From: David A. Cooper
To: Regenscheid, Andrew R. (Fed)
Subject: Re: Stateful HBS Key Backups
Date: Friday, April 12, 2019 9:56:06 AM

On 4/12/19 9:33 AM, Regenscheid, Andrew (Fed) wrote:

> Dave,
>
> I heard you had been thinking about how backups might work with stateful hash based signatures. Can you pass along any emails/thoughts?
>
> -Andy

Hi Andy,

The wording could use improvement, but here is the current text that I have in the draft SP on stateful HBS:

> When a copy of a private key needs to be made, this document recommends against cloning the private key; i.e., making a copy of the private key in which the state information for the copy is the same as for the original. Instead, the state reservation technique described in [6] should be used. In addition to any secret information needed to generate signatures, each copy the private key will include a state variable indicating the set of OTS keys that remain available for use. When a "copy" of the key is made, the keys that are made available for use in the copy are marked as unavailable in the original. The system needs to ensure that the original is updated before the copy is released, in case a failure occurs during the copying process.
>
> As an example, a key may initially be generated as a 25-level Merkle tree with 2^{25} OTS keys. The state variable for this key would initially have the set of available OTS keys as $[0…2^{25}-1]$. Two "copies" of this key may then be made – one for operational use and one as a second copy for disaster recovery. The initial value for the state variable for the first "copy" might indicate its set of available OTS keys as $[0…2^{23}-1]$, and the second "copy" might be assigned OTS keys $[2^{23}…2^{24}-1]$. After the two "copies" had been made, the original's set of available keys would have been updated to $[2^{24}…2^{25}-1]$. The original and the second "copy" could then be stored in separate vaults, where they could be accessed in case the operational copy of the key became unusable. In some cases, multiple operational copies of the key may be made, each with its own unique set of available OTS keys.
>
> When a message is to be signed the OTS key to be used is removed from the list

of available keys before the signature is output. In the above example, the list of available keys for the operational key would be updated to [1…2^{23}-1]. If multiple messages needed to be signed, more than one OTS key could be reserved at once in order to increase efficiency. As noted in [6], if the private key is not stored and used in a hardware cryptographic module, particular care needs to be taken to ensure that the state of the private key has been updated before any signatures are output, as caching mechanisms may delay the actual update of the key in nonvolatile memory.

[6] David McGrew, Panos Kampanakis, Scott Fluhrer, Stefan-Lukas Gazdag, Denis Butin, and Johannes Buchmann, State Management for Hash-Based Signatures, Cryptology ePrint Archive, Report 2016/357. https://eprint.iacr.org/2016/357.pdf. 2016.