

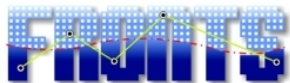
FRONTS Research Activities

Privacy, Security and Trust

Giuseppe Persiano

Dipartimento di Informatica ed Appl.
"Renato M. Capocelli"
Università di Salerno

PerADA Workshop on Security, Trust and Privacy



Foundations of Adaptive Networked Societies of Tiny Artefacts

Thanks

Thanks to

Shlomi Dolev, Mirosław Kutylowski and Andrea Vitaletti

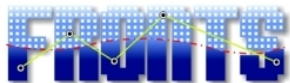
for providing slides

Overview

- A more challenging scenario than Internet security
 - **severly resource-constrained** devices;
 - more serious **privacy threats** than the Internet;
 - new threats deriving from **physical locality**.
- Three approaches
 - **Conservative**: use Cryptography
 - **Progressive**: new execution framework
 - get help from the environment;
 - **Game Theoretic**: base trust on selfishness and rationality;

The new challenges

- **low** computational power;
 - need for a new framework for security protocols;
 - need to re-design security protocols;
 - new crypto primitives;
- **myriads**:
 - no centralized control;
 - no a-priori trust structure;
 - mobile device must adapt to environment;
- **spatial localization**:
 - location-based security;
 - location privacy;
 - new attacks are possible (physical attacks);



The conservative approach

Base Security on Cryptography

The conservative approach

Base Security on Cryptography

but...

Base Cryptography on Adversary Limitations (not just computing power)

- Adversary has bounded storage capacity
- Adversary can only capture a fraction of the devices

Shared Key Establishment

A FRONTS result

A source of random bits broadcasts more traffic than adversary can store

- Defining blocks/sections of random sequences, rather than bits
- Random permutation of the bits among the concatenation of the chosen sections
- Fit multi-frequency wireless communication
- Choice subset of frequencies implies exponentially growing security parameter
- Establishing short secret from scratch.

Shared Key Establishment

Pool of keys

- the SYSTEM generates a large pool of n keys
- each device receives a subset of keys of cardinality k
- two devices determine the session key based on the keys that they share

Capturing keys

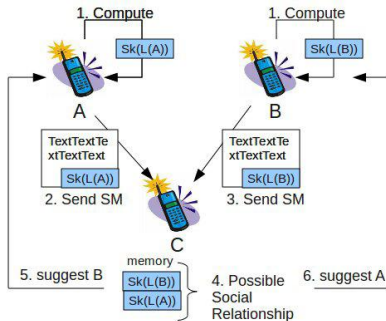
- an adversary can reverse engineer some devices
- no more protection with the captured keys

Shared Key Establishment

A FRONTS result

- each temporal key encrypted **by m randomly chosen predistribution keys**
- the number of shared keys increases, but their positions change after each re-distribution.
- adversary needs to hold most keys to impersonate a device

Privacy through more traditional means



$Sk(X)$ = a sketch, i.e., a compact representation of user X's profile
 Similarity between sketches (Jaccard coefficient) "implies" some kind of social relationships

Strong security

From weak privacy...

- Sketches are not completely secure
- As an example of the type of information that is leaked by the sketch $sk(A) = (\min_1(A), \dots, \min_m(A))$ of profile A , we point out that if $h_i(x) < \min_i(A)$ then certainly $x \notin A$.

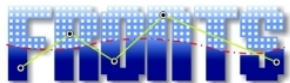
...to strong privacy – A FRONTS result

We present a protocol that uses an additively homomorphic encryption scheme (Paillier cryptosystem), to securely compute the Jaccard coefficient of two profiles.

The progressive approach

Getting help from the environment

- computational load for carrying out a protocol can be shared among a group of **security proxies**;
- security proxies can be woven into an **active** environment;
- private information must not be leaked from the device to the proxies;
- proxies are not trusted;
- efficiency;
- no (or very little) infrastructure should be assumed;



Privacy

- RFID will broadcast its content every time it is queried;
- the item to which it is attached (and its owner) can be traced;
- do not want to remove RFID for post-sale management (e.g., return of unwanted items, warranty)
- cannot remove if RFID needed to track borrowed items (e.g., public library)

Randomizing Encryption for RFID Tags

- objects are tagged so that owner can store info on tags;
- info are encrypted so that only owner can decrypt it;
- ciphertexts can be traced;

- **randomizers** are woven into the environment;
- every time a tag is within range
 - the randomizer reads the tag;
 - and re-writes it;
 - without modifying the encrypted content;

A FRONTS Result: solution based on pairings.

Random beacon: a simple security proxy

- introduced by Rabin for Byzantine Agreement;
- at regular intervals, a number of random bits are announced to all players;
- physically implementable and thus no trust model!

Cryptography vs Game Theory

The Crypto Approach

Authorization is granted based on “*who you are*”.

Major security task: identify who you are, and act accordingly.

Cryptography vs Game Theory

The Crypto Approach

Authorization is granted based on “*who you are*”.

Major security task: identify who you are, and act accordingly.

The Game Theory Approach

Identity is not well defined.

Authorization is granted based on “*how you behave*”.

Major security task: keep track of history.

Goal

Design a protocol for the players:

Design criteria

- the protocol is in equilibrium
 - no player benefits from deviating from the protocol;
- the protocol guarantees a “good” global performance;

Goal

Design a protocol for the players:

Design criteria

- the protocol is in equilibrium
 - no player benefits from deviating from the protocol;
- the protocol guarantees a “good” global performance;

Trust

- is based on **selfishness** and **rationality**:
 - it is in my interest to follow the protocol;
- is not based on **friendship**:
 - I prove to you that I am on your list of friends;

The trust model of correlated equilibria

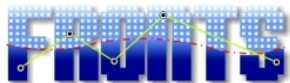
Trust model

- mediator assumed to sample the correct distribution;
- mediator assumed not to tell the output given to other party;
- private channels between mediator and each of the party.

The trust model of Stackelberg leader

Trust model

- leader assumed to sample the correct distribution;
- leader assumed not to tell the output in advance.



FRONTS findings

Artefacts must share common resource and trust each other:

- 1 correlated equilibria solution
- 2 better solution with repeated games
- 3 better performance with Stackelberg

Who designs the algorithm

Algorithm designer has to have (almost) complete knowledge of the scenario.

Impossible in highly dynamic scenari.

Who designs the algorithm

- what happens in repeated games?
- in Nature, **evolution** is the algorithm designer;
- in advanced societies, **culture** (through imitation) is the algorithm designer;
- for small artefacts, **adaptive heuristics** can lead to good equilibria;

Conclusions

- A more challenging scenario than Internet security
 - **severely resource-constrained** devices;
 - more serious **privacy threats** than the Internet;
 - new threats deriving from **physical locality**.
- Three approaches
 - **Conservative**: use Cryptography but assuming adversary limitations other than time.
 - **Progressive**: new execution framework
 - get help from the environment;
 - **Game Theoretic**: base security of selfishness and rationality;