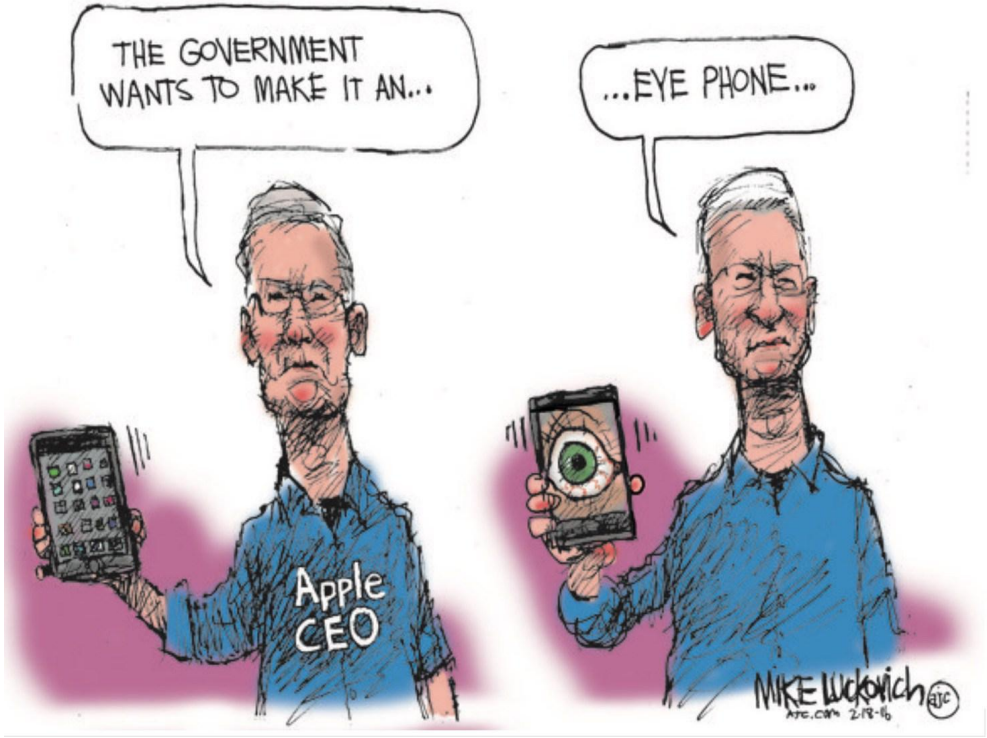
Exceptional Access Protocols

Alex Tong

Motivation

- “Crypto Wars”
- FBI vs. Apple
- What is the job of engineers?



“Requirements”

Government

- Decryption without notice to the user
- Ubiquitous international capability
- Decryption time of less than two hours
- Communications and Data at rest

Crypto Community

- Forward Security
- Well-defined technical requirements
- Low additional system complexity
- Decentralized targets

H. Abelson et al. “Keys Under Doormats” (2015)
H. Abelson et al. “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption” (1997)

Existing Compromise Solutions

- “Clipper Chip” NSA (1993-1996)
- Key Escrow
  - “Oblivious Key Escrow” M. Blaze et al. (1996)
  - “Partial Key Escrow” A. Shamir (1995)
- Recent Work
  - “Key Recovery: Inert and Public” C. Boyd et al. (2016)
  - “DEcryption Contract ENforcement Tool (DECENT)” P. Linder (2016)

Key Escrow

Oblivious Key Escrow

- Threshold cryptography amongst a large number of servers
- Oblivious to who holds the key share to a particular key, preventing coercion
- Angry mob cryptanalysis

Criticism

- Parameter Tuning
- Difficult / Impossible to implement

Partial Key Escrow

- Escrow of part of private key
- Requires computational power to obtain a targeted key
- Prevents mass surveillance

Criticism

- Parameter Tuning
- Cost of recovering a key is unknown, unpredictable, decreasing, and potentially private

Recent Attempts: High level overview

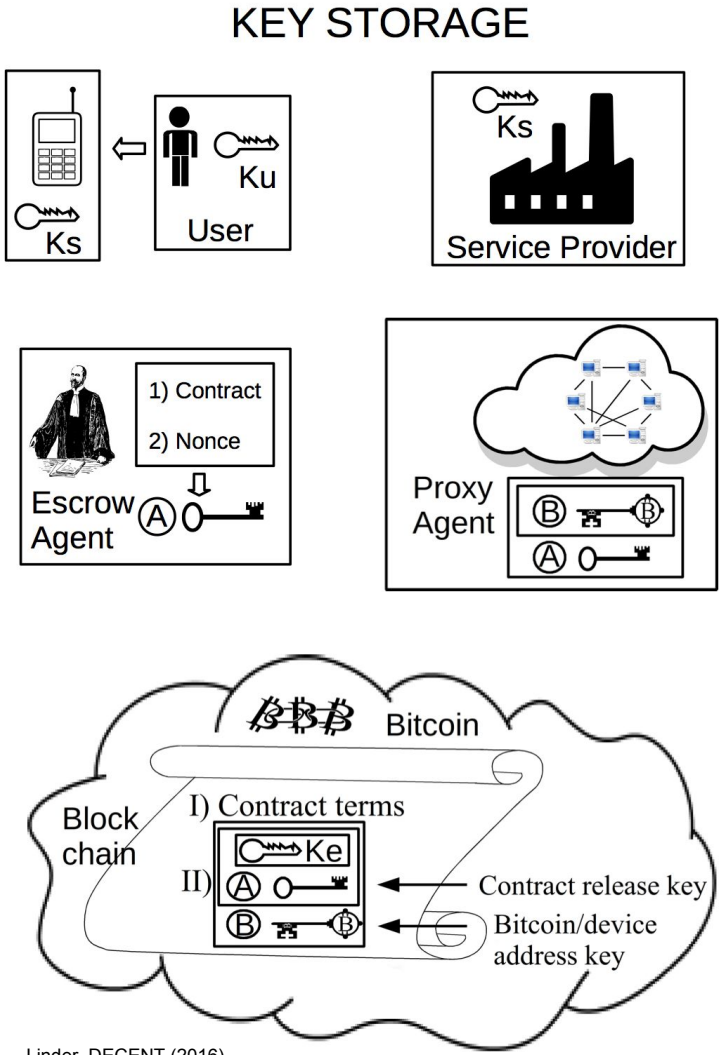
DECENT

- Developed by Assured Enterprises
- Uses 2 of 3 threshold cryptography between User, Corporation, Escrow Agent
- Uses Blockchain to maintain accountability

Key Recovery: Inert and Public

- Based on recent cryptocurrency development (Ethereum)
- Revival of oblivious and partial key escrow
- Uses unrealized public cryptography scheme adaptable to proof-of-work

DECENT



Linder. DECENT (2016)

DECENT

KEY USAGE

Data = Ku, User + Ks, Service + Ke, Escrow
Any 2 of 3 can decrypt

Normal cell phone operation:
Data = Ku, User known + Ks, Locked in device

Data recovery from cloud backup:
Data = Ku, User known + Ks, Special User request from Service Provider
Invalidate keys & issue new ones after decryption

Data recovery from forgotten user key:
Data = Ks Locked in device + Ke, Special User request from Escrow Agent
Invalidate keys & issue new ones after decryption

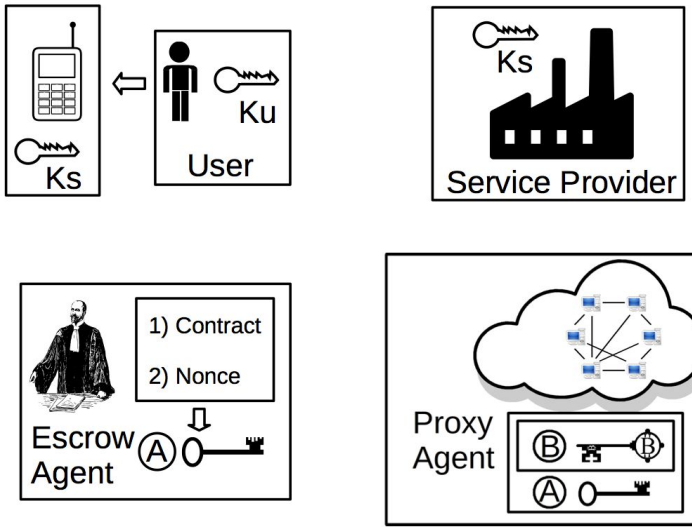
Data recovery for law enforcement:

From device if device is available:
Data = Ks Locked in device + Ke, Contract release by Escrow Agent

OR

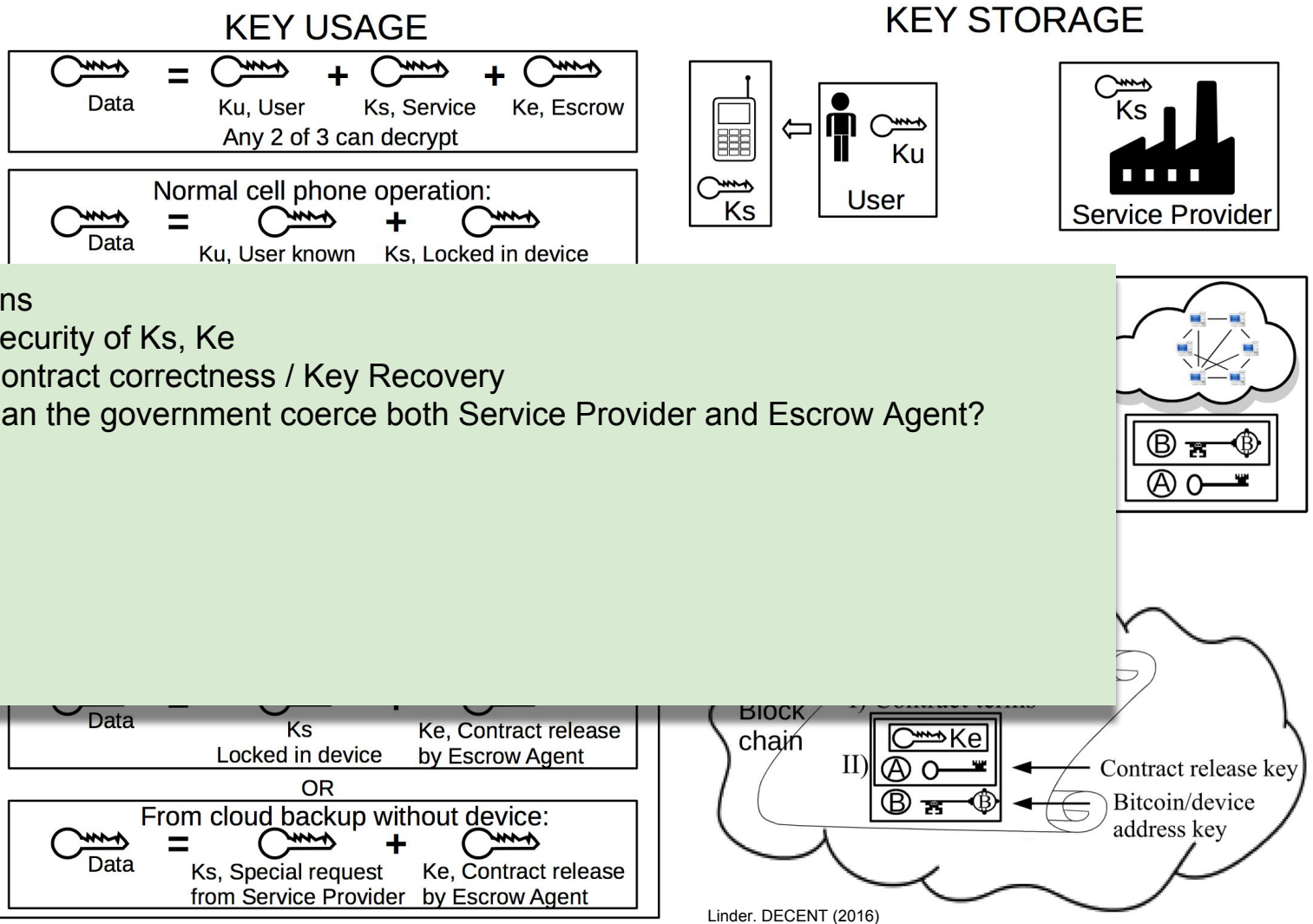
From cloud backup without device:
Data = Ks, Special request from Service Provider + Ke, Contract release by Escrow Agent

KEY STORAGE



Linder. DECENT (2016)

DECENT



Concerns

- Security of Ks, Ke
- Contract correctness / Key Recovery
- Can the government coerce both Service Provider and Escrow Agent?

Linder. DECENT (2016)

Boyd Key Recovery: Goals

Mimic physical world in the cryptographic world

- **Inert** - Recovery cost should increase with the number of keys
- Public - Attempted key recovery must be public
- Strong Keys - Long lived keys
- Resistance to Sybil Vulnerability

Boyd Key Recovery

(1) Decentralised Oblivious Key Escrow

- Implemented Using Smart Contracts
  - Whitebox Execution
- Share sharded key to random selection of participating nodes

(2) Partial Key Escrow

- Use new POW scheme with 4 criteria based on public key encryption
- Unclear of how to measure the security under key length

Boyd Key Recovery

(1) Decentralized Oblivious Key Escrow
(2) Partial Key Escrow
(3) Combination

Table 1. Comparison of main properties of the three proposals

	Partial escrow	Oblivious escrow	Prop. 1	Prop. 2	Prop. 3
Public	✗	✗	✓	✓	✓
Inert	✓	✓	✓	✓	✓
Future secure	✗	✓	✓	✗	✓
Sign up not required	✓	✗	✗	✓	✓[a]
Sybil resistant	✓	✗	✗	✓	✓
Traffic analysis resistant	✓	✗	✗	✓	✓

[a] There is a requirement for pre-registration for the oblivious part of the key escrow.

Boyd Key Recovery

(1) Decentralized Oblivious Key Escrow
(2) Partial Key Escrow
(3) Combination

Table 1. Comparison of main properties of the three proposals

					. 3
Pub					
Ine					
Fut					
Sig					
Sybil resistant	✓	✗	✗	✓	✓
Traffic analysis resistant	✓	✗	✗	✓	✓

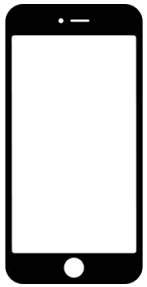
[a] There is a requirement for pre-registration for the oblivious part of the key escrow.

Concerns

- Relies heavily on theoretic public key construction
- Requires tuning many parameters correctly
- Insecure against a large enough botnet

Assumptions

- No magic bullet for Exceptional Access
- Distributed attacks are legally difficult to prosecute
- Only concerned with data at rest
- Physical access to device



https://d3nj7353mvgauu.cloudfront.net/media/categories/iphone-77-plus-40-b1ac.png http://courseminer.com/2017/09/30/bitcoin-mining-warehouse-

Main Idea

Extend physical premises analogy with locality

My Key Recovery: Goals

Mimic physical world in the cryptographic world

- **Inert** - Recovery cost should increase with the number of keys
- Public - Attempted key recovery must be public
- Strong Keys - Long lived keys
- Resistance to Sybil Vulnerability
- **Physically Centralized**

“Requirements”

Government

- **Decryption without notice to the user**
- Ubiquitous international capability
- Decryption time of less than two hours
- Communications and **Data at rest**

Crypto Community

- **Forward Security**
- **Well-defined technical requirements**
- Low additional system complexity
- Decentralized targets

H. Abelson et al. “Keys Under Doormats” (2015)
H. Abelson et al. “The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption” (1997)

Proposal - Recovery Mode

Phone

1. Recovery Mode enabled by key held by manufacturer
2. Phone displays challenge based on private key and current time for T time
    a. Bitcoin block mean propagation time ~12 seconds
3. If receives acceptable nonce where sha256(challenge, nonce) < difficulty

Recoverer

1. Attempts to find nonce where sha256(challenge, nonce) < difficulty

Legal framework

- Registration of sufficiently powerful data centers
- Government can request access to recovery mode key in exceptional circumstances

http://i0.kym-cdn.com/photos/images/original/001/293/153/4b8.png

Proposal - Advantages

- Forces centralization of potential illegal access
- Uses encryption scheme where there is monetary incentive to exploit vulnerabilities
- Inert - Preventing mass surveillance by other agencies
- Small number of adaptable parameters

Conclusions

- Purely technical solutions are insecure and insufficient
- Key recovery is not a single solution space
- Any solution can only guard against the default case

Questions

- Are these assumptions reasonable?
- Is it better to use a well known algorithm (sha256) or a more exotic one?