Life, Universe, and Everything

November 24, 2010

A consistent key(context) is defined as a key that does not introduce internal inconsistencies. A (partially) propagated KSK must have a fully propagated ZSK.

$$
\begin{aligned}
ConsistentKeys \equiv \{k | k \in \mathbb{K},\\
&\neg H(Ds(k)) \rightarrow O(Dnskey(k)) \wedge\\
&\neg H(Dnskey(k)) \rightarrow O(Rrsig(k)) \wedge\\
&(\\
&\quad H(Dnskey(k)) \vee\\
&\quad ksk = Roles(k) \rightarrow \exists k' \in \mathbb{K} \cdot (\\
&\quad\quad zsk \in Roles(k') \wedge\\
&\quad\quad Alg(k) = Alg(k') \wedge\\
&\quad\quad O(Dnskey(k')) \wedge\\
&\quad\quad O(Rrsig(k'))\\
&\quad)\\
&)\\
\}
\end{aligned}
$$

SafeKeys are keys that might be internally inconsistent but for which a consistent counterpart exists.

$$
\begin{aligned}
SafeKeys \equiv \{k | k \in \mathbb{K},\\
&k \in ConsistentKeys \vee\\
&\forall r \in Roles(k) \cdot (\\
&\quad \exists k' \in \mathbb{K} \cdot (\\
&\quad\quad Alg(k') = Alg(k) \wedge\\
&\quad\quad r \in Roles(k') \wedge\\
&\quad\quad k \in ConsistentKeys \wedge\\
&\quad\quad \neg H(Ds(k)) \rightarrow O(Ds(k')) \wedge\\
&\quad\quad \neg H(Dnskey(k)) \rightarrow O(Dnskey(k'))\\
&\quad)\\
&)\\
\}
\end{aligned}
$$

A zone is valid if no single key breaks validity and at least one complete chain for any algorithm exists. An insecure zone is represented by a NULL key.

$$
\begin{aligned}
&Valid(\mathbb{K}) \Leftrightarrow \\
&\quad \forall k \in \mathbb{K} \cdot k \in SafeKeys \wedge \\
&\quad \exists k \in \mathbb{K} \cdot (\\
&\qquad ksk \in Roles(k) \wedge \\
&\qquad O(Ds(k)) \wedge \\
&\qquad O(Dnskey(k)) \wedge \\
&\qquad O(Rrsig(k)) \wedge \\
&\qquad \exists k' \in \mathbb{K} \cdot (\\
&\qquad\quad zsk \in Roles(k') \wedge \\
&\qquad\quad O(Dnskey(k')) \wedge \\
&\qquad\quad O(Rrsig(k')) \wedge \\
&\qquad\quad Alg(k) = Alg(k') \\
&\qquad) \\
&\quad)
\end{aligned}
$$