Experiment 3. To prevent the attack shown in Figure 3, we add encrypt and unwrap to the list of conflicting attribute pairs. Another new attack is discovered (see Figure 4) of a type discussed by Clulow, [4, Section 2.3]. Here the key k_2 is first wrapped under k_2 itself, and then unwrapped, gaining a new handle $h(n_3, k_2)$. The intruder then wraps k_1 under k_2, and sets the decrypt attribute on handle $h(n_3, k_2)$, allowing him to obtain k_1.

Initial state: The intruder knows the handles $h(n_1, k_1)$, $h(n_2, k_2)$; n_1 has the attributes sensitive, extract and whereas n_2 has the attribute extract set.

Trace:

Set_wrap:	$h(n_2, k_2)$	$\rightarrow$	$\mathsf{wrap}(n_2)$
Wrap:	$h(n_2, k_2), h(n_2, k_2)$	$\rightarrow$	$\mathsf{senc}(k_2, k_2)$
Set_unwrap:	$h(n_2, k_2)$	$\rightarrow$	$\mathsf{unwrap}(n_2)$
Unwrap:	$h(n_2, k_2), \mathsf{senc}(k_2, k_2)$	$\xrightarrow{\text{new } n_4}$	$h(n_4, k_2)$
Wrap:	$h(n_2, k_2), h(n_1, k_1)$	$\rightarrow$	$\mathsf{senc}(k_1, k_2)$
Set_decrypt:	$h(n_4, k_2)$	$\rightarrow$	$\mathsf{decrypt}(n_4)$
SDecrypt:	$h(n_4, k_2), \mathsf{senc}(k_1, k_2)$	$\rightarrow$	k_1

Figure 4. Attack discovered in Experiment 3