Security and Privacy in Wireless Networks

Mohammad Hossein Manshaei
manshaei@gmail.com

Chapter 3: (secowinet.epfl.ch)

Trust vs Security and Cooperation, Malice and Selfish, Adversary Model

TRUST ASSUMPTIONS AND ADVERSARY MODELS

Trust

- The **trust model of current wireless networks** is rather simple
  - subscriber – service provider model
  - subscribers trust the service provider for providing the service, charging correctly, and not misusing transactional data
  - service providers usually do not trust subscribers, and use security measures to prevent or detect fraud

- In the **upcoming wireless networks** the trust model will be much more complex
  - entities play multiple roles (users can become service providers)
  - number of service providers will dramatically increase
  - user – service provider relationships will become transient
  - how to build up trust in such a volatile and dynamic environment?

- Yet, trust is absolutely **fundamental** for the future of wireless networks
  - pervasiveness of these technologies means that all of us must rely on them in our everyday life!

Reasons to Trust Organizations and Individuals

- **Moral values**
  - Culture + education, fear of bad reputation
- **Experience about a given party**
  - Based on previous interactions

} Will lose relevance

- **Rule enforcement organization** → Scalability challenge
  - Police or spectrum regulator
- **Usual behavior** → Can be misleading
  - Based on statistical observation
- **Rule enforcement mechanisms**
  - Prevent malicious behavior (by appropriate security mechanisms) and encourage cooperative behavior

Trust vs. Security and Cooperation

- **Trust preexists security**
  - all security mechanisms require some level of trust in various components of the system
  - security mechanisms can help to *transfer* trust in one component to trust in another component, but they cannot create trust by themselves

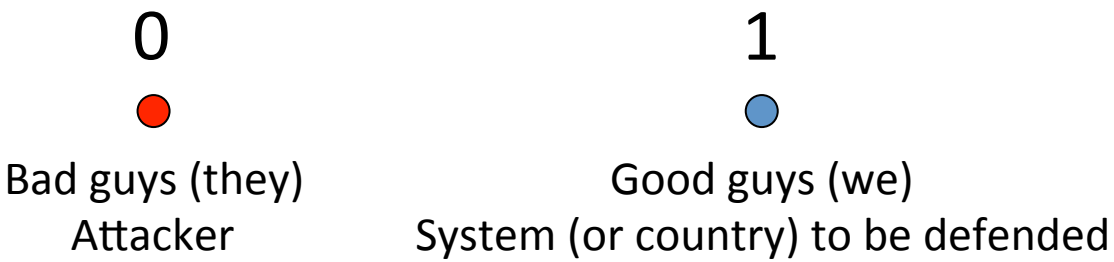
- **Cooperation reinforces trust**
  - trust is about the ability to *predict* the behavior of another party
  - cooperation (i.e., adherence to certain rules for the benefit of the entire system) makes predictions more reliable

New Type of Attackers in Commercial Applications

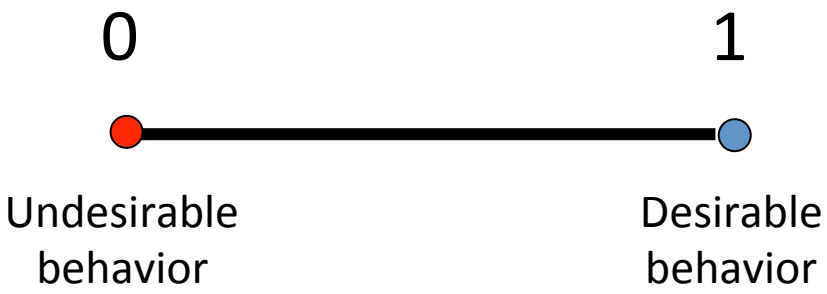
- The attacker is **much more difficult to identify**
- **Those who deploy the security mechanisms** are not necessarily those who benefit from them
- The attempts to **overuse the network resources** (as is the case with spam) can be very difficult to thwart

From Discrete to Continuous

Warfare-inspired Manichaeism:



The more subtle case of commercial applications:



- **Security** often needs **incentives**
- **Incentives** usually must be **secured**

Misbehavior

A misbehavior is the action of a party or group of parties consisting in deliberately **departing** from the **standardized** or otherwise prescribed behavior **in order to reach a specific goal**.

Malicious vs Selfish

A *misbehavior* is **selfish** (or greedy, or strategic) if it aims at obtaining an advantage that can be quantitatively expressed in the units (bitrate, joules, or coverage) of wireless networking or in a related incentive system (e.g., micropayments);

any other misbehavior is considered to be **malicious**.

Malice and Selfishness

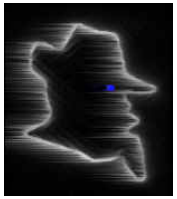
- **Malice**
  - willingness to do harm no matter what
- **Selfishness**
  - overuse of common resources (network, radio spectrum, etc.) for one's own benefit

✧ Traditionally, security is concerned only with malice

✧ But in the future, **malice and selfishness must be considered jointly** if we want to seriously protect wireless networks

Who is malicious? Who is selfish?

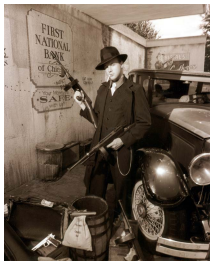
Harm everyone: viruses,…



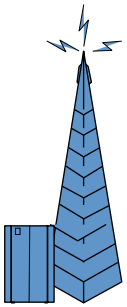
Big brother

Selective harm: DoS,…

Spammer



Cyber-gangster:
phishing attacks,
trojan horses,…



Greedy operator

Selfish mobile station

There is no watertight boundary between malice and selfishness
➔ Both security **and** game theory approaches can be useful

Adversary Model [Dolev and Yao]

- Attacker can be **a legitimate party** (e.g., a registered network user)
- Attacker **can send and receive messages** to any party in the network
- Attacker can be **a potential "man-in-the-middle"** everywhere in the network (meaning that she is able to read, modify, block, replay, or insert any message anywhere in the network)

❖ This model assumes that the cryptographic primitives are unbreakable.

Modification of Adversary Model in Upcoming Wireless Networks

- We need **to include selfish opponents**
- The attacker of a wireless network **does not necessarily have access to *all* communication** links between all devices
- The notion of **physical location** of the (wireless) parties becomes very important
- The **topology and the communication primitives** of the network become very relevant
- The risk of **capture and cloning** must be taken into account
- The huge number of parties makes **key management** a challenge *per se*.

Cryptography for Upcoming Wireless Networks

- Specific attention must be devoted to the assumption of unbreakability of the cryptographic primitives:

- Calling for the design of ***ad hoc*** **cryptographic primitives**