Novel GPG Key Server using DNS based Authority Delegation

Samuel Johnson
Scientist/Engineer SC
Physical Research Laboratory,
Department of Space ,
Ahmedabad, India

Chauhan Pruthvirajsinh Rajendrasinh
M.E. Scholar
Department of Computer Engineering
Gujarat Technological University,
Ahmedabad, India

Gardas Naresh Kumar
Coordinator
Centre for Development of
Advanced Computing,
Pune, India

***Abstract*— GNU Pretty Good Privacy (GPG) is a widely used open source standard to ensure privacy and authenticity of digital communications. It achieves this by use of public key encryption. Public key needs to be easily accessible by others who may want to communicate with the owner of that key. GPG Public Key Servers (PKS) are usually used to achieve this. PKS stores public keys of its users and makes them easily available using HKP Protocol over HTTP. Current GPG Environment uses a concept of Web of Trust (WoT) to verify authenticity of the public Key. This method is not reliable both technically and practically. Hence this paper proposes a method which allows users to verify authenticity of the key without using WoT. Our approach needs delegations of authority of an email domain to a PKS Server. To achieve this we use DNS TXT Records. This paper describes architecture and working of the proposed system and why it is better than current systems.**

Keywords—GPG; Security; Distributed Systems; Synchronization; DNS; Public; Cryptography; TXT; Records; PRL;Web Of Trust; PKS

I. INTRODUCTION

From the days of face to face vocal communication the need to keep communication private and secret from others is indeed essential. In digital communication this need is satisfied mostly by use of encryption. Problem of exchanging secret keys gave rise to Public Key Cryptography. In Public Key Cryptography the private key always remains private to the owner and is not needed to be shared with anyone. Only the public key is accessible to everyone.

By choosing some algorithms from all the available encryption algorithms an open source standard GPG was devised.GPG made possible for users across different platforms to communicate using securely using encryption.

GPG uses a concept of Web of Trust to verify the authenticity of the public key and almost all of the publically available PKS use it or support it. There are several problems with current PKS and WoT.

Following is the list of some of the problems that current PKS faces as discussed in [1].

WoT Problems

- Social Challenges
- Long Trust Paths
- Lack of control after upload
- Lack of Authority

GPG Problems

- Unlimited Key Size
- Arbitrary Content Type

Synchronization Problems

- Lack of Deletion
- DoS Attacks
- Different Local Copyright Laws
- Lack of Notification

In current GPG infrastructure there are multiple geographically dispersed PKS deployed on the internet. If a user uploads a key to any one of these connected servers then it will be eventually synchronized to every other PKS in the network.

Currently GPG Key servers do not support deletion of the keys. Every instance of the server is considered equal and a key given by any one server has to be accepted by other servers. No Server can issue a delete request to others. Even if one server did delete a key from its local database others will give that key back to it and the server has to accept it.

Even after more than two decades of inception of GPG most of the servers suffer from above problems.

To overcome above problems we propose a PKS system which uses email and DNS TXT Records to verify the authenticity of the key uploaded to the server.

II. DNS TXT RECORDS

A. DNS Server

DNS Server is the back bone of the World Wide Web. Its main function of Name Resolution is explained in the figure below.

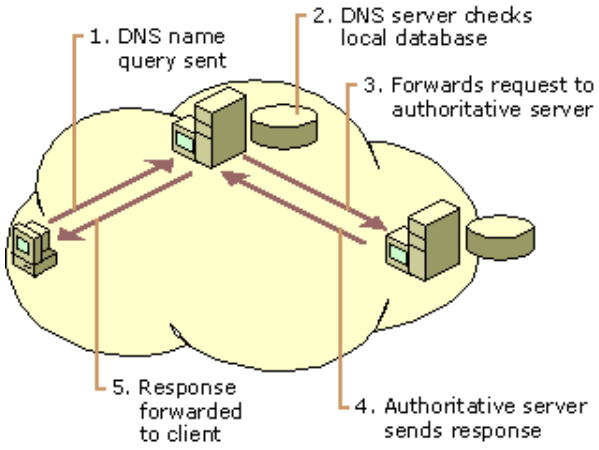

Figure 1. Working of Domain Name System

Other than name resolution DNS Entries are also used to store important information regarding domain of that entry. This information is stored in a mechanism called DNS Records.

Since connection to DNS Servers is a must to be "Online", we can convey information to everyone using DNS as storage of that information. But the limitation is the size of the information as we can store very little amount of information in DNS Records. DNS has registered standards about types of records that can be stored in DNSDNS Records

The DNS records are mapping files that tell the DNS server which IP address is associated with the domain. When a client visits a web site, a request is sent to the DNS server and then the request is forwarded to the web server provided by a web hosting company. This web server contains the actual data of the site.

Various predefined combination of English Alphabetical letters are used as identifiers/commands that dictate the actions to be performed. These predefined combinations are known as DNS syntax. Some of the widely used DNS records syntax are A, AAAA, CNAME, MX, PTR, NS, SOA, SRV, TXT, and NAPTR.

B. TXT Records

TXT Records are defined to store arbitrary text [2]. Owner of the DNS Entry can insert any textual information of limited length in TXT record of that entry.

TXT Records are standardized by very liberal key value pair based system.

To store arbitrary information, the TXT record uses a structured format in its TXT-DATA field. This format consists of the attribute name followed by the value of the attribute. The name and value are separated by an equals sign (=).

Example:

example.com IN TXT "colors I like=blue green black red"

The general syntax is:

<owner> <class> <TTL> TXT "<attribute name>=< value>"

C. Attribute Names

Any arbitrary ASCII character is permitted for the attribute name. If an equals sign is embedded in the attribute name, it must be preceded with a back quote. A back quote in Attribute Name must also be quoted with an additional back quote itself.

D. Attribute Values

Any arbitrary ASCII character is permitted in the attribute value. No delimiter like back quote is required in value field. Whenever the first unquoted equals sign in the TXT record is encountered it is taken as the name/value delimiter. All the following characters form the attribute value.

III. TERMINOLOGY OF THE PROPOSED SYSTEM

A. Domain:

A domain is a Fully Qualified Domain Name or FQDN.

Each and every GPG key has a primary ID. This id consists of name of the owner, email and comment. Hence the domain of the key is the domain of the email of the primary ID of the key.

For example a key having primary email "alice@example.com" falls in to domain of example.com.

For our system to work the domains have to be disjointed which FQDN satisfies as an FQDN is unique across the Internet.

B. Authority:

An Authority is defined as an entity having power to enforce rules and command other entities to perform a certain task.

In the context of proposed system an authority has the power over the keys of a certain domain. No entity can issue commands for the keys which doesn't fall in to domains under its own authority. Even if it did it will be rejected by others.

C. Delegation:

When a domain owner gives authority of its domain to some other party then it is called delegation of authority. The delegated party has authority for the keys under domain of the domain owner and now every other entity will obey the commands from the delegated party.

D. "Deln" Record

It is the TXT record in the world wide DNS server. "Deln" Record is used to tell the world that authority over the keys of this particular domain has been delegated to certain entity. This record resides in the DNS Entry of the domain.

E. Key ID

It is the full length ID of the GPG Public Key. Each Key in the world has unique ID. It is very difficult if not possible to create two different keys which have same key ID.

IV. AUTHORITY DELEGATION

To decide an authority for a domain the server will make a DNS lookup on the domain name. This domain's DNS Entry

must contain a DNS TXT Record which indicates who has authority over that domain.

For delegating authority of domain to a keyserver the domain's Admin must enter a TXT Record called Deln Record of the following format in to its domain's DNS entry.

A. *Deln Record Format*

Attribute Name	Attribute Value
authority	Web Address of the key server which will have authority for keys of this domain
keyid	ASCII 64bit GPG Public key ID of the Key Server
hash	ASCII Hash of the public key of the authority
since	ASCII String of Time when the authority information was last updated

B. *Working of Authority Delegation*

Following example shows working of DNS based mechanism for domain of prl.res.in.

TXT Record in DNS Entry of prl.res.in:

Auth=keyserver.prl.res.in; 0x37E1C77770086AEA; L9ThxnotKPzthJ7hu3bnORuT6xI=; Mon Jan _6 15:04:05 2014

Here we have used ";" as the delimiter in the value field. Hence the parser has to be implemented in such a way that it recognizes ";" as a delimiter.

The actual TXT Record is of the above form but it is parsed and then interpreted in to following table.

Attribute Name	Attribute Value
authority	keyserver.prl.res.in
keyid	0x37E1C77770086AEA
hash	L9ThxnotKPzthJ7hu3bnORuT6xI=
since	Mon Jan _6 15:04:05 2014

A keyserver having web address of keyserver.prl.res.in is given authority for the keys of domain prl.res.in

Any node will accept an update request for a key of domain prl.res.in, only if the sender supplies an authorized state signed using private key having same ID as stored in TXT Record of the prl.res.in.

To counter birthday attack, sha1 hash of the public key is also supplied in the text record.

To let others know the time when the information was updated "since" field is set. It shows the time when the details were uploaded to the DNS.

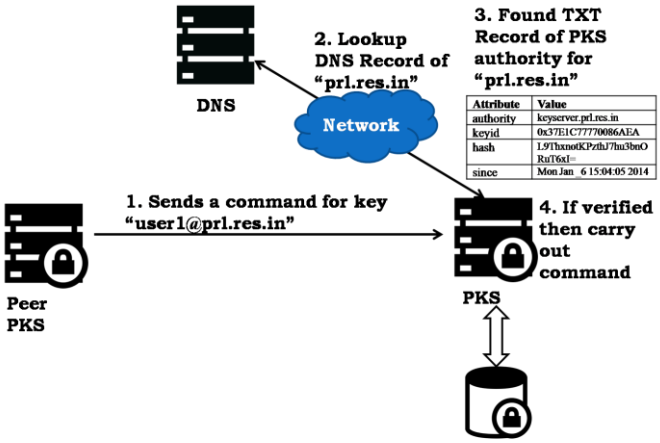

Figure 2. Working Authority Delegation mechanism

Using this mechanism the owner of the web domain has full control over who has the authority over the keys of his domain.

Because it is a DNS based mechanism we can easily supply changes in authority details to all the servers by just one single update in DNS record.

V. PROPOSED GPG KEY SERVER

A. *Key owner Verification*

Because of delegated authority we can verify the owner of the key without using WoT. In proposed PKS the key insertion scenario looks like the figure below.

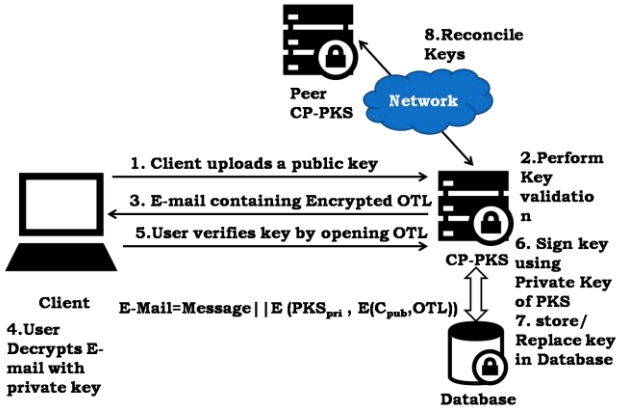

Figure 3. Insert/Update a Public Key

Since the PKS is signing the uploaded public key with its own private key, others can verify the key using public key of the PKS only.

B. *Key Deletion*

The proposed PKS will be supporting deletion of the key. Since this new PKS system gives authority to certain entities, those entities can now issue delete command to other entities.

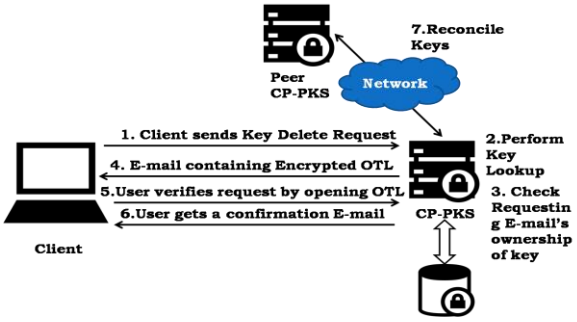

Figure 4. Delete a Public Key

An add/delete request for a key can only be made to the authority of that key. E.g. you cannot make a delete request to delete a key of prl.res.in to keyserver of cdac.in. You have to make request directly to the keyserver of prl.res.in.

VI. COMPARISON

Following Table shows comparison between current PKS and proposed PKS.

Current PKS	Proposed PKS
No Central or Distributed authority	Distributed Authority
Only Provides storage to upload keys	Provides Key verification and security on top of storage
Keys are manually verified by users using "Web of Trust", which is not reliable	Keys are automatically verified at the time of upload using E-mail based OTL verification mechanism
Anyone can upload key of anyone's E-mail address.	Only owner of the E-mail address can authorize upload , update or deletion of the key
Prone to PGP and Reconcile based DoS Attacks	Resilient to such attacks by validating key size and format
Prone to Birthday Attack	Resilient to Birthday Attack as ID of key is checked for such attacks
Key once uploaded can't be deleted due to reconciliation.	Provides Deletion of a key with improved reconciliation algorithm.
Not prone to DNS Spoofing attack	Prone to DNS spoofing attack

VII. CONCLUSION AND FUTURE WORK

By introducing authority over a domain and delegation of authority to other entity we can solve most of the problems that are faced by current PKS. Since DNS servers are always connected with all the clients on the web our solution is usable by any organization. If any organization wants keys of its domain handled by a particular GPG Keys server deployed on the web then the admin just has to add a single line of TXT record in his domain's DNS entry. If later he wants to change the delegation than he doesn't need to tell everyone but just have to change DNS entry only. Hence these novel ways of delegating authority using DNS TXT record is fast, reliable, robust and relatively secure then current PKS.

Future work includes devising Reconciliation algorithm based on concept of domain and authority so that PKS can benefit more from the above mechanism.

REFERENCES

[1] Pruthvirajsinh R. Chauhan, Samuel Johnson, Gardas Naresh Kumar. "A Review of Completely Public, PGP Public Key Servers ", Vol.2 - Issue 12 (December - 2013), International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, www.ijert.org
[2] Rosenbaum, R. "Using the Domain Name System To Store Arbitrary String Attributes". IETF, 1993.
[3] Shaw, D. *IETF Draft – "The OpenPGP HTTP Keyserver Protocol (HKP)"*. IETF, March, 2003.
[4] L. Donnerhacke, H. Finney,R. Thayer,J. Callas. IETF RFC 2440 - OpenPGP Message Format.IETF, November 1998
[5] Koch, Werner. The GNU Privacy Guard Manual. Boston : the Free Software Foundation, August 2013.
[6] Jason Hogg, Don Smith, Fred Chong. Web Service Security - Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0. Microsoft, 2005.
[7] Caronni, Germano, "Walking the Web of Trust. Gaithersburg" IEEE, June, 2000. ISBN - 0-7695-0798-0.
[8] Penning, Henk P. "Analysis of the strong set in the PGP web of trust." http://pgp.cs.uu.nl/plot/.
[9] P. Zimmermann, W. Stallings,D. Atkins. IETF RFC-1991, "PGP Message Exchange Formats." IETF, August,1996.