Secret Sharing and Reliable Cloud Computing

Yvo Desmedt
University College London, UK

November, 2011

OVERVIEW

1. Clouds: examples of deployment
2. Clouds: a security nightmare?
3. Secret sharing: a brief introduction
4. Threshold adversary: sometimes unrealistic
5. Secure multiparty computation: a quick survey
6. Other applications of secret sharing
7. Why is a standard needed?
8. Secret sharing: the way forward

1. CLOUDS: EXAMPLES OF DEPLOYMENT

Examples are:

- Washington Post (April 17, 2011):

  > The [US] government is also getting ready to move about 75 agency-identified programs to cloud — or Web-based — computing to comply with the new “cloud-first” policy . . . .

  Note: “cloud-first” policy was announced in November 2010, see Washington Post (November 22, 2010)

- At several universities worldwide student e-mails are in reality stored at cloud mail servers. Motivation: savings by making employees redundant.

- The new generation saves pictures on . . . and text documents on . . . . However, for the moment, they keep music stored locally.

The customer’s impression is that there is no need to back up data.

IT industry has failed to make backup user-friendly!

2. Clouds: a security nightmare?

Recently a few newspapers/magazines have commented on the vulnerabilities of such cloud computing. For example,

- On February 2, IT Business (Canada) wrote:

  > The countrywide Internet blackout Egypt is experiencing may resonate with a lot of Canadian small and medium sized businesses especially as more and more companies adopt cloud-based applications services.

- On Sunday 6 February 2011, the Guardian wrote:

  > The speed with which Amazon and PayPal dropped WikiLeaks should be a wake-up call to anyone who thinks that Cloud Computing services can be trusted to protect the interests of their customers when the government cuts up rough.

- On August 21, 2011 (as corrected on August 23) the New York Times in their article on “Federal Push for ‘Cloud’ Technology Faces Skepticism” wrote:

  > Several disruptions of online cloud systems made headlines this spring, including in April, when technical problems with Amazons cloud service disrupted an undisclosed number of private sector Web sites. Amazon, which manages several federal Web sites, including the Treasurys main site, introduced a cloud service last week specifically for government clients.

- On October 21, 2011, Computing wrote:

  > The entire world, consumers and businesses, are moving most, if not all, their data, applications and services to the cloud . . . However, the recent outage that denied up to 70 million

> BlackBerry users access to their email for four days earlier this month highlights the perils of trusting any hosted IT service models that rely so heavily on a distributed network to function.

Besides above problem, we need to realize that

> there is no guarantee that companies involved in this storage will still exist in a few years. Indeed, DEC used to be the 2nd largest computer manufacturer in the world, but vanished after being bought by Compaq, which merged with HP.

What are the potential problems:

- Privacy: your data is in hands of an untrusted party,
- Availability: above examples illustrate the problems,
- Authenticity: your data could be modified by an untrusted party.

3. Secret sharing: a quick introduction

Secret sharing is a technology existing for more than 30 years (1979: Blakley, Shamir). Shamir 2nd most cited paper. Still not widely implemented, except in RAIDs.

Main concepts:

- Secret: the private document
- Parties: computers (or safety deposit box, or memory sticks, . . .) each storing a:
- Share (or shares), satisfying properties explained further on.

When $\mathcal{P}$ is the set of parties, an access structure $\Gamma_{\mathcal{P}}$ is a list of subsets of $\mathcal{P}$ such that each such subset is trusted.

In a monotone access structure $\Gamma_{\mathcal{P}}$ we have that if $A \in \Gamma_{\mathcal{P}}$ and $A \subset B$, then $B \in \Gamma_{\mathcal{P}}$.

We call the complement of $\Gamma_{\mathcal{P}}$ an adversary structure. Formally, the adversary structure is $\mathcal{A}_{\mathcal{P}} = 2^{\mathcal{P}} \setminus \Gamma_{\mathcal{P}}$.

A secret sharing scheme satisfies two conditions:

1. Any trusted subset B of parties, i.e., $B \in \Gamma_{\mathcal{P}}$ could recover the secret from their shares.

2. Any untrusted subset A of parties, i.e., $A \in \mathcal{A}_{\mathcal{P}}$, can not find any information about the secret better than guessing (their shares are independent of the secret).

A popular access structure is a $t+1$-out-of-n secret sharing scheme, in which $|\mathcal{P}| = n$ and any $t+1$ parties in $\mathcal{P}$ can recover the secret, while any t cannot. Such schemes are called threshold schemes.

Shamir's secret sharing scheme is a threshold scheme.

Note: the Karnin-Greene-Hellman variant is optimal.

4. Threshold adversary: sometimes unrealistic

As pointed out by Burmester-Desmedt (Comm. ACM 2004), see also Desmedt-Wang-Burmester (ISAAC 2005) the threshold adversary model is unrealistic. Indeed, modern attacks can be replicated.

This concept was generalized to critical infrastructures by Burmester-Desmedt-Wang (IASTED 2003). Some motivating examples:

- the Hengchun earthquake on Tuesday December 26, 2006 caused several underwater internet cables to fail in Asia,
- Fukushima nuclear disaster after the Friday, 11 March 2011 Tohoku earthquake: same design, at same location with same vulnerabilities: 4 failures.

Adversary structure proposed: each party's platform is indicated by a color. Formally,

Definition 1. A k-*color* adversary structure over $\mathcal{P}$ consists of a tuple $(\mathcal{P}, C, f)$, where is C the set of colors, and f a map from $\mathcal{P}$ onto C and the adversary structure

$$\mathcal{Z}_{C,k} = \{Z \mid Z \subset \mathcal{P} \text{ and } |f(Z)| \leq k\}.$$

So, when a platform fails (or is attacked) all parties with the color corresponding to that platform are considered untrusted.

It is easy to make a secret sharing scheme for color-based adversary structures. Indeed, give all parties that have the same color the same share (i.e., replicate these shares)!

5. SECURE MULTIPARTY COMPUTATION: A BRIEF SURVEY

Goal: Suppose we have parties in $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ who have, respectively, as private input: x_1, x_2, . . . , x_n and one would like to compute $f(x_1, x_2, \ldots, x_n)$ in such a way that nothing leaks more than what follows from the output.

Today it uses secret sharing. The focus has been on the case the adversary is threshold based.

Terminology (brief):

- Passive adversary: execute specified program, while that restriction is removed in case the adversary is active.
- Static adversary: subset of $\mathcal{P}$ remains static during protocol.
- Most protocols require synchrony.

Note: fully homomorphic encryption seems best suited in the case of a single file server. Moreover, it is extremely slow.

6. OTHER APPLICATIONS OF SECRET SHARING

Secret sharing is also the key technology behind:

- Key escrow: NIST standard; did not take redundancy into account.

- Threshold cryptography: in threshold decryption, no single entity can decrypt. One needs a trusted subset of the parties. Note: this trusted subset does not recover the secret, only the plaintext. Threshold signatures are similar: one needs a trusted subset of the parties to be able to sign.

- Perfectly Secure Message Transmission: when a sender and a receiver do not share keys, they can still privately communicate over a point-to-point network, provided the number of nodes the adversary can control is limited and the network is connected enough. Additionally, one can achieve protection against an adversary that tries to block the communication or attempts to modify the message.

Some variants have been proposed.

7. WHY IS A STANDARD NEEDED?

When a user wants to use several cloud servers, shares could be stored instead of documents. These cloud servers could be from different organizations. This last approach is essential to achieve longevity (see DEC's demise).

Since the US Government is moving towards the cloud and since longevity is crucial, a standard addressing the privacy and reliability (longevity) of storage is obviously important.

8. Secret sharing: the way forward

We just explained the motivation for a standard on secret sharing. What should be considered include:

- Optimality issues,
- Speed
- Access structure (threshold is a first logical choice).

Longer term standards on:

- Perfectly Secure Message Transmission,
- threshold schemes for Threshold Cryptography,
- VSS (verifiable secret sharing),
- Secure Multiparty Computation,

should be a possibility, depending on the demand.

It is best that the secret sharing scheme chosen allows for above applications.