Anonymity in XIA

Nicolas Feltman, David Naylor

December 10, 2011

1 Introduction

The desire for anonymous communication in the Internet has made it a much-discussed issue in both technical and non-technical circles. Users have identified several reasons for wanting online anonymity; in [2], interviews revealed motivations ranging from protecting personal safety to hiding political activity from governments to unknown fears. In one shocking interview from this study, a Romanian woman describes being abducted after posting personal information about herself on a Web site.

Several standard approaches to anonymity have emerged, normally involving some number of explicitly identified proxies (e.g., Tor). Although none of these methods are perfect, they generally meet most users' needs from a technical standpoint. Where many fall short, however, is in making these systems easy to understand and configure for non-technical users; part of our project addresses this issue.

Our goal is three-fold. First, we consider existing methods for achieving anonymous communication in the context of the eXpressive Internet Architecture (XIA) [1]. As we discuss below, novel features of XIA in many cases allow these existing techniques to be implemented more elegantly. Second, we introduce an extension to the XIA socket API, which provides application developers a dead-easy way to use anonymous communication over XIA. Finally, we consider users. We create a preference pane providing OS level control over the extended API functionality. Anonymization settings are controllable by the user through an intuitive, easily understood GUI.

The rest of this paper is organized as follows: in Section 2 we introduce pertinent features of XIA and review common terminology related to anonymity from the literature. Section 3 examines the use of existing approaches in XIA as well as new ones made possible novel features of the architecture. In Section 4 we compare these approaches to one another in terms of the threats against which they provide protection and we compare the "current" version of each method to its XIA counterpart. Finally, Section 5 presents our implementation and in Section 6 we summarize and conclude.

2 Background

Before we discuss anonymity in XIA, we will first discuss XIA itself to highlight the features we will make use of later. Then, we will bring some precision to the term "anonymity" by presenting a review of the terminology used in previous work.

2.1 XIA

Some features of XIA have implications when it comes to anonymity. We briefly describe the key ideas here and elaborate on their impact on anonymous communication later.

2.1.1 Principal-Based Communication

In contrast with today's host-based Internet, XIA provides a framework for communication among *principals*. The idea of principal-based communication is that users should be able to address packets directly

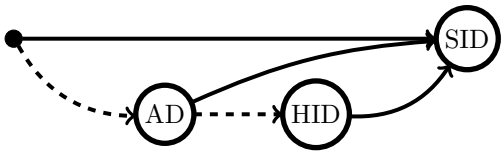

Figure 1: A typical DAG with two fallbacks. Note that higher edges have higher priority; SID is the primary intent, so the network attempts to route it first. If a router does not know the location of SID, or does not understand services, it uses the first fallback and instead routes the packet to SID's AD. Once in the AD, if a router cannot find SID, the packet is routed to HID, the second fallback, before finally being delivered to the service.

to their primary *intent*. For example, a user searching for books on Amazon wishes to communicate with `www.amazon.com`; he doesn't care which particular Amazon server responds to his request.

In this example, `www.amazon.com` can be viewed as a *service* principal. In the case where communication with a particular machine truly is the intent, traditional host-based communication can still be achieved via the *host* principal. Other principals include static *content* (e.g., images) and *autonomous domains* (similar to today's autonomous systems).

2.1.2 DAG-Based Addressing

Addresses in XIA are represented as DAGs (directed acyclic graphs). Using DAGs allows senders to give the network very detailed instructions about how a packet should be routed. DAGs also allow senders to provide *fallback* routes to be used in case the network cannot find the sender's primary intent or does not understand a new principal type. For example, in the scenario above, the user's browser might include the address of a particular Amazon server as a backup in case a packet reaches a router that doesn't know how to find the service `www.amazon.com` directly.

2.1.3 Intrinsic Security

All addresses (or, better put, identifiers) in XIA are *intrinsically secure*; exactly what this means varies among principals. For example, a content identifier (CID) is the cryptographic hash of the content itself, enabling anyone receiving the content to verify its integrity. Hosts and services are required to have a public/private key pair; therefore their corresponding identifiers (HIDs and SIDs) are simply the hashes of public keys. A host can sign any communication it generates with its private key and anyone can publicly verify the signature using the host's ID.

2.2 Anonymity

We adopt terminology proposed by Pfitzmann and Köhntopp [3] to precisely describe various meanings of the term *anonymity*:

Anonymity The state of not being identifiable within a set of subjects, the *anonymity set*.

Unlinkability Two or more items (e.g., subjects, messages, events, actions, etc.) are no more and no less related than they are related to any other item.

Sender Anonymity A particular message is not linkable to any sender and no message is linkable to a particular sender.

Recipient Anonymity A particular message cannot be linked to any recipient and no message is linkable to a particular recipient.

Unobservability The state of messages being indistinguishable from no messages at all.

3 Approach

3.1 Proxies

Nico

3.2 Temporary SIDs

David

3.3 Principal-Based Control

David

4 Comparison

4.1 Services vs. Features

4.2 Threats vs. "Meatures"

5 Implementation

We implemented a single proxy and a version of the API.

5.1 Single Proxy DAG Manipulation

Nico

5.2 In-Network Services Issues

Nico

5.3 OS Integration and API

David

6 Conclusion

References

[1] Ashok Anand, Fahad Dogar, Dongsu Han, Boyan Li, Hyeontaek Lim, Michel Machadoy, Wenfei Wu, Aditya Akella, David Andersen, John Byersy, Srinivasan Seshan, and Peter Steenkiste. XIA: An architecture for an evolvable and trustworthy internet. Technical Report CMU-CS-11-100, Department of Computer Science, Carnegie Mellon University, February 2011.

[2] Ruogu Kang, Sara Kiesler, Peter Kinnaird, Colleen Stuart, and Laura Dabbish. Perceptions about anonymity on the internet. 2011.

[3] Andreas Pfitzmann and Marit Köhntopp. Anonymity, unobservability, and pseudonymity —a proposal for terminology. In Hannes Federrath, editor, *Designing Privacy Enhancing Technologies*, volume 2009 of *Lecture Notes in Computer Science*, pages 1–9. Springer Berlin / Heidelberg, 2001.