Diffie-Hellman e Problema do Logaritmo Discreto (DLP)

Teórica #9 de Criptografia Aplicada

Problema do Logaritmo Discreto (DLP)

O problema do logaritmo discreto defende que existe pelo menos uma solução que satisfaça a condição:

```
a^m (=congruente)1 (mod(n))
```

Primitive Root (raiz primitiva): Sendo `(a, n) = 1`, *a* é chamada de raiz de primitiva de *n*, se a ordem de `a (mod(n)) = φ(n)`. Nem todos os inteiros tem raizes primitivas, sendo que estes apenas existem em {2, 4, p^n, 2*p^n, p = odd prime}

Existe também a noção de "*i* é índice de *b*", sendo *p* um número primo e *a* uma raiz primitiva de *p*, se:

```
b (=congruente) a^i (mod(p))
```

Diffie-Hellman (DH)

A Alice (A) e Bob (B) desejam comunicar sobre um canal não seguro. Para tal, estes vão usar o Diffie-Hellman para cifrar as mensagens enviadas no canal de comunicação. Antes de produzir as chaves públicas e privadas, estes precisam de concordar no intervalo público multiplicativo *Zp* que vão utilizar, de forma a que se saiba qual o número primo *p* e a base *g* pertencentes ao intervalo Zp.

As chaves privadas são produzidas de forma aleatórias, pertencentes ao intervalo Zp ($a, b \in Zp$). As chaves publicas são produzidas com o valor das chaves privadas, sendo:

```
A = g^a (mod(p))
B = g^b (mod(p))
```

O valor secreto *k* não tem que ser partilhado no canal, porque ambos sabem o calcular:

```
k = A^b = (g^a)^b ) = g^a*b = (g^b)^a = B^a
```

Este valor é usado para produzir uma ou mais chaves simétricas, através do uso de uma KDF (Key Derivation Function - função que produz uma string aleatória com o tamanho da chave).

A segurança do Diffie-Hellman é dado por dois fatores:

- O valor *g* deve ser uma raiz primitiva de *p*, caso contrário apenas um pequeno conjunto de valores pode ser gerado como valores secretos partilhados;
- Os parâmetros de DH produzidos (i.e., valores primos produzidos) devem ser *seguros*, no sentido em que estes são um valor primo seguro *p* (p = prime e (p - 1 / 2) = prime). A utilização destes valores primos seguros, garante que não existam valores no intervale que sejam fáceis de "partir" o DH.

É de notar que a produção destes valores primos seguros é 1000x mais lenta que produzir parâmetros RSA, para o mesmo nível de segurança/bits.

CDH e DDH

O Computation Diffie-Hellman e Decisional Diffie-Hellman, são dois problemas associados a possíveis ataques ao Diffie-Hellman. No CDH, o problema está no calculo do valor secreto partilhado `g^a*b`, apenas através dos valores públicos `g^a` e `g^b`, sem recorrendo aos valores privados *a* e *b*, ou seja, **descobrir o valor secreto partilhado apenas com a informação pública**. Por consequência, este problema partilha algumas similaridades com o RSA, onde o algoritmo GNFS o "parte". Para o CDH existe o algoritmo NFS (number field sielve), que resolve o DLP e por consequência, "parte" o CDH.

No DDH, o problema está associado no calculo dos primeiros 32bits do valor secreto `g^a*b`, dado os 2048-bits dos valores públicos `g^a` e `g^b`, o que permite a um atacante conhecer mais sobre o valor secreto partilhado. Este problema é resolvido ao escolher-se o valor secreto sem que o atacante saiba que este foi escolhido aleatoriamente do intervalo.

Se o DDH é dificil de se resolver, então o CDH também o é. Resolvendo o CDH permite também resolver o DDH.

Modelos de Ataque para Key Agreement Protocols (KAP)

Existem três tipos de ataques que podem ser realizados em protocolos que utilizam chaves para trocar informação e realizar acordos:

- ***Eavesdropper***, que descreve um atacante que observa as mensagem transmitidas entre duas entidades, podendo modificar, quebrar ou alterar as mensagens. Protege-se a comunicação contra o eavesdropper ao não partilhar informação sobre o valor secreto partilhado;
- ***Data Leak***, que descreve um atacante que adquire uma chave de sessão e todos os valores secretos temporários usados no protocolo, mas não os valores permanentes;
- ***Breach***, que descreve um atacante que adquire as chaves secretas permanentes, podendo impressionar qualquer entidade após obter as chaves.

Objetivos de Segurança em Key Agreement Protocols (KAP)

Os quatro objetivos mais relevantes para a segurança em KAP são:

- ***Authentication***, que descreve que as duas entidades a comunicar devem poder-se autenticar entre si, de forma a criar autenticação mútua;
- ***Key Control***, que descreve que nenhuma das duas entidades a comunicar deve por escolher ou influenciar o valor secreto final a partilhar;
- ***Forward Secrecy***, que garante que mesmo que os valores secretos permanentes sejam adquiridos, não é possível obter os valores secretos previamente partilhados;
- ***Resistance to key-compromise impersonation (KCI)***, que descreve que o protocolo a ser usado deve prevenir a falsificação da comunicação.

Tipos de Diffie-Hellman

Existem diferentes tipos de Diffie-Hellman, sendo estes:

- Anonymous Diffie-Hellman, que descreve a versão mais simples do DH, onde nenhum dos participantes consegue verificar a identidade de quem está a comunicar, sendo assim sujeito a ataques de eavesdropping;
- Authenticated Diffie-Hellman, que descreve um protocolo DH mais seguro, protegido de eavesdropping, mas não protegido de data leaking;
- Menezes-Qu-Vanstone (MQV), ou Diffie-Hellman em “esteroides”, sendo este mais sofisticado e seguro que o Authenticated DH. Em comparação com este, o MQV permite enviar apenas duas mensagens de formar arbitrária, mensagens mais curtas e não precisa de enviar uma assinatura explicita ou mensagens de verificação.