TPM-Software für Linux

Trusted Platform Modules nach TPM-2.0-Spezifikation lassen sich jetzt leichter unter Linux nutzen. Entwickler von Intel, Infineon und Fraunhofer SIT haben ein Open-Source-Programmpaket für TPM-Sicherheitschips auf GitHub veröffentlicht.

Die Kooperationspartner wollen die Verbreitung von TPMs in Embedded Systems für IoT, Fahrzeuge, Medizintechnik, Kassensysteme und dergleichen fördern. Dazu steht eine freie Version der Enhanced System API (ESAPI) des standardisierten TPM 2.0 Software Stack (TSS2) bereit. Eine Nutzungsmöglichkeit ist OpenSSL, dafür gibt es die tpm2-tss-engine.

Ein **TPM stellt ähnliche Funktionen wie eine SmartCard bereit**, etwa geschützten Speicher für kryptografische Signaturen und Hash-Werte. Außerdem führt das TPM einige sicherheitskritische Krypto-Funktionen selbstständig und unabhängig vom eigentlichen System aus. Dadurch sind diese Funktionen gut gegen Manipulationen geschützt – ähnlich wie die PIN-Prüfung am Geldautomaten in der Chipkarte oder beim Handy in der SIM-Karte. Außer Infineon liefert etwa auch STMicro diskrete TPM-2.0-Chips, weiter verbreitet zumindest in x86-Systemen sind aber Firmware-TPMs (fTPMs).

(ciw@ct.de)

TPM-2.0-Chips wie der Infineon SLB9665TT20 lassen sich nun leichter unter Linux nutzen, etwa für OpenSSL.

Kurz & knapp: Embedded Systems

Das **ATX-Netzteil Bicker BEA-750H mit zusätzlichem 24-Volt-Ausgang** versorgt außer einem PC-Mainboard noch weitere Systemkomponenten. Es liefert insgesamt 500 Watt, die 24-Volt-Schiene ist mit 7 A belastbar.

Phytec fertigt **Entwicklerboards mit dem ARM-SoC NXP i.MX8**. Der Chip vereint bis zu acht Rechenkerne der Typen Cortex-A72, -A53 und -M4F und steuert bis zu 64 GByte LPDDR4-Speicher an. Außerdem sind DSP- und GPU-Kerne eingebaut.

Das SD Port Lock CSK-SDD10 von Smartkeeper **sichert SD-Kartenleser gegen unbefugte Nutzung** und lässt sich nur mit einem speziell kodierten Schlüsselwerkzeug entfernen. Ähnliche „Schlösser" gibt es nun auch für USB Typ C, HDMI und eSATA.

Kontron hat mit dem TRACe HMID104 ein **lüfterloses 10-Zoll-Bedienterminal für Schienenfahrzeuge mit Touchscreen** im Angebot. Es ist mit Intels Atom E3845 (Bay Trail) bestückt und erfüllt Eisenbahn-Vorschriften wie DIN EN 50155.

Anzeige

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover