15-744 Project Proposal

Nicolas Feltman and David Naylor

9/28/11

1 Problem Statement

The desire for anonymous communication in the Internet has made it a much-studied issue. Several standard approaches to anonymity have emerged, normally involving some number of explicitly identified proxies due to the dumb nature of current routers. Although none of these methods are perfect, they generally meet most users' needs. The development of new Internet architectures, however, will necessitate new studies: a direct translation of old methods may very well be susceptible to new attacks, whereas new methods may become feasible.

We propose to consider anonymity in the context of one particular future Internet architecture: the eXpressive Internet Architecture, or XIA [1]. We believe that this will be a rich problem because of both the variety of types of actors in XIA and XIA's intrinsic security. Specifically, we will identify scenarios in which one might want to anonymously communicate in XIA, describe how existing techniques might still be used, and develop approaches for XIA-specific anonymity, either at the general level or in the context of specific applications.

2 Related Work

Existing work related to anonymity can be roughly categorized as either discussion of what it means to communicate anonymously or techniques for doing so.

2.1 Types of Anonymity

The term "anonymity" alone is somewhat vague. When implementing anonymous methods, one must consider three questions: 1) Who wants to remain anonymous? 2) From whom? 3) To what degree? In response to (1), Pfitzmann and Waidner [3] consider three scenarios: *sender anonymity*, *recipient anonymity*, and *sender-recipient unlinkability*. As for (2), one typically anticipates either an attacker with limited knowledge (a single host or a small number of colluding hosts) or one with global knowledge (achieved through a large number

of colluding hosts). And regarding (3), Reiter and Rubin [4] propose three classifications: *beyond suspicion*, *probable innocence*, and *possible innocence*.

2.2 Techniques

Most existing techniques involve routing traffic through a proxy of some kind. In its simplest form, this amounts to forwarding your packet (an HTTP request, perhaps) to the proxy which will in turn forward to its actual destination. There are many ways to improve on this basic idea; in *onion routing*, packets are forwarded through multiple proxies with the use of cryptography to hide all but the next hop address at each step, and *MIXes* [2] require the proxy to wait until it has received packets to forward from several users, after which it forwards them on in a different order.

Other techniques include using broadcasts or multicasts to hide the intended recipient or return address spoofing to protect the sender.

3 Rough Action Plan

3.1 Analyze anonymity in XIA

We plan to begin our exploration of anonymity in XIA by discussing in detail how the new architecture changes what it might mean for a user to want to act anonymously, how attackers can compromise a user's anonymity, and how new techniques can achieve anonymity.

Two of XIA's key features, *principals* and *intrinsic security*, will likely come into play in a big way here. Principals, which allow for communication beyond host-to-host communication (e.g., communication directly with 'services' or 'content'), may introduce new methods of communication which users may want to anonymize. Intrinsic security, in essence, means that communication with any principal must be publicly verifiable; this may pose a challenge to anonymity.

3.2 Offer new techniques

After considering anonymity in XIA in general, we will develop one or two specific strategies/algorithms for achieving anonymity in XIA in particular situations.

3.3 Implement a proposed technique

Depending on exactly what comes of (3.2), we may attempt to implement one of our proposed techniques on top of an XIA prototype.

References

[1] A. Anand, F. Dogar, D. Han, B. Li, H. Lim, M. Machadoy, W. Wu, A. Akella, D. Andersen, J. Byersy, S. Seshan, and P. 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] D. L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24:84–90, February 1981.

[3] A. Pfitzmann and M. Waidner. Networks without user observability. *Computers & Security*, 6(2):158 – 166, 1987.

[4] M. K. Reiter and A. D. Rubin. Crowds: anonymity for web transactions. *ACM Trans. Inf. Syst. Secur.*, 1:66–92, November 1998.