A Methodology for Evaluating Threats to Multiple Virtual Identities

Christian Hauser

Institute of Communication Networks and Computer Engineering
University of Stuttgart
christian.hauser@ikr.uni-stuttgart.de

ABSTRACT

Future will spread communicating applications further into users' lives. Not only for this reason, privacy protection increases in relevance. One approach for a user to protect his private sphere is to appear under several virtual identities. However, this bears new threats. In this paper, a model and an evaluation methodology are presented to evaluate systems regarding those specific threats.

1. INTRODUCTION

Telecommunication networks undergo drastic changes, currently. It is widely expected that current walled-garden business models will be broken up and smaller, specialized service providers and network operators will enter the field. Those providers do not have to provide for the full set of functionality ranging from the access networks over consumer services up to a full billing infrastructure, which will lower the burden to enter the market.

Such a multi-operator scenario introduces new challenges in trust as well as the design and placement of security mechanisms. For instance, users will not trust all (potentially small) future operators to the same extent than they trust today's large well-established operators with respect to the protection of their private data. Thus, privacy protection mechanisms will grow in importance.

This tendency is supported by the growing diversity of networked applications. More and more aspects of the user's private as well as professional life will be penetrated by networked applications. This leads to a growing number of personal aspects to be represented in the connected system and thus, potentially being subject to abuse.

Satisfying the growing importance of technical privacy protection measures, a promising approach is the use of multiple *virtual identities* (VIDs) per user. A VID consists of a pseudonym with an arbitrary set of (personal) attributes. Accordingly, the user can appear as different virtual users in the system, thereby only disclosing the minimal necessary set of attributes for each specific service use. Thus, it is possible for the user to split up the rich data trace left in the system spanning across all used services into several smaller ones only comprising data of one or a few service usages. These smaller data traces are assumed to be generally less privacy intrusive as the probability to contain sensitive facts is lower in a smaller data set. For instance, it is acceptable that a service knows a user's location every now and then but not over a full period of time covering months as this would lead to a detailed personal profile.

Figure 1 illustrates this idea by an example of splitting the overall profile of a user containing data from all services into two separate VIDs both containing only a part of the sensitive information.

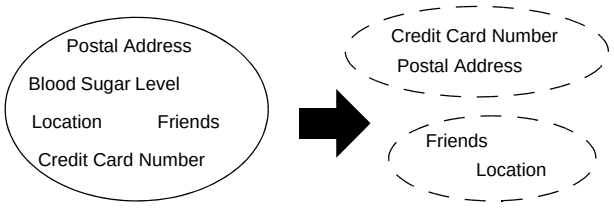

Figure 1. Splitting overall user profile into virtual identities

It is straight forward to see that the goal of potential attackers will be to extend their (restricted) view on the user. This can happen in three ways: First of all, the attacker can observe more than he already knows, e.g., by scanning a wireless link over a longer time. Second, attackers can deduce new facts about the user from the aspects they are knowing, e.g., by deducing the user's location from the IP address. Finally, attackers can link several VIDs allowing for a merge of the fact sets of both VIDs, e.g., by observing an identical IP address at the same time at both VIDs (knowing that an IP address can only be used by one user at a time).

Those attacks can be focused on specific (mostly user related) data items in a system. They can also be based on knowledge outside the technical system, e.g., if an attacker sees a user in real life. The latter attacks are out of scope here as the goal of our methodology is to analyze systems regarding threats they are adding to real life. Moreover, different attackers can have different capabilities of attacking the VIDs of a user. Some attackers can make more observations than others, e.g., scan more wireless links, and some know more sophisticated interpretation rules for the deduction of sensitive facts from the observations than others do.

Therefore, an analysis of an IT system regarding protection capabilities of multiple VIDs requires a definition of the so-called universe of discourse or miniworld, that will be considered. This miniworld consists of

- the relevant data items under consideration,
- the relevant relations between them, i.e., the considered semantics,
- the interpretation rules taken into account as attacks.

In Section 2, an approach for modeling the universe of discourse is presented, followed by a methodology for evaluating a system regarding threats on VIDs in Section 3. Throughout the paper, the example of Mobile IPv6 [1] as system under evaluation is used. Finally, Section 4 concludes.

2. MODEL

In this section, at first some definitions are given. Then, the rules for interpretation of the knowledge by an attacker are presented. Finally, a simplified model of Mobile IP is explained to illustrate the idea. The goal is to identify, which items of the miniworld, i.e., which elements in the system, are sensitive with respect to applying one of the rules to them.

2.1 Definitions

Here, some definitions are given in order to understand the model and its use in the evaluation methodology.

- Fact: A fact is information about a state or the transition of a state (an event). A fact is an instantiation of a fact type. A fact has a value and a timestamp, when this value was known to be true. Two facts being identical in time and value are the same fact.
  Example: The information that at time T a certain IP address had the value 129.69.170.1 is a fact of the type IP address.
- Fact Set: A fact set are several facts that are known by the attacker to be about the same user. A fact set is a fact itself in the sense that it can be treated in a rule like a common fact. A fact can be contained in several fact sets.
  Example: Three values of a care-of address belonging to the same device are building a fact set with elements of the type care-of address.
- Observation: An observation is a special fact set, which is directly observed by an attacker, i.e., not deduced from other facts.
  Example: An IP address as seen by an attacker on the wireless link is an observation.
- Knowledge: The knowledge of an attacker is the sum of all facts known by this attacker.
  Example: All IP addresses of a certain device an attacker has ever seen.
- Rule: A rule is a prescription how to interpret knowledge to gain new facts. Here, rules can be for the deduction of new facts or for the merging of two fact sets.
  Example: If the IP address is known and it is created by encoding the MAC address, the MAC address is also known.

2.2 Interpretation Rules

In this section, the rules for interpretation of knowledge by an attacker are presented. There is a rule about when a deduction of

new facts from known facts is possible and when a merge of two fact sets is possible.

Deduction Rule

A deduction of a new fact from a known fact is possible if

1. facts of type of the known fact can be mapped uniquely on facts of type of the new fact
2. AND the function of this mapping is known

An example can be an autoconfigured IP address, which contains the MAC address. A fact of the type IP address can be mapped uniquely onto a fact of the type MAC address and this mapping function is known: "Take the least valued 48 Bits". Thus, if an IP address is known, the corresponding MAC address can be deduced.

Merging Rule

It is possible to merge two fact sets, i.e., to identify that they are both about the same user, if

1. there is a fact of identical type in both fact sets
2. AND those two facts have the same value and timestamp
3. AND this fact type can be uniquely mapped onto the user, i.e., an identity of such facts implies an identity of the corresponding users

In the example of the MAC address, this means that if there are two fact sets containing a fact of the type MAC address each, and these facts are identical, it is obvious that both fact sets are about the same user as a MAC address is only owned by one user (assuming a scenario where user's don't change their devices). Thus, both fact sets can be merged. If both fact sets belong to different VIDs, they can be linked by an attacker.

2.3 Model of Mobile IP

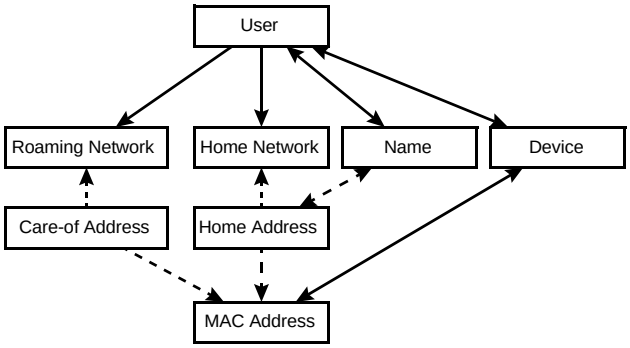

Figure 2. Simplified Model of Mobile IP

Figure 2 shows a simplified model of Mobile IP. The model expresses the miniworld under consideration. Everything, which is not in the model will not be considered in the following evaluation. The relevant data items in the square boxes are found by extracting the attributes of the system, which directly contain user-related information or which can be mapped uniquely on items containing user-related information. Examples for such data items are protocol fields or addresses. The arrows are found by examining the cardinality of the relations thinking in an entity-relationship model. If one item of the left type refers to several items of the right type (e.g., one Roaming Network serves several users), there is an arrowhead on the left and no arrowhead on the right. If it's a one to one relation (e.g., one MAC address per Device and one Device per MAC address), there are two arrowheads.

The model can be used to determine the interpretation possibilities by attackers. First of all, it shows possibilities of merging fact sets. If there is a path of arrows of a certain fact type to the type *User* following only arrows in the direction of an arrowhead, it means that there is an N:1 relation of this type to the type *User* or in other words, facts of this type can be uniquely mapped to one user (requirement 3 of the Merging Rule). Thus, an identity of two facts of the given type directly imply an identity of the user. If those two facts are from different fact sets, those fact sets can thus be merged.

The model also shows possibilities of deducing new facts from known ones. The arrows mean the existence of a unique mapping function in the direction of their arrowheads (requirement 1 of the Deduction Rule) and a dashed arrow means that the mapping function is assumed to be known by potential attackers (requirement 2 of the Deduction Rule).

An attacker can be modeled by marking those data items, which can be observed by him. The model also shows the attacker's power in terms of possible interpretations by indicating the known mapping functions. Finally, the model expresses the assumed scenario in the sense, e.g., that devices are only used by one user and that IP addresses contain the MAC addresses.

3. EVALUATION METHODOLOGY

The model can be used to evaluate a system with respect to protection of VIDs. Thus, a methodology for evaluating a given system about its VID protection properties is to follow this procedure:

1. Define the miniworld by modeling the system's relevant properties like shown above.
2. Mark those fact types, which can be observed by an attacker.
3. Mark those fact types containing personal information.
4. Evaluate the possibilities to deduce fact types containing personal information from observable fact types by applying the Deduction Rule.
5. Evaluate the possibilities to merge fact sets of different VIDs by applying the Merging Rule.

In case of different attackers to be considered, steps 2-5 are to be followed for each attacker.

By the evaluation, weaknesses can be clearly identified and it can be determined where improvements of the system can start. There are protection patterns for the specific problems, which can occur, i.e., deduction and merging. Those patterns can be assembled to a new overall system with improved VID protection capabilities, thus yielding in a well reasoned solution. An obvious example for such an improvement is to avoid the weakness that IP addresses containing the identical MAC address (arrow from Home Address to MAC Address) allow for merging of fact sets. A protection can be achieved by building IP addresses in a different way without the MAC address, e.g., like in [2]. Then, an identical IP address can be assigned to different devices at different times and thus, only leads to a link of fact sets if it is observed simultaneously.

This methodology has been used to design an architecture for mobile IP-based communication focused on VID protection. In its core, it is configurable by the user to suit his personal trade off between privacy protection and scalability [3].

4. CONCLUSIONS

The model and the evaluation methodology can be used to analyze existing IT systems regarding privacy threats, especially concerning the VID approach. This is the first work in supporting the evaluation and design of systems for protection of multiple virtual identities to the knowledge of the author. Existing work usually focuses on general security evaluations of IT systems in companies like, e.g., [4], [5] and is less formalized. There is also work in finding metrics for unlinkability [6], which is relevant for the protection of virtual identities, although it is another focus than the work presented here.

5. REFERENCES

[1] D. Johnson, C. Perkins, J. Arkko: Mobility Support in IPv6, RFC3775, June 2004.

[2] T. Narten, R. Draves: Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 3041, January 2001.

[3] C. Hauser: Mobility Management Meets Privacy – the Failure of Existing Proposals and a New, Future-Proof Approach, Proceedings of the ACM International Workshop on Mobility Management and Wireless Access, Philadelphia, PA, 2004.

[4] (CCEB) Common Criteria Editorial Board: Common Criteria for Information Technology Security Evaluations. Report, 1998.

[5] IT-Grundschutz-Kataloge, Bundesamt für Sicherheit in der Informationstechnik (BSI), http://www.bsi.bund.de/english/gshb/index.htm, 2005.

[6] S. Steinbrecher and S. Köpsell: Modelling unlinkability, in R. Dingledine, editor, Privacy Enhancing Technologies (PET), LNCS 2760, pages 32-47. Springer-Verlag, 2003.