On the security of the Blockchain BIX Protocol and Certificates

Federico Pintore[1]

joint work with **R. Longo, G. Rinaldo, M. Sala**

Perugia, 1^{st} February 2018

[1]University of Trento

Reference

Longo, R.; Pintore, F.; Rinaldo, G.; Sala, M.

"On the Security of the Blockchain BIX Protocol and Certificates"

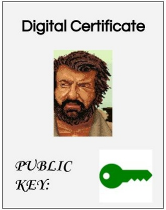
in *2017 IEEE International Conference on Cyber Conflict: Defending the Core, Tallin, Estonia*.

Digital identities

In a PKI (Public Key Infrastructure), to every digital identity corresponds a pair of cryptographic keys:

- the PUBLIC KEY;
- the PRIVATE KEY.

Digital identities are bound with corresponding public keys through **digital certificates**, that are managed by Certification Authorities (CAs) in a **centralized system**.



Blockchain technology

In 2015 Prof. Sead Muftic (KTH) proposed a blockchain-based protocol that allows distribution and management of digital certificates without the need of CAs.

Muftic, Sead. "*Bix certificates: Cryptographic tokens for anonymous transactions based on certificates public ledger.*" Ledger 1 (2016): 19-37.

Blockchain technology

In 2015 Prof. Sead Muftic (KTH) proposed a blockchain-based protocol that allows distribution and management of digital certificates without the need of CAs.

Muftic, Sead. "*Bix certificates: Cryptographic tokens for anonymous transactions based on certificates public ledger.*" Ledger 1 (2016): 19-37.

New users **register** themselves to the system via an Instant Messaging (IM) system, obtaining a **unique identifier**, called *BIX Identifier*.

Users interact with the system via a **PC or smartphone application**.

Chains of certificates

Muftic's system is composed by **chains of BIX certificates**, named *BCL's* (Bix Certificates Ledger), where certificates are **cryptographically double-linked**.

Chains of certificates

Muftic's system is composed by **chains of BIX certificates**, named *BCL's* (Bix Certificates Ledger), where certificates are **cryptographically double-linked**.

After the registration, users can request the **issuing of a BIX certificate**, to be added to a preexisting *BCL* or to a new one.

BIX Certificates

HEADER (H_i)

- Sequence number
- Version
- Date

ISSUER (S_{i-1})

- BIX ID of S_{i-1}
- PublicKey (PK_{i-1})

Issuer Signature

SUBJECT (S_i)

- BIX ID of S_i
- PublicKey (PK_i)

Subject Signature

NEXT SUBJECT (S_{i+1})

- BIX ID of S_{i+1}
- PublicKey (PK_{i+1})

Next Subject Signature

BACKWARD CROSS-SIGNATURE

- Signature of ($H_i||H(S_{i-1})||H(S_i)$) by SK_{i-1}
- Signature of ($H_i||H(S_{i-1})||H(S_i)$) by SK_i

FORWARD CROSS-SIGNATURE

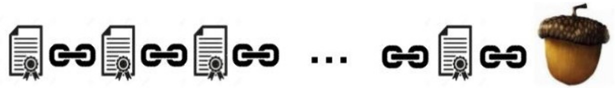
- Signature of ($H_i||H(S_i)||H(S_{i+1})$) by SK_i
- Signature of ($H_i||H(S_i)||H(S_{i+1})$) by SK_{i+1}

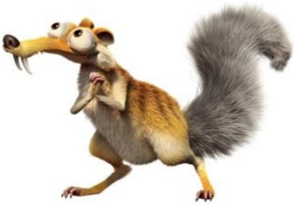
Certificate request

The user that owns the tail certificate (standard certificate in which some fields are not populated) will become the **issuer for the next certificate**.

Attack scenario - 1

An attacker tries to attach his certificate to a preexisting *BCL* without interacting properly with the last user of the *BCL*.





Formal proof of security of a protocol

Cryptographic schemes base their security upon the computational difficulty of solving some well-known mathematical problems.

Goal

Model the possible attacks on the protocol and prove that a successful breach implies the solution of a hard, well-known mathematical problem.

If the mathematical problem cannot be solved in reasonable time, a **contradiction is reached** and the protocol is secure.

Cryptographic primitives used in the protocol

A **collision resistant hash function** and a **secure** Digital Signature Scheme (ECDSA).

Collision resistance for R

A hash function H is collision resistance if, given $R \subset \{0,1\}^r$, there is no polynomial-time algorithm finding distinct $m_1, m_2 \in L$ such that $H(m_1) = H(m_2)$ with non-negligible probability.

Security of a Digital Signature Scheme

A Digital Signature Scheme DSS is said **secure** if an adversary A, given a public key PK - corresponding to a secret key SK - and some digital signatures $s_i = Sign(m_i, SK)$, is not able to identify a message $m \neq m_i \ \forall i$ and compute s such that $Ver(m, s, PK) = True$ in polynomial-time complexity with non-negligible probability.

Attack scenario - 1

Theorem (Longo, _ , Sala, Rinaldo - 2016)

Let A be an adversary that manages to succesfully perform the **first attack** *with probability ϵ, then a simulator S might be built that, with probability at least ϵ, either solves the Collision Problem for the hash function relatively to the set L of all possible Subject fields, or breaks the Digital Signature Scheme.*

Corollary (Longo, _ , Sala, Rinaldo - 2016)

If the Digital Signature Scheme used in Muftic's protocol is secure and the hash function is collision resistant for the set L, where L is the set of all possible Header fields, then the BIX protocol is secure against the first attack.