TOR is running – why do we need research?

Dogan Kesdogan, Vinh Pham
Email: kesdogan@ur.de, pham@wiwi.uni-siegen.de

Abstract

TOR is running, but there is still a need for new researches to achieve a better anonymity. It is not enough to change the theory and to make it applicable to TOR as the Entropist paper seems to suggest. As a Chinese proverb tells, "If you do not change direction you will end up where you are going." If you do not change direction in this context, you will stay with a week technique. Thus, there are many reasons to change the direction radically. The most important reason is to provide a stronger anonymity.

Introduction

When Onion Routing (the predecessor of TOR) was suggested [GRS96], we had a similar idea and proposed a similar technique [FKK96], as confirmed in a follow-up paper of OR [RSG98]. Therefore, we can assume that we had the same reason and idea to suggest such a technique: it was the time to do something that is practical and applicable to *the Internet*.

It is certain that security is not for free. Doing something practical means that we have to omit some costly features of the original MIX technique. Therefore, we have suggested, e.g., to omit the batch feature (i.e. the collection of a certain number of messages). This is because of our evaluations that show that batching was too time consuming and costly at that time.

Coming back to the paper of Paul Syverson that claims that, if we can find a proper theory for TOR then the anonymity problem is solved. We claim that it is difficulties to find the right theory for TOR, because TOR is based on something that we call "fuzzy anonymity".

The evaluation problem of TOR starts with the attacker model. Even though the attacker is a local attacker, TOR provides in some cases no anonymity, if the attacker controls the right ORs. If we try to evaluate this then we have to deal with fuzziness by assuming that certain stations are trustworthy and thus unlikely controlled by the attacker. This general problem does not change, if we add a trustworthiness parameter *p* as suggested in the Entropist paper. It makes the problem even more severe, since we have no chance to precisely determine this parameter in reality.

What we should provide to users is an anonymity technique that is trusted by users, because of its provable anonymity. If we cannot control our anonymity protocol with a security parameter that we can determine (like the key length in cryptography) then we do not provide a dependable system.

We think that it is the right time to (re)think about the cost assumption. Seventeen years ago, it was a good idea to omit batching. But now, with the technical and theoretical progress, it might be the right approach to encourage researchers to find ways to resolve the old problem of cost versus security. Otherwise we will not solve the simple and the most dangerous attack, the correlation attack with a weak adversary that just observes the end points.

Andreas Pfitzmann and his group claimed, e.g., in [PPW91] that batching alone is insufficient for anonymity. Therefore they suggested redesigning the network to provide a maximal anonymity (see also [PW87]). As the network research community is currently working on topics like the Future Internet and new protocols, there is great opportunity to take part in that discussion. Yes, also as security and privacy researchers, we should to be a part of the redesign approach. Otherwise, we have to live with the results that the network researchers will provide.

Literature

[GRS 96]David M. Goldschlag, Michael G. Reed, Paul F. Syverson. "Hiding routing information." *Information Hiding*. Springer Berlin Heidelberg, 1996.

[RSG 98] Micheal G. Reed, Paul F. Syverson, David M. Goldschlag. "Anonymous connections and onion routing." *Selected Areas in Communications, IEEE Journal on* 16.4 (1998): 482-494.

[FKK 96] A. Fasbender, D. Kesdogan, O. Kubitz, (1996, May). Variable and scalable security: Protection of location information in mobile IP. In *Vehicular Technology Conference, 1996.'Mobile Technology for the Human Race'., IEEE 46th* (Vol. 2, pp. 963-967). IEEE.

[PPW 91] A. Pfitzmann, B. Pfitzmann, M. Waidner. "ISDN-mixes: Untraceable communication with very small bandwidth overhead." *Kommunikation in verteilten Systemen*. Springer Berlin Heidelberg, 1991.

[PW 87] A. Pfitzmann, M. Waidner. "Networks without user observability." *Computers & Security* 6.2 (1987): 158-166.