ITU Workshop on “Security Aspects of Blockchain” (Geneva, Switzerland, 21 March 2017)

Federation for the Masses (Impact of Blockchain and FIDO)

Abbie Barbir, Ph.D
Senior Security Advisor, Aetna
barbira@aetna.com

Geneva, Switzerland, 21 March 2017
FIDO modern authentication

- MUST eliminate symmetric shared secrets
- Address poor user experiences and friction
- **FIDO is a building block**
  - complements federation solutions

**Impact**
- Identity binding is essential
- Strong identity proofing a must

Source: FIDO
Federation

First Mile

- Standards are catching up on mile one
- Mile two is getting more mature
- Federation need improvement
- No prior relationship
  - SAML: Dynamic AuthN/Z
  - OAuth, OIC dynamic end point
  - Blockchain Opportunity

Second Mile

- How about identity assurance?
  - Poorly deploying strong authentication is the same as weak authentication
- FIDO solves the PW problem but mandates better identity binding at the relaying part
- Proper Identity vetting/proofing becomes essential
Identity proofing and account recovery

Account Login Current Pain Points
- I forgot my password
- I cannot find/lost my phone
- I am locked out of my account

Account Recovery Options
- KBA (static and/or dynamic)
- Email account (compromised)
  - Password reset link
  - Or a new password
  - Enrolling back in FIDO

Identity Proofing
- Binding a FIDO authenticator to a user account on relying party requires performing an Identity vetting step
  - Trust anchor (aka Bootstrapping problem)
- Currently pre-established Authenticators are used as anchors of Trust (such as passwords)

Online identity proofing is challenging and still relies on something “you know”
Blockchain technology

• Blockchain – distributed data store
• Public Key Cryptography (PKI)
• Peer to peer connected nodes

• Consensus mechanism (PoS, PoW, etc)
• Smart contracts

Permisionless
• Proof of work (PoW)
• Open node participation
• Weak(er) governance
  – Role of determined entities
• Performance
  – Mileage may vary

Permissioned
• Controlled participation
  – Authorized entities
• Improved Governance
• Entities are vetted
• Potentially faster consensus
Blockchain for identity verification

- Blockchain does not hold individual identity
- Trusted Nodes (act like a Federation)
- Individual identity data is stored off chain
  - Avoid storing private attributes on a public ledger (even when encrypted)
  - Stores references to data
- Originators retain control of their data
- Permission based system
  - Nodes on the network are known
  - Can be double permissioned based on mining protocols
  - Limited to a Consortium (affiliation model)

**For the client**
- No data about me without me
- No blanket permission (finer grained control)
- Will know who can attest for their data
  - What data is being shared and for what purpose
- Control for binding and unbinding an identity to a device
- Unconsent support

- Client acquire policy
- Client goes to Application Website to enrol
- Enrolment step requires Identity Verification equivalent of KYC
- Identity is asserted thorough Attestations on the blockchain
- More importantly with FIDO a binding between a device and identity can be asserted

- Avoid storing private attributes on a public ledger (even when encrypted)
- Stores references to data
- Originators retain control of their data
- Permission based system
  - Nodes on the network are known
  - Can be double permissioned based on mining protocols
  - Limited to a Consortium (affiliation model)

- For the client
  - No data about me without me
  - No blanket permission (finer grained control)
  - Will know who can attest for their data
  - What data is being shared and for what purpose
  - Control for binding and unbinding an identity to a device
  - Unconsent support
Going Forward

- Investigate a core consortium of trusted entities
- Share individual identity data attributes that all parties agree on exchange mechanisms, data structure, semantics and the context under which it is shared based on relationship and purpose
- Enable large scale trust and federation without the need of one to one relationship
- Global Federation capabilities
  - Dynamic SAML and OAuth
  - Improved Security and No need for prior negotiation
- Enable interoperable system of data exchange of healthcare records
Thank you

Questions