Hang With Your Buddies to Resist Intersection Attacks

Executive Summary - full preprint available at http://arxiv.org/abs/1305.5236

David Isaac Wolinsky, Ewa Syta, and Bryan Ford
Yale University
{david.wolinsky,ewa.syta,bryan.ford}@yale.edu

ABSTRACT

Some anonymity schemes, such as DC-nets and MIX cascades, can guarantee anonymity even against traffic analysis—provided messages are independent and unlinkable. Users in practice often desire *pseudonymity*—sending messages intentionally linkable to each other but not to the sender—but pseudonymity in dynamic networks exposes users to *intersection attacks*. We present Buddies, the first systematic attempt to offer intersection attack resistant pseudonyms in practical anonymity systems. Buddies groups users dynamically into *buddy sets*, controlling message transmission to make buddies within a set behaviorally indistinguishable to a traffic-monitoring adversary. Intersection attack resistance does not come "for free," of course, and Buddies offers users control over the inevitable tradeoffs between anonymity, latency, and the useful lifetime of a pseudonym.

Introduction

Some anonymous group communication systems, such as DC-nets [2, 16, 3] and MIX cascades [**?** 1], offer traffic analysis resistance even against powerful adversaries—*provided* all messages are independent of each other and/or the set of participants never changes. Realistic systems exhibit *churn* in the set of users online at a given time, however, and users often wish to send messages intentionally linkable to each other or to a common *pseudonym*. By sending linkable messages in the presence of this churn, however, users can quickly lose anonymity to statistical disclosure or intersection attacks [13, 9**?**].

Suppose Alice writes a blog reporting on corruption in her local city government. To protect herself, she always connects via Tor [6] to the server hosting her blog, and never reveals any personally identifying information on her blog or to the server hosting it. Carol, a corrupt local official targeted in Alice's blog, deduces from the blog's content that its owner is local, and calls her friend Mallory, a network administrator in the monopolistic local ISP. Mallory cannot directly compromise Tor, but he can read from Alice's blog the times and dates each of her 57 blog entries were posted, and he can analyze the ISP's access logs to see which customers were online at each of those times. While there were thousands of customers online at each posting time, Mallory finds that each customer—*except* for Alice—was offline during *some* posting event. The *intersection* of the 57 relevant online user sets thus completely de-anonymizes Alice.

Buddies Architecture

As a step toward addressing such risks we introduce Buddies, the first anonymous communication architecture we are aware of designed to protect users systematically from network-monitoring adversaries capable of long-term intersection attacks. Figure 1 shows a high-level conceptual model of Buddies' architecture. Buddies assumes there is some set

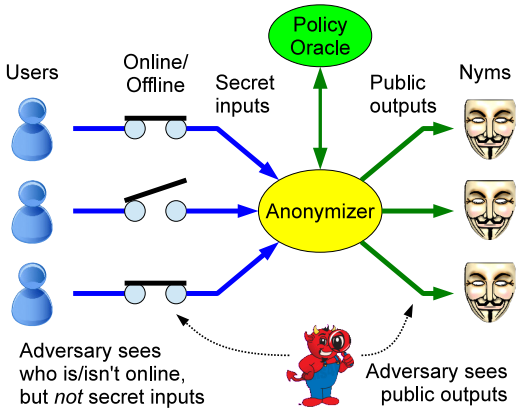

Figure 1: Conceptual model of Buddies architecture

of *users*, each of whom has a secret (i.e., securely encrypted) network communication path to a component we call the *Anonymizer*. Each Buddies user "owns" some number of *Nyms*, each representing a pseudonymous identity under which the owner may post: e.g., an anonymous chat handle or blog. Users may secretly submit messages to be posted to Nyms they own, which the Anonymizer scrubs of identifying information and publicly "posts" to that Nym.

To make various operational decisions, the Anonymizer consults a *Policy Oracle*. The Policy Oracle uses publicly available information to *simulate* a virtual Adversary, by continuously performing an "intersection attack" against each Nym. By design the Policy Oracle has no access to sensitive information: it makes decisions based purely on public information available to anyone.

Measuring Vulnerability to Intersection Attack

Buddies works by continuously maintaining an anonymized user database of participating users and their online status, and uses this information to *simulate* intersection attacks that a network-monitoring adversary might perform. These simulations yield two relevant anonymity metrics that Buddies reports continuously, as an indication of potential vulnerability to intersection attack: a *possibilistic* metric roughly measuring "plausible deniability," and a more conservative *indistinguishability* metric indicating vulnerability to more powerful statistical disclosure attacks [**?**].

Possibilistic anonymity: "Possinymity".

To form a simple *possibilistic* anonymity set P_N for a given Nym N, we assume the adversary intersects the filtered user sets $\mathbb{P}_i$ across all rounds i for which Nym N was scheduled to transmit, *and* a nonzero message appeared: i.e., $P_N = \bigcap_i \{O_i \mid T_i = N \wedge m_i \neq 0\}$. Thus, P_N represents the set of users that might *conceivably* own Nym N, consistent with the observed set of non-null messages that have appeared for Nym N up to any point in time. We define the size

of a Nym's possibilistic anonymity set, $|P_N|$, as Nym N's *possibilistic anonymity*, which for convenience we suggest the abbreviation *possinymity*.

While possinymity is similar to many useful anonymity metrics already proposed [10, 11], and perhaps a simplistic one, we feel it captures a useful measure of "plausible deniability." If for example a user is dragged into court, and the judge is shown network traces of a Buddies system in which the accused is one of $|P_N|$ users who *may in principle* have posted an offending message, then a large possibilistic anonymity may help sow uncertainty of the user's guilt. We fully acknowledge the weaknesses of plausible deniability in general, however, especially in environments where "innocent until proven guilty" is not the operative principle.

Probabilistic indistinguishability: "Indinymity".

A smarter adversary can use probabilistic reasoning to learn also from rounds in which *no* message appears. For example, if exactly one user goes offline permanently at exactly the time messages stop appearing from exactly one pseudonym, the adversary might draw a strong probabilistic conclusion even if there's no irrefutable linkage. Many such attacks are addressed admirably in prior work [5, 14].

Instead of relying on the dubious relevance of any *particular* probabilistic analysis—which may break the moment anyone slightly refines an existing attack—Buddies' resistance to probabilistic attacks relies on an *indistinguishability* principle that applies to all attacks of this form independent of specific probabilities involved. In particular, if two users A and B have exhibited *identical* histories with respect to inclusion or exclusion into each round's filtered user set $\mathbb{P}_i$, across *all* rounds i in which a given Nym N was scheduled, then under any probabilistic analysis of the above form the adversary must assign identical probabilities to A and B owning Nym N. We call such probabilistically indistinguishable users *buddies*: equivalence classes of users who "hang together" under probabilistic intersection attacks, so that individual members do not "hang separately."

We thus define a second anonymity metric, *indistinguishability set size*, or *indinymity* for short, as the size of the *smallest* buddy-set for a given Nym N. Since we do not know how a real attacker will actually assign probabilities to users, indinymity represents the minimum level of anonymity a member of *any* buddy set can expect to retain, even if the adversary correctly intersects the owner's anonymity set down to the members of that buddy set. Thus, the attacker cannot (correctly) assign a probability greater than $1/|B_N|$ to *any* user—including, but not limited to, the owner of N.

Active Control of Anonymity Loss

Beyond measuring potential vulnerability, as prior work in metrics [5, 14] and alternate forms of anonymity [8] have done, Buddies attempts to offer *active control* over anonymity loss under intersection attack. Users set per-pseudonym policies to balance attack protection against communication responsiveness and availability. Active control depends on a *policy module* that monitors and filter the set of users active in each round, forcing the system to behave as if some online users were actually offline. Mitigation policies can enforce lower bounds on anonymity metrics, preventing Alice from revealing herself to Mallory by posting at the wrong time for example. Policies can also reduce the *rate* of anonymity loss to intersection attacks, for example by tolerating anonymity set members who are normally reliable and continuously online but lose connectivity for brief periods. Finally, policies can adjust posting rates or periods, enabling Buddies to aggregate all users coming online within a posting period into larger anonymity sets. If Alice sets her blog's posting period to once per day, for example, then Buddies can maintain Alice's anonymity among all users who "check in" at least once a day—*any time* during each day—even if many users check in only briefly at varying times.

Practical Intersection Attack Resistance

Buddies' architecture may be treated as an extension to various existing anonymous communication schemes, but is most well-suited to schemes already offering some measurable protection guarantees against traffic analyis, such as MIX cascades [**?** 1], DC-nets [2, 15, 16], or verifiable shuffles [12, 7]. We have built a working prototype of Buddies atop Dissent [3, 16, 4], a recent anonymous communication system that combines verifiable shuffle and DC-net techniques.

Our working prototype builds on Dissent to illustrate solutions to practical challenges, such as to decentralize Buddies' design and distributed trust, to create and manage pseudonyms while maintaining their independence, and to allow users to attach different policies to each pseudonym. We explore two usage scenarios: group chat forums such as IRC, where users may wish to retain short- or long-lived pseudonyms representing "chat handles"; and anonymous Web browsing scenarios, where a browser's long-lived communication state can lead to intersection attack vulnerabilities. Our prototype treats chat handles or browsing sessions as Nyms offering users measurable risk indicators, and enabling users to discard a Nym or move to a different location *before* their anonymity drops below a given threshold.

References

[1] O. Berthold, A. Pfitzmann, and R. Standtke. The disadvantages of free MIX routes and how to overcome them. In *Workshop on Design Issues in Anonymity and Unobservability*, pages 30–45, July 2000.

[2] D. Chaum. The Dining Cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, pages 65–75, Jan. 1988.

[3] H. Corrigan-Gibbs and B. Ford. Dissent: accountable anonymous group messaging. In *17th CCS*, Oct. 2010.

[4] H. Corrigan-Gibbs, D. I. Wolinsky, and B. Ford. Proactively accountable anonymous messaging in Verdict. In *22nd USENIX Security*, Aug. 2013.

[5] C. Díaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity. In *Proceedings of the 2nd international conference on Privacy enhancing technologies*, PET'02, 2003.

[6] R. Dingledine, N. Mathewson, and P. Syverson. Tor: the second-generation onion router. In *12th USENIX Security*, Aug. 2004.

[7] J. Furukawa and K. Sako. An efficient scheme for proving a shuffle. In *CRYPTO*, pages 368–387, Aug. 2001.

[8] N. Hopper and E. Y. Vasserman. On the effectiveness of k-anonymity against traffic analysis and surveillance. In *WPES*, Oct. 2006.

[9] D. Kedogan, D. Agrawal, and S. Penz. Limits of anonymity in open environments. In *5th International Workshop on Information Hiding*, Oct. 2002.

[10] D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila. Towards mathematically modeling the anonymity reasoning ability of an adversary. In *IPCCC*, pages 524–531. IEEE, 2008.

[11] D. J. Kelly. *A taxonomy for and analysis of anonymous communications networks*. PhD thesis, Wright Patterson AFB, OH, USA, 2009. AAI3351544.

[12] C. A. Neff. A verifiable secret shuffle and its application to e-voting. In *CCS*, pages 116–125, Nov. 2001.

[13] J.-F. Raymond. Traffic analysis: Protocols, attacks, design issues and open problems. In *Workshop on Design Issues in Anonymity and Unobservability*, pages 10–29, 2000.

[14] A. Serjantov and G. Danezis. Towards an information theoretic metric for anonymity. In *Proceedings of the 2nd international conference on Privacy enhancing technologies*, PET'02, 2003.

[15] E. G. Sirer, S. Goel, M. Robson, and D. Engin. Eluding carnivores: File sharing with strong anonymity. In *SIGOPS EW*, Sept. 2004.

[16] D. I. Wolinsky, H. Corrigan-Gibbs, A. Johnson, and B. Ford. Dissent in numbers: Making strong anonymity scale. In *10th OSDI*, Oct. 2012.