Ansökan om examensarbete

Bastian Fredriksson bastianf@kth.se

December 22, 2016

1 Blockchains in distributed PKI

Identity on the internet today, is largely[1] administered by certificate authorities (CA), by means of X.509 certificates. The information contained in these certificates are signed by the CA, using a public-key cryptosystem (typically RSA). Certificates no longer in use, or otherwise compromised through leakage of the client's private key, must be revoked. Current revocation mechanism involves use of certificate revocation lists (CRL)[4] and validation of a certificate through a protocol called OSCP[8].

The highly centralized nature of the current PKI system has several disadvantages. First and foremost, a CA constitutes a single point of failure, which makes it an obvious target for attacks. One compromised CA will endanger the trust of the whole system, as shown by the DigiNotar accident in 2011[6]. Secondly, a CA is responsible for not only issuing certificates, but also act as OSCP responders and provide CRLs. This will most certainly put a lot of strain on the CAs, when more and more devices needs to be equipped with a digital identity. Thirdly, it is possible for an identity to be linked to several public keys, which complicates the revocation process and leads to poor identity retention.

A blockchain, which is a append-only, public ledger, shared among all nodes in a large P2P-network, originally designed to store transactions for the Bitcoin cryptocurrency[7], might solve some of these issues. A decentralized approach offers better protection against denial of service and enhanced trust compared to any centralized infrastructure. Users would also benefit from protection against domain seizures and protection against MITM-attacks since the public key would be pinned on the blockchain. Current research on this topic involves the design and implementation of Certcoin[3], which uses a blockchain to associate domain names with public keys, Namecoin[1] a replacement for DNS, and using blockchains for decentralized, anonymous credentials[5].

The purpose of my thesis would be to investigate how and if a blockchain can be used to improve the security, reliability and scalability of current PKI solutions, either by completely replacing the CAs with a decentralized trust structure, or through a hybrid approach where a CA can attest to someone's digital identity and transactions are performed on a blockchain.

[1] Another mechanism of trust which is commonly used, e.g by Linux packet managers, is Web of Trusts which is described in the OpenPGP standard[2].

References

[1] Namecoin website. https://namecoin.org/. Accessed: 2016-12-06.

[2] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and Thayer, R. Openpgp message format. RFC 4880, RFC Editor, November 2007. http://www.rfc-editor.org/rfc/rfc4880.txt.

[3] Conner Fromknecht, Dragos Velicanu, S. Y. A decentralized public key infrastructure with identity retention. Cryptology ePrint Archive, Report 2014/803, 2014. http://eprint.iacr.org/2014/803.

[4] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and Polk, W. Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. RFC 5280, RFC Editor, May 2008. http://www.rfc-editor.org/rfc/rfc5280.txt.

[5] Garman, C., Green, M., and Miers, I. Decentralized anonymous credentials. In *21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014* (2014).

[6] Leyden, J. Inside 'operation black tulip': Diginotar hack analysed. Newspaper article, The Register, 2011. http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/.

[7] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. White paper, May 2009. http://www.bitcoin.org/bitcoin.pdf.

[8] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C. X.509 internet public key infrastructure online certificate status protocol - ocsp. RFC 6960, RFC Editor, June 2013. http://www.rfc-editor.org/rfc/rfc6960.txt.

2 Uppgiftsbeskrivning

Preliminär titel Blockchains in distributed PKI

Bakgrund/förutsättningar Examensarbetet skall genomföras i samarbete med PrimeKey. För PrimeKey, som arbetar med PKI, är det viktigt att förstå hur nya teknologier såsom blockchains kan förändra marknaden och förbättra deras produkter.

Forskningsområde Kryptografi

Vetenskaplig frågeställning Hur kan blockchains användas för att förbättra säkerheten och tillförlitligheten hos nuvarande PKI-system?

Undersökningsmetod Jag ämnar studera existerande blockchain-baserade system som används för att hantera digitala identititer, med utgångspunkt från Certcoin och sedan jämföra hur denna teknik presterar i termer av säkerhet, skalbarhet och tillförlitlighet jämfört med nuvarande hierarkiska PKI-system. I de fall det hierarkiska PKI-systemet innebär fördelar, kommer jag försöka föreslå förbättringar hos det blockchain-baserade systemet eller ge förslag på hur man kan kombinera det hierarkiska systemet med en blockchain. Mitt arbete kommer inkludera en proof of concept-implementation som löser en eller flera problem som beskrivs i uppsatsen.

Preliminär hypotes PKI would benefit, in terms of security and reliability, from introducing a decentralized entity which maps keys to identities.

Utvärdering Arbetet skulle kunna utvärderas genom att titta på i vilken utsträckning uppsatsen ger tillfredsställande svar på följande frågor:

1. In which way are blockchains more suitable than a class PKI in terms of reliability and security?
2. How should keys on the blockchain be administered, in terms of security and usability?
3. How should revocation and updating of identities be handled on a blockchain?
4. Should CAs be involved in order to map a physical entity to a digital one? Is it possible to do this without reintroducing the problems we have with the current class PKI?
5. How can any scalability and possible latency issues with a blockchain-based approach be thwarted?
6. How should security issues related to the blockchain be addressed?

3 Om mig

Jag började på KTH år 2012 och har studerat kandidatprogrammet i datalogi. Efter kandidaten fortsatte jag på masterprogrammet i datalogi med spårkurser i IT-säkerhet. Relevanta kurser jag har läst listas nedan:

- Foundations of Cryptography (DD2448) med Douglas Wikström.
- Network Security (FIT5037) med Phu Le på Monash University.
- Advanced Networked Systems Security (EP2510) med Panagiotis Papadimitratos.
- Software Security (FIT5003) med Ron Steinfeld på Monash University.
- Advanced Topics in Security (FIT5124) med Ron Steinfeld på Monash University.

4 Om PrimeKey

PrimeKey supportar och utvecklar open-source mjukvara, t ex EJBCA Enterprise som används för att hantera digitala identiteter och SignServer Enterprise som används för att signera dokument. PrimeKey står också bakom ”kryptolådan” PrimeKey PKI Appliance som drivs med hjälp av EJBCA.

Handledare Min handledare kommer vara Tomas Gustavsson som är tekniskt ansvarig på PrimeKey. Mobil: `+46 (0)707421096` Email: `tomas@primekey.se`. Tomas involvering i projektet kommer vara att ge teknisk handledning och att se till att projektet går framåt. Det finns bred kompetens inom PKI hos PrimeKey, vilket innebär att jag kommer kunna få hjälp även om Tomas är bortrest.

5 Behörighet och studieplanering

Jag försäkrar på heder och samvete att jag har läst samtliga kurser som krävs för kandidatexamen samt mer än 60 hp kurser på avancerad nivå, varav en av dessa kurser är Vetenskapsteori och vetenskaplig metodik för dataloger (DA2210). Jag kommer under vårterminen 2017 läsa kursen Tyska B2 för ingenjörer (LS2426). Efter att denna kurs, tillsammans med mitt examensarbete är slutfört, kommer jag kunna ta ut min kandidat- magister och civilingenjörsexamen.

Förslag på examinator Mitt förslag på examinator är Prof. Johan Håstad.

6 Versionshistorik

0.1 Första utkast
0.2 Rättade stavfel

Stockholm, den 16:e december 2016
Bastian Fredriksson