RZ 3496 (# 99317) 05/26/03
Computer Science 5 pages

Research Report

Establishing Trust in Distributed Storage Providers

Germano Caronni

Zurich Information Security Center
Swiss Federal Institute of Technology
ETH Zentrum
8092 Zurich
Switzerland
gec@acm.org

Marcel Waldvogel

IBM Research
Zurich Research Laboratory
8803 Rüschlikon
Switzerland
mwl@zurich.ibm.com

Research
Almaden · Austin · Beijing · Delhi · Haifa · T.J. Watson · Tokyo · Zurich

Establishing Trust in Distributed Storage Providers

Germano Caronni and Marcel Waldvogel*

Abstract

Corporate IT as well as individuals show increasing interest in reliable outsourcing of storage infrastructure. Decentralized solutions with their resilience against partial outages are among the most attractive approaches. Irrespective of the form of the relationship, be it based on a contract or on the more flexible cooperative model, the problem of verifying whether someone promising to store one's data actually does so using multiple replicas remains to be solved. In this paper, we introduce a lightweight mechanism that allows the *data originator* or a dedicated *verification agent* to build up trust in the *replica holder* by means of protocols that do not require prior trust or key establishment. We show how naive versions of the protocol do not prevent cheating, and then strengthen it by adding means that make it economically attractive to be honest. This provides a foundation for further work in providing trustworthy distributed storage.

1 Introduction

The outsourcing of storage infrastructure is becoming increasingly interesting for corporate IT as well as for individuals. Besides the tainted use of peer-to-peer (P2P) content sharing systems such as Gnutella [1], the idea of completely decentralized storage is very appealing. Ranging from niche applications such as censor-resistant publishing (e.g., Freenet/Eternity [2, 3] and Publius [4]), to the scalable use of promising overlay networks based on distributed hash tables (DHT) [5–9], the potential of storing Petabytes of data accessible whenever and wherever required has spurred great enthusiasm. The advent of DHTs has given such systems a strong boost, as DHTs allow an efficient, scalable, and often failure-tolerant addressing of stored documents. These and similar other file distribution and storage mechanisms also make sense in more traditional scenarios, ranging from distributed backup and mirroring facilities to distributed storage facilities for gridware [10] or a gridware-like environment.

There is, however, one crucial problem with independent agents holding copies of your data: How can you make sure that they really store a copy locally, and not just claim to do so? The existence of this problem becomes immediately evident in collaborative environments. Even in the presence of contracts, how can you verify that the storage providers are actually providing the promised number of replicas? If you ask them to provide you with some file content, they can easily forward that request to another replica holder without your knowledge. The most immediate risk here is that replicas of your data are being retained in fewer places than you ask for. In the extreme, this can lead to the existence of a single point of failure, exactly the scenario distributed storage eagerly tries to avoid. If storing your data gives replica holders the right to store some of their data at your place, a financial compensation, or some other kind of tangible benefit, the economic incentive for falsely claiming to store your data becomes clear.

1.1 Our Contribution

In this paper, we introduce a mechanism that returns power to the *data originator*. It allows the originator to establish trust into the *replica holder*. We show that naive approaches are susceptible to cheating by the replica holder. Our proposed lightweight protocol allows building up trust, even without a prior phase of authenticated key exchange and trust establishment, both major criteria in collaborative systems. The resulting protocol does not provide a direct proof of storage, but requires dishonest replica holders to use significantly more resources than an honest replica holder would have to use. It does not, however, prevent malicious, resource-rich entities from performing their intentionally malicious goal at considerable expense. Using appropriate cost functions, the protocol provides the necessary leverage against "lazy" replica holders, whose goal it is to obtain a seizable advantage and which we expect to be the common cheating candidate. Our symmetrical protocol limits the possibilities of Denial-of-Service (DoS) attacks.

---

*G. Caronni is with the Zurich Information Security Center (ZISC) at ETH Zurich and with Sun Microsystems Inc., Sun Laboratories. He can be reached at `gec@acm.org`. M. Waldvogel is with IBM Research, Zurich Research Laboratory. He can be reached at `mwl@zurich.ibm.com`.

1.2 Organization of the Paper

In Section 2, we first introduce and then improve methods that help verify whether a replica holder actually keeps its promises. Section 3 describes how to minimize the impact of DoS attacks. In Section 4, we present related work, and in Section 5, we draw our conclusions.

2 Verification of Content

Standard solutions to verify whether a replica holder has a copy of some file are to either ask it to send the file back to the verifier, or to compute a (potentially keyed) hash value over the file. Unfortunately, they require considerable bandwidth (both in terms of network traffic and in terms of storage-to-CPU data transfers) or CPU power for each request, respectively. The exclusive use of optimizations such as hash trees over the file are not appropriate, because the supposed replica holder can just precompute them, thus obviating the need for storing the entire document.

A viable compromise is to have the verifier request the hash value to be computed only over a chunk of the data at one time, with the chunk being selected at random. Thus a smooth trade-off between full verification and partial verification as well as between CPU/disk load and bandwidth usage is achieved.

Let us now take this as the most naive practical starting point. By considering the different ways in which a replica holder might cheat and adapting our protocol accordingly, this initial idea will steadily evolve into a simple, efficient, and secure protocol.

2.1 Options of Dishonest Replica Holders

As mentioned above, a replica holder can try to cheat in many ways. It can pre-compute information and only remember that data; it can try to forward the request for verification to another (potentially colluding) replica holder; and it can download the file or parts of the file that are needed for verification from another replica holder on demand.

The following subsections will look at each of these possibilities, and discuss how they can be counteracted. The attempt at using pre-computed data is most easily thwarted by making all computations over the data involve some fresh nonce to be used as the key to a message authentication code or to make the range of data to be verified sufficiently random (see also Section 2.4).

Step	A		B
1	$A, R_1, H(R_1 \| R_2)$	$\longrightarrow$	
2		$\longleftarrow$	$B, R_3, H(R_3 \| R_4)$
3	R_2	$\longrightarrow$	
4		$\longleftarrow$	R_4, K

R_i are random values; A, B are not easily forgeable identities to deter work delegation. The result of the protocol, the key K, is defined as $K = H(A \| B \| R1 \| R2 \| R3 \| R4)$.

Figure 1: Key exchange protocol

2.2 Delegation to Unsuspecting Replica Holders

The first idea a smart fraudulent replica holder might have is not to perform any work at all, but simply to try and forward the verification request from a client to another legitimate replica holder. One way to counter this would be to have the data originator produce “personalized” replicas for each holder, e.g. by tying them to the identity[1] of the replica holder. However, this would require the underlying replication architecture to be strictly star-shaped. No replica holder would be able to forward its copy to somebody else, without going first through the data originator. This contradicts the goal of avoiding single points of failure and performance bottlenecks.

A far more effective, but still simple solution is to use a key for a Message Authentication Code (MAC) [11] that is derived from random inputs of both verifier and replica holder in a secure fashion. In this way, neither party can *a priori* force a result with specific parameters. Therefore, the replica holder cannot forward the request, as a delegation attempt would use a different key. The initial agreement can be kept simple because no confidentiality or authenticity issues exist. For example, a man-in-the-middle trying to hijack the protocol can only persuade the verifier that the replica holder has no copy, an accusation that can be achieved more easily by means of a DoS attack, including simply dropping the packets (Section 3).

A sample key agreement protocol is shown in Figure 1. Note that B’s messages are not chained to A’s messages, until the key is sent back. The inclusion of the identities of A and B is required to prevent a dishonest replica holder B from transparently forwarding traffic between A and C.

---

[1] Identities, as used in this paper, might be as simple as the addresses used by the communications protocols, e.g., IP addresses. They are neither required to be cryptographically strong nor signed by a central authority.

Table 1: Latency and bandwidth comparison

	Disk	LAN	MAN	Intra-	Inter-
				continental	
Latency [ms]	10[a]	1	10	50…100	100…400
Bandwidth [Mbps]	250…500	10…1000	1…100	1…10	0.1…10

---

[a] Time for random seek; track-to-track seek is around 1ms. As disks typically buffer at least an entire track, seek times within a track become basically negligible.

2.3 Delegation to Colluding Replica Holders

In Section 2.2, we have seen how to prevent a dishonest replica holder from abusing an honest one. But the problem becomes much harder if the two replica holders actively collaborate and share information beyond what is exchanged in the protocol in Figure 1. This might include having random number generators running in lockstep, exchanging the random values R_3 and R_4, or allowing the key K to be set without going through the key exchange.

While there are possibilities that might help detecting collusion between replicas, this requires the colluding replicas to be relatively far away. Then, this additional delay might be detected by making the actual hash calculation involve numerous synchronous message exchanges between verifier and the fake replica holder. Given the uncertainties in detecting colluding replica holders, we currently do not feel that the effort is worthwhile.

We believe, however, that economic considerations do not motivate collusion. Consider the following scenario: A partnership of colluders provides a substantial portion of the storage infrastructure, say, 10%. In addition, assume that the typical customer requests two replicas. Given a random selection of replica holders, the dishonest service could be offered at a storage savings of about 1% of the infrastructure. We believe that the savings obtained are not worth the risk of suddenly being put out of business because of the fraudulent behavior. A company owning the sizable business of 10% of the total storage market should not take this risk lightly.

Therefore, the incentives at work against collusion in both large (business risk) and small (no profit gain) partnerships are expected to support honesty.

2.4 Download on Demand

Whenever a verifier requests a check from a replica holder, the replica holder could theoretically go and request the specific data to be covered by a check from other replica holders. This works well when the range to be verified is mostly contiguous and relatively small. Otherwise, the efforts and bandwidth spent by the fraudulent replica in downloading the data are large compared with the storage space saved.

The predicament for the replica holder can be made even stronger, in that the range to be verified consists of several hundred very small chunks (e.g. only a single byte), each residing a random distance apart from the previous chunk. The selection of actual distances should discourage downloading large chunks.

At this point, we can compare the different behavior of network and local access to data, see Table 1.

These differing properties can be used to differentiate between honest replica holders that access the document from a disk and dishonest replica holders that access it over a network. Differences exist in both bandwidth and delay, but the latter can easily be magnified by preventing the fraudulent replica holder from parallelizing the download requests. Even if it has enough bandwidth available, each request will have to be processed sequentially, and thus the response will reveal this through high latency.

Such an effect is achieved by making the steps between the bytes to be verified data dependent. They still should be spaced such that

1. for fraudulent replica holders it is at least as efficient to request the ranges separately, than requesting the entire range as a whole, and
2. honest replica holders obtain reasonable efficiency by having different chunks reside within the realm of a single disk access.

As a first cut, consider the verification procedure in Listing 1. Given the amount of randomness involved in selecting the bytes to verify, we cannot conceive of any way a dishonest replica holder would use this to precompute and store information about the verification value. Thus we suggest to use an inexpensive checksumming function such as Adler-32 [12], instead of a more expensive cryptographically strong hash function.

Listing 1 First-cut verification procedure

```
Verifier and replica holder agree on common key (Figure 1)
Verifier specifies chunk size, maximum step size, and upper number of steps.
Replica holder and verifier seed their stepping function (RC4) with the key
current position ← 8 bytes out of RC4 (modulo file size)
while number of steps $<$ upper number of steps do
    value ← chunk at current position in file
    insert value into hash
    step size ← (value + 8 bytes out of RC4) (modulo maximum step size)
    next position ← (current position + step size) (modulo file size)
end while
```

Using Listing 1 with the data provided in Table 1, we need about 1 s disk drive time (probably much less CPU time) to check some 30 MB available on the local disk, independent of the number of samples, assuming a contiguous layout of the file. Over a network (50 ms at 1 MB/s (∼10 Mb/s), which is roughly the rate with which medium-sized enterprises connect to the Internet), it takes 30 s to download everything; the same time is achieved by requesting 1200 data-dependent samples.

Even at higher bandwidths, the replica being exploited also needs to have the same bandwidth available and the dishonest replica needs to be willing to waste this (expensive) bandwidth to save some (cheap) disk space. By using this scheme, we can easily remove any economic incentives that cheating may have had.

3 Denial-of-Service Considerations

The verification protocol as outlined so far is an excellent way to run a DoS attack on replica holders: Just have them perform unlimited verification operation. That will keep them busy and unable to provide their normal service. Although this situation can be prevented by intricate identity and ownership management of files, we choose not to explore this direction. Instead, we keep things simple and again base trust only on verifiable behavior. We balance costs such that a verifier has to spend at least as much effort on continued verification processes as the replica holder does.

The first mechanism to limit DoS opportunities against replica holders is by giving the replica holder the option to require the verifier to perform a hash-cash [13, 14] operation. Thus, the verifier has to "pay" for the verification with CPU cycles. The amount of hash-cash will be defined by the current load experienced by the replica holder. The result of the calculation is a ticket of limited lifetime that grants access to the actual verification. Should the replica holder repeatedly pose impossibly high hash-cash challenges, the verifier can assume the replica holder does not comply with the protocol.

When replica holder and verifier are in symmetric positions, i.e., both are interested in verifying each other's content, then a second ticket-granting mechanism becomes available: A successfully executed verification of one party will grant this party the right to request a slightly larger verification from the other side by issuing an appropriate ticket. Here, both sides actually perform useful work, eliminating the waste of CPU cycles performed by hash-cash.

A man-in-the-middle attacker can use the proposed mechanism for DoS by falsifying or suppressing the messages exchanged (see also Section 2.2). Even though this attack is typically not controlled by the replica holder, the replica holder becomes an unreliable storage provider. The use of overlay networks may help circumvent such packet dropping or modification attacks, but this is beyond the scope of this paper.

4 Related Work

Trust has been a research topic for decades [15], ranging from agreements even in the presence of untrusted entities [16] to the total trust in a peer in a web-of-trust [17] setting. In practice, however, trust is often handled through centralized hierarchies: Everyone ultimately trusts a single entity, which in turn delegates some of its trust to other principals, who may or may not have the right to delegate this further.

As all of these systems have weaknesses, people have started working on other, more immediate ways to deal with this issue, namely, reputation systems [18]. Advogato [19] uses a hybrid system in which users can rank their peers; the overall reputation of a ranked individual then depends on the result of a network flow calculation. Mobile ad-hoc networks are a prime area of reputation research to determine whether intermediate nodes actually do forward the packets or prefer to behave egotistically and instead conserve their own power by not helping the others [20, 21]. In this domain, it is relatively simple to see the result, either through reciprocal reception of the radio signal, through the help of other nodes, or by seeing communications progress and getting the desired answer from the communication peer. Systems such as CONFIDANT [22] use reputation gossip to augment their first-hand experience.

5 Conclusions

In this paper we have presented a first algorithmic approach at fairly verifying whether replica holders indeed perform the service they promised. Our protocol is based on a checksum or hash that is calculated over key-defined ranges of shared data. This check is performed in an iterative fashion with alternating roles, or compensated by the calculation of responses to challenges to prevent DoS attacks. At the same time this builds a trust relationship between replica holder and verifier which can be reused in later rounds of the protocol.

To the best of our knowledge, this is the first paper raising the issue of verification of storage in order to build trust in the storage provider. Given the increased interest in (potentially massively) distributed storage, the need for a lightweight mechanism is well covered in the protocol developed herein. We believe that it will give first answers to some of the issues that have arisen in the peer-to-peer and distributed storage communities, but also raise new questions and challenges. Open issues include tightening many of the loose ends and gathering experience in a real environment.

References

[1] Eytan Adar and Bernardo A. Huberman. Free riding on Gnutella. *First Monday*, September 2000.

[2] Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. Freenet: A distributed anonymous information storage and retrieval system. http://freenetproject.org/, 1999.

[3] Ross J. Anderson. The Eternity service. In *Proceedings of Pragocrypt '96*, 1996.

[4] Marc Waldman, Aviel D. Rubin, and Lorrie Faith Cranor. Publius: A robust, tamper-evident, censorship-resistant, web publishing system. In *Proc. 9th USENIX Security Symposium*, pages 59–72, August 2000.

[5] Sylvia Ratnasamy, Paul Francis, Mark Handley, Richard Karp, and Scott Shenker. A scalable content-addressable network. In *Proceedings of ACM SIGCOMM*, September 2001.

[6] Anthony Rowstron and Peter Druschel. Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems. In *IFIP/ACM International Conference on Distributed Systems Platforms (Middleware)*, pages 329–350, Heidelberg, Germany, November 2001.

[7] Ben Y. Zhao, John Kubiatowicz, and Anthony Joseph. Tapestry: An infrastructure for fault-tolerant wide-area location and routing. Technical Report UCB/CSD-01-1141, University of California, Berkeley, April 2001.

[8] Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, and Hari Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In *Proceedings of ACM SIGCOMM 2001*, pages 149–160, San Diego, CA, USA, August 2001.

[9] Marcel Waldvogel and Roberto Rinaldi. Efficient topology-aware overlay network. In *Proceedings of ACM HotNets-I*, October 2002.

[10] Sun cluster grid architecture. `http://www.sun.com/software/grid/whitepapers.html`, 2002.

[11] Gene Tsudik. Message authentication with one-way hash functions. *ACM Computer Communication Review*, 22(5):29–38, 1992.

[12] Peter Deutsch and Jean-Loup Gailly. ZLIB compressed data format specification version 3.3. RFC 1950, Internet Engineering Task Force, May 1996.

[13] Adam Back. Hashcash—A Denial of Service Counter-Measure. `http://www.cypherspace.org/∼adam/hashcash/`, 1997.

[14] Manuel Blum, William S. Evans, Peter Gemmell, Sampath Kannan, and Moni Naor. Checking the correctness of memories. In *IEEE Symposium on Foundations of Computer Science*, pages 90–99, 1991.

[15] Matt Blaze, Joan Feigenbaum, John Ionnidis, and Angelos D. Keromytis. The role of trust management in distributed systems security. In *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, pages 185–210. Springer Verlag, 1999.

[16] L. Lamport, R. Shostak, and M. Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, July 1982.

[17] Ueli Maurer. Modelling a public-key infrastructure. In *ESORICS: European Symposium on Research in Computer Security*. LNCS, Springer-Verlag, 1996.

[18] Paul Resnick, Richard Zeckhauser, Eric Friedman, and Ko Kuwabara. Reputation systems. *Communications of the ACM*, 43(12):45–48, 2000.

[19] Advogato's trust metric. `http://www.advogato.org/trust-metric.html`, February 2000.

[20] Pietro Michiardi and Refik Molva. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Sixth IFIP Conference on Security Communications, and Multimedia (CMS 2002)*, Portoroz, Slovenia, 2002.

[21] Krishna Paul and Dirk Westhoff. Context aware inferencing to rate a selfish node in dsr based ad-hoc networks. In *Proceedings of the IEEE Globecom Conference*, Taipeh, Taiwan, November 2002. IEEE.

[22] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes—Fairness In Dynamic Ad-hoc NeTworks. In *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, Lausanne, June 2002.