Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 19, 2014

C. Jennings
S. Nandakumar

January 15, 2014

Trustable Cloud Systems - Strategies and Recommendations
draft-jennings-perpass-secure-rai-cloud-01

Abstract

The Internet technical community is looking at ways to address pervasive attacks as described in several other internet drafts. [I-D.barnes-pervasive-problem] describes threat model to characterize various pervasive attacks on the Internet communications. There are many systems that need to be secured against such attacks but this paper considers one possible way to secure cloud based collaborations systems. At a high level, this paper sugests that users or enterprises could run a key server that manages the keys to access their content. The cloud service provider would not have access to decrypt the data stored in the cloud but various users of the cloud service could get the keys to encrypt and decrypt the contents of collaboration sessions facilitated by the cloud service. This does not protect the meta data of who is talking to who but can help protect the content of the conversations.

1. Introduction

The problem with today's cloud services is that a whole bunch of data is kept by the cloud service providers and that provides a target for attackers to collect and analyze the data. The strategy laid out in this document is to minimize the amount of data exposed to service providers by combining encryption and anonymization techniques. A user trusted Identity Provider (IdP) facilitates user key access and key management between devices. Such a solution must meet the following criteria to be usable at a larger scale.

- Housley Criteria: Be able to detect if your communications have been compromised

- Support voice, video, instant message, stored messages, file sharing and more

2. Trustable Cloud Services

The basic approach can be described as the following:

- Cloud Service sees only the encrypted data and envelope information.
- All users have public/private key.
- The user's Identity Provider manages the user's private keys and provides public keys to others.
- Identity providers authenticate to others using Certificate from the Certificate Authority.
- Content is encrypted by clients and the information to decrypt it is encrypted with the public keys of all the users authorized to view it.

3. Data Protection

The approach to stop the attacker from obtaining user data from service provider are:

- Each piece of content belongs to a group. Each group has one content owner.
- Data touched by the cloud is encrypted.
- The content encryptions keys are encrypted using the public keys of all users authorized to read this content.
- If others user can modify this data, the signature key for this content is encrypted with the public key of all users authorized to write this content.
- The content is encrypted and signed and bundled with all the relevant meta data.
- List of authorized users to read/write a piece of given content is managed by identity server for the content owner.

The goal is to encrypt as much as of the information as possible and then try to anonymizing un-encrypted data as much as possible.

- Encryption: TLS Everywhere
- Anonymization: Overlay routing (eg. TOR, P2P with RELOAD)

4. Trust - Roles of IdP and CA

This section outlines the guiding principles that define the roles of Identity Providers and Certificate Authorities in establishing end to end trust relationship and key management issues.

Its very hard to design systems where you do not trust your Identity Provider (IdP). The approach here is to separate the Identity Provider from the cloud provider and allow the Identity Provider to be run by someone you can trust. For example, an enterprise may run it's own IdP for it's employees.

- One has to trust their Identity Provider.
- Each user's device authenticates to IdP to get that users' private key.
- IdP provides public keys to others.
- IdP authenticates by having certificate for domain it serves.
- IdP for a user is discovered using domain name of the user identity.
- Each device talks to IdP to find out list of public keys for any groups that users owns.
- IdP provides API to manage group membership.

The security of the IdP discovery relies on having Certificate Authority (CA) that we can trust. The CA

- Provides TLS style certificates.
- Provides an audit log enabling list of certificates generated by a CA.
- If the CA creates bad certificates, which it can, the security of the whole system can be compromised but the goal is to be able to detect this.

Things do go wrong, devices get lost, and any practical system need to be able to deal with this. The approach for Key Revocation is:

- Relies on the Identity Providers and Cloud Service cooperating to get rid of the old key

- If a private key for a user is compromised, it is replaced with a new key by the IdP and the Cloud Service is informed to deprecate old key

- For any content that the old compromised private key could access, the Cloud Service asks the Identity Provider that owns that content to provide new meta data for that content with the new private key.

There is also the ability to check Key Continuity as follows:

- Any times a client detects a key has changed for a user, it can inform the user, Identity Provider, and Cloud Service to try and detect compromises

- Any time the Certificate changes for an Identity Provider or Cloud Service the Client can inform the user and the Identity provider.

5. Content Freshness

A common problem for encrypted cloud system is around how to find current content.

- Any time that the Cloud Service gets new content, it provides that content to all the Identity providers for users that can read that content along with an URL to be associated with the content.

- Each Identity Provider can index that content for future search as it has the private keys to decode it.

- Clients can perform a search using their Identity Provider based on the URI matching to retrieve set of Cloud Service URIs that matches the search.

6. Summary

Thus the proposed recommendation can be considered as guidelines to build a more elaborate architecture for building cloud services that are trustable based on the ideas of

- End to End Encryption Techniques based on Strong Cryptographic Algorithms
- Anonymization of metadata and un-encrypted data
- IdP and CA based Trust Certificate chain establishment

6.1. Possible Standardization

Following are some of the areas where more work needs to be done as far as standardization is concerned:

- Verification of all CA certifications issued
- IdP Discovery
- IdP Authentication of Client
- IdP API for management of IdP
- IdP API for public/private keys
- IdP API for search
- KeyRevocation API
- Key Continuity API
- Formats for encrypted objects and metadata
- Crypto Recommendations

7. Acknowledgements

- Design motivated by SiRiUS (Goh, Shacham, Modadugu & Boneh)
- Thanks to Eric Rescorla, Richard Barnes

8. Informative References

[I-D.barnes-pervasive-problem]
Barnes, R., Schneier, B., Jennings, C., and T. Hardie, "Pervasive Attack: A Threat Model and Problem Statement", draft-barnes-pervasive-problem-00 (work in progress), January 2014.

Authors' Addresses

Cullen Jennings

Email: fluffy@cisco.com

Suhas Nandakumar

Email: snandaku@cisco.com