Technologies for making privacy violations transparent and accountable

Mark Ryan

Professor of Computer Security
Security and Privacy Research Group
University of Birmingham

Sensing and Privacy Workshop
Queen Mary, University of London
20 June 2017

Contents

Contents

Privacy is a human right

Reasons:

- **Privacy from governments** is needed, to prevent abuse of power, by current or future government agencies, or abuses by government officers or other insiders that legitimately or illegitimately access the data, or by hackers.
- **Privacy from corporations** is needed, to prevent abuses arising from trading in personal info, leading to unfair denial of insurance, jobs, loans, . . . , and to prevent abuses by insiders/hackers.
- **Privacy from individuals (family, friends, colleagues)** is needed. Humans have a need to keep secrets, in order to maintain purposeful relationships with others; and also to prevent blackmail or extortion.

There is a call to use personal data in order to catch terrorists and other criminals

- The Investigatory Powers Act 2016:
  - Allows targeted and bulk interception of communications, and bulk collection of communications data;
  - Permits targeted and bulk 'equipment interference', that is, hacking into computers or devices to access their data
- Apparently, legislation of this kind has foiled **???** terrorism attempts, and led to **???** convictions.
  NSA chief Keith Alexander: *"There's* **no other way** *to protect Americans than to collect billions of phone and internet records."*
- Hard to evaluate such claims, because of *asymmetry of the debate*.
- Insufficient transparency, about the quantity/nature of the privacy violations, and the outcomes.

Two futures, both undesirable

"Security trumps privacy"

Totalitarian surveillance

All aspects of our lives are monitored. There's CCTV in every bathroom.

"Big brother" controls all communication channels, and perhaps even your brain-computer interface.

BB knows everything you say, do, wish, or think.

No-one is free.

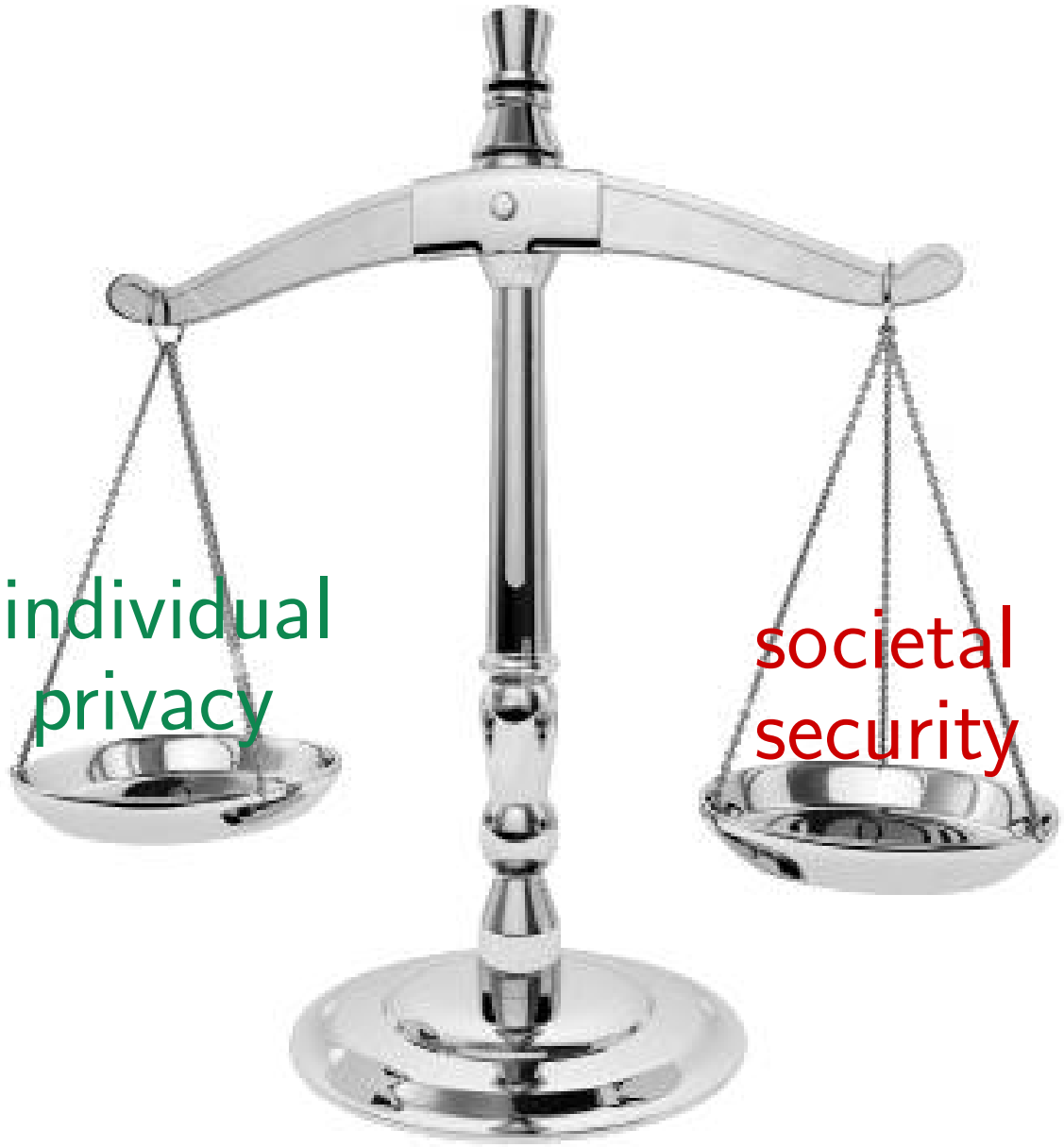
"Privacy trumps security"

Paranoid cyberpunk

Everything is private. All payments are made using anonymous cryptocurrencies.

No-one pays tax; there is no state. No-one can he held accountable. Crimes can effectively be committed without fear of repercussions.

Super-wealthy asset owners control everything, but are unaccountable and act with impunity. No-one can find out who owns what (land, buildings, vehicles, companies, . . .)


individual
privacy
societal
security

A legal perspective

The right to privacy is one right among many (rights to life, liberty, pursuit of happiness, free expression, due process of law, freedom of association, . . .).

Rights and security reinforce each other.

- You can't exercise your rights unless there is security in the world.
- Security exists in order to protect rights.
- Rights legitimise security.

Rights are the fundamental thing. The tension exists between your rights, and my rights (not between rights and security, as I previously thought).

Security is only the mechanism by which rights are protected.

Contents

Principles for privacy violations

1. **Necessity**
2. **Proportionality**
3. **Transparency**
4. **Accountability**

Principles for privacy violations

1. **Necessity**
2. **Proportionality**
3. **Transparency**

   When privacy rights are violated,
   - the violation is recorded and observable
   - the benefits (outcomes) arising from such violations are visible

   Transparency can't be forged. Correctness of the transparency records is verifiable by users.

   Transparency might not be fine-grained (in order to preserve the confidentiality of operations). For example, it might reveal the quantity of decryptions (rather than the individual ones).
4. **Accountability**

Principles for privacy violations

1. **Necessity**
2. **Proportionality**
3. **Transparency**

   When privacy rights are violated,
   - the violation is recorded and observable
   - the benefits (outcomes) arising from such violations are visible

   Transparency can't be forged. Correctness of the transparency records is verifiable by users.

   Transparency might not be fine-grained (in order to preserve the confidentiality of operations). For example, it might reveal the quantity of decryptions (rather than the individual ones).
4. **Accountability**

   When privacy rights are violated, the violaters have to explain their reasons.

Contents


Gmail


HSBC

Requirements

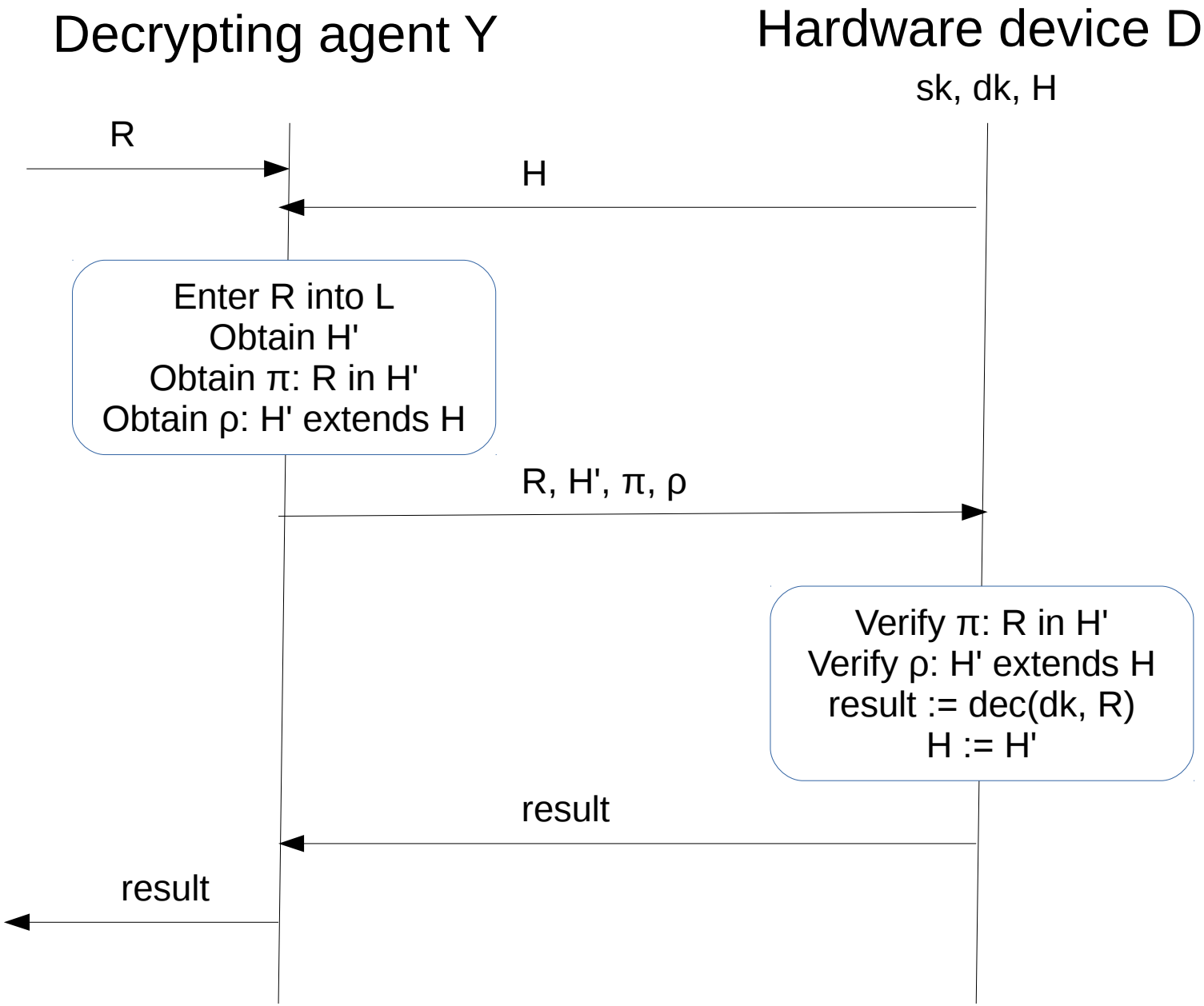
- Users create ciphertexts using a public key *pk.*
- Decrypting agent *Y* is capable of decrypting the ciphertexts *without any help from the users*.
- When *Y* decrypts ciphertexts, it unavoidably creates evidence *e* that is accessible to users. The evidence cannot be suppressed or discarded without detection.
- By examining *e*, users gain some information about the quantity and nature of the decryptions being performed.

This requires hardware

- If Y has a ciphertext and a decryption key, it is impossible to detect whether she applies the key to to ciphertext or not.
  - The decryption key has to be guarded by a hardware device D that controls its use.
- ***What is a minimal specification for D that will give us the desired properties?***
- Idea of this paper: propose a simple generic design that achieves the desired functionality.

The log L

- There is a log L in which all decryption requests are recorded.
  - D will perform a decryption only if the request is accompanied by a proof that it has been entered into L.
- The log L is organised as an append-only Merkle tree
- The maintainer periodically publishes the root tree hash (RTH) H of L
- The maintainer is capable of generating two kinds of proof about the log's behaviour:
  - A proof π that some data item d is in the tree with RTH H;
  - A proof ρ that the tree with RTH H' is an append-only extension of the tree with RTH H.


Decrypting agent Y
Hardware device D
sk, dk, H
R
H
Enter R into L
Obtain H'
Obtain π: R in H'
Obtain ρ: H' extends H
R, H', π, ρ
Verify π: R in H'
Verify ρ: H' extends H
result := dec(dk, R)
H := H'
result
result

Proposal: a device D with two protocols

D stores: H, dk, sk

- Input: R, H', π, ρ
- Compute:
  - Verify π: R in H'
  - Verify ρ: H' extends H
  - result := dec(dk, R)
  - H := H'
- Output: result

- Input: v
- Compute
  - Result := Sign(sk, (v,H))
- Output result

Contents

Background 1: public key cryptography (El Gamal)

Let G be a a cyclic group of order q, with generator g. These are public parameters.

Key generation. Alice chooses an x randomly from $\{1, \ldots, q-1\}$ as her private key.
Alice computes $X := g^x$ and publishes X as her public key.

Encryption. To encrypt data for Alice, anyone can convert the data into a group element d. Then, that person selects a random element r from $\{1, \ldots, q-1\}$, and outputs the encryption:

$$(g^r, d \cdot X^r)$$

Decryption. Given a ciphertext (C_1, C_2), Alice can decrypt it to obtain the plaintext

$$d = \frac{C_2}{C_1^x}$$

Background 2: Distributed decryption

In El Gamal, if *a set* of agents A_i $(i \in I)$ have private keys x_i and public keys $X_i = g^{x_i}$ respectively, then they can compute a joint public key $X = \prod_{i \in I} X_i$.

Data d encrypted under this public key

$$(g^r, d \cdot X^r)$$

can be decrypted only with the participation of each agent A_i $(i \in I)$:

$$d = \frac{C_2}{\prod_{i \in I} C_1^{x_i}}$$

Background 2: Distributed decryption continued

Using this standard cryptography, a decryption capability can be distributed across several agents, each of which must participate in the decryption.

One can combine this method of *distributing trust* with the method of *anchoring the trust in hardware*. For example, some of the "custodians" could be organisations, while others are purely automatic (but accountable) decryptors, anchored in several different "roots of trust".

Contents

Transparent and accountable message interception

Suppose we can make decryption transparent and accountable (as described).

To make message interception transparent and accountable, a message sender would need to encrypt message data, such that it can be decrypted:

- either by the intended recipient (who has a certain key);
- or by an escrow holder (who also has a key).

Decryptions by the escrow holder are made transparent.

Joint decryption capability

Alice's *escrow public key* ePK_A:

$$ePK_A := \left(g^s, g^{s(a+c)}, g^{sac}\right)$$

(c, g^c): custodian's private/public key pair.

Registration:

- Alice selects custodians $\{g^{c_i}\}_{i \in I}$ from a pre-defined list
- Alice computes $g^c = \Pi_{i \in I}\ g^{c_i}$
- Alice chooses her private key a

$$\text{Alice} \xrightarrow{(g^a,\ g^c,\ g^{ac})} CA \xrightarrow[\text{certify and publish}]{ePK_A := \left(g^s,\ g^{s(a+c)},\ g^{sac}\right)}$$

Joint decryption capability

Alice's *escrow public key* ePK_A:

$$ePK_A := \left(g^s, g^{s(a+c)}, g^{sac}\right)$$

(c, g^c): custodian's private/public key pair.

Accountably-Escrowed Encryption (AEE):

- Encryption

$$\left(C_1 := g^{sr},\ C_2 := g^{s(a+c)r},\ C_3 := m \cdot g^{sacr}\right)$$

- Decryption

$$m = \frac{C_3}{\left(\frac{C_2}{{C_1}^a}\right)^a} \text{ or } \frac{C_3}{\left(\frac{C_2}{{C_1}^c}\right)^c}$$

Properties of accountably-escrowed encryption

1. The encryption is IND-CPA secure (under 3-DDH assumption)
2. The encryptor cannot avoid the escrow.

Conclusions

1. Privacy is a fundamental right, but even fundamental rights are not absolute rights.

2. Research is needed into how technologies can support making privacy violations transparent and accountable. That means:
   - Making the violations observable (some approaches have been outlined in this talk)
   - Making the outcomes visible (e.g., by means of private set intersection).

3. I welcome feedback of all kinds!