Web of Trust

Rafael Lammel Marinheiro

Histórico

- O *Web of Trust* é um conceito que surge a partir do PGP.
- Qualquer um consegue gerar uma chave PGP.
- Para verificar a autenticidade de uma mensagem, utilizamos a chave pública do proprietário.
- Mas será que a chave pública é realmente de quem diz ser?
- Podemos utilizar um sistema de CAs que gera certificados e verificar em um CA confiável que tenha assinado a chave pública, dessa forma, podemos confiar nela. Esse é um modelo **Centralizado**.
- Mas existe uma alternativa: ao invés de verificarmos em uma CA ou semelhante, podemos verificar com outra pessoa que temos confiança, onde ela me diz que confia na chave pública que procuro. Isso é a *Web of Trust*, um modelo **Descentralizado**.

Como Funciona - Explicação

- Cada pessoa dentro dessa rede possui uma lista de pessoas (chaves públicas) nas quais confia.
- Para cada pessoa que eu confio, eu assino a sua chave pública, gravando a lista de chaves que confio. Isso tem o nome de ***keyring***.
- Dessa forma, quando preciso verificar uma chave, eu busco os certificados de meu ***keyring*** para ver se tenho alguém que assinou a chave que procuro:
    - Se algum deles assinou a chave, eu posso dizer que confio na chave pois quem assinou a chave está na minha lista de confiança.
    - Se nenhum deles assinou, o processo se repete até encontrar a chave que procuro.
- Essa busca acaba criando uma espécie de rede, justificando o nome: *Web of Trust* (Rede de Confiança).

Como Funciona - Confiança e Validação

- Apesar disso, precisamos tomar cuidado: quanto maior o tamanho de uma rede, mais chances dela conter falhas.

- Por esse motivo, em *Web of Trust* temos que levar em consideração dois fatores importantes: **Confiança** e **Validação**.

    - **Confiança**: É o quanto você confia em uma pessoa dentro da rede. É uma atribuição feita de forma privada para cada pessoa que você queira guardar um nível de confiança. É guardado separado da sua **validação** de chaves, pois você pode validar a chave de alguém, sem confiar nela ou confiando marginalmente. O nível de confiança determina o número de assinaturas necessárias para validar uma chave posteriormente.

    - **Validação**: Verifica se você deve considerar a chave como válida ou inválida na hora de validar. Isso vai depender em como o algoritmo de verificação está implementado e no nível de confiança atribuído nos certificados que você teve que passar para validar a chave em questão.

Como Funciona - Níveis de Confiança

- Abaixo temos uma tabela indicando os níveis mais comuns de **confiança** em *Web of Trust*.

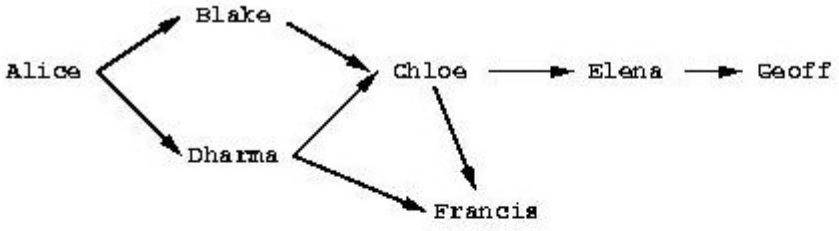
Nível de Confiança	Descrição
Desconhecido	Nada se sabe sobre a reputação do proprietário dessa chave
Nenhuma	É sabido que o proprietário faz assinaturas impróprias
Marginal	O proprietário entende as implicações de se assinar uma chave validando as chaves antes de assiná-las
Completo	O proprietário tem conhecimento pleno sobre assinaturas de chave, e você confia nas assinaturas dele como se fossem suas

Como Funciona - Validação

- Tendo os níveis de confiança atribuídos e chaves em seu ***keyring***, é possível validar outras chaves por meio do *Web of Trust*, da maneira que foi explicado nos slides anteriores.
- A validação utiliza do nível de confiança atribuído da seguinte maneira:
- Importante: Apesar do nível de confiança ser separado da validação, a chave do proprietário precisa ser **válida** para seguir a tabela abaixo.

Nível de Confiança no Proprietário da Assinatura	Necessário para validar uma chave
Desconhecido/Nenhuma	Chaves assinadas por proprietários desse nível nunca são validadas.
Marginal	É necessário um número X de assinaturas marginais (definido pelo algoritmo, geralmente 2 ou 3) para que eu possa validar a chave em questão
Completo	Basta uma assinatura desse nível para que a chave em questão seja válida

Como Funciona - Ilustração



trust		validity	
marginal	**full**	**marginal**	**full**
	Dharma		Blake, Chloe, Dharma, Francis
Blake, Dharma		Francis	Blake, Chloe, Dharma
Chloe, Dharma		Chloe, Francis	Blake, Dharma
Blake, Chloe, Dharma		Elena	Blake, Chloe, Dharma, Francis
	Blake, Chloe, Elena		Blake, Chloe, Elena, Francis

Exemplos de Uso

- O maior exemplo de uso do modelo de *Web of Trust* são em alguns provedores de e-mail, que também utilizavam o PGP.

Exemplos de Como “Confiar” com GPG

```
alice% gpg --edit-key blake

pub  1024D/8B927C8A  created: 1999-07-02 expires: never      trust: q/f
sub  1024g/C19EA233  created: 1999-07-02 expires: never
(1)  Blake (Executioner) <blake@cyb.org>

Command> trust
pub  1024D/8B927C8A  created: 1999-07-02 expires: never      trust: q/f
sub  1024g/C19EA233  created: 1999-07-02 expires: never
(1)  Blake (Executioner) <blake@cyb.org>

Please decide how far you trust this user to correctly
verify other users' keys (by looking at passports,
checking fingerprints from different sources...)?

 1 = Don't know
 2 = I do NOT trust
 3 = I trust marginally
 4 = I trust fully
 s = please show me more information
 m = back to the main menu

Your decision? 3

pub  1024D/8B927C8A  created: 1999-07-02 expires: never      trust: m/f
sub  1024g/C19EA233  created: 1999-07-02 expires: never
(1)  Blake (Executioner) <blake@cyb.org>

Command> quit
[...]
```

Motivos Para Não Ter Tanto Uso

- O sistema **centralizado** que utiliza CAs ao invés de confiar em outros usuários é mais adotado em aplicações.

- O usuário precisa gerenciar suas chaves, e não existem muitas ferramentas para facilitar esse processo.

- Construir uma *Web of Trust* é complexo. Precisa que todos dentro da rede estejam usando a mesma implementação do PGP e precisa de muitas assinaturas para que se possa começar a conseguir validações pela rede.

Referências

- https://www.gnupg.org/gph/en/manual/x334.html
- https://www.gnupg.org/gph/en/manual/x547.html
- https://www.rubin.ch/pgp/weboftrust.en.html

Obrigado!

...