UPoA: A Scalable Untrusted Privacy-Preserving Transparency Overlay with Applications to Auditable Software Distribution

November 6, 2016

Abstract

Transparency overlays such as Certificate Transparency (CT) and Bitcoin seek to bring auditability to security-critical applications that rely on sets of authoritative messages. However such overlays tend to either have poor scalability (Bitcoin) or require trust in a set of distributed actors (CT), and trust-reducing CT protocols such as gossiping suffer from privacy and complexity issues.

In this work, we present a general-purpose transparency overlay that builds on the untrusted nature of blockchains—or distributed ledgers—such as Bitcoin. By using blockchain transactions with relaxed validation constraints, we achieve high scalability for an untrusted privacy-preserving transparency overlay that detects but not prevents misbehaviour. Our overlay makes use of a blockchain for log commitments and Untrusted Proof of Auditability (UPoA), with monitors for detecting misbehaviour. We implement this for the application of auditable software distribution and we test it at scale on the Debian software repositories.

1 Introduction

Critical Internet services are often provided by trusted third parties that have the ability to misbehave without being immediately detected—such as TLS certificate authorities that have issued unauthorised certificates for major websites.[1][2]

Consequently, a number of projects have emerged to bring transparency to Internet services. One of these projects is Certificate Transparency (CT), a framework for monitoring and auditing TLS certificates to make it possible to detect unauthorised certificates issued by certificate authorities.[3]

CT however still requires trust in a third party actor. The log servers that auditors communicate with to check that certificates have been logged are trusted, because they may misbehave by presenting a "split view" of their operations (i.e. log servers may say that they have seen a certificate to one auditor but not to other auditors).[4]

CT "gossiping" protocols have therefore been drafted to help detect misbehaviour of log servers.[4][5] This reduces but not eliminates the trust required in log servers, partly because gossip is not guaranteed to reach the wider Internet if a long-term man-in-the-middle attack takes place. This makes gossiping unsuitable for threat models where a device is connected to the same network for a long period of time and an adversary sits on the device's network (e.g. ISP). Additionally, CT gossiping suffers from a number of privacy problems and fingerprinting attacks.[4]

Bitcoin is decentralised peer-to-peer electronic cash system that takes a different approach to transparency. Instead of merely employing transparency to detect misbehaviour or placing trust in any actors, Bitcoin makes misbehaviour economically expensive by using an auditable untrusted consensus protocol based on proof-of-work—the blockchain. This prevents users from double spending their coins without access to 51% of the processing power that generates proof-of-work in the network.[6]

All full nodes (nodes that have the ability to bootstrap other nodes) in the peer-to-peer network that maintains the blockchain must store a copy of all the transactional data in the blockchain. This means adding new data to the blockchain is an expensive operation, making scalability while keeping the network decentralised a difficult problem.

Systems such as Certificate Transparency and the blockchain can be generalised as transparency overlays because they can adapted to provide transparency for any number of different applications.[7] For example, it is possible to define an electronic cash system based on a CT-like overlay where users trust a set of distributed actors[7] and centrally banked cryptocurrencies have been proposed using similar distributed schemes.[8]

The tradeoff between different the approaches has been that a decentralised overlay is poorly scalable and expensive, but a distributed overlay is trusted.

Mustafa: Add note explaining why this is particularly unsuitable for transparent software distribution and introduce the problem space.

Mustafa: Add a citation about fees associated with storage size of transactions in systems like Ethereum.

1.1 Our Contributions

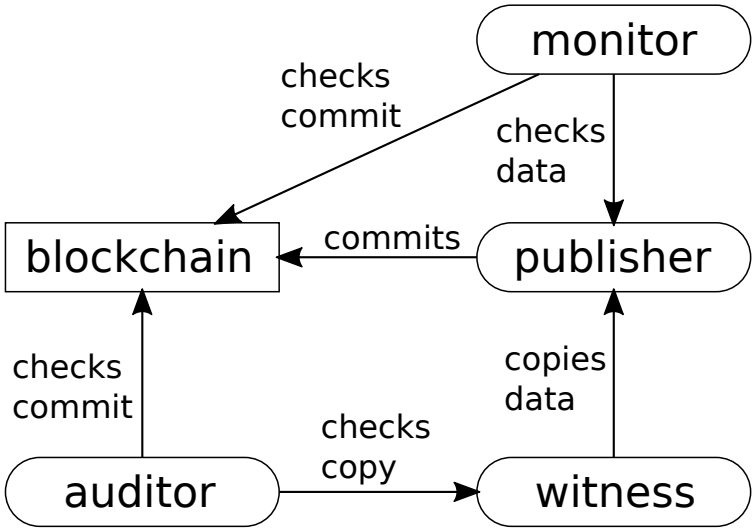
We contribute a unique, third type of transparency overlay where misbehaviour is detected (but not prevented) in an untrusted manner, by drawing on concepts from both types of decentralised and distributed approaches.

Mustafa: Incomplete.

1.2 Related Work

2 Background

3 Protocol



References

[1] D. Goodin, "Google warns of unauthorized tls certificates trusted by almost all oses," 2015.

[2] J. Leyden, "Inside 'operation black tulip': Diginotar hack analysed," 2011.

[3] B. Laurie, A. Langley, and E. Kasper, "Rfc6962 - certificate transparency," 2013.

[4] L. Nordberg, D. Gillmor, and T. Ritter, "Gossiping in ct," 2016.

[5] L. Chuat, P. Szalachowski, A. Perrig, B. Laurie, and E. Messeri, "Efficient gossip protocols for verifying the consistency of certificate logs," *2015 IEEE Conference on Communications and Network Security (CNS)*, 2015.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[7] M. Chase and S. Meiklejohn, "Transparency overlays and applications," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[8] G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," *Network and Distributed System Security Symposium 2016*, 2016.