HAL
archives-ouvertes.fr

Linking a Social Identity to an IP Address

Arnaud Legout, Walid Dabbous

▶ **To cite this version:**

Arnaud Legout, Walid Dabbous. Linking a Social Identity to an IP Address. ERCIM News, ERCIM, 2012, Special theme: Cybercrime and Privacy Issues, 90, pp.2. hal-01270464

HAL Id: hal-01270464
https://hal.inria.fr/hal-01270464

Submitted on 4 Mar 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Linking a Social Identity to an IP Address

by Arnaud Legout and Walid Dabbous

Linking a social identity such as a name to an IP address is generally believed to be difficult for an individual with no dedicated infrastructure or privileged information. Although an individual's ISP has access to this information, it is kept private except in the case of a legal decision. Similarly, some big Internet companies such as Facebook and Google might be privy to this information but it will never be communicated as it is an industrial secret used for targeted advertisements. In the context of the bluebear project, we show that it is possible for an individual to inconspicuously make the link between social identity and IP address for all Skype users.

The privacy threat that exists online is a growing concern. Most academics and journalists focus on the threat posed by the huge amount of data collected by big companies such as Google or Facebook. However, the case of individuals, with no dedicated infrastructure or privileged information, trying to infringe Internet users' privacy is largely overlooked owing mainly to the misconception that it is impossible for a single individual to spy on Internet users at a large scale. The goal of the bluebear project, led by researchers at Inria in collaboration with researchers at the Polytechnic Institute of New York University (NYU-Poly), is to explore whether individuals can infringe Internet users privacy at a large scale.

In a first study, we have shown that an individual can monitor all BitTorrent downloads in real time for all Internet users without any dedicated infrastructure. To prove this, we collected 148 million IP addresses downloading more than one million contents for 103 days, and managed to identify 70% of users who first insert content in BitTorrent. We have also shown that using Tor, the anonymizing overlay, does not help; Tor does not protect against the exploitation of an insecure application (eg BitTorrent) to reveal the IP address of a TCP stream. Even worse, because Tor sends application data together over a single circuit, the IP address found for a given application can be associated with all other applications of the same circuit.

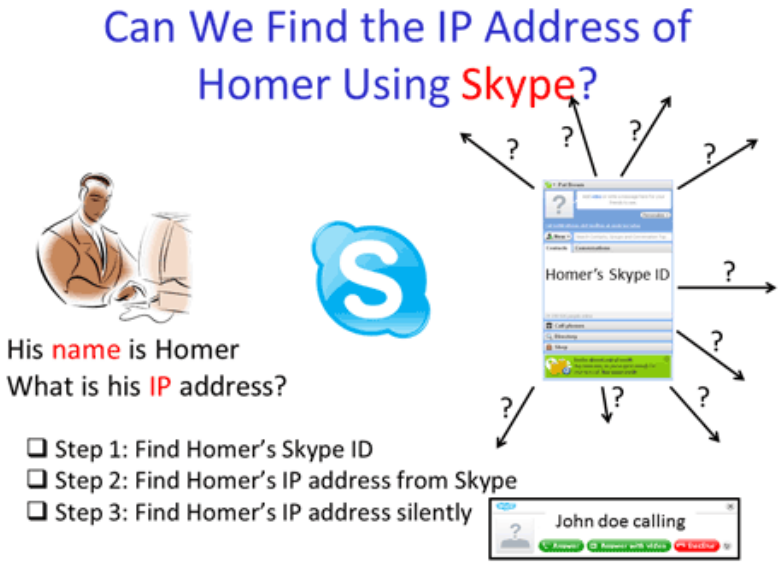

Figure 1: High-level description of the social identity and IP address linkage exploiting Skype.

Although profiling Internet users by IP addresses raises ethical concerns, it pales in comparison to profiling by social identity. Associating a social identity to a profile enables very severe privacy

infringements that might lead to real world attacks such as blackmail or targeted phishing attacks. We used Skype as a case study to show that an individual can link a social identity and an IP address. In particular, we have shown that an individual can inconspicuously retrieve the IP address of any Skype user. As 88% of Skype users provide a name associated with the account and 82% provide additional information like a country or Web page, most Skype accounts can be directly associated with a social identity, thus making it possible to link social identity and IP address. In addition, we can follow the mobility of Skype users. Interestingly, on a sample of 10,000 random Skype users, we observed that over a two week period 4% of them moved from one country to another, 19% moved from one ISP to another, and 40% moved from one city to another. Therefore, we identified real mobility patterns for a regular Skype user.

Even more of a concern, by tracking the mobility of an Internet user along with the mobility of acquaintances (retrieved from a social network profile like Facebook or LinkedIn) it is possible to track social interactions, that is who an Internet user meets and where. This has worrying implications for both the personal and professional lives of Internet users.

The technique we use to map a social identity to an IP address is based on the identification of specific communication patterns that are inherent to any peer-to-peer system. Therefore, we do not rely on a specific bug in Skype that exposes the IP address, but on the intrinsic peer-to-peer architecture used by Skype and the lack of privacy of the IP protocol used on the Internet. As a consequence, the kind of attacks we have documented can be adapted to most systems that use a peer-to-peer architecture. In addition, it is extremely hard, without a major architectural change to Internet communications, to make such attacks impossible.

Our goal in the next few years is to participate in the design of a more secure, privacy preserving Internet communication infrastructure.

Link:
http://planete.inria.fr/bluebear

References:
[1] S. Le Blond, C. Zhang, A. Legout, K. Ross, and W. Dabbous, “I Know Where You are and What You are Sharing: Exploiting P2P Communications to Invade Users' Privacy”. In Proc. of ACM SIGCOMM/USENIX IMC'11, Nov. 2--3, 2011, Berlin, Germany.
http://hal.inria.fr/inria-00632780/en/

[2] S. Le Blond, A. Legout, F. Lefessant, W. Dabbous, M. Ali Kaafar, “Spying the World from your Laptop - Identifying and Profiling Content Providers and Big Downloaders in BitTorrent”. In Proc. of LEET'10, April 27, 2010, San Jose, CA, USA. http://hal.inria.fr/inria-00470324/en/