From: David A. Cooper
To: Dang, Quynh H. (Fed); Dworkin, Morris J. (Fed); Davidson, Michael S. (Fed); Miller, Carl A. (Fed); Apon, Daniel C. (Fed)
Subject: Re: A statement about state management.
Date: Thursday, April 25, 2019 10:23:29 AM

Hi Quynh,

The text in the Security Considerations section is still in progress. I also expect to add something to Section 1 about use of hardware.

One could certainly imagine the possibility of faulty hardware reusing a OTS key. However, this isn't a problem that is unique to stateful HBS. There have been numerous cases of private key compromise as a result of faulty cryptographic modules (including hardware modules). I'm particularly thinking about cases in which the key generation process was flawed, making it possible for others to determine the private key from the public key.

Dave

On 4/25/19 8:38 AM, Dang, Quynh (Fed) wrote:

> Hi everyone,
>
> The security requirement/consideration section is still soft on requiring the use of HSMs.
>
> Also, I don't know if an HSM can be faulty so it could end up signing with the same OTS key multiple times.
>
> Quynh.

> **From:** David A. Cooper <david.cooper@nist.gov>
> **Sent:** Monday, April 15, 2019 9:39:24 AM
> **To:** Dang, Quynh (Fed); Dworkin, Morris J. (Fed); Davidson, Michael S. (Fed); Miller, Carl A. (Fed); Apon, Daniel C. (Fed)
> **Subject:** Re: A statement about state management.
>
> Hi Quynh,
>
> On Friday I got started on some introductory text for our SP. I just uploaded it to the SharePoint site and I copied it below. It doesn't go as far as you suggest, but it does try to discourage use of stateful HBS. I think the text below should be followed by some more text placing further restrictions on the use of stateful HBS (e.g., only in a highly-controlled environment, perhaps only using a hardware security module). Of course, all of this would be in addition to text in Section 7.1 (One-Time Signature Key Reuse).

Dave

> This publication supplements FIPS 186-4 [4] by specifying two additional digital signature schemes, both of which are stateful hash-based signature (HBS) schemes. All of the digital signature schemes specified in FIPS 186-4 will be broken if large-scale quantum computers are ever built. The security of the stateful HBS schemes in this publication, however, only depend on the security of the underlying hash functions – in particular the infeasibility of finding a preimage or a second preimage – and it is believed that the security of hash functions will not be broken by the development of large-scale quantum computers.
>
> While there is an effort underway to develop standards for post-quantum-secure digital signature schemes that can be used as drop-in replacements for the schemes that are specified in FIPS 186-4, there are a few applications for which it may be deemed impractical to wait until these new standards are available before transitioning to a post-quantum-secure digital signature scheme. Stateful HBS schemes may be used in these cases, but they are not drop-in replacements for the schemes specified in FIPS 186-4, since the stateful HBS schemes impose a requirement for state management.
>
> In a stateful HBS scheme, a key pair consists of a large set of one-time signature (OTS) key pairs. An HBS key pair may contain thousands, millions, or billions of OTS keys, and the signer needs to ensure that no individual OTS key is ever used to sign more than one message. If an attacker were able to obtain digital signatures for two different messages created using the same OTS key, then it would become computationally feasible for that attacker to forge signatures on arbitrary messages. As a result of this risk, NIST recommends against the use of stateful HBS schemes except in cases in which it would be impractical to wait until post-quantum-secure digital signature schemes that do not require this state management become available. If a stateful HBS scheme is used, then, as described in Section 7.1, extreme care needs to be taken in order to ensure that no OTS key is ever reused.

On 4/15/19 7:16 AM, Dang, Quynh (Fed) wrote:

> Hi everyone,
>
> If we standardize stateful hash-based signatures, then it would be when, not if: the matter of time when the public knows someone screws up their system.
>
> In the case we standardize them, if we provide references or/and guidance for methods used to avoid OTS private key reuse problem, it would create an implied policy that we want people to use stateful hash-based signatures and here is how to do it right. When someone screws up, there would be more reason for the public to blame us. (*).
>
> Instead, if we use the policy I suggested in the previous email (basically, if you are not sure that you have a perfect method to handle the issue, don't use stateful hash-based signatures.), then

there would be less reasons for the public to blame us.

The (*) approach would bring the benefit that some people who benefit from our references and/or guidance may appreciate our work. But, a lot of people just think that that is our job and we want to do it and don't have a strong appreciation for that particular guidance that we provide.

But, when a bad thing happens, pretty much only the voices of "don't do this" would be counted.

Quynh.

From: Dang, Quynh (Fed)
Sent: Saturday, April 13, 2019 6:27:50 AM
To: Cooper, David A. (Fed); Dworkin, Morris J. (Fed); Davidson, Michael S. (Fed); Miller, Carl A. (Fed); Apon, Daniel C. (Fed)
Subject: A statement about state management.

Hi everyone,

It's weird and sad that my dream did not have anything sweet, but hash-based signatures.

I think some statement like below would be good if we decide to standardize stateful hash-based signatures.

"Before using any option of the stateful hash-based signature algorithms in this standard, you shall/must have a perfect strategy/technique to make sure that any used OTS private key will not be reused during the life time of your system including all situations that your system might face. Some of the situations are below.

1) The system crashes during a signing operation, then your system needs to be rebooted.

2) The system is backed up then get restored later.

3) The system is updated or integrated with other systems which creates a risk of the state of the system is messed up etc..

If you don't have a perfect method to make sure that none of OTS private keys will be used more than once during the life time of your system under any circumstances, then don't use any of the stateful hash-based signature algorithms in this standard. "

Quynh.