Experiment 6. Version 2.20 of the PKCS#11 standard includes a new feature intended to improve security: trusted keys. Two more attributes are introduced: wrap_with_trusted and trusted. In addition to testing that a key to be wrapped is extractable, Wrap now tests that if the key to be wrapped has wrap_with_trusted set, then the wrapping key must have trusted set. Only the security officer (SO) can mark a key as trusted. Additionally, wrap_with_trusted is a sticky attribute - once set, it may not be unset.

This mechanism would appear to have some potential: as long as the security officer only logs into the device when it is connected to a trusted terminal, he should be able to keep his PIN secure, and so be able to control which keys are marked as trusted. We took our configuration from Experiment 5, and added the trusted key features, marking n_1 as wrap_with_trusted, and n_2 as trusted. We discover another attack, given in Figure 5. Here, the intruder first attacks the trusted wrapping key, and then obtains the sensitive key.

Initial state: The intruder knows the handles $\mathsf{h}(\mathsf{n}_1, \mathsf{k}_1)$, $\mathsf{h}(\mathsf{n}_2, \mathsf{k}_2)$ and the key k_3; n_1 has the attributes sensitive, extract and wrap_with_trusted whereas n_2 has the attributes extract and trusted set. The intruder also knows the public key $\mathsf{pub}(\mathsf{s}_1)$ and its associated handle $\mathsf{h}(\mathsf{n}_3, \mathsf{priv}(\mathsf{s}_1))$; n_3 has the attribute unwrap set.

Trace:

Intruder:	$\mathsf{k}_3, \mathsf{pub}(\mathsf{s}_1)$	$\rightarrow$	$\mathsf{aenc}(\mathsf{k}_3, \mathsf{pub}(\mathsf{s}_1))$
Set_unwrap:	$\mathsf{h}(\mathsf{n}_3, \mathsf{priv}(\mathsf{s}_1))$	$\rightarrow$	$\mathsf{unwrap}(\mathsf{n}_3)$
Unwrap:	$\mathsf{aenc}(\mathsf{k}_3, \mathsf{pub}(\mathsf{s}_1))$, $\mathsf{h}(\mathsf{n}_3, \mathsf{priv}(\mathsf{s}_1))$	$\xrightarrow{\text{new } \mathsf{n}_4}$	$\mathsf{h}(\mathsf{n}_4, \mathsf{k}_3)$
Set_wrap:	$\mathsf{h}(\mathsf{n}_4, \mathsf{k}_3)$	$\rightarrow$	$\mathsf{wrap}(\mathsf{n}_4)$
Wrap:	$\mathsf{h}(\mathsf{n}_4, \mathsf{k}_3), \mathsf{h}(\mathsf{n}_2, \mathsf{k}_2)$	$\rightarrow$	$\mathsf{senc}(\mathsf{k}_2, \mathsf{k}_3)$
Intruder:	$\mathsf{senc}(\mathsf{k}_2, \mathsf{k}_3), \mathsf{k}_3$	$\rightarrow$	k_2
Set_wrap:	$\mathsf{h}(\mathsf{n}_2, \mathsf{k}_2)$	$\rightarrow$	$\mathsf{wrap}(\mathsf{n}_2)$
Wrap:	$\mathsf{h}(\mathsf{n}_2, \mathsf{k}_2), \mathsf{h}(\mathsf{n}_1, \mathsf{k}_1)$	$\rightarrow$	$\mathsf{senc}(\mathsf{k}_1, \mathsf{k}_2)$
Intruder:	$\mathsf{senc}(\mathsf{k}_1, \mathsf{k}_2), \mathsf{k}_2$	$\rightarrow$	k_1

Figure 5. Attack discovered in Experiment 6