System Security

Jing Jin 11/29/10

Flicker (Cont’d)

Flicker: TCB- PAL itself

SKINIT – “Dynamic root of trust”

- Disable interrupts
- Disable DMA to PAL

• All in the memory loaded before executing SKINIT
  → Doesn’t clear memory

• Quote (data)
  Returns signature $\text{sig}(S_H, h \mid | \text{data})$

- Set up PAL
- Set up inputs
- Save state of OS
- SKINIT

***** PAL execute *****

- $C = \text{quote(NULL)}$
  Return (outputs, c)

Example: SETI @ home

$$h = H(H(H(\text{PAL}) \mid | \text{inputs}) \mid | \text{outputs}) \mid | 0)$$

$$C_{\text{PAL}} = \text{Sig}(S_H, h \mid | \text{NULL})$$

OS should trust the PAL, the PAL should trust OS
- H (PAL) is SKINIT saved in the hardware
- The PAL did some extend operations
- “0” is the end of computation

Verifier (NASA)
- Verify $C_H$ and extend $P_H$
- Recompute $h$ from PAL, inputs and outputs

Recomputed the correct hash function, $H$ is the public well-known hash function
- Verify $C_{PAL}$ using $h$ and $P_H$

PAL trusted?
- SandBox PAL e.g. NaCl
- Prevent special instructions
- Limited computation time

Therefore PAL might sometimes fail to generate outputs

When jmp, it can go to an counter, when the counter goes back to 0, it will return.

Every time the verifier sees the jmp, it will
\[
\begin{align*}
\text{dec} & \quad \text{JMPCTR (Jump counter)} \\
\text{be} & \quad \text{RETFUNC (to springboard)} \\
\text{jmp} & \quad \text{br0}
\end{align*}
\]

Downside:

SKINIT is a slow instruction. The transition between App os and PAL is expensive and slow.
Flicker VS Terra

- Flicker: setup time overhead
- Terra: VM overhead
- Flicker: exclusion

-/+ Flicker: Small Code

Small code: small trust computing base ---- Good

Flicker cannot easily support large secure components ---- not good

- OS: agnostic

In Flicker, we should trust TCM. Different OS has different implements of PAL.

- NASA doesn’t need to trust the flicker module.
- When OS is commuting with the flicker, it will stop all the interrupts.
- User should not trust PAL, but, trust that PAL cannot take control over OS and rewrite it.
- How? Inline Reference Monitors
- So if OS receives requests from Apps saying ‘Please run by PAL’, OS will follow the steps of verifying PAL code.

The system cannot do anything unless Flicker completed its tasks