Telecommunications Policy 37 (2013) 748–756

Contents lists available at ScienceDirect

Telecommunications Policy

URL: www.elsevier.com/locate/telpol

Application-layer design patterns for accountable–anonymous online identities

Josephine Wolff*

Massachusetts Institute of Technology, 77 Massachusetts Avenue, 32-G806, Cambridge, MA 02139, USA

ARTICLE INFO

Available online 14 June 2013

Keywords:
Accountability
Anonymity
Online identity
Application design
Privacy
Social networks

ABSTRACT

Both anonymity and accountability play important roles in sustaining the Internet's functionality; however, there is a common misconception that increasing the anonymity of Internet identities requires diminishing their accountability, and vice versa. This paper argues that by implementing accountability mechanisms and anonymity protections at the application layer of the Internet, rather than the network layer, it is possible to develop a variety of different types of accountable–anonymous virtual identities, tailored to meet the needs of numerous, diverse online applications. Examples are drawn from several identity mechanisms used by existing applications and general design patterns for implementing accountability are discussed, with particular emphasis on designing identity investment–privilege trade-offs, conditional anonymity schemes, and aggregated, identity management systems, as well as the role of scoped identities and linked identities in promoting online accountability.

1. Introduction

Both anonymity and accountability play important roles in sustaining the Internet's functionality. Without anonymity, a broad swath of users, ranging from activists living under oppressive regimes to people wishing to discuss their sensitive medical conditions, might be unable to pursue their online activities in comfort and privacy. Without accountability, however, it is impossible to curb the numerous forms of misconduct that interfere with users' online experiences and threaten the continued utility of the network. Some advocates have called for the Internet's underlying protocols to be redesigned to embed accountability as a higher priority at the network layer. Former Director of National Intelligence for the United States Mike McConnell (2010) advocated such an approach, writing: "We need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment—who did it, from where, why and what was the result—more manageable." However, several researchers have noted that embedding a strong attribution scheme at the network layer in the manner McConnell suggests could fail to solve some of the most pressing security issues associated with cyber attacks, particularly those routed through multiple computers, while simultaneously posing clear threats to the personal anonymity protections enabled by the current Internet architecture (Clark & Landau, 2010; Knake, 2010).

How, then, can accountability be promoted on the Internet to more effectively prevent and punish misbehavior, without sacrificing all the benefits afforded by online anonymity? Achieving this goal of combining both anonymity protections and effective accountability mechanisms online requires the implementation of a variety of different, context-specific accountability mechanisms at the Internet's application layer, rather than a single, uniform mechanism at the network layer.

[*] Tel.: +1 908 307 6612; fax: +1 617 253 2673.
E-mail address: jwolff@mit.edu

0308-5961/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.telpol.2013.04.001

Examining the strengths and weaknesses of existing application identity schemes leads to identification of effective methods of establishing accountable–anonymous online identities that leverage the power of multiple control points on the Internet and can be used to improve the identity mechanisms of the vast number of applications which benefit from both some degree of anonymity and some means of holding users accountable.

2. The accountability–anonymity axes

There is a common perception that online anonymity protections are irreconcilable with effective accountability mechanisms (Davenport, 2002). This traditional, one-dimensional notion of accountability and anonymity, in which having more of one necessitates having less of the other, is illustrated in Fig. 1.

However, some researchers have criticized this idea that accountability and anonymity are a zero-sum game, pointing out that accountability can exist even in the absence of strong authentication (Farkas, Ziegler, Meretei, & Lorincz, 2002; Johnson, Crawford, & Palfrey, 2004; Schneier, 2006). To clarify the range and variety of accountability and anonymity options available to application designers, an alternate, two-dimensional framework is proposed, shown in Fig. 2. These accountability–anonymity axes represent spectrums along which different degrees of anonymity and accountability may be combined with each other, and the resulting four quadrants provide a framework for classifying and analyzing different online identity schemes.

While the traditional zero-sum framing allows only for identities that fall into either the upper left (strong accountability–weak anonymity) or lower right (strong anonymity–weak accountability) quadrants, the proposed framework opens up two additional quadrants, providing a richer and more nuanced perspective on the interplay between accountability and anonymity. These new quadrants, especially the upper right one which combines both strong accountability mechanisms and strong anonymity protections, are essential for understanding both the challenges posed and the full range of possibilities permitted by an application-layer approach to accountability. To more clearly illustrate these possibilities, it is helpful to populate the proposed accountability–anonymity axes with some representative applications, as shown in Fig. 3.

The upper left quadrant is home to the applications that would pose the greatest security risks if accessed by unauthorized or malicious users, such as military and classified data networks, banking applications, or nuclear power plant systems. In these cases, where all legitimate parties involved in the online transaction—for instance, both a bank and a bank account holder—would reasonably wish for strong and secure authentication of the other participating parties, anonymity is not called for. Instead, robust authentication schemes allow for stronger security and accountability mechanisms that depend largely on identifying the responsible actors in the real world and holding them accountable for their actions in a traditional legal and regulatory manner. The risks associated with unauthorized infiltration of these sorts of networks are simply too high, and the benefits of allowing anonymous activity too minimal, to merit implementing any weaker forms of online identification or alternative, pseudonymous accountability mechanisms.

By contrast, the lower right quadrant is populated with applications where anonymity trumps accountability and users may enjoy very strong identity protections while encountering relatively weak accountability mechanisms. For instance, the express purpose of the application Tor is to protect the anonymity of its users and, in doing so, it has played an important role

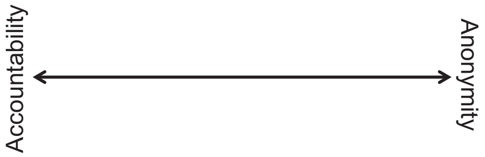

Fig. 1. Traditional framing of accountability and anonymity as a zero-sum game.

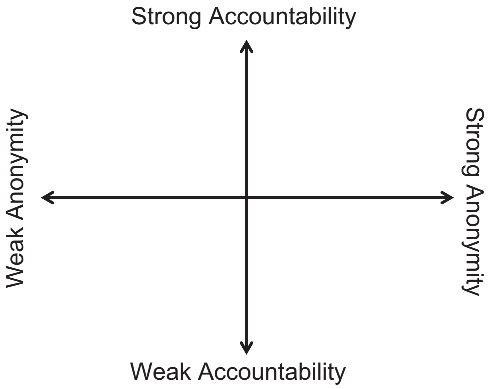

Fig. 2. Proposed four-quadrant space for online accountability and anonymity.