From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain

Duane Wilson[1(✉)] and Giuseppe Ateniese[2]

[1] Department of Computer Science, Johns Hopkins University, Baltimore, USA
mr.duanewilson@gmail.com
[2] Department of Computer Science, Sapienza University of Rome, Rome, Italy

Abstract. PGP is built upon a Distributed Web of Trust in which a user's trustworthiness is established by others who can vouch through a digital signature for that user's identity. Preventing its wholesale adoption are a number of inherent weaknesses to include (but not limited to) the following: **1)** Trust Relationships are built on a subjective honor system, **2)** Only first degree relationships can be fully trusted, **3)** Levels of trust are difficult to quantify with actual values, and **4)** Issues with the Web of Trust itself (Certification and Endorsement). Although the security that PGP provides is proven to be reliable, it has largely failed to garner large scale adoption. In this paper, we propose several novel contributions to address the aforementioned issues with PGP and associated Web of Trust. To address the subjectivity of the Web of Trust, we provide a new certificate format based on Bitcoin which allows a user to verify a PGP certificate using Bitcoin identity-verification transactions - forming first degree trust relationships that are tied to actual values (i.e., number of Bitcoins transferred during transaction). Secondly, we present the design of a novel Distributed PGP key server that leverages the Bitcoin transaction blockchain to store and retrieve our certificates.

1 Introduction

In a recent article, Yahoo announced its intentions to add an extension that will provide its customers with the ability to digitally sign and encrypt messages using Pretty Good Privacy (PGP). Yahoo plans to use a fork of Google's End to End OpenPGP plugin that is currently in development. Yahoo follows the likes of Google, Facebook and Microsoft, who also recently announced they would encrypt internal traffic in response to the Snowden spying revelations [1]. Traditional methods of securely sharing between two or more parties rely on the use of Public-Key Encryption within a Public Key Infrastructure (PKI). In a traditional PKI scheme, a certificate authority or certification authority (CA) is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a Trusted Third Party (TTP) that is trusted by both the

M. Qiu et al. (Eds.): NSS 2015, LNCS 9408, pp. 368–375, 2015.
DOI: 10.1007/978-3-319-25645-0_25

subject (owner) of the certificate and the party relying upon the certificate. CAs are characteristic of many PKI schemes [2]. Currently, the most viable alternative for Public Key Crytography based on a CA is PGP. PGP is built upon a Distributed Web of Trust in which a user's trustworthiness is established by others who can vouch for that user's identity. Preventing its wholesale adoption are a number of inherent weaknesses to include (but not limited to) the following: **1)** Trust Relationships are built on a subjective honor system, **2)** Only first degree relationships can be fully trusted, **3)** Levels of trust are difficult to quantify with actual values, and **4)** Issues with the Web of Trust itself: **Certification.** It is currently difficult to get certified if the key is new. In general people complain that it is hard to find endorsers to enhance the trustworthiness of a new key - which will limit its use. **Endorsement.** Competence and willingness of endorsers. There is currently no incentive to endorse a key of someone you know - much less someone you indirectly know through a friend or relative.

Bitcoin is a form of digital currency, created and held electronically [3]. According to "Crypto Coin News", the number of active Bitcoin users worldwide will reach 4.7 million by the end of 2019, marking a significant gain over the 1.3 million last year, according to a report from Juniper Research [4]. As a result of its popularity, we introduce a new Bitcoin-Based PGP certificate format, certificate validation methodology, and certificate endorsement model that overcomes the issues we have highlighted above. Issues 1 and 2 with the Web of Trust can be easily solved using our new Bitcoin-Based PGP certificate format and verification system. Issue 4 can be resolved by use of endorsement fee. The amount of the fee can be determined by the user and will vary based on the current value of a Bitcoin - which has been relatively stable of late [5]. In Issue 2, the bitcoin payment ensures that the endorser follows the "authentication" procedure otherwise they risk losing bitcoins - which demonstrates both their competence and willingness to serve as a viable certificate endorser.

There are some interesting properties of our trust establishment protocol that could result in safer use of PGP. Property 1) People have the option of using previous transactions before using a certificate OR directly establishing a trust relationship themselves with a certificate owner (i.e., direct trust). Property 2) As mentioned above, because of the risk of losing bitcoins via the identity-verification process, people will be less likely to leverage our certificates without a direct trust establishment. Property 3) The block chain and associated identity-verification transactions provide transparency into the trustworthiness of others. In addition to these benefits, we also provide the design of a novel PGP Key Server based on the blockchain's ability to store pieces of data since the 0.9.0 release. The 0.9.0 release of Bitcoin Core added a new standard transaction type granting access to a previously disallowed script function, *OP-RETURN* [6]. This function accepts a user-defined sequence of up to 80 bytes. Once realized, this new key server will be completely de-centralized and serve as an appropriate repository for Bitcoin-Based PGP Certificates. Our work specifically provides the following contributions:

- **Bitcoin-Based PGP Certificate:** Contains Bitcoin address for identity verification and certificate revocation.
- **Identity-Verification and Revocation Transactions:** Serves as alternative means of verifying a certificate owner's Public Key contained in a Bitcoin-Based PGP Certificate. Also provides a mechanism for certificate revocation.
- **PGP Trust Levels:** Allows users to specify the amount of Bitcoins they are willing to "risk" in order to verify a particular Bitcoin-Based PGP certificate.
- **Bitcoin-Based PGP Key Server Design:** Demonstrates method of using the Bitcoin Transaction Blockchain for PGP Key Storage and Retrieval

The rest of this paper is organized as follows: Section 2 discusses the work related to this area of research, Section 3 provides an overview of our Bitcoin-Based PGP certificate, Section 4 presents an overview of PGP threats addressed by our contributions, Section 5 discusses the design of our application and new key server, and Section 6 concludes the paper and identifies areas for future work.

2 Related Work

According to [7], BitPay has launched a project that leverages bitcoin technology to facilitate a decentralized authentication system. Called BitAuth, the system uses cryptographic signatures in place of server-side password storage. BitAuth is a way to do secure, password-less authentication using the same elliptic-curve cryptography as Bitcoin. Instead of using a shared secret, the client signs each request using a private key and the server checks to make sure the signature is valid and matches the public key. A nonce is used to prevent replay attacks and provide sequence enforcement [8]. Similar to our novel Bitcoin-Based PGP certificate, BitAuth provides "portable" identity in that the same identity can be used with multiple services. BitAuth is a promising new method of authentication, but currently relies heavily on the System Identification Number (SIN). The SIN is a new concept that is similar to a Bitcoin address, however, is not widely adopted. Whereas, our scheme relies on popular Bitcoin primitives - address, transactions, and the block chain - that are widely being used. Additionally, since the focus of BitAuth is on authentication, it cannot be used to protect the confidentiality of information shared between two parties - as is the primary benefit of our Bitcoin-Based PGP Certificate.

Off-the-Record (OTR) Messaging is a protocol designed for private social communications. According to [9,10], the notion of an off-the-record conversation captures the semantics one intuitively wants from private communication - only the two parties involved are privy to the contents of the conversation; after the conversation is over, no one (not even the parties involved) can produce a transcript; and although the participants are assured of each other's identities, neither they nor anyone else can prove this information to a third party. Current versions of the OTR protocol, support mutual authentication of users using a

shared secret through the socialist minimalist protocol. This feature makes it possible for users to verify the identity of the remote party and avoid a man-in-the-middle attack without the inconvenience of manually comparing public key fingerprints through an outside channel. OTR's primary weakness lies in the fact that it is primarily applicable in the domain of instant messaging - whereas our Bitcoin-Based PGP certificate can be used in virtually any domain in which secure information sharing is desired. According to the authors of the OTR protocol, "The high latency of email communication makes using our "off-the-record" protocol impractical in the setting of email."

In [11], a secure replacement for CAs is proposed. Rather than employing a traditionally hard-coded list of immutable CAs, Convergence allows one to configure a dynamic set of Notaries which use network perspective to validate user communications. It provides the following guarantees: Trust Agility, Robustness, Backwards Compatibility, Extensibility and Anonymity. This all occurs within a distributed environment in which anyone can serve as a trust notary. Convergence originated from the ideas originally developed by the Perspectives Project at Carnegie Mellon University [12]. Convergence has great promise in the domain of web browser security and other areas where SSL is prominent. However, it suffers from the fact that the number of notaries currently in existence for performing CA functions is limited (due to it being a fairly new effort). As a result, this could lead to potential Denial of Service (DoS) attacks in the event the notaries become overwhelmed with requests. The Bitcoin infrastructure - upon which our certificate primarily relies - has successfully processed nearly 40 million transactions (to date) [13]. This makes it robust against volume-based security attacks such as DoS and DDoS - when applicable.

3 Bitcoin-Based PGP Certificates

Our Bitcoin-Based PGP certificate contains all the relevant elements found in a traditional PGP Certificate but also includes a Bitcoin Address for Identity-Verification and one used for Certificate Revocation. A Bitcoin address is an identifier of 27-34 alphanumeric characters, beginning with the number 1 or 3, that represents a possible destination for a Bitcoin payment. A Bitcoin transaction is a signed section of data that is broadcast to the network and collected into blocks. It typically references previous transaction(s) and dedicates a certain number of bitcoins from it to one or more new public key(s) (Bitcoin address) [14]. Because transactions must be verified by miners, Bitcoin users are sometimes forced to wait until they have finished mining. The bitcoin protocol is set so that each block takes roughly 10 minutes to mine. In the case of a purchase, some merchants may make users wait until this block has been confirmed, which will delay the receipt of the digital goods that have been paid for - whereas in other cases (e.g., low value transactions), a merchant will give access to the goods prior to the transaction being verified by the miners [15]. In our case, the delay does not pose a major problem since it will only take place when a trust relationship is being established for the first time - not upon certificate generation.

The value of using Bitcoin in the context of a PGP certificate centers around the fact that because it is built upon a peer-to-peer network, it is able to perform its functions (e.g., money transfers, double-spending prevention) without the aid of a CA - similar to the traditional web of trust. This is advantageous in any context where end-to-end data confidentiality is needed or desired (e.g., email, text message, cloud sharing, or social network communications). Users are more likely to trust an infrastructure that is independent of any CAs, but can still offer the same cryptographic guarantees (i.e., confidentiality and integrity) as an environment that is under their full control or purview.

4 PGP Threats and Security Goals

In this section, we expound on the threats we identified in the introduction and describe our security goals. We make the primary assumptions that PGP users are leveraging all of the features of PGP to include the Web of Trust, Levels of Trust, and Validity. Although there are a number of well documented issues with PGP, we primarily focus on threats relating to certificate validation, endorsement, and trust relationship establishment. With our new endorsement process offered via Bitcoin, the threat of assigning invalid levels of trust or validity would be mitigated by the following constructs of our scheme: 1) Certificate Signing MUST precede the incentive fee. A fixed fee of 0.001 BTC is sent to the Bitcoin address provided by the certificate endorser (fee is paid from the certificate owner's bitcoin address - as available - and can change based on the owner's discretion). This fee serves as a small incentive to willing and competent endorsers, 2) Endorsement process is not automated. Our prototype forces users to go through a step by step process in order to sign a certificate stored on our server, and 3) Levels of Trust are established by the certificate endorser, not certificate owner. In our scheme, when performing an identity-verification transaction, any amount of Bitcoins can be sent for verification purposes. These Bitcoins are 'at risk' until the certificate owner returns them. As a result, this serves as a very clear indication of trust between certificate endorser and owner.

A few additional threats to consider with leveraging Bitcoin as an alternative method of certificate verification are those related to rogue certificate owners, wealthy endorsers, and untrustworthy endorsers. In the first case, a certificate owner can generate a PGP key and use it for collecting payments and never return incoming identity-verification transactions to endorsers. To further complicate this scenario, a wealthy endorser risks very little by endorsing such users. To address these threats, we still rely on the PGP trust model that allows for out-of-band methods of certificate verification and a web of trust. The inference is that users will not initiate an identity-verification transaction with someone they do not already know and trust from prior interactions. Additionally, in the case of the wealthy endorser, only one verification transaction is considered valid for a particular certificate. Thus, their credibility (over time) will come into question as they continue to endorse untrustworthy certificates. Lastly, we consider the scenario where endorsers are suspected of being malicious by endorsing 'just

for the sake of endorsing'. Since our endorsement scheme does not invalidate - but augments - the endorsement process provided by PGP, over time a malicious endorser would be classified as someone who cannot be trusted - especially if they are endorsing both questionable and legitimate certificates. A legitimate case to consider is someone who is a professional certificate endorser. Someone whose professional responsibility is to endorse new certificates has their job (and reputation) to consider if they are found to be endorsing certificates that are not legitimate - over time.

5 Prototype Design

The primary motivations for creating a new certificate server are to 1) Accommodate our new Bitcoin-Based PGP certificates, 2) Enable Identity-Verification and Revocation transactions, and 3) Enable Certificate Signing Endorsements. To facilitate these "features", our certificate server will provide the following functions: Generate, Revoke, Verify, and Sign. Each Bitcoin-Based PGP certificate will contain a set of required parameters prior to generation and items that will be automatically generated by the prototype application. One thing to note is that we do not modify the original PGP certificate format - but leverage the PGP comment field to store Bitcoin addresses. In PGP, users can revoke their certificate if they feel like the certificate has been compromised. PGP also allows a user to designate a certificate revoker. With PGP certificates, the user usually posts the revoked certificate on a certificate server. To enable an easier revocation process for our Bitcoin-Based PGP certificate, we perform a transaction between the 2 addresses within the certificate. With information from the blockchain, one can find out how much value belonged to each address at any point in Bitcoin history [17].

Key revocation is arguably the most important component of any certificate-based identification system. Our implementation deliberately forces the user to make a valid Bitcoin transaction to a legitimate Bitcoin address in his possession. Alternatively, the revocation status could be stored in *OP-RETURN* fields if our decentralized approach is adopted. Our current method, however, has an important technical advantage: It makes verification of a certificate status extremely efficient since revocation transactions will be stored in the Bitcoin Unspent Transaction Outputs (UXTO) database and propagated among all nodes automatically. The UXTO are redeemable transactions and the information on certificate status will be kept in main memory for efficient verification. An identity-verification transaction is the primary mechanism by which a user can verify another user's Public Key in a Bitcoin-Based PGP certificate.

Blockchain PGP Key Server Historically, the use of bitcoins blockchain to store data unrelated to bitcoin payments has been a controversial subject. Many developers consider such use abusive and want to discourage it. Others view it as a demonstration of the powerful capabilities of blockchain technology and want to encourage such experimentation. Those who object to the inclusion of non-payment data argue that it causes "blockchain bloat", burdening those

running full bitcoin nodes with carrying the cost of disk storage for data that the blockchain was not intended to carry. Moreover, such transactions create UTXO that cannot be spent, using the destination bitcoin address as a free-form 20-byte field. Because the address is used for data, it does not correspond to a private key and the resulting UTXO can never be spent [18]. As a result, these transactions continue to increase the size of the blockchain over time. In version 0.9 of the Bitcoin Core client, a compromise was reached with the introduction of the *OP-RETURN* operator. *OP-RETURN* allows developers to add 40 bytes (now 80 bytes) of nonpayment data to a transaction output. However, unlike the use of "fake" UTXO, the *OP-RETURN* operator creates a (provably) unspendable output, which does not need to be stored in the UTXO set. *OP-RETURN* outputs are recorded on the blockchain, so they consume disk space and contribute to the increase in the blockchains size, but they are not stored in the UTXO set and therefore do not bloat the UTXO memory pool and burden full nodes with the cost of more expensive RAM [18].

STORAGE: Depending on the size of PGP key generated, the size could range from 1018 bytes (1024-Bit key) to 3100 bytes (4096-Bit key). PGP supports up to an 8192-Bit key which corresponds to an even larger on-disk or memory capacity for storage purposes. Keeping this in mind, along with the fact that the blockchain only accepts 'data' transactions of up to 80 bytes in size, our storage leverages an innovative certificate fragmentation mechanism to enable both logical storage and efficient retrieval. A message within our PGP Key Server will consist of a 5 Byte Header which will include the PGP Key ID (4 bytes), Fragment ID (4 bits), Total Fragments (4 bits), and the Message Data (75 bytes).
RETRIEVAL: The Retrieval of a PGP Key from the blockchain is similar to the defragmentation process of an IP datagram. At a high level, the user will request a certificate by either Bitcoin Address or KeyID. Once the transactions associated with the query string is returned, the number of total fragments are computed. If all transactions were retrieved successfully, application will reassemble the Key and return it to user.

6 Conclusions and Future Work

In this paper we presented a number of enhancements to PGP and associated Web of Trust - which has suffered from a litany of issues since its inception. Specific issues of certification, endorsement, and ambiguous levels of trust have prevented its wide scale adoption. Future work will consist of examining alternative methods of employing Bitcoin for identity-verification using actual Bitcoin Distributed Contracts or alternative methods that do not require modification of the original PGP certificate format. Keybase.io allows you to get a public key, safely, starting just with someone's social media username(s), but also provides other mechanisms of verifying a particular key (e.g., pgp fingerprint and bitcoin addresses) [19]. A potential area for future work would be to enable verifiers to leverage one or more of the online identifications provided by Keybase.io to

strengthen the trust of certificate stored on our server (via their API). Additionally, the integration of Bitcoin-Based PGP Certificates into infrastructures where secure sharing is offered (via text messaging, chat applications, and Secure Cloud Storage servers) would demonstrate their usefulness in actual environments. Lastly, a stronger form of certificate revocation should be explored that builds on the procedure we present. Full version of paper can be found at http://arxiv.org/.

References

1. Saarinen, J.: Yahoo to Provide PGP Encryption for Mail. ITnews for Australian Business. ITnews, August 08, 2014. Web August 26, 2014
2. Froomkin, A.M.: 1996 A.Michael Froomkin: The Essential Role Of Trusted Third Parties in Electronic Commerce. 1996 A.Michael Froomkin: The Essential Role of Trusted Third Parties in Electronic Commerce. N.p., October 14, 1994. Web February 18, 2014
3. Coindesk. What Is Bitcoin? CoinDesk RSS. Coindesk, March 20, 2015. Web August 13, 2015
4. Maras, E.: Bitcoin Users To Approach 5 Million Mark By 2019, Juniper Research Reports - CCN: Financial Bitcoin/Cryptocurrency News. CCN Financial Bitcoin Cryptocurrency News. CCN.LA, March 17, 2015. Web August 13, 2015
5. Torpey, K.: The Bitcoin Price Has Been Remarkably Stable Lately. The Bitcoin Price Has Been Remarkably Stable Lately. Inside Bitcoins, February 27, 2015. Web August 13, 2015
6. Apodaca, R.: OP-RETURN and the Future of Bitcoin. Bitzuma July 29, 2014. Web April 29, 2015
7. Cawrey, D.: BitPay Seeks to Decentralize Digital Identification with BitAuth. CoinDesk. CoinDesk, July 01, 2014. Web July 06, 2014
8. Bitpay. BitAuth, for Decentralized Authentication. Bitpay, July 01, 2014. Web July 06, 2014
9. Goldberg, I.: Off-the-Record Messaging. OTR Development Team (2012). Web February 25, 2014
10. Goldberg, I., Borisov, N., Brewer, E.: Off-the-Record Communication or, Why Not to use PGP. Zero-Knowlege Systems and U.C. Berkely, (2012). Print
11. Thoughtcrime Labs. Convergence Details. Convergence. Thoughtcrime Labs (2011). Web May 02, 2014
12. Wendlandt, D., Anderson, D.G., Perrig, A.: Perspectives: Improving SSH-style Host Authentication with Multi-Path Probing. Carnegie Mellon University (2011). Print
13. Bitcoin. Bitcoin Charts Various Bitcoin Charts and Currency Statistics. Bitcoin Charts. The Bitcoin Foundation (2009). Web. 02 May 2014
14. Bitcoin.org. Transacations. Bitcoin. Bitcoin.org (2014). Web May 06, 2014
15. CoinDesk. How Do Bitcoin Transactions Work? CoinDesk RSS March 06, 2014. Web July 02, 2014
16. Poor Decision-Making Can Lead to Cybersecurity Breaches Communications of the ACM. (n.d.) Web May 04, 2015. (Retrieved from http://cacm.acm.org/news/183571-poor-decision-making-can-lead-to-cybersecurity-breaches/fulltext)
17. Bitcoin. Block Chain. Bitcoin Wiki. Bitcoin, April 21, 2014. Web July 15, 2014
18. O'Reilly. Transactions. Mastering Bitcoin. O'Reilly (2013). Web May 01, 2015
19. Krohn, M.: Keybase. Keybase. Caroline Hadilaksono, n.d. Web February 10, 2015