Very basic estimates on the risk of reusing the Winternitz signatures

September 1, 2017

This is just a *very* rough back-of-envelope calculation on the risk of reusing the (modified) Winternitz signatures used in IOTA. If there was only one spending from the address, the attacker needs to do around $27^{54} \simeq 2^{256}$ tries[1] in average in order to forge the signature, which is unfeasible.

Then, assume that there were $n \geq 2$ outgoing transactions from an address. Then, the probability of being able to reuse the sig in one bin is *typically* around $\frac{n}{n+1}$; this follows from the fact that

$$\mathbb{E} \min\{U_1, \ldots, U_n\} = \frac{1}{n+1},$$

where $U_1, \ldots, U_n$ are independent Uniform$[0,1]$ random variables. So, the average number of attacker's tries in order to be able to forge the signature is roughly $\left(\frac{n+1}{n}\right)^{54}$. We have

$$\left(\frac{n+1}{n}\right)^{54} \simeq \begin{cases} 2^{32}, & \text{for } n = 2, \\ 2^{22}, & \text{for } n = 3, \\ 2^{17}, & \text{for } n = 4, \\ 2^{14}, & \text{for } n = 5, \end{cases}$$

etc.

Conclusions. It is safe to *keep* tokens on an address from which there was only one spending, since it is virtually impossible to forge once-used signature. After the second outgoing transaction (which also transfers all funds to a new address) is

[1] recall that there is that restriction on the sum, so the attacker would have to get exactly the same profile

issued, an attacker would have to do around 2^{32} iterations to be able to issue a double-spending transaction; *provided that* the legitimate transaction is quickly confirmed, the attacker's transaction would have very little chance to win the competition against the legitimate transaction. Still, there is still *some* risk for the user at the time the second transaction is issued, especially in the case when the attacker's computational power is large and/or that second transaction takes a lot of time to be confirmed.

On the other hand, after two uses the security deteriorates very quickly, as shown above.