Jesse Victors, Ming Li, and Xinwen Fu

The Onion Name System

Tor-powered Distributed DNS for Tor Hidden Services

Abstract: Tor hidden services are anonymous servers of unknown location and ownership which can be accessed through any Tor-enabled web browser. They have gained popularity over the years, but since their introduction in 2002 still suffer from major usability challenges primarily due to their cryptographically-generated non-memorable addresses.

In response to this difficulty, in this work we introduce the Onion Name System (OnioNS), a privacy-enhanced distributed resolution service. OnioNS allows Tor users to reference a hidden service by a meaningful globally-unique verifiable domain name chosen by the hidden service operator. We construct OnioNS as an optional backwards-compatible plugin for Tor, simplify our design and threat model by embedding OnioNS within the Tor network, and provide mechanisms for authenticated denial-of-existence with minimal networking costs. We also introduce a lottery-like system to reduce the threat of land rushes and domain squatting. Finally, we integrate our client software with the Tor Browser and conduct performance analysis of our prototype.

1 Introduction

As the prevalence of the Internet and other communication has grown, so too has the development and usage of privacy-enhancing systems. These are protocols that provide privacy by obfuscating the link between a user's identity or location and their communications. Following a general distrust of unsecured Internet communications and in light of the 2013-current revelations by Edward Snowden of international Internet mass-surveillance, users have increasingly turned to these tools for their own protection.

Jesse Victors: Utah State University
E-mail: jvictors@jessevictors.com
Ming Li: University of Arizona
E-mail: lim@email.arizona.edu
Xinwen Fu: University of Massachusetts Lowell
E-mail: xinwenfu@cs.uml.edu

Tor [8] is a third-generation onion routing system and is the most popular low-latency anonymous communication network in use today. In Tor, users construct a layered encrypted communications circuit over three onion routers in order to mask their identity and location. As messages travel through the circuit, each onion router in turn decrypts their encryption layer, exposing their respective routing information. The first router is only exposed to the user's IP address, while the last router conducts Internet activities on the user's behalf. This provides end-to-end communication confidentiality of the sender.

Tor users interact with the Internet and other systems over Tor via the Tor Browser, a security-enhanced fork of Firefox ESR. This achieves a level of usability but also security: Tor achieves most of its application-level sanitization via privacy filters in the Tor Browser; unlike its predecessors, Tor performs little sanitization itself. Tor's threat model assumes that the capabilities of adversaries are limited to traffic analysis attacks on a restricted scale; they may observe or manipulate portions of Tor traffic, that they may run onion routers themselves, and that they may compromise a fraction of other existing routers. Tor's design centers around usability and defends against these types of attacks.

1.1 Motivation

Tor also supports *hidden services* – anonymous servers that intentionally mask their IP address through Tor circuits. They utilize the .onion pseudo-TLD, typically preventing hidden services from being accessed outside the context of Tor. Hidden services are only known by their public RSA key and typically referenced by their address, 16 base32-encoded characters derived from the SHA-1 hash of the server's key, i.e. 3g2upl4pq6kufc4m.onion. This builds a publicly-confirmable one-to-one relationship between the public key and its address and allows hidden services to be accessed via the Tor Browser by their .onion address within a distributed environment.

Tor hidden service addresses are distributed and globally collision-free, but there is a strong discontinuity between the address and the service's purpose. As their addresses usually contain no human-readable

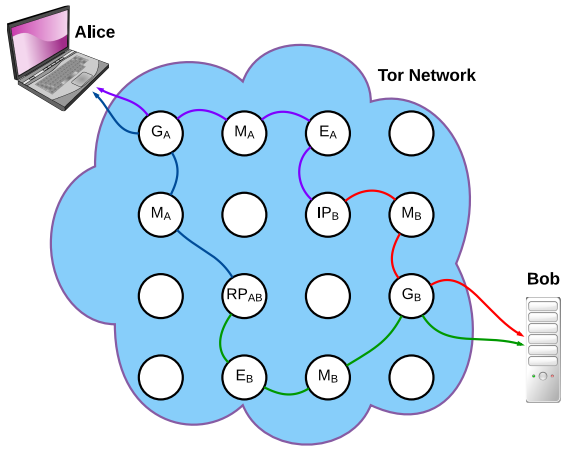

Fig. 1. A Tor client, Alice, and a hidden service, Bob, first mate two Tor circuits (purple and red) at one of Bob's long-term *introduction points* (IP). They then renegotiate and communicate over another pair of Tor circuits (blue and green) at an ephemeral *rendezvous point* (RP). This achieves communication with bi-directional anonymity [21].

information, a visitor cannot categorize, label, or authenticate hidden services in advance. While a Tor user may explore and bookmark hidden services within the Tor Browser, this is a very narrow solution and does not scale well past a few dozen bookmarks. Over time, third-party directories – both on the clearnet and darknet – have appeared in an attempt to counteract this issue, but these directories must be constantly maintained and the approach is neither convenient nor does it practically scale past several hundred entries. The approximately 27,000 hidden services currently on the Tor network (Figure 2) and the potential for continued growth both suggest the strong need for a more complete and wider solution to solve the usability issue.

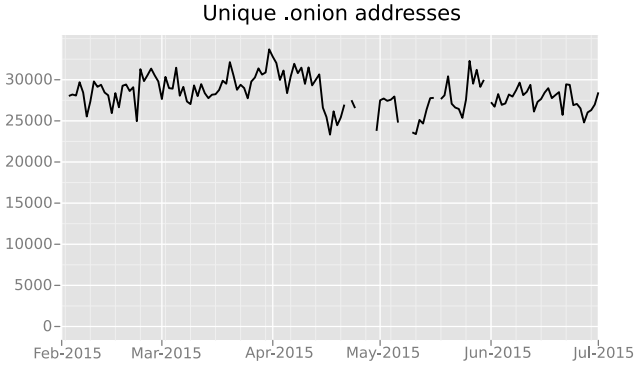

Fig. 2. The number of unique .onion addresses seen in the Tor network between February 2015 and July 2015 [13, 23].

1.2 Contributions

In this paper, we present the design, analysis, and implementation of the Onion Name System, (OnioNS) a distributed, secure, and usable domain name system for Tor hidden services. Any hidden service can claim a meaningful human-readable domain name without loss of anonymity and clients can query against OnioNS in privacy-enhanced and verifiable manner. OnioNS is powered by a random subset of nodes within the existing Tor network, significantly limiting the additional attack surface. We devise a distributed database that is resistant to node compromise and provides authenticated denial-of-existence. We provide a backwards-compatible plugin for the Tor Browser and demonstrates the high usability and performance of OnioNS. To the best of our knowledge, this is the first alternative DNS for Tor hidden services which is distributed, secure, and usable at the same time.

Paper Organization: This paper is divided into four main sections. In section 2 we define our design objectives and explain why existing works do not meet our goals. We also define our threat model, which includes Tor's assumptions and the capabilities of our adversaries. In section 5, we describe the system overview and define several key protocols. In section 6 we analyse the security of our assumptions and examine other attack vectors. Last, in section 7 we describe our implementation prototype, perform performance analysis tests, and demonstrate that our software allows the Tor Browser to load a hidden service under a meaningful domain name.

2 Problem Statement

To integrate with Tor, we must provide a secure system, preserve user privacy, and avoid compromising other areas of the Tor network. Additionally, we seek to achieve all three properties of Zooko's Triangle (section 2.2.1) and to providing a mechanism for authenticated denial-of-existence (section 2.2.2).

2.1 Design Objectives

Tor's privacy-enhanced environment introduces distinct challenges to any new infrastructure. Here we enumerate a list of requirements that must be met by any naming system applicable to Tor hidden services. In Section 3 we analyse existing works and show how these systems

do not meet these goals and in Section 5 we demonstrate how we overcome them with OnioNS.

1. **Anonymous registrations**: The system should not require any personally-identifiable or location information from the registrant. Tor hidden services publicize no more information than a public key and a set of Introduction Points.

2. **Privacy-enhanced queries**: Clients should be anonymous, indistinguishable, and unable to be tracked by name servers. Tor already tunnels most Internet DNS queries over circuits, thus any alternative naming system should continue to preserve user privacy during lookups.

3. **Strong integrity**: Clients must be able to verify that the domain-address pairing that they receive from name servers is authentic relative to the authenticity of the hidden service. This objective provides a defence against phishing attacks.

4. **Globally unique domain names**: Any domain name of global scope must point to at most one server. For naming systems that generate names via cryptographic hashes, the key-space must be of sufficient length to resist cryptanalytic attack. Unique domain names prevent fragmentation of users and also provides a defence against phishing attacks.

5. **Distributed control**: Central authorities carry absolute control over the system and root security breaches can easily compromise the integrity of the entire system. They may also be able to compromise the privacy of both users and hidden services or may not allow anonymous registrations.

6. **High usability**: Most Tor users are not security experts or have technical backgrounds. The system must resolve protocols with minimal input from the user and hide non-essential details.

7. **Optional**: Not all hidden services require meaningful names. For example, applications such as Ricochet [4] may create ephemeral hidden services where names may not be appropriate or necessary. Thus a naming system should be optional but not required. Systems that provide backwards compatibility by preserving the Tor hidden service protocol also achieve this property.

8. **Lightweight**: In most realistic environments clients have neither the bandwidth nor storage capacity to hold the system's entire database, nor the capability of meeting significant computation burdens. The system should have a minimal impact on Tor clients and hidden services.

2.2 Challenges

2.2.1 Zooko's Triangle

In 2001, Zooko Wilcox-O'Hearn described three desirable properties for any persistent naming system: distributed design, assignment of human-meaningful names, and globally unique names. In a statement now known as Zooko's Triangle, [9, 26] he claimed any naming system could only achieve two of these properties. This is illustrated in Figure 3.

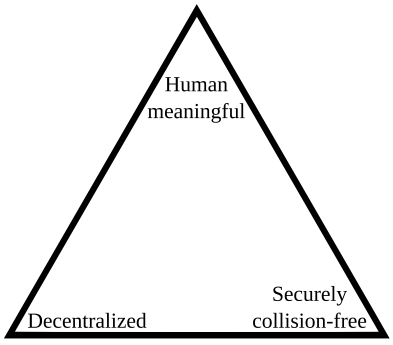

Fig. 3. Zooko's Triangle.

Some examples of naming systems that achieve only two of these properties include:

- **Securely unique and human-meaningful** — Internet domain names.
- **Decentralized and human-meaningful** — Human names and nicknames.
- **Securely unique and decentralized** — PGP keys and Tor .onion addresses.

2.2.2 Authenticated Denial-of-Existence

When a client queries a name server for a name, the server may respond in three distinct ways:

1. It may return the correct destination.
2. It may return a spoofed destination.
3. It may claim that an existing name does not exist.
4. It may choose not to answer.

Cases two and three may be expected by a malicious name server and constitute significant threats to the client. On the Internet, the second case is addressed with SSL certificates and a chain of trust to root Certificate Authorities (CAs) but the third case is not addressed by

DNS and remains a possible attack vector. DNSSEC includes an extension for Hashed Authenticated Denial of Existence (NSEC3) which provides signed non-existence claims on a per-domain basis. However, DNSSEC has not seen widespread use, storing per-domain denial-of-existence records introduces significant storage requirements, and to our knowledge no alternative DNS provides mechanisms for authenticated denial-of-existence. Closing this attack vector is not easy; the naïve solution of generating proof individually or en-masse for every non-existent domain is infeasible since the domain space is likely too large to practically enumerate.

3 Related Works

Vanity key generators (e.g. Shallot [14]) attempt to find by brute-force an RSA key that generates a partially-desirable hash. Vanity key generators are commonly used by hidden service operators to improve the recognition of their hidden service, particularly for higher-profile services. For example, a hidden service operator may wish to start his service's address with a meaningful noun so that others may more easily recognize it. However, these generators are only partially successful at enhancing readability because the size of the domain key-space is too large to be fully brute-forced in any reasonable length of time. If the address key-space was reduced to allow a full brute-force, the system would fail to be guaranteed collision-free. Nicolussi suggested changing the address encoding to a delimited series of words, using a dictionary known in advance by all parties [20]. While Nicolussi's encoding improves the readability of an address, like vanity key generators it does not allow addresses to be completely meaningful.

The Internet DNS is already well established as a fundamental abstraction layer for Internet routing. However, despite its widespread use and extreme popularity, the Internet DNS suffers from several significant shortcomings and fundamental security issues that make it inappropriate for use by Tor hidden services. Generally speaking, the Internet DNS by default does not use any cryptographic primitives. DNSSEC is primarily designed to prevent forgeries and DNS cache poisoning from intermediary name servers and it does not provide any degree of query privacy [28]. Additional extensions and protocols such as DNSCurve [2] have been proposed, but DNSSEC and DNSCurve have not yet seen widespread full deployment across the Internet. Cachin and Samar [5] extended the Internet DNS and decreased the attack potential for authoritative name servers via threshold cryptography, but the lack of default security in the Internet DNS and the logistical difficulty in globally implementing their work prevents us from using their system for hidden services.

OnionDNS [25] is a seizure-resistant alternative resolution service for the Internet. OnionDNS is based on DNS and uses unmodified BIND client software but anonymizes the root server by hosting it as a hidden service. While OnionDNS is highly usable and provides DNSSEC and other authentication mechanisms, the system is centralized by a single root server and thus highly vulnerable if the root is malicious or is compromised.

The GNU Name System [28] (GNS) is a decentralized alternative DNS. GNS distributes names across a hierarchical system of zones constructed into directed graphs. Each user manages their own zone and distributes zone access peer-to-peer within social circles. However, GNS does not guarantee that names are *globally* unique. Furthermore, the selection of a trustworthy zone to use would be a significant challenge for using GNS for Tor hidden services and such a selection no longer makes the system distributed. Awerbuch and Scheideler, [1] constructed a distributed peer-to-peer naming system, but like GNS, made no guarantee that domain names would be globally unique.

Namecoin [6] is an early fork of Bitcoin [18] and is noteworthy for achieving all three properties of Zooko's Triangle. Namecoin holds information transactions in a distributed ledger known as a blockchain. Transactions and information are added to the head of the blockchain by "miners," who solve a proof-of-work problem to generate the next block. While Namecoin is often advertised as capable of assigning names to Tor hidden services, it has several practical issues that make it generally infeasible to be used for that purpose. First, Namecoin does not provide a mechanism for proving ownership of domain names; this makes it difficult for a client to prove that the owner of the hidden service private RSA key also maintains the Namecoin secp256k1 ECDSA private key. Second, Namecoin generally requires users to prefetch the blockchain which introduces significant logistical issues due to high bandwidth, storage, and CPU load. Third, although Namecoin supports anonymous ownership of information, it is non-trivial to anonymously purchase Namecoins, thus preventing domain registration from being truly anonymous. These issues prevent Namecoin from being a practical alternative DNS for Tor hidden services.

4 Assumptions and Threat Model

We assume that Tor circuits provides privacy and anonymity; if Alice constructs a three-hop Tor circuit to Bob with modern Tor cryptographic protocols and sends a message m to Bob, we assume that Bob can learn no more about Alice than the contents of m. This implies that if m does not contain identifiable information, Alice is anonymous from Bob's perspective. This also implies an assumption on the security of cryptographic primitives and a lack of backdoors or analogous breaks in cryptographic libraries. The security of Tor circuits is also dependent on the assignment of consensus weight; we assume that the majority of directory authorities are at least semi-honest and that consensus weight is an effective defence against Sybil attacks. The aforementioned assumptions are shared by the Tor network.

We assume that Eve controls some percentage of dishonest colluding Tor routers as well as semi-honest routers, however this percentage is small enough to avoid violating our second assumption. We assume a fixed percentage of dishonest and semi-honest routers; namely that the percentage of routers under an Eve's control does not increase in response to the inclusion of OnionNS into Tor infrastructure. This assumption simplifies our threat model analysis but we consider it realistic because while Tor traffic is purposely secret as it travels through the network, we consider OnioNS information public so we don't consider the inclusion of OnioNS a motivating factor to Eve.

We assume no upper-bound on the computational capabilities of any adversary, with the exception that they are unable to compromise cryptographic primitives. However, we assume that the adversary has a fixed budget, namely that they have a quota on the memory and CPU hours that they can allocate against our system. We also assume that an adversary may run operate any of the non-authoritative name servers.

4.1 Use Cases

As hidden services require no more than a configured Tor client and a socket listener and are thus cheap to create, we anticipate that actors in our system will perform any of the following use cases:

1. **Create many hidden services to register many names.**
2. **Create one hidden service to register many names.**
3. **Create many hidden services to register a single name.**
4. **Create one hidden service to register a single name.**

Sceneries one and two are expected to be performed by adversaries attempting to register all popular names in a "land rush" for financial gain or as a denial-of-registration attack. Scenario three may indicate an attempt by many legitimate actors to claim a highly desirable name, while scenario four is the expected behaviour of innocent actors. As hidden services are anonymous by nature, it is not straightforward to construct a system that differentiates and selects between a single actor performing the first scenario and many actors performing the fourth scenario. However, as well-known hidden services cannot change their public key, we expect innocent actors to follow the fourth use case.

5 Solution

5.1 Cryptographic Primitives

OnioNS utilizes hash functions, digital signature algorithms, a proof-of-work scheme, and a global source of randomness.

- Let $\mathcal{H}(x)$ be a cryptographic hash function. We define $\mathcal{H}(x)$ as SHA-384.
- Let $S_{RSA}(m, r)$ be a RSA digital signature function that accepts a message m and a private RSA key r and returns a digital signature. Let $S_{RSA}(m, r)$ use $\mathcal{H}(x)$ as a digest function on m in all use cases. We define $S_{RSA}(m, r)$ as EMSA4/EMSA-PSS.
- Let $V_{RSA}(m, R)$ validate an RSA digital signature by accepting a message m and a public key R, and return true if and only if the signature is valid.
- Let PoW(k) be a one-way function that accepts an input key k and returns a deterministic output. We suggest the scrypt [22] key derivation function with a fixed salt.
- Let $\mathcal{G}(t)$ be a cryptographically-secure generator of random or pseudorandom timestapped numbers. $\mathcal{G}(t)$ deterministically returns a value for time t in the present or past.
- Let $\mathcal{R}(s)$ be a pseudorandom number generator that accepts an initial seed s and returns a list of

pseudorandom numbers. In our design, $s = \mathcal{G}(t)$, so $\mathcal{R}(s)$ does not need to be cryptographically secure. We suggest MT19937, commonly known as the Mersenne Twister. This generator is widely used throughout most programming languages and is well known for its speed, long period, and the high quality of its pseudorandom output [16].

5.2 Definitions

domain name The syntax of OnioNS domain names mirrors the Internet DNS; we use a sequence of name-delimiter pairs with a .tor pseudo-TLD. The Internet DNS defines a hierarchy of administrative realms that are closely tied to the depth of each name. By contrast, OnioNS makes no such distinction; we let hidden service operators claim second-level names and then control all names of greater depth under that second-level name.

A **ticket** is a small and fundamental data structure. It contains *type*, *name*, *contact*, *rand*, *signature*, and *pubHSKey*. Tickets by default have *type* set to "ticket", but this data structure becomes a **record** if *type* is set to any of the operations described in section 5.4.9.

A **mirror** is Tor router that is acting as a name server within the OnioNS network. Mirrors maintain a textual database of system information and respond to client queries but usually do not accept new DNS records or other information from hidden services. We note that mirrors may be outside the Tor network, but this scenario is outside the scope of this work.

Quorum candidates are mirrors that provide proof in Tor's consensus documents that they hold a current copy of the database and that they have sufficient CPU and bandwidth capabilities to handle OnioNS communication in addition to their normal Tor duties.

The **Quorum** is authoritative subset of Quorum candidates who have active responsibility over the OnioNS database. Quorum nodes accept and process information from hidden services but do not respond to client queries. The Quorum is randomly chosen from the set of Quorum candidates and is rotated periodically, as described in section 5.4.

L_Q	size of the Quorum
L_T	number of routers in the Tor network
Q_i	the ith Quorum where i is an iteration counter
Δq	lifetime of the Quorum

Table 1. Frequently used notation.

5.3 Infrastructure

We embed OnioNS infrastructure within the Tor network by utilizing existing Tor nodes as hosts for OnioNS mirrors. Each Tor node may opt to run a hidden services which then powers a OnioNS mirror running on localhost. As these hidden services are part of OnioNS, they must be accessed by their traditional .onion address, but this is acceptable as these servers are never accessed directly by end-users. Our reliance on hidden services allows us to recycle existing TLS links between Tor nodes and leverage Tor circuits to obscure all communication between end-users and OnioNS infrastructure without requiring a modification to the Tor executable. In essence, all communication with or within OnioNS is hidden from outside observers by ephemeral internal Tor circuits that need not pass through exit routers, increasing privacy and reducing our attack surface.

We authenticate servers in our infrastructure using Ed25519 [3] keys; as of Tor 0.2.7, Tor routers generate and manage Ed25519 keypairs and include their public key in the network consensus. We use Ed25519 because of its strength, size, and speed advantages over Tor's original RSA-1024 identity keys. OnioNS servers provide proof-of-knowledge of their private Ed25519 key for all outbound traffic on their hidden service, achieving end-to-end authentication of all OnioNS communication. Throughout the remainder of this paper, "hidden services" refers exclusively to hidden services that are not part of the OnioNS infrastructure.

Each mirror maintains two distinct databases; "main" and "ephemeral", which both contain records. Newly received records are temporarily stored in the ephemeral database, which is periodically merged into the main database. Mirrors use their main database to respond to clients, who can then authenticate the responses against information published by Quorum nodes. Quorum nodes maintain an additional and secret database that contains lottery tickets.

5.4 Protocols

We now describe the protocols fundamental to OnioNS functionality.

5.4.1 Random Number Generation

We use $\mathcal{G}(t)$ as a basis for several of our protocols, although we note that $\mathcal{G}(t)$ has applications in Tor beyond OnioNS. One straightforward definition of $\mathcal{G}(t)$ is the SHA-384 hash of Tor's consensus documents. If the Tor network is dynamic enough to provide significant amounts of entropy into the consensus documents, then $\mathcal{G}(t)$ may be considered cryptographically secure. However, this assumption does not hold because current router descriptors are publicly available before the consensus documents are published, allowing $\mathcal{G}(t)$ under this approach to be easily manipulated by a few malicious Tor routers. The attack becomes significantly easier in the final moments before the directory authorities publish the consensus.

Instead, we suggest implementing $\mathcal{G}(t)$ as the commitment scheme proposed by Goulet and Kadianakis [12]. Their algorithm modifies the consensus voting protocol that is run once an hour by Tor directory authorities. In their scheme, at 00:00 UTC each authority commits a SHA-256 hash of a secret value x into each consensus vote across a 12 hour period. Then at 12:00 UTC, each directory authority reveals x across the next set of 12 consensuses. Then at 24:00 UTC, the revealed values are hashed together to create a single random number, which is then embedded in the consensus documents so that it is efficiently distributed to both Tor routers and clients. A different random number thus appears in the consensus every 24 hours. While this implementation of $\mathcal{G}(t)$ defines t as an integer of 24 hours, Δq may be greater than 24 hours, as discussed in **??**. Therefore, throughout the remainder of this document we will use the notation $\mathcal{G}(i)$ to reference the $\mathcal{G}(t\dot{2}4\dot{\Delta}q)$ that defines Q_i.

The two time boundaries in this implementation of $\mathcal{G}(t)$ trigger events within our system. The publication of $\mathcal{G}(i)$ at midnight defines the selection of the next Quorum, causes all mirrors to publish the state of their database, marks the beginning of the next lottery, and determines the winners of the previous lottery. The first reveal at 12:00 UTC ends the lottery and contains the pool of Quorum candidates. We clarify our distinction of these boundaries in section **??**.

5.4.2 Authenticated Denial-of-Existence

We described in section 2.2.2 that a malicious name server may forge a response or may falsely claim non-existence of a name. These are attack vectors that remain open by naming systems that do not provide authentication mechanisms. We use a Merkle tree [17] to defend against these attacks with minimal networking costs. This tree is a fundamental authentication mechanism for both existing and non-existing names. All mirrors, including Quorum nodes, perform this algorithm. The tree's root hash is then checked by clients during other protocols.

1. Charlie fills an array list l with the $r_i(name) \,\|\, \mathcal{H}(r_i)$ for each record r_i received from hidden services.
2. Charlie sorts *arr* by the *name* field.
3. Charlie constructs a Merkle tree T from l.
4. Charlie publishes the root hash of T in the consensus as described in section 5.4.3.

We note that a sorted Merkle tree does not support dynamic record updates and must be rebuilt at each update. While similar data structures exist that support proof of existence and non-existence and allow efficient updates, such as a skip list [11], these structures are significantly more complicated. We consider it sufficient to use a Merkle tree as it is only rebuilt once per day in $\mathcal{O}(n \log(n)$ time.

5.4.3 Quorum Qualification

Quorum candidates must prove that they are both up-to-date mirrors and that they have sufficient capabilities to handle the increased communication and processing demands from OnioNS protocols, an additional burden on top of their traditional Tor responsibilities.

The naïve solution to demonstrating the first requirement is for all participants to simply ask mirrors for their internal database, and then compare the recency of its database against the databases from the other mirrors. However, this solution does not scale well; Tor has ≈ 2.1 million daily users [23]: it is infeasible for any single node to handle queries from all of them. Instead, at 00:00 UTC each day, let each mirror merge the ephemeral database into the main database, recompute the Merkle tree, and place the root hash inside the Contact field of its router descriptor so that the hash appears in the network consensus. The Contact field is typically used to hold the email address and PGP fingerprint of the router's administrator, but our use of the Contact field allows us to distribute the hash without modifying Tor infrastructure. Mirrors should also distribute their hidden service address in the same way.

Tor provides a mechanism for demonstrating the latter requirement; Quorum candidates must have the Fast, Stable, and Running flags. Tor routers with higher CPU or bandwidth capabilities relative to their peers also receive a proportionally larger consensus weight from the directory authorities. This consensus weight in turn strongly influences router selection during circuit construction: routers with higher weights are more likely to be chosen in a circuit. This scheme also increases Tor's resistance to Sybil attacks. Thus, we can benefit from this infrastructure by selecting the Quorum from the pool of Quorum candidates by a similar mechanism.

5.4.4 Quorum Formation

Mirrors and Tor clients can check the aforementioned qualifications to locally derive the current or any previous Quorum in $\mathcal{O}(L_T)$ time locally without performing any network queries. Without loss of generality, let a client Alice run this algorithm. Alice must download consensus documents from some source, however these documents are timestamped and signed by Tor directory authorities and thus may be retroactively authenticated regardless of where they are archived.

1. Alice obtains and validates two consensus documents: cd_a, which is published at 00:00 UTC and contains $\mathcal{G}(i)$; and cd_b, which is the document published 12 hours prior to cd_a.
2. Alice constructs a list l from cd_b of Quorum candidates that have the Fast, Stable, and Running flags.
3. For each group $g_1..g_k \in l$ that publishes an identical root hash, Alice computes $s_n = \sum_{j=0}^{k} l_j(w)$, where $1 \leq n \leq k$ and $l_j(w)$ is l_j's consensus weight as determined by Tor directory authorities. The Quorum candidates, qc, is the group with the largest value of s_n.
4. Alice uses $\mathcal{R}(\mathcal{G}(i))$ to select $\min(\text{size}(qc), L_Q)$ Quorum nodes from qc with selection probability $P(Q_i) = \frac{Q_j(w)}{s_n}$.

5.4.5 Database Selection

Database updates are usually done in near real-time in a peer-to-peer fashion. At startup, OnioNS mirrors subscribe to new information by opening authenticated circuits to the Quorum and attempting to read from the circuit. All Quorum nodes subscribe to each other, forming a complete graph. Assuming that all mirrors are online and at least semi-honest, all mirrors will be processing the same ephemeral and main databases. However, some mirrors may drop offline temporarily or new ones may appear on the network, and these must synchronize with the network to update their databases. Mirrors select certain Quorum nodes to synchronize against by the following algorithm. Let Charlie be a mirror.

1. Charlie asks each Quorum node for $\mathcal{H}(database_{ephemeral})$ and $\mathcal{H}(database_{main})$.
2. Charlie finds the largest group of Quorum nodes that return the same hashes.
3. Charlie downloads the ephemeral and main databases from any of these nodes.
4. Charlie verifies that $\mathcal{H}(database_{ephemeral})$ and $\mathcal{H}(database_{main})$ match the group's hashes.
5. Charlie verifies the integrity of all records in both databases.
6. Charlie merges the downloaded databases into his local databases.

Quorum nodes that were temporarily offline conduct the same algorithm, but may also ask other Quorum nodes to replay new tickets so that they may update that database too. Non-Quorum mirrors subscribe to Quorum nodes according to the same algorithm.

5.4.6 Ticket Generation

A hidden service operator, Bob, may enter into the OnioNS lottery by generating a ticket, containing a second-level domain name for his hidden service. The Quorum verifies the validity of his ticket and it may be further checked by mirrors and clients if his ticket wins the lottery, so Bob must follow this protocol to ensure that his ticket is accepted by all parties.

1. Bob sets *type* to "ticket".
2. Bob sets *name* to a meaningful domain name.
3. Bob sets *subdomains* to a map of domains of level three or higher and their respective destinations, which may be to either .tor or .onion domains.
4. Bob optionally sets *contact* to his PGP key fingerprint.
5. Bob sets *rand* to $\mathcal{G}(i)$.
6. Bob sets *signature* as the output of $S_{RSA}(type \parallel name \parallel subdomains \parallel contact \parallel rand, r)$ where r is Bob's private RSA key.
7. Bob saves his RSA public key in *pubHSKey*.

Bob's ticket is valid when PoW(*signature*) $\leq d$ where d is a constant that specifies the work difficulty. Each iteration of PoW(*signature*) results in a different and one-way output because EMSA-PSS (EMSA4) is a probabilistic digital signature scheme. Bob must repeatedly resign and recompute scrypt until the formula is satisfied. Once this is the case, Bob sends his ticket to all Quorum nodes.

5.4.7 Ticket Processing

A Quorum node $Q_{i,k}$ listens for tickets from hidden service operators. When a ticket t is received, $Q_{i,k}$

1. Rejects t if t is not valid according to the protocol described in section 5.4.6.
2. Rejects t if t's *name* already exists in its lottery, ephemeral, or main databases.
3. Rejects t if the hidden service does not have a descriptor in Tor's distributed hash table.
4. Rejects t if the hidden service cannot answer an HTTP GET request.
5. Rejects t if the response from an HTTP GET matches any other response from previous tickets.
6. Otherwise, it accepts t, records t in its lottery database, and sends t to all other Quorum nodes.

5.4.8 Lottery Management

In section 5.4.6 we describe a proof-of-work (PoW) protocol that acts as a barrier-of-entry. It is straightforward to design a system where a name is awarded after the completion of this PoW; however such a system is vulnerable to attacks by adversaries with strong computational capabilities who may quickly register many names, as we described in section 4.1. In an attempt to resolve this problem, we introduce a lottery-like system, managed by Quorum nodes.

The lottery starts at the formation of the Quorum. During the lottery, the Quorum accepts requests (or "tickets") for names for hidden services, creating a list T_i. The lottery ends when Q_i is cycled to Q_{i+1}. At this time, each node in Q_i performs the following algorithm. Let Charlie $\in Q_i$.

1. Charlie publishes T_i to all subscribers.
2. For each $T_i(k) \in T_i$, Charlie computes $V_i(k) = \text{count}(T_i(k) \oplus G_{i+1})$, where count($x$) counts the number of 1 bits in x.
3. Charlie sorts V_i in descending order.
4. Charlie sets the list of winners, W_i, to the hidden services corresponding to the first M members of V_i, where M is a fixed number.
5. Charlie merges W_i into his main database, letting them receive names.

All mirrors or other parties may verify W_i and update their main database accordingly through the same protocol because T_i is now public. As this algorithm occurs at 00:00 UTC, mirrors then update their Merkle root hash per the protocol described in section 5.4.3.

In order to defend against the one-to-many and many-to-one attacks described in section 4.1, each Quorum node only accepts the first ticket per hidden service and the first ticket per name. A many-to-many (either "land rush" or denial-of-registration) attack primarily increases the chances of the adversary winning names. However, our countermeasure is straightforward. First, the Quorum remembers a value max(size(T)), representing the highest number of tickets received by any past Quorum. Then, if Q_i receives more tickets than this amount, Q_i tells Q_{i+1} to increase the difficulty of ticket generation according to the formula $\frac{\max(\text{size}(T))}{\text{size}(T_i)}$. The increase in ticket difficulty reduces the impact of the attack in the next lottery under our assumptions, as we detail in section **??**.

5.4.9 Record Operations

OnioNS also supports common operations on names. Owners of named hidden services may construct modify, renew, transfer, or delete records and issue the records to the Quorum. Once received, mirrors add these records to their ephemeral database. These records can be send to and authenticated by clients within 24 hours, as mirrors merge their ephemeral database into their main database and update their Merkle root publication at 00:00 UTC every day. In all cases, Bob sets the *type* field to the appropriate record type.

Bob can modify his registration by changing either his *subdomains* or *contact* fields. Bob may also transfer the registration to a new owner by issuing a transfer record, which contains *recipientKey*, the public RSA key of the new hidden service. Bob may also relinquish control of his name by issuing a delete record. Bob does not need to recompute proof-of-work for any of these records as these operations are cheap for the Quorum to apply. However, OnioNS names expire after 30 days, so name owners must periodically renew registrations

to maintain ownership. This can be done by issuing a renew ticket with an updated $\mathcal{G}(i)$ and recalculating the proof-of-work algorithm.

5.4.10 Domain Query

Alice only needs Bob's ticket or his latest record to contact Bob by his meaningful name. She then uses the Merkle tree structure to verify that her name server responds with the correct ticket or record, or to achieve authenticated denial-of-existence if her query has no corresponding data structure. Let Alice type a domain d into the Tor Browser.

1. Alice contacts a name server Charlie via his hidden service.
2. Alice asks Charlie for a ticket or record r containing d.
3. Charlie extracts the second-level name n from d.
4. If r exists, Charlie returns r, the leaf node containing n, and all the nodes from the leaf to the root and their sibling nodes.
5. If r does not exist, Charlie returns two adjacent leaves a and b (and the nodes on their paths and siblings) such that $a(name) < n < b(name)$, or in the boundary cases that a is undefined and b is the left-most leaf or b is undefined and a is the right-most leaf.
6. Alice verifies the authenticity or non-existence of r by
   (a) Asserting that n is either contained in the subtree or that n is spanned by the subtree leaves, respectively.
   (b) Asserting the correctness of the hashes in the subtree.
   (c) Asserting that the root hash matches the hash published by the largest agreeing set of Quorum nodes.
7. If these assertions fail, Alice knows that Charlie is dishonest and she must repeat this protocol with a different mirror.
8. If d in r points to a domain d_2 which has a .tor pseudo-TLD, Alice jumps to 2 and queries for d_2.
9. Alice computes Bob's .onion address from $r(pubHSKey)$ and contacts him in the hidden service protocol.

While Alice can verify the authenticity and uniqueness of r by synchronize against the OnioNS network and downloading the database from the Quorum, but this is impractical in most environments. Tor's median circuit speed is often less than 4 Mbit/s, [23] so for the sake of convenience data transfer must be minimized. Therefore Alice can simply fetch minimal information and rely on her existing trust of members of the Tor network.

5.4.11 Onion Query

OnioNS also supports reverse-hostname lookups. In an Onion Query, Alice issues a hidden service address *addr* to Charlie and receives back all Records that have *addr* as either the owner or as a destination in their *subdomain*. Alice may obtain additional verification on the results by issuing Domain Queries on the source .tor domains. We do not anticipate Onion Queries to have significant practical value, but they complete the symmetry of lookups and allow OnioNS domain names to have Forward-Confirmed Reverse DNS matches. We suggest caching destination hidden service addresses in a digital tree (trie) to accelerate this lookup; a trie turns the lookup from $\mathcal{O}(n)$ to $\mathcal{O}(1)$, while requiring $\mathcal{O}(n)$ time and $\mathcal{O}(n)$ space to pre-compute the cache.

6 Security Analysis

In this section, we analyse the security of the Onion Name System with regard to our security goals and expected threat model.

6.1 Global Randomness

We implement $\mathcal{G}(t)$ using [12]. Commitment protocols have been studied in other works [19, 24] and are well understood. If all parties are at least semi-honest then the commitment protocols generally display correctness, privacy, and binding. However, if some participants are malicious, they demonstrate known weaknesses. Namely, while reveals must demonstrably match commits, each participant may choose to reveal or not. If they do not reveal, their value is lost and the protocol produces a different output. If Eve controls b participants, she can make this choice with each participant in turn, allowing 2^b different outcomes.

[12] relies on nine directory authorities, which are maintained by prominent members of the Tor community. The security of the Tor network rests on the as-

sumption that five or more are at least semi-honest, thus their commitment scheme has at most $2^4 = 16$ different outcomes in the worst case without violation of our assumptions. Given the statistical calculations and the safety margin introduced by the recommendations in section **??**, we do not consider this a significant threat to our system and conclude that the Quorum Formation protocol is secure under our design assumptions. The unpredictability of the reveals and the low probability of compromise shown in Figures 8 and 9 provides the strongest defence against Quorum-level attacks.

Assuming that all directory authorities reveal at 12:00 UTC, the design of [12] allows $\mathcal{G}(i)$ to be calculated up to 12 hours before $\mathcal{G}(i)$ is published in the consensus. If we select the Quorum from the 00:00 UTC consensus containing $\mathcal{G}(i)$, an adversary could calculate $\mathcal{G}(i)$ to add or remove routers from the consensus in order to deterministically inject malicious routers into the Quorum. As a countermeasure, the protocol in section 5.4.4 selects the Quorum from the consensus containing the first set of reveals.

6.2 Integrity Guarantees

Merkle trees are widely used to achieve secure verification of very large data structures. They are an integral component in the ZFS file system, Bitcoin, [18] Apache's Cassandra NoSQL database, [10] and in many other applications. The security of the Merkle tree largely rests on the underlying hash function and its resistance to second pre-image attacks. During a domain query, clients fetch a subtree from mirrors, verify the integrity of the ticket or record against the leaf node, and recompute and verify the hashes of the subtree. The cryptographic strength of SHA-384 prevents mirrors from forging or falsely claiming non-existence of a ticket or record. Clients also check the subtree value against the Quorum's published hashes, preventing mirrors from forging the subtree or returning an obsolete subtree. This approach provides strong integrity guarantees for both existent and non-existent records even if the mirror is malicious.

6.3 Lottery

$V_i(k) = \text{count}(T_i(k) \oplus G_{i+1})$, where $\text{count}(x)$ counts the number of 1 bits in x.

TODO

As T_i is initially blinded, it is difficult for the adversary to determine in advance if this threshold is reached. This scheme also means that the system adapts in response to an increase in global average computational speed as the barrier-of-entry becomes too low.

6.4 Proof-of-Work

The proof-of-work formula is satisfied when $\text{PoW}(S_{RSA}(c, r)) \leq d$, where c is static data, r is Bob's private key, and d is the work difficulty. We integrated the proof-of-work step into our registration protocols in order to create a barrier-of-entry, with the expectation that Bob run the scrypt function himself. However, our algorithm does not entirely prevent Bob from outsourcing this expensive computation to a secondary computational resource, Craig, whom we assume does not have r.

First, Bob repeatedly computes $S_{RSA}(c, r)$, producing a large list of digital signatures. Craig then tests $\text{PoW}(x) \leq d$ for each digital signature x until the formula is satisfied. Bob then sets the ticket's *signature* field to this x value, producing a valid ticket. Bob can minimize the size of his precomputed list by sending each signature individually to Craig for testing. However, as scrypt is an purposely computationally-expensive function, this still incurs a cost upon Craig that must be financially compensated by Bob. Thus, the algorithm always places a cost to Bob.

Alternative algorithms may more tightly couple the scrypt and RSA-PSS components and prevent Bob from outsourcing the proof-of-work step. However, we are unaware of any existing algorithm that combines proof-of-work with digital signatures. The next generation of Tor hidden services [**?**] replaces RSA-1024 hidden service keys with Ed25519; in future work we will explore whether the Ed25519 deterministic signature scheme may be tightly combined with scrypt.

6.5 DNS Leakage

Accidental leakage of .tor lookups over the Internet DNS via human mistakes or misconfigured software may compromise user privacy. This vulnerability is not limited to OnioNS and applies to any pseudo-TLD; Mohaisen and Thomas observed .onion lookups on root DNS servers at a frequency that corresponded to external global events and highlighting the human factor in those leakages [27]. Closing this leakage is difficult; arguably the simplest

approach is to introduce whitelists or blacklists into common web browsers to prevent known pseudo-TLDs from being queried over the Internet DNS. Such changes are outside the scope of this work, but we highlight the potential for this leak.

7 Evaluation

7.1 Implementation

We have build a reference implementation of the Onion Name System in C++11 as a supplement to this work. We utilize Boost Asio [15] for our networking engine and use the Botan [7] library for most cryptographic operations. We encode all the data structures in JSON; JSON is significantly more compact than XML, but retains user readability and its support of basic primitive types is highly applicable to our needs. Our code is licensed under the Modified BSD License, identical to Tor, and is available for Linux through a software repository at http://onions55e7yam27n.onion.

We divided our software into three parts: OnioNS-client, OnioNS-server, and OnioNS-HS, with OnioNS-common as a shared library dependency. The client-side software interacts with the Tor binary, intercepts user requests for .tor domain names, performs a Domain Query, and rewrites the request to a .onion address before allowing Tor to bind the request to a circuit. This approach preserves backwards-compatibility with the Internet DNS and the .onion pseudo-TLD, achieving a design objective and enhancing usability.

7.2 Integration Test

We have deployed a small testing network of Quorum and mirror servers. We first created a hidden service for our project, set up a small web server, and used Chutney to generate a semi-meaningful address, "onions55e7yam27n.onion". We then used our command-line tool to create a lottery ticket for "example.tor" and then to transmit it to the Quorum. This sole ticket won the lottery and we received our name. Our ticket then propagated through the network to mirrors. Finally, we installed our client software into Tor Browser 5.5, a fork of Firefox 38.4.0 ESR. We typed "example.tor" into the Tor Browser and the request was intercepted, resolved through a Domain Query, and rewritten to "onions55e7yam27n.onion". The Tor binary then communicated with our hidden service and returned the contents back to the Tor Browser. This process did not require any further user input and occurred behind-the-scenes, so the Tor Browser retained the "example.tor" name in the address bar and in the mouse-over text for relative hyperlinks. We illustrate the result in Figure 4. The software performed asynchronously and allowed normal browsing to both the Internet and other hidden services, even while the OnioNS domain was resolving.

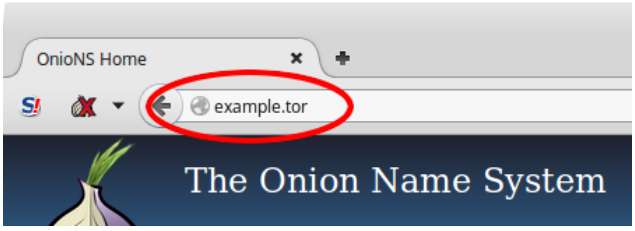

Fig. 4. We load the OnioNS' hidden service, "onions55e7yam27n.onion", transparently under the "example.tor" domain. The OnioNS software launches with the Tor Browser.

7.3 Results

7.3.1 Performance

Our experiment involves two machines, A and B. Both were hosted on 1 Gbit connections on a university campus. Machine A has an Intel Core2 Quad Q9000 (Penryn architecture) @ 2.00 GHz CPU from late 2008 and Machine B has an Intel i7-2600K (Sandy Bridge architecture) @ 4.3 GHz CPU from 2011, representing low-end and medium-end consumer-grade computers, respectively.

We selected the parameters of scrypt such that it consumed 128 MB of RAM during operation. We consider this an affordable amount of RAM for low-end consumer-grade computers. We created a multi-threaded implementation of the Record Generation protocol and used all eight virtual CPU cores on Machine B to generate our Record. As expected, our RAM consumption scaled linearly with the number of scrypt instances executed in parallel; we observed approximately 1 GB of RAM consumption during Record Generation. We set our difficulty level so that Records took approximately six hours on average to become valid on Machine B.

We conducted several performance measurements for the Domain Queries. We measured and averaged 200 samples of the CPU wall-time required for both machines to validate the Record.

Description	A (ms)	B (ms)
Parsing JSON	5.21	2.42
Validating scrypt	448.184	294.963
$V_{RSA}(m, E)$	6.35	2.74
Total Time	459.744	300.123

As expected, Machine B outperformed Machine A in all instances and we observed that single iteration of scrypt dominated the total validation time. This is a CPU cost introduced to Tor clients, Mirrors, and Quorum nodes for each Record.

Clients must also check the Merkle root signatures from all L_Q Quorum nodes. We use Ed25519 to reduce the signature space requirements and CPU time required for verification: $S_{ed}(m, e)$ signatures fit into 64 bytes and may be verified in batch form. Bernstein et al. reports that a quad-core Westmere-era CPU can generate 109,000 signatures per second and verify 71,000 signatures per second with 134,000 CPU cycles per signature [3]. Therefore, even with large Quorums, we anticipate clients to be able to verify signatures from all Quorum nodes in sub-second time on moderate hardware.

7.3.2 Latency

Although Tor is a low-latency network, as Domain Queries occur over a Tor circuit the three-hop path still introduces some latency into the communications between the client and a Mirror. The time is highly dependent on the circuit's network distance and the speed of each Tor router. This adds an additional delay between the time that a user enters an OnioNS domain into the Tor Browser and when Tor begins loading the hidden service. Fortunately, latency and load times across Tor circuits have been well studied. Domain Queries transfer both a Record, a Merkle subtree, and a collection of ed25519 signatures. We estimate the size of this information to be approximately 50 KB. We provide the distribution of circuit performance in Figure 5.

This network latency to query a OnioNS Mirror is supplemental to the time to verify the Record and Merkle subtree. We avoid additional latency costs by implementing a client-side cache in order to allow subsequent queries to be resolved locally. We also reduce the expense of circuit construction by building the circuit on startup.

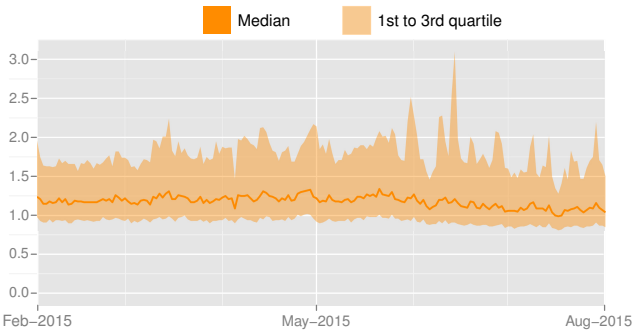

Fig. 5. The average performance to download 50 KB files over Tor circuits, as measured by Tor bandwidth authorities. The first and third quartiles are shown with the median time shown in orange [23].

7.3.3 Usability

Our software maximizes usability in for two main groups of users: hidden service administrators and Tor end-users. The OnioNS-HS command-line utility provides minimal prompts: it asks the user for the main domain name, a list of subdomains and destinations, and the user's PGP key if they choose to disclose it. It then loads the hidden service private key, performs the proof-of-work to validate the Record, and automatically uploads the Record to the Quorum. We released a beta test of our software to Tor developers and volunteers and received positive feedback on the simplicity of the registration process.

Our client software integrates well into the Tor Browser and starts and stops with the Tor Browser environment. As shown in Figure 4, OnioNS resolves and loads hidden services under a meaningful name transparently without requiring any user interaction, similar to traditional DNS requests over Tor circuits. We observed that queries for unknown domains added several seconds of latency to the load time of hidden services, matching our above analysis. Similar to the BIND software for DNS, OnioNS-client caches known Records in local storage, allowing further queries for their domains to be resolved nearly instantaneously. This mechanism also accelerates load times if those Records are part of a chain of resolutions. Local resolution also minimizes a Mirror's exposure to the popularity of domain names.

We achieve another primary usability benefit by introducing an automatic naming system for Tor hidden services: it is no longer necessary for the Tor community to construct and maintain directories of hidden services. The automatic resolution of domain names allows scaling beyond human-maintained directories, which only efficiently scales to several hundred names at most. OnioNS should provide a significant usability to Tor users and the community at large.

7.4 Discussions

In this section we further discuss and compare OnioNS with related works.

GNS and Namecoin

In this section we further discuss and compare our work with related works. The Onion Name System and Namecoin both achieve all three properties of Zooko's Triangle, and while the two systems share some design similarities, each system is constructed with different threat models and different objectives in mind.

Namecoin's security rests on two primary assumptions: that its network is resistant to Sybil attacks and that more than 50 percent of the network's computational power is at least semi-honest. An attacker who gained the majority of the computational power (a "51% attack") may double-spend transactions, prevent new transactions from entering the honest blockchain, and prevent honest miners from contributing blocks. A successful Sybil attack on Namecoin's network allows an attacker to disrupt the network by purposefully not relaying blocks or transactions, providing attacker-controlled data to clients, or by increasing the potential for double-spending attacks. Namecoin's blockchain has an indefinite length in order to allow the network to trace transactions and ownership of Namecoins back to their originating source. It relies on each participant in the Namecoin network to hold, validate, and read from its own local copy of the blockchain. The CPU, bandwidth, and memory requirements for anyone holding the blockchain scales linearly as the age and popularity of the Namecoin system increases.

By contrast, OnioNS' central security assumption is that circuits through the Tor network provide privacy. This assumption implies that the Tor network remains resistant to Sybil attack, traffic analysis, and that the majority of the directory authorities remain semi-honest. We have shown that a sufficiently-large Quorum remains strongly resistant to large-scale Sybil attacks on the Tor network. Thus, we do not introduce a new network for our naming system and instead utilize the Tor network to achieve both communication privacy and the infrastructure for OnioNS. If an attacker gains control of the Tor network (such as by Sybil attack or by compromising the directory authorities) then circuits no longer provide privacy, hidden services can be de-anonymized, and a privacy-enhanced naming system no longer becomes necessary. We do not also rely on assumptions of computational power: unlike Namecoin, attackers with large computational capacities are not able to disrupt network communication or to provide malicious responses to client queries.

Both Namecoin and OnioNS require each member of the network to maintain a copy of the system's database.

Both Namecoin and OnioNS utilize append-only data structures for long-term storage. Namecoin typically requires clients to either hold their own copy of the blockchain, rely on the honesty of their Namecoin-compatible DNS server, or to utilize a Simplified Payment Verification [18] (SPV) scheme which allows clients to download and verify minimalistic information from a central server. These latter two cases are vulnerable to a variety of attacks if the server is malicious and neither approach provides authenticated denial-of-existence. OnioNS does also not require clients to download the Pagechain; instead, clients receive a minimal number of mappings, a Merkle subtree, and Quorum signatures on the root hash. Our protocols prevent a malicious server from acting dishonestly, including spoofing mappings or falsely claiming non-existence. The security of the response depends on our security assumptions regarding the Quorum.

Namecoin and OnioNS allow full enumeration of all registered domains; name registrations are assumed to be public knowledge immediately after they are uploaded to either network. We do not consider this a significant threat to our system as registrations do not contain personal information. Similar to Namecoin, anyone may obtain a complete copy of the Pagechain and Mirrors must be able to access and verify all information in the Pagechain in order to respond to client queries.

Both OnioNS and Namecoin operate under weaker adversarial models than the GNU Name System. GNS assumes than attacker may participant in any role, may infiltrate the network by large-scale Sybil attack, and is assumed to have more computational power than all honest participants combined. Neither Namecoin, OnioNS, nor Tor provide full defences against such well-resourced adversaries. Tor hidden services may become de-anonymized under GNS' adversarial model so we do not assume that our adversaries are that powerful. End-

users should select their naming system carefully according to their threat model.

8 Conclusions and Future Work

We have presented the Onion Name System (OnioNS), a distributed, secure, and usable alternative DNS that maps globally-unique and meaningful .tor domains to .onion hidden service addresses, and achieve all three properties of Zooko's Triangle. We enable any hidden service operator to anonymously claim a human-readable name for their server and clients to query the system in privacy-enhanced manner. We introduce a distributed blockchain-based database and mechanisms that let clients authenticate and verify denial-of-existence claims. Additionally, we utilize the existing and semi-trusted infrastructure of Tor, which significantly narrows our threat model to already well-understood attack surfaces and allows our system to be integrated into Tor with minimal effort. Our reference implementation demonstrates high usability and shows that OnioNS successfully addresses the major usability issue that has been with Tor hidden services since their introduction in 2002.

In future work we will expand our implementation and pursuit integrating it into Tor. OnioNS requires a few changes to Tor, namely a new .tor pseudo-TLD and Ed25519 router keys, but we introduce no changes to Tor's hidden service protocol. Should Tor's developers introduce changes to the hidden service protocol, OnioNS can become forwards-compatible with a few changes. Additionally, our implementation currently only supports ASCII characters in domain names, so in future work we will explore implementing Punycode to provide support for international character sets. Unlike the Internet DNS, we will disallow digits zero and one (similar to base32 encoding) in order to reduce the threat of phishing attacks from spoofed domains with indistinguishable characters.

9 Acknowledgements

We would like to thank Roger Dingledine, George Kadianakis, Yawning Angel, and Nick Mathewson for their support, commentary, and assistance with Tor technical support.

10 Appendix

In this section we statistically analyse the Tor network and provide recommendations for the size and rotation rate of the Quorum.

10.1 Quorum Size

In section 4, we assume that an attacker, Eve, controls some fixed f_E fraction of routers on the Tor network. Quorum selection may be considered as an L_Q-sized random sample taken from an L_T-sized population without replacement, where the population contains $L_T \cdot f_E$ entities that we assume are compromised and colluding. Then the probability that Eve controls L_E Quorum nodes is given by the hypergeometric distribution, whose probability mass function is shown in Equation 1. Eve controls the Quorum if either $> \frac{L_Q - L_E}{2}$ honest Quorum nodes disagree or if $L_E > \frac{L_Q}{2}$. The former scenario is difficult to model theoretically or in simulation, but the probability of the latter may be calculated. If all Quorum nodes are selected with equal probability, then $\Pr(L_E > \frac{L_Q}{2})$ is given by the p-value of the hypergeometric test for over-representation, expressed in Equation 2.

$$\Pr(L_E) = \frac{\binom{L_T \cdot f_E}{L_E}\binom{L_T - L_T \cdot f_E}{L_Q - L_E}}{\binom{L_T}{L_Q}} \tag{1}$$

$$\Pr(L_E > \frac{L_Q}{2}) = \sum_{i=\lceil \frac{L_Q}{2} \rceil}^{L_Q} \frac{\binom{L_T \cdot f_E}{i}\binom{L_T - L_T \cdot f_E}{L_Q - i}}{\binom{L_T}{L_Q}} \tag{2}$$

Odd choices for L_Q prevents the network from splintering in the event that the Quorum is evenly split across two databases. We provide the statistical calculations of Equation 2 for various Quorum sizes in Figure 6.

However, we select Quorum members according to consensus weight, akin to router selection in a Tor circuit. The distribution of consensus weight (and thus the selection probabilities) for routers with the Fast, Stable, and Running flags closely follows an exponential distribution, as shown in Figure 7. The figure suggests that the Tor network contains a low number of high-end routers and a large number of low-end routers.

TODO: REDO FROM HERE TO IMAGE

We now re-examine Equation 2 with regard to this distribution of consensus weight. Consider that the hypergeometric distribution describes the probability of selecting k Eve-controlled routers in an L_Q-sized Quo-

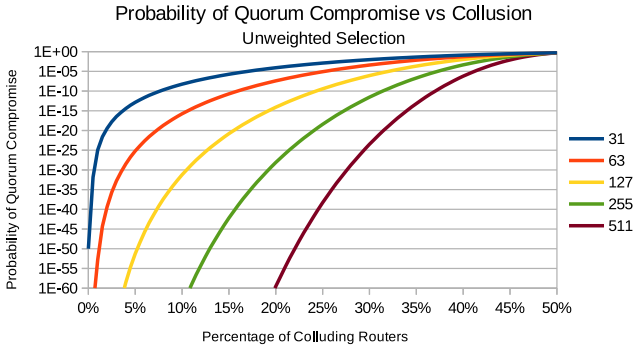

Fig. 6. The values for $\Pr(L_E > \frac{L_Q}{2})$ for Quorum sizes of 31, 63, 127, 255, and 511. All probabilities exceed 0.5 when more than 50 percent of the Tor network is under Eve's control. We set our population to 4540 routers; the average number of routers with the Fast, Stable, and Running flags across all consensuses in July 2015 [23].

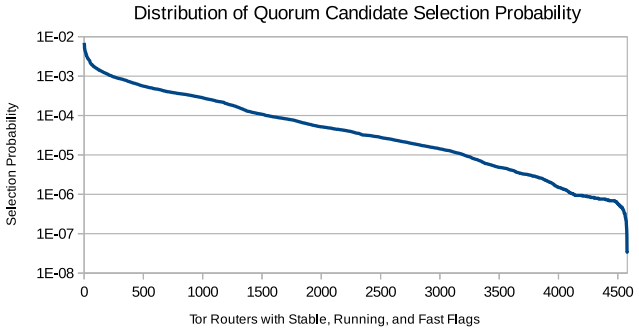

Fig. 7. The normalized distribution of consensus weights of Quorum candidates in July 2015, reflecting the probabilities of inclusion in the Quorum. The distribution may be modelled by an exponential trendline with $R^2 = 0.9884$, but appears slightly super-exponential.

rum from an N-sized population containing K Eve-controlled routers. Let $L(x)$ be the probability distribution of selecting a router whose consensus weight is at the lowest x percentile. Then the probability of compromise is given by Equation 4 where K, the expected number of routers in a population of size N, is given by Equation 3, and R is the probability that routers outside $L(x)$ are compromised. Since $L(x)$ describes probabilities and N must be a natural number, $(N \in \mathbb{N})$ this approach provides an approximation of the probability of compromise.

We illustrate the probabilities against discrete values of x and various Quorum sizes in Figure 8 using $N = 4540$, consistent with the population in Figure 6.

$$K = N \cdot \left(\int_0^x (L(x)) + R \cdot \int_x^1 (L(x)) \right) \quad (3)$$

$$\Pr(L_E > \frac{L_Q}{2}) = \sum_{i=\lceil \frac{L_Q}{2} \rceil}^{L_Q} \frac{\binom{K}{i}\binom{N-K}{L_Q-i}}{\binom{N}{L_Q}} \quad (4)$$

In contrast to Figure 6 which demonstrates that an unweighted selection leads to a high probability of compromise with small levels of collusion, Figure 8 suggests that biasing Quorum selection by consensus weight provides a strong defence against large-scale Sybil attacks. Indeed, even when 60 percent of the low-end Quorum candidates are malicious, most Quorum sizes produce negligible probabilities of compromise. We consider it reasonable to assume that low-end routers are under Eve's control; these routers are the cheapest and logistically easiest to operate. Our approach remains resistant to this attack: these routers will be included in the Quorum very infrequently because of their low consensus weight.

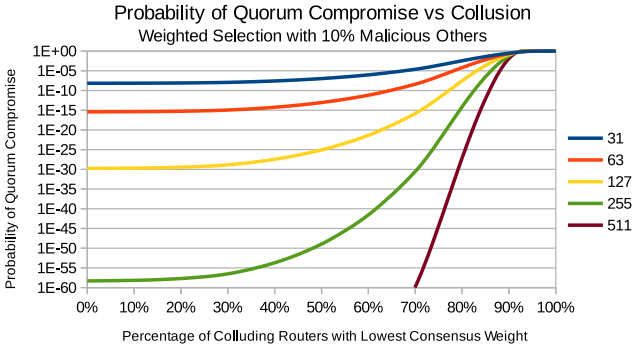

Fig. 8. The values for $\Pr(L_E > \frac{L_Q}{2})$ from Equation 4 for various Quorum sizes. We assume that all routers $\in L(x)$ are under Eve's control, while routers $\notin L(x)$ have a 10 percent chance of being under Eve's control.

Small Quorums are also more susceptible to node downtime or denial-of-service attacks. Figure 8 shows that the choices of $L_Q = 31$ is suboptimal; it is more easily compromised even with low levels of collusion. $L_Q = 63$ is more resistant, but not significantly more so. We therefore recommend $L_Q \geq 127$.

10.2 Quorum Rotation

In section 4, we assume that f_E is fixed and does not increase in response to the inclusion of OnioNS on the

Tor network. If we also assume that L_T is fixed, then we can examine the impact of choices for Δq and calculate the probability of Eve compromising any Quorum over a period of time t. Eve's cumulative chances of compromising any Quorum is given by $1-(1-f_c)^{\frac{t}{\Delta q}}$ where f_c is Eve's chances of compromising a single Quorum. We estimate this over 10 years in Figure 9.

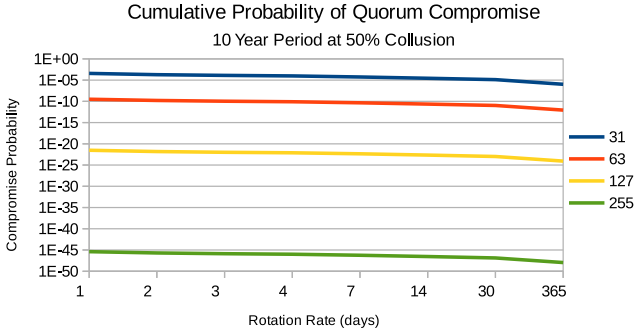

Fig. 9. The cumulative probability that Eve controls any Quorum at different rotation rates over 10 years at $f_E = 50$ for Quorum sizes 31, 63, 127, and 255. We base these statistics on the probabilities from Figure 8 at 50 percent collusion.

Figure 9 suggests that although larger values of Δq positively impact security, the choice of L_Q is more significant. Furthermore, even "Stable" routers in the Tor network may be too unstable for very slow rotation rates, and small values for Δq also reduces the disruption timeline for a malicious Quorum. Therefore, based on Figure 9, we further reiterate our recommendation of $L_Q \geq 127$ and suggest $\Delta q = 7$. Although a malicious Quorum would have the capabilities to deploy a variety of attacks on the network, the proper selections of L_Q and Δq reduces the likelihood of this occurring to near-zero probabilities. We consider this a stronger solution than introducing countermeasures to specific Quorum-level attacks.

References

[1] Baruch Awerbuch and Christian Scheideler, *Group spreading: A protocol for provably secure distributed name service*, Automata, Languages and Programming, Springer, 2004, pp. 183–195.

[2] Daniel J Bernstein, *Dnscurve: Usable security for dns*, http://dnscurve.org/, 2009.

[3] Daniel J Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang, *High-speed high-security signatures*, Journal of Cryptographic Engineering **2** (2012), no. 2, 77–89.

[4] John Brooks, *Anonymous peer-to-peer instant messaging*, https://github.com/ricochet-im/ricochet, 2015.

[5] Christian Cachin and Asad Samar, *Secure distributed dns*, Dependable Systems and Networks, 2004 International Conference on, IEEE, 2004, pp. 423–432.

[6] Ryan Castellucci, *Namecoin*, https://namecoin.info/, 2015.

[7] Botan Developers, *Botan: Crypto and tls for c++11*, http://botan.randombit.net/, 2015.

[8] Roger Dingledine, Nick Mathewson, and Paul Syverson, *Tor: The second-generation onion router*, Tech. report, DTIC Document, 2004.

[9] Md Sadek Ferdous, Audun Jøsang, Kuldeep Singh, and Ravishankar Borgaonkar, *Security usability of petname systems*, Identity and Privacy in the Internet Age, Springer, 2009, pp. 44–59.

[10] Apache Software Foundation, *The apache cassandra project*, https://cassandra.apache.org/, 2015.

[11] Michael T Goodrich, Roberto Tamassia, and Andrew Schwerin, *Implementation of an authenticated dictionary with skip lists and commutative hashing*, DARPA Information Survivability Conference & Exposition II, 2001. DISCEX'01. Proceedings, vol. 2, IEEE, 2001, pp. 68–82.

[12] David Goulet and George Kadianakis, *Random number generation during tor voting*, https://gitweb.torproject.org/torspec.git/tree/proposals/250-commit-reveal-consensus.txt, 2015.

[13] George Kadianakis and Karsten Loesing, *Extrapolating network totals from hidden-service statistics*, Tech. report, The Tor Project, 2015.

[14] katmagic, *Shallot*, https://github.com/katmagic/Shallot, 2012.

[15] Christopher Kohlhoff, *Boost asio*, http://www.boost.org/doc/libs/1_59_0/doc/html/boost_asio.html, 2015.

[16] Makoto Matsumoto and Takuji Nishimura, *Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator*, ACM Transactions on Modeling and Computer Simulation (TOMACS) **8** (1998), no. 1, 3–30.

[17] Ralph C Merkle, *A digital signature based on a conventional encryption function*, Advances in Cryptology-CRYPTO'87, Springer, 1988, pp. 369–378.

[18] Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, Consulted **1** (2008), no. 2012, 28.

[19] Moni Naor, *Bit commitment using pseudo-randomness*, Advances in Cryptology—CRYPTO'89 Proceedings, Springer, 1990, pp. 128–136.

[20] Simon Nicolussi, *Human-readable names for tor hidden services*, Bachelor thesis, Leopold–Franzens–Universitat Innsbruck, Institute for Computer Science, 2011, http://www.sinic.name/docs/bachelor.pdf.

[21] Lasse Overlier and Paul Syverson, *Locating hidden servers*, Security and Privacy, 2006 IEEE Symposium on, IEEE, 2006, pp. 15–pp.

[22] Colin Percival and Simon Josefsson, *The scrypt password-based key derivation function*, Tech. report, September 2012, https://tools.ietf.org/html/draft-josefsson-scrypt-kdf-00.

[23] The Tor Project, *Tor metrics*, https://metrics.torproject.org/, 2015.

[24] Ronald Rivest, *Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer*, Unpublished manuscript (1999).

[25] Nolen Scaife, Henry Carter, and Patrick Traynor, *OnionDNS: A seizure-resistant top-level domain*, IEEE Conference on Communications and Network Security (2015).

[26] Marc Stiegler, *Petname systems*, Tech. report, Hewlett-Packard, 2005, http://www.hpl.hp.com/techreports/2005/HPL-2005-148.pdf.

[27] Matthew Thomas and Aziz Mohaisen, *Measuring the leakage of onion at the root*, Tech. report, Verisign Labs, 2014.

[28] Matthias Wachs, Martin Schanzenbach, and Christian Grothoff, *A censorship-resistant, privacy-enhancing and fully decentralized name system*, Cryptology and Network Security, Springer, 2014, pp. 127–142.