

A Static Diffie-Hellman Attack on Several Direct Anonymous Attestation Schemes

Ernie Brickell¹ Liqun Chen² Jiangtao Li¹

1. Intel Corporation, Hillsboro, Oregon, USA

2. Hewlett-Packard Laboratories, Bristol, UK

InTrust 2012

Royal Holloway, University of London
Egham, UK

December 17 – 18, 2012

Background

Direct Anonymous Attestation (DAA)

Static Diffie-Hellman (DH) Problem

Our Contributions in this Paper

In several DAA schemes, TPM is a static DH oracle, but this feature was missing in DAA security analysis

- Static DH in RSA-DAA
- Static DH in ECC-DAA

Two Mitigation Suggestions

Relevant ISO/IEC Standards

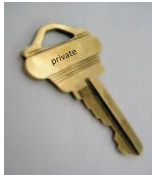
Summary and Discussion

Signatures with Signer Privacy

It is all about the keys



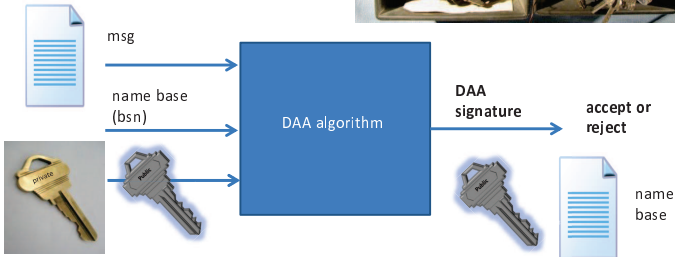
DAA is an Anonymous Digital Signature Scheme



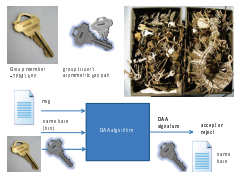
Group member
- TPM's key



group issuer's
asymmetric key pair



DAA is a Special Type of Group Signature



- ▶ It involves a group manager (called group issuer), a set of group members and a set of verifiers.
- ▶ A verifier uses the issuer's public key to verify the signature, cannot identify the individual signer, but may be able to link signatures from the same signer.
- ▶ A group issuer is NOT able to trace the signer's identity from a signature.
- ▶ A signer can split into two parts: a principle signer (TPM) and an assistant signer (Host).

RSA-DAA & ECC-DAA

- ▶ The first DAA scheme was designed in 2003 for the Trusted Computing Group (TCG) and used in TCG TPM Version 1.2.
- ▶ The security definition and formal description of this scheme was published in ACM CCS 2004. Security of the scheme is based on the strong RSA problem; it is called RSA-DAA.
- ▶ After that many DAA schemes have been developed. Most of them make use of elliptic curves, and they are called ECC-DAA.
- ▶ TPM2 will support ECC-DAA.
- ▶ It is generally believed that the security level of RSA-DAA is 104-bit and ECC-DAA is 128-bit. In this paper we argue that these two values may be incorrect for several DAA schemes!

The Static Diffie-Hellman (DH) Problem

Definition (Static DH Oracle)

Let \mathbb{G}_ρ be a cyclic group of prime order ρ . Let x be a value in \mathbb{Z}_ρ^* . Given any $r \in \mathbb{G}_\rho$, the static DH oracle on x computes and outputs r^x .

Definition (Static DH Problem)

Let \mathbb{G}_ρ be a cyclic group of prime order ρ . Given $g, h \in \mathbb{G}_\rho$ such that $h = g^x$, the static DH problem is to compute x given access to a static DH oracle on x .

- ▶ The static DH assumption is that it is computationally infeasible to solve the static DH problem.
- ▶ The static DH assumption is stronger than the discrete logarithm assumption, although it is still believed that the static DH problem is a computationally hard problem.

The Brown and Gallant Technique

Theorem

Let \mathbb{G}_ρ be a cyclic group of prime order ρ such that $\rho = uv + 1$ for positive integers u and v . There exists an algorithm that solves the static DH problem on \mathbb{G}_ρ with u queries to the static DH oracle and about $2(\sqrt{u} + \sqrt{v})$ off-line group operations in G_ρ .

- ▶ If there exists $u \approx \rho^{1/3}$, then an adversary can solve the static DH problem in about $\rho^{1/3}$ group operations. A normal attack to the discrete log problem would require $\rho^{1/2}$ group operations.
- ▶ E.g., using 256-bit ρ , one can query the static DH oracle $O(2^{85})$ times and solve the discrete log problem with $O(2^{85})$ computations instead of $O(2^{128})$ computations.

In Which Circumstance a TPM is a Static DH Oracle?

- ▶ Let sk_T be a TPM's secret key, and cre be a DAA credential, where

$cre = \text{a signature on } sk_T \text{ by a DAA Issuer.}$

- ▶ When Linkability is not required, a DAA signature is

$SPK\{(sk_T, cre) : \text{a randomised } cre\}(msg).$

- ▶ When Linkability is required, a DAA signature is

$SPK\{(sk_T, cre) : \text{a randomised } cre \wedge$

$\text{a committed } sk_T = (hash(bsn))^{sk_T}\}(bsn, msg).$

In this case, a TPM is a static DH oracle, particularly if an adversary can manipulate $hash(bsn)$.

- ▶ The adversary could be the Host, the Issuer or both.

Static DH in RSA-DAA (I)

- ▶ In two places, the value $(hash(bsn))^{sk_T}$ is generated.
 - ▶ In DAA Joining, a DAA credential request is

$$SPK\{(sk_T) : \text{a committed } sk_T = \underline{(hash(bsn_I))^{sk_T}}\}(bsn_I, msg).$$

- ▶ In DAA Signing, when Linkability is required, a DAA signature is

$$SPK\{(sk_T, cre) : \text{a randomised } cre,$$

$$\text{a committed } sk_T = \underline{(hash(bsn_V))^{sk_T}}\}(bsn_V, msg).$$

- ▶ TPM is a static DH oracle if an adversary can manipulate either $hash(bsn_I)$ or $hash(bsn_V)$.

Static DH in RSA-DAA (II)

- ▶ The Brown-Gallant algorithm works in one of the following two cases:
 - ▶ If the adversary compromises the Host, and suppose that the honest Issuer chooses a random ρ , then the security level of RSA-DAA could be any number between 104-bit and 70-bit.
 - ▶ If the adversary compromises both the Issuer and Host, the malicious Issuer can choose $\rho = uv + 1$ with $u \approx \rho^{1/3}$, then the security level is then downgraded from 104-bit to roughly 70-bit.
- ▶ The connection between the static DH problem and RSA-DAA security was not addressed in the security proof of RSA-DAA.

Static DH in ECC-DAA

- ▶ In one place, the value $(\text{hash}(\text{bsn}))^{sk_T}$ is generated.
 - ▶ In DAA Signing, when Linkability is required, a DAA signature is

$$SPK\{(sk_T, cre) : \text{a randomised } cre, \\ \text{a committed } sk_T = \underline{(\text{hash}(\text{bsn}_V))^{sk_T}}\}(\text{bsn}_V, msg).$$

- ▶ TPM is a static DH oracle if an adversary can manipulate $\text{hash}(\text{bsn}_V)$.
- ▶ Similar to RSA-DAA, the Brown-Gallant algorithm works when the adversary compromises the Host or both the Issuer and Host. The later case allows the adversary to make a more powerful attack.
- ▶ This weakness is not captured in the security proofs of several ECC-DAA schemes.

First Mitigation: Choose Safe Prime

- ▶ Modify the issuer setup algorithm to choose the group order ρ as a safe prime.
- ▶ This is suitable for RSA-DAA.
- ▶ But for ECC-DSA, it may not always be possible to choose ρ as a safe prime.
- ▶ Many pairing-friendly curves have to be constructed in a special way. For example, the Barreto-Naehrig curves have the requirement that $\rho = 36w^4 + 36w^3 + 18w^2 + 6w + 1$ for some integer w . If ρ is 256-bit, then w is roughly 63-bit. An adversary can set $u = w$ and $v = 36w^3 + 36w^2 + 18w + 6$ and use u, v to perform the Brown-Gallant attack.

Second Mitigation: Avoid $\text{hash}(\text{bsn})$ to Be Manipulated

Ask a TPM to create or verify $\text{hash}(\text{bsn})$.

This is not cost free, but a TPM can handle this.

International Standards

A few ISO/IEC standards are related to the content of this paper. Some of them are in development.

- ▶ ISO/IEC 11889 Trusted Platform Module
- ▶ ISO/IEC 20008 Anonymous Digital Signatures
- ▶ ISO/IEC 20009 Anonymous Entity Authentication
- ▶ ISO/IEC 18370 Blind Signatures

Summary and Discussion

- ▶ We have not broken any DAA scheme.
- ▶ DAA has not been broken, as far as we understand, if implementation follows the original design principle.
- ▶ DAA still has a room for further research and improvement.
- ▶ Privacy is a big concern in today's life. Technology of achieving privacy is a challenge.

Many Thanks!

Any Questions?