UNIVERSITY OF STUTTGART

Hauptseminar: The Logjam Attack

Li Yang Wu

June 5, 2017

CONTENTS

ABSTRACT

[Adrian et al., 2015] developed a new attack called Logjam to break many cryptographic systems using the Diffie-Hellman key exchange mechanism. This review elucidates its technical details and summarize overall results of their paper.

1 INTRODUCTION

If it comes to network security, the Diffie-Hellman key exchange is the standard wildly used in practice and declared to be safe. However, [Adrian et al., 2015] could break the security on many popular and browser certified websites. They demonstrated this so called Logjam attack on the Transfer Level Security protocol that supports Diffe-Hellman as key exchange. They also implemented an attack exploiting weak and misconfigured groups using the Pohling-Hellman algorithm.

The second result the authors present is an estimate on cost of computing logs from key sizes of 1024 bits. I will briefly summarize their assumptions for the estimate and the results.

2 DIFFIE-HELLMAN KEY EXCHANGE

[Diffie and Hellman, 1976] was the first paper presenting a practical solution to the privacy and the authentication problem that does not rely on secure communication channels. These kinds of channels are often not given or so inefficient to use that the benefit of telecommunication is nullified. Hence, it was a historical and great advance in computer networking and cryptography. They presented an asymmetric approach with trap door functions that have an exponential cipher-cryptanalyst ratio. Because of this, a security system can choose feasible large private keys that are at the same time infeasible to infer from public keys and encrypted messages w.r.t. computation time.

2.1 PROBLEM FORMULATION

Given:

- A, B, the communication partners.
- Only insecure communication channels are available.
- $\{M\}$, a finite message space which contain all possible messages M to be exchanged.

Determine:

- $C = (\{E_K\}_{K\in\{K\}}, \{D_K\}_{K\in\{K\}})$, a *public key cryptosystem* with mutual inverse functions

- $E_K : \{M\} \to \{M\}$
- $D_K : \{M\} \to \{M\}$

denoted as *encryption* and *decryption transformation* respectively.

- $\{K\}$, a suitable set of keys.
- Such that
  1. $\forall K \in \{K\} : M = D_K(E_K(M))$
  2. $\forall K \in \{K\}, M \in \{M\} : E_K(M), D_K(M)$ are easy to compute.
  3. $\forall^\infty K \in \{K\}, \alpha : \{E_K\}_{K\in\{K\}} \to \{D_K\}_{K\in\{K\}} : D_K = \alpha(E_K)$ is infeasible to compute.
  4. $\forall K \in \{K\} \exists \beta : \{K\} \to (\{E_K\}_{K\in\{K\}}, \{D_K\}_{K\in\{K\}}) : \beta(K) = (E_K, D_K)$ is feasible to compute.

2.2 Solutions

Key Exchange The solution the authors propose is to draw private and public keys (D, E) from finite fields of sizes equal to prime numbers $\mathrm{GF}(q) \cong \mathbb{Z}/q\mathbb{Z}$, i.e.

$$D, E \in \mathrm{GF}(q) = \{x \mod q \mid x \in \mathbb{Z}\}. \tag{2.1}$$

By choosing the private key as the logarithm of the public key and an arbitrary basis $\alpha \in \mathrm{GF}(q)$,

$$D = \alpha^E \mod q, \tag{2.2}$$
$$E = \log_\alpha Y \mod q, \tag{2.3}$$
$$1 \leq D, E \leq q - 1, \tag{2.4}$$

the requirements 3. and 4. are fulfilled. Calculating D from E has logarithmic time complexity in q. Inversely, calculating E from D has a complexity of $\sqrt{q}$. Therefore the cipher-cryptanalyst ratio is exponential. Note that this is not a proven bound. We use the best known algorithms for these problem to get this ratio. Better algorithms have not been found for decades, therefore this method is considered safe. Also, one need to find good primes q in order to assure worst or near worst case log-computation time.

Now if A and B want to exchange a session key, they first choose public and private keys D_A, D_B, E_A, E_B with a q of sufficient size and exchange their public keys over the insecure communication channel. Then, they can calculate the common session key

$$\begin{aligned} K_{A,B} &= \alpha^{E_A E_B} \mod q && (2.5)\\ &= (\alpha^{E_A})^{E_B} \mod q && (2.6)\\ &= {D_A}^{E_B} \mod q && (2.7)\\ &= (\alpha^{E_B})^{E_A} \mod q && (2.8)\\ &= {D_B}^{E_A} \mod q. && (2.9) \end{aligned}$$

While A calculates the right term in 2.7, B calculates the right term in 2.9 and both of them have now the same session key $K_{A,B}$.

The trap-door property of this mechanism allows us to use it for one-way authentication. A signature s of some user A is $D_A(s)$. No one can forge it, since D_A is private. A cannot deny his or her signature, since everyone can confirm $E_A(D_A(s)) = s$.

CRYPTANALYSIS The attacker can compute $K_{A,B}$ either by computing E_A from D_B or E_B from D_A, both are log-problems in finite fields. Thus, the attacker is successful, iff he or she can effort exponentially more computation power that A and B.

3 NUMBER FIELD SIEVE ALGORITHM

4 THE LOGJAM ATTACK

5 OTHER ATTACKS

6 POHLING-HELLMAN ALGORITHM

7 DISCUSSION

TODO

REFERENCES

Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., and Zimmermann, P. (2015). Imperfect forward secrecy: How diffie-hellman fails in practice. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 5–17, New York, NY, USA. ACM.

Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654.