended in discovering this is essentially wasted. Thus, it makes more sense to periodically announce each node's location, thus making it possible to use location as a reliable current address of the destination. We claim that, if a sufficient

[1]Department of Computer Science, University of California, Irvine. gts_AT_ics.uci.edu

fraction of all nodes change locations between successive updates, tracking of nodes becomes infeasible. Moreover, if nodes have a way to authenticate their routing updates in an anonymous and un-linkable fashion, the network becomes more secure than is possible with current secure MANET routing techniques. The biggest challenge is to come up with a MANET architecture that allows this kind of operation in an efficient manner.

Cellular/Mobile Phone Security

Security in cellular phone networks has been studied extensively since early 90-s and there is a large body of literature on the subject. However, two prominent problems remain, as we highlight below.

Secure Pairing: sometimes referred to as *Secure First Connect*, this issue has to do with establishing a secure means of communication between two devices, at least one of which is a cell phone. The problem is exacerbated by three factors:
- heterogeneous devices (both phones and others) varying widely in terms of features (means of input/output)
- lack of any standard security infrastructure such as a common PKI
- inability to rely solely upon human-imperceptible means of communication due to man-in-the-middle attacks
- consequent reliance on the human user, which requires minimizing user burden while offering sufficient security

Notable secure pairing techniques proposed to-date involve using so-called location-limited side-channels. Each requires some direct involvement of the human user but they differ in the type and degree thereof. It has been widely accepted that involving the human user is unavoidable. At the same time, no technique is universal, even when it comes to pairing two similar cellphones. On the one hand, the design space of possible secure pairing techniques has not been thoroughly explored. (Methods like "Resurrecting Duckling", "Talking-to-Strangers", "Seeing-is-Believing", "Loud-and-Clear" and "HAPADEP" notwithstanding.) Moreover, usability studies have been undertaken only recently and much more work is remains to be done to adequately assess usability factors of already proposed techniques.

Anonymous Roaming: This issue refers to the ability to use one's cellular phone without exposing the phone's long-term identifier (e.g. IMSI in GSM) to the roaming network/provider. While most, if not all, cellular networks in operation today require the notion of "home" for each subscriber (SIM or phone unit, depending on the underlying standard), there is no inherent need to disclose the long-term identifier (There is, however, a legitimate need to disclose the "home" provider, however, that is a far cry from disclosing the actual phone identifier.) The need for roaming anonymously has been recognized for quite some time. However, despite the fact that the technology (protocols, designs, cryptographic primitives) is readily available, anonymous roaming is not available on any current cellular network.

The research challenge in anonymous roaming is not great; it boils down to coming up with concrete set of secure cryptographic protocols that support roaming anonymity and convincing the providers as well as manufacturers to offer anonymity as a service.

Some Issues in MANET, Wireless & Cellular Security/Privacy

Gene Tsudik
UC Irvine
gts_AT_ics.uci.edu

1

Outline

- WSNs:
  - Survivability & Intrusion Resilience
  - Secure Scalable Initialization
  - Graceful Degradation
- MANETs:
  - Oblivious Routing
  - Location-based Addressing
- Cellular:
  - Secure Association
  - Anonymous Mobility

2

WSNs

- Survivability & Intrusion Resilience
  - Not all sensors network; many don't
  - Collect data, wait for pickup
  - Irregular pickups + possibly long intervals
  - Hostile environment -- intrusion/compromise possible
  - How to protect collected data?
    - Storage, Computation and Bandwidth constraints
- Secure Scalable Initialization
  - Sensors manufactured in large quantities
  - Key pre-distribution not always viable
  - How to quickly and securely "pair" groups of sensors?
    - Scalability? Usability?
- Graceful Degradation
  - Strong security can kill sensors
  - When death is near, is strong security important?
  - How to gracefully degrade/relax security services?
  - What metrics to use when degrading?
- Whither RFID/Sensor hybrid?

3

MANETs

- Oblivious Routing
  - Fixed node population
  - Nodes move, topology changes
  - Hostile environment
  - How to protect topology (even from insiders)
    - But keep security
- Location-based Addressing
  - Nodes don't have identities
  - Node instances known by current location
  - Node instances must be authentic
  - How to keep node behavior (movements) private?
    - Most routing protocols can't hack it..

4

Cellular (Wireless Devices)

- Secure Association/Pairing
  - Heterogeneous devices
  - No PKI, no history
  - Insecure wireless medium
  - How to establish a secure channel?
    - Human-as-a-limited-side-channel
    - Many techniques proposed, usability uncertain!
- Roaming with Privacy
  - Not a research challenge, just an annoying problem

5