Notes About the Simple TPM Attester Protocol

John D. Ramsdell

October 4, 2013

See the associated MITRE Technical Report (MTR) before looking at these notes.

The Simple TPM Attester Protocol (STAP) message algebra displayed in Figure 1 extents the one in the MTR by adding hashing and tags. It also adds the sort M for the state of the TPM, and two operations bt and ex, for boot and extend. Thus a state is a term of sort M.

Sorts:	M	
Operations:	$\mathsf{bt} : \mathsf{M}$	Boot
	$\mathsf{ex} : \top \times \mathsf{M} \to \mathsf{M}$	PCR extension

The *transition relation* is τ, where $(m_0, m_1) \in \tau$ iff $m_1 = \mathsf{bt}$ (boot), $\exists t : \top.\, m_1 = \mathsf{ex}(t, m_0)$ (extend), or $m_0 = m_1$ (observe). An infinite sequence π is a *path* if $\forall i \in \mathbb{N}.\, (\pi(i), \pi(i+1)) \in \tau$.

The encoding of TPM states as messages follows.

$$\begin{aligned} pcr &: \mathsf{M} \to \mathsf{S} \\ pcr(\mathsf{bt}) &= \mathsf{s}_0 \\ pcr(\mathsf{ex}(t, m)) &= \#(t, pcr(m)) \end{aligned}$$

Theorem 1 in the state world is imported into the strand space world as a bridge lemma.

Sorts:	$\top$, A, S, D, E, M		
Subsorts:	$\mathsf{A} < \top$, $\mathsf{S} < \top$, $\mathsf{D} < \top$, $\mathsf{E} < \top$		
Operations:	$(\cdot, \cdot)$	$: \top \times \top \to \top$	Pairing
	$\{\!\lvert \cdot \rvert\!\}_{(\cdot)}$	$: \top \times \mathsf{A} \to \top$	Asymmetric encryption
	$\{\!\lvert \cdot \rvert\!\}_{(\cdot)}$	$: \top \times \mathsf{S} \to \top$	Symmetric encryption
	$(\cdot)^{-1}$	$: \mathsf{A} \to \mathsf{A}$	Asymmetric key inverse
	$(\cdot)^{-1}$	$: \mathsf{S} \to \mathsf{S}$	Symmetric key inverse
	$\#$	$: \top \to \mathsf{S}$	Hashing
	$\mathsf{a}_i, \mathsf{b}_i$	$: \mathsf{A}$	Asymmetric key constants
	s_i	$: \mathsf{S}$	Symmetric key constants
	d_i	$: \mathsf{D}$	Data constants
	e_i	$: \mathsf{E}$	Text constants
	g_i	$: \top$	Tag constants
	bt	$: \mathsf{M}$	TPM boot
	ex	$: \top \times \mathsf{M} \to \mathsf{M}$	TPM extend
Equations:	${\mathsf{a}_i}^{-1} = \mathsf{b}_i \quad {\mathsf{b}_i}^{-1} = \mathsf{a}_i$		$(i \in \mathbb{N})$
	$\forall k \colon \mathsf{A}.\, (k^{-1})^{-1} = k$		$\forall k \colon \mathsf{S}.\, k^{-1} = k$

Figure 1: Crypto Algebra with State Signature

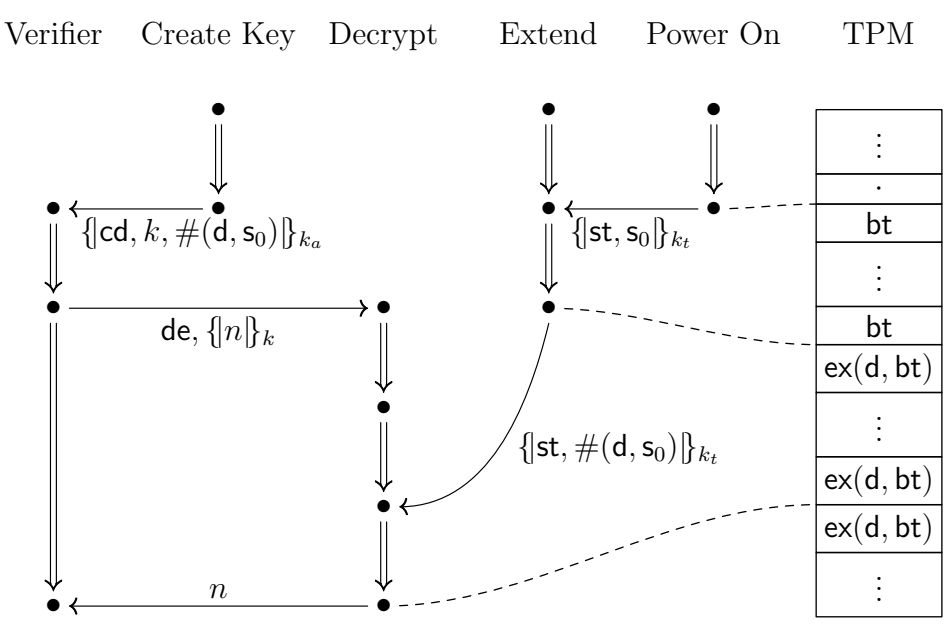

Figure 2: STAP Message-Passing and State History

Theorem 1 (Stable Boot Extend)**.**

$$
\begin{array}{l}
\forall \pi \in \mathit{path}, t\colon \top, i, j \in \mathbb{N}. \\
\quad i < j \wedge \pi(i) = \mathsf{bt} \wedge \pi(k) = \mathsf{ex}(t, \mathsf{bt}) \supset \\
\qquad \exists j \in \mathbb{N}. \\
\qquad\quad i \leq j \wedge j < k \wedge \pi(j) = \mathsf{bt} \wedge \\
\qquad\quad \forall \ell \in \mathbb{N}.\, j < \ell \wedge l \leq k \supset \pi(\ell) = \mathsf{ex}(t, \mathsf{bt})
\end{array}
$$

Much text has yet to written following this point...

Annotated STAP Roles. Some of the tags used in the protocol.

$\mathsf{st} = \mathsf{g}_0$	State
$\mathsf{cd} = \mathsf{g}_1$	Key Created
$\mathsf{de} = \mathsf{g}_2$	Decrypt
$\mathsf{d} = \mathsf{g}_3$	Desired PCR Value

STAP Shape. The shape and its connection to state is in Figure 2.