

```

1  (* Bitlocker protocol.
2
3  Found in "Formal analysis of protocols based on TPM state registers."
4  by Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel
5  in Proceedings of the 24th IEEE Computer Security Foundations Symposium
6  (CSF'11), pp. 66–82, IEEE Computer Society Press, Cernay-la-Ville, France, June
7  2011.
8  *)
9
10 (* ****
11    ***   TPM Declaration   ***
12    **** *)
13
14 free c:channel.
15 free pcr:channel [private].
16
17 type type_key.
18
19 free bindk:type_key.
20 free sealk:type_key.
21
22 type private_key.
23 type public_key.
24
25 type value_pcr.
26 free nil:value_pcr.
27
28 (* Functions of the TPM *)
29
30 fun hpcr(value_pcr,bitstring) : value_pcr.
31 free init : value_pcr.
32
33 fun pk(private_key) : public_key.
34 fun certPCR(private_key,value_pcr,bitstring) : bitstring.
35 fun certKey(private_key,public_key,value_pcr) : bitstring.
36
37 reduc forall sk:private_key, v:value_pcr, d:bitstring ;
38 check_certPCR(certPCR(sk,v,d),pk(sk)) = (v,d).
39 reduc forall sk:private_key, v:value_pcr, xpk:public_key ;
40 check_certKey(certKey(sk,xpk,v),pk(sk)) = (xpk,v).
41
42 fun aenc(public_key,bitstring) : bitstring.
43 reduc forall sk:private_key, d:bitstring; adec(sk,aenc(pk(sk),d)) = d.
44
45 free aik:private_key [private].
46 free srk:private_key [private].
47 table keyloaded(private_key,public_key,type_key,value_pcr).
48
49 fun wrap(public_key,private_key,type_key,bitstring,value_pcr) : bitstring.

```

```

50  reduc forall x_pk:public_key, x_key:private_key, t_key:type_key, data:bitstring,
51  x_pcr:value_pcr;
52  unwrap(wrap(x_pk,x_key,t_key,data, x_pcr)) = (x_pk,x_key,t_key,data,x_pcr)
53  [private].
54
55  fun seal(public_key,bitstring,bitstring,value_pcr) : bitstring.
56  reduc forall x_pk:public_key, d:bitstring, p:bitstring, v:value_pcr;
57  unseal(seal(x_pk,d,p,v)) = (x_pk,d,p,v) [private].
58
59  (*****
60  ***   TPM Functionality   ***
61  *****)
62
63  (* The commands *)
64  free load: bitstring.
65  free read: bitstring.
66  free quote: bitstring.
67  free wrap_key : bitstring.
68  free certify : bitstring.
69  free unbind : bitstring.
70  free seal_data: bitstring.
71  free unseal_data: bitstring.
72  free extend : bitstring.
73  free reboot : bitstring.
74  free tpm_proof: bitstring [private].
75
76  (* Read the value of the PCR *)
77  let Read =
78    in(c,=read);
79    in(pcr,v:value_pcr);
80    out(pcr,v);
81    out(c,v).
82
83  (* Generate a certificate of an input value. *)
84  let Quote =
85    in(c,(=quote,x:bitstring));
86    in(pcr,v:value_pcr);
87    out(pcr,v);
88    out(c,certPCR(aik,v,x)).
89
90  (* Create Wrap Key *)
91  let CreateWrapKey =
92    in(c,(=wrap_key,x_pk:public_key,t:type_key,v_lock:value_pcr));
93    in(pcr,v_cur:value_pcr);
94    out(pcr,v_cur);
95    get keyloaded(x_key:private_key,=x_pk,t':type_key,v:value_pcr) in
96    if v = nil || v = v_cur then
97      new key[v_cur,v_lock]:private_key;
98      out(c, (pk(key),wrap(x_pk,key,t,tpm_proof,v_lock))).

```

```

99
100 (* Load wrapped key *)
101 let LoadKey2 =
102   in(c,(=load,x_pk:public_key,x_w:bitstring));
103   let (y_pk:public_key,x_key:private_key,t:type_key,=tpm_proof,x_pcr:value_pcr) =
104   unwrap(x_w) in
105   if pk(x_key) = x_pk then
106     in(pcr,v:value_pcr);
107     out(pcr,v);
108     get keyloaded(x_sk:private_key,=y_pk,t':type_key,v':value_pcr) in
109     if v = v' || v' = nil then
110       insert keyloaded(x_key,x_pk,t,x_pcr).
111
112 (* Certify Key *)
113 let CertifyKey =
114   in(c,(=certify,x_pk:public_key));
115   get keyloaded(x_key:private_key,=x_pk,t:type_key,v:value_pcr) in
116   out(c,certKey(aik,x_pk,v)).
117
118 (* Unbind *)
119 let Unbind =
120   in(c,(=unbind, x_pk:public_key, cypher:bitstring));
121   in(pcr,v:value_pcr);
122   out(pcr,v);
123   get keyloaded(x_sk:private_key,=x_pk,=bindk,v':value_pcr) in
124   if v' = nil || v = v' then
125     out(c,adec(x_sk,cypher)).
126
127 (* Seal *)
128 let Seal =
129   in(c,(=seal_data, d:bitstring, x_pcr:value_pcr, x_pk:public_key));
130   in(pcr,v:value_pcr);
131   out(pcr,v);
132   get keyloaded(x_sk:private_key,=x_pk,=sealk,v':value_pcr) in
133   if v' = nil || v = v' then
134     out(c,seal(x_pk, d, tpm_proof, x_pcr)).
135
136 (* Unseal *)
137 let Unseal =
138   in(c,(=unseal_data, x:bitstring));
139   let (x_pk:public_key,d:bitstring,=tpm_proof,v':value_pcr) = unseal(x) in
140   in(pcr,v:value_pcr);
141   out(pcr,v);
142   get keyloaded(x_sk:private_key,=x_pk,=sealk,v'':value_pcr) in
143   if (v' = nil && v'' = nil) || (v' = nil && v = v'') || (v' = v && v'' = nil) || (v' = v && v''
144   = v) then
145     out(c,d).
146
147 (* Extend *)

```

```

148 let Extend =
149   in(c,(=extend, x:bitstring));
150   in(pcr,v:value_pcr);
151   out(pcr,hpcr(v,x)).
152
153 let Initialisation =
154   insert keyloaded(srk,pk(srk),bindk,nil) | out(c, pk(srk)).
155
156 let Main_TPM =
157   Initialisation | ! (Read | Quote | CreateWrapKey | LoadKey2 | CertifyKey |
158   Unbind | Seal | Unseal | Extend).
159
160 free deny:bitstring.
161
162 (** Alice role **)
163
164 free vmk:bitstring [private].
165 free bios:bitstring.
166 free loader:bitstring.
167
168 fun abs_secret(bitstring,bitstring):bitstring [private].
169
170 let Alice =
171   out(c,(wrap_key,pk(srk),sealk,nil));
172   in(c,(x_pk:public_key,w:bitstring));
173   out(c,(load,x_pk,w));
174   get keyloaded(x_sk:private_key,=x_pk,=sealk,v':value_pcr) in
175   out(c,seal(x_pk,vmk,tpm_proof,hpcr(hpcr(init,bios),loader))).
176
177 let reboot_and_measure_BIOS_and_loader =
178   in(c,(x_bios:bitstring,x_loader:bitstring));
179   in(pcr,v:value_pcr);
180   if x_bios = bios && x_loader = loader
181   then out(pcr,hpcr(hpcr(hpcr(hpcr(init,x_bios),x_loader),deny))
182   else if x_bios = bios
183   then out(pcr,hpcr(hpcr(hpcr(hpcr(init,bios),x_loader))
184   else out(pcr,hpcr(hpcr(hpcr(hpcr(init,x_bios),x_loader),deny))
185
186 let first_boot_measure_BIOS_and_loader =
187   in(c,(x_bios:bitstring,x_loader:bitstring));
188   if x_bios = bios && x_loader = loader
189   then out(pcr,hpcr(hpcr(hpcr(hpcr(hpcr(init,x_bios),x_loader),deny))
190   else if x_bios = bios
191   then out(pcr,hpcr(hpcr(hpcr(hpcr(hpcr(init,bios),x_loader))
192   else out(pcr,hpcr(hpcr(hpcr(hpcr(hpcr(init,x_bios),x_loader),deny))
193
194 let Main_Process =
195   (! (Alice | reboot_and_measure_BIOS_and_loader) ) | Main_TPM |
196   first_boot_measure_BIOS_and_loader.

```

```
197
198 query attacker(vmk).
199
200 process Main_Process | ! in(pcr,x:value_pcr); out(pcr,x)
201
```