2. Dagstuhl Seminar – Outline of ideas

Günter Müller, Michael Kreutzer, Alf Zugenmaier

Privacy-protecting Addressing In Spontaneous Networking: Location Addressing Instead Of Using A Device Address

Abstract

In the initial stages of data processing, protection of the private sphere was guaranteed by data protection based on centralized data processing. Through the creation of the Internet and the increasing networking of the computer, particularly between enterprises, new security problems arose which are solved by copying the old model of the firewall and strengthening authentification (PKI). These mechanisms, i.e. firewalls and PKI, are reaching their limits through the trend of spontaneous networking and the miniaturizing of intelligent end devices, together with the mobility of the user and end devices.
Increasingly smaller mobile and stationary devices are spontaneously networking with one another. With each transaction, data tracks are left which ultimately enable a linkage of a clearly identified device to a place and time and the relating to an individual. In such an environment, security, particularly the privacy of the user, is up for consideration: data accumulates on a massive scale over which the user has hardly any more control with regard to collection, access, alteration and distribution.
As a result, many experts proclaim the end of privacy through ubiquitous computing. They prophecy the omnipresence of computers, similar to the invisible presence of everyday electric motors.
The following problems arise:
Which models and abstraction processes can enable security in an environment in which devices network spontaneously with one another, i.e. without direct administrative intervention?
Mechanisms (like cryptography) are often no longer possible, as there is no more room on the chip for these functions due to miniaturization of the devices. Can privacy still be nevertheless protected? If yes, with which mechanisms?
In this paper, we propose a new device addressing which keeps the data track to a minimum: merely the location is used for addressing a device in spontaneous networking (e.g. in a radio-based network). For the analysis of this new way of addressing, we have produced the concept for a prototype as proof of feasibility. The theoretical analysis is based on a hybrid process which contains the element of qualitative and quantitive argumentation.

I. Motivation

In future, the information will be on devices in networks which constantly newly reconfigurate when devices and services re-register or ones logged-in quit the networks. In addition, these devices can also be mobile. In the course of this mobility, devices register themselves in other networks, for example when they enter into their radio communication range. The operating authority

of other devices of this radio communication network have no interest, however, in the data protection of the remaining registered devices.
Spontaneous networking means: devices can “communicate” directly with one another (i.e. without explicit, external network infrastructure, therefore without involving the networking operator). The radio-based technologies like Bluetooth and IEEE 802.11 point in this direction. Optical networking is also being examined for minute devices. As soon as a device comes into the “network hemisphere” (mostly the attainable radio communication range) of another device, the devices start to communicate with one another. What data is hereby exchanged, how the devices recognize one another and disclose their identity and, above all, how the data flow can be controlled, has not yet been investigated during this technical discussion, feasibility and miniaturization were in the forefront.
Through mobility, the physical location of the user takes on a new significance, the context of a user can be derived from the location. A brand new working group of the IETF is working on “spatial location information”.

II. Related Work

Many scenarios are feasible with regard to the new developments in the sphere of spontaneous networking, mobility and their effects on privacy and security.
In Langenheinrich’s article [Lang01], six principles for privacy protection are proposed, which are invariant towards these scenarios. These principles are abbreviated in the following and repeated with reference to the results.

1) Notice. Whenever devices carry out security-related actions, the people concerned should be informed. This can take place, for example, analogous to the radio data system (RDS) for radio traffic service, whereby the playing of a CD or music cassette is interrupted for the traffic announcement.
2) Choice and Consent. As stipulated in the various guidelines on data protection, it is not sufficient just to inform people about data collection, the users should be able to actively decide, whether and which data about them is being collected and also be able to have access to the data, to alter or erase it.
3) Anonymity and Pseudonymity. As far as possible, data should not be able to be linked to individuals and one should be able to conceal one’s true identity as far as possible with pseudonyms.
4) Proximity and Locality. Proximity and locality should always be applied when the three points above cannot be completely fulfilled. Suppose, for example, there were a public printer which archived all the documents it had ever printed. It should at least be impossible to retrieve this data from a distance. Anyone who rummages in this database should at least be physically near the printer, just as the searching for evidence by police can only take place at the scene of the crime.
5) Adequate Security. For confidentiality in information and communication technology, cryptography is “classically” regarded as the main mechanism. However, the use of cryptographical algorithms is frequently no longer possible with strongly limited system resources of the

new small devices. Security models which are mainly based on these should be reconsidered. If points 1 to 4 are strictly observed, then it is perhaps possible to operate the basic infrastructure without an explicit security model.

6) Access and Recourse. Alongside the principle of the data-saving collection of data only for a specific purpose, this point emphasizes the possibility of objection and of recourse in the event of conflict. Non-denial mechanisms are required for this.

The realization of these demands is not even guaranteed in the spontaneous networking environment. These problems become more evident in ubiquitous computing.

III. Location Addressing: Privacy in Spontaneous Networking

Our proposal ensures that communication is anonymous without additional procedure. The addressing of devices should no longer primarily be by way of device identification but only via location addressing. The realization of the concept will be examined in an e-commerce scenario, theoretical analyses are being conducted by means of a hybrid methodology with elements of qualitative and quantitative argumentation.

Definition of Location Addressing and Potential Advantages

As a starting point, the following variation of the Client-Server-Model is examined: devices use services of existing networks as clients. The location addressing is a new way of addressing for the clients. It enables a device to be addressed which is at a physical location and which does not have to give any device identification. With radio-based networks, it is transformed as multicast on all devices in a certain volume in which none, one or several devices could be located. With mains connected networks, the network connection is addressed without knowledge of a device identification of the connected device.
This addressing is as such “natural” as it only uses the physical location, therefore a quality of the real world, as address.
This new way of addressing can protect privacy. It provides the basis for negotiations on the revelation of identity.
Location addressing also has the following properties:

- Privacy is protected without expensive mechanism.
- Location addressing is simple as technical and natural perspectives converge.
- Location addressing has a high commitment towards random pseudonyms as it specifies the location as “delivery address”. This can be verified.
- Location and time are obtained by radio-based networks virtually as by-products and are natural coordinates of the real world. As such, they remain constant, even if the technical properties of networks should change. They thereby survive future developments.
- Location coordinates prevent misuse: individuals cannot easily initiate a fraudulent act from several positions (a “distributed attack”). In the event of suspicion of a fraudulent act, the device is located, if the fraud

is also there, he can be arrested (for the arrest of individuals their location must be known).
- Location addressing can constitute authorizing support. Anyone who is in a certain sphere has, for example, other access rights than someone who externally accesses a system (compare [Goll00] and [LeMa98]).
- Location addressing enables routing: switching nodes pass the traffic on according to the location coordinates.

Location addressing cannot make reachability of a device and thereby of a mobile individual available from outside. In mobile radio networks, this property will, for example, be gained through a directory service which allocates the device address a location, namely the exchange station, in which the mobile telephone has logged in. Suppose an individual possesses a mobile telephone and a device which can be addressed by location addressing. Through the external tracking, the device which only uses location addressing can also be linked with the user. A new model of reachability should be developed in the research project which can prevent this catenation.

How far is the individual's private sphere violated through transactions with devices?

An individual conducts a transaction at one location with one device. His private sphere is then affected when the relationship between individual and action (anonymity) or the relationship between individual and location is unintentionally disclosed.

With location addressing there is the relationship action-device-location-person, whereby here the relationship device-location is concealed through the omission of the device address.

We thereby have a comparison of the ways of addressing in relation to the protection of privacy. The likelihood of an individual remaining at one location should also be considered here, with a location such as "Friedrichstr. 50, Room 04019, Freiburg" the anonymity group is generally much lower than a location such as " Cathedral Square Freiburg, in front of the hot-dog stand".

The end devices and kiosks in this setting produce the location addressing as follows: Infrared should be used in the lowest layer. Layers 2 and 3 are programmed so that the dot address is converted into a location address. The device address in the IrDA standard are encapsulated so that no new implementations have to be created here. The mechanisms for spontaneous networking and the service administration are programmed in Jini on the application layer.

If a dealer insists on higher commitment (due to the size of the amount for example), then more commitment can be negotiated (i.e. ultimately by stronger authentication). The negotiation proceeds, for example, as follows: in an initial step, the exact time (for producing a nonce) can be determined, in a next step, the location and time information can be digitally signed (time and location stamp service). If this does not suffice, then chainable pseudonyms or even revealing identity or intermediate phases can be the subject of negotiation, similar to the Freiburg identity manager.

As a result of the examination of the first hypothesis we expect that location addressing will prove to be the best privacy-protecting way of addressing for

certain scenarios in ubiquitous computing. These scenarios are characterized in that the user moves with devices which have hardly any or no capabilities whatsoever of implementing cryptographic algorithms and therefore cannot use any strong anonymity and unobservability mechanisms like Mixes. The mobile use of location addressing therefore conceals the relationship between individual and device. The question as to whether it does this adequately - with regard to privacy - should be answered in the research project.
Location addressing should not replace other unobservability and anonymity mechanisms, but supplement them. If the user is in his apartment for example, then his small mobile devices can connect with the home network which in turn is connected to the Internet via MIX cascades.

The following questions were raised and should be answered with the aid of the prototype – at least in principle:

- Can a device actually be addressed when it is in motion (reachability)?
- How exact must the addressing of the location be, particularly when the transactions take longer than the device remains in one location (handover) and other devices are in the vicinity?
- Is a transactional cover always necessary?
- Does the solution scale?
- How does one prevent the illegal use of devices and how is the use of services remunerated?

IV. Literature

[Goll00] Dieter Gollmann: Computer Security, New York, Wiley, ISBN: 0471978442, 2000

[Lang01] Marc Langheinrich: Privacy by Design – Principles of Privacy – Aware Ubiquitous Systems.
Submitted for publication, May 2001; accessed on 31st May 2001 under
http://www.inf.ethz.ch/vs/publ/papers/privacy-principles.pdf

[LeMa98]Ulf Leonhardt and Jeff Magee. Security Considerations for a Distributed Location Service. Journal of Network and Systems Management, 6(1): 51-70, March 1998.

[ScHo97] Björn Schieffer, Günter Hotz: Diagnosis of Tank Ballast Systems.; *In Proceedings of the 2nd International Symposium on Intelligent Data Analysis,* IDA97, Springer LNCS 1280; (see also
http://www-hotz.cs.uni-sb.de/schieffer/publications/IDA97.ps.gz accessed on 31.5.2001)