De Trusted Boot Module – hardware en software voor het beschermen van gedistribueerde systemen

De Trusted Boot Module is een combinatie van software en hardware die bedoeld is om eenvoudige (ARM-gebaseerde) systemen, waaronder de Raspberry Pi maar ook routers en zelfs laptops, te beveiligen. De door Whitebox Systems ontwikkelde Trusted Boot Module omvat hardware die samenwerkt met vertrouwde (trusted) boot management software, die als eerste op het systeem draait. Deze software valideert *images* die een operating systeem en applicaties bevatten, om te zien of deze images ondertekend zijn door een vertrouwde partij. Door het systeem regelmatig te herstarten en steeds te controleren of het systeem de laatst beschikbare software draait kan voorkomen worden dat kwetsbaarheden blijvend op een systeem aanwezig blijven.

Het platform waarvoor de TBM is ontwikkeld en als eerste wordt gebruikt is de Whitebox. Dit is een gedistribueerd systeem bestaande uit ARM-gebaseerde servers (Whiteboxen) die bij huisartsen staan waarmee zij op een controleerbare en veilige manier gegevens kunnen uitwisselen met andere artsen. De Whitebox gebruikt het LIME2 ontwikkelbord van Olimex, waarop Linux-gebaseerde, voor beveiliging geoptimaliseerde software is geïnstalleerd die specifiek voor de Whitebox is ontwikkeld. Het onderliggende code signing model van de Whitebox is gebaseerd op reproduceerbare builds en een eenvoudig hiërarchisch vertrouwensmodel, maar andere trust modellen zijn ook mogelijk.

Het TBM project brengt de mogelijkheid voor *trusted boot* naar de markt van eenvoudige ARM-gebaseerde servers en services. Het systeem is geschikt voor toepassingen met een eenvoudig vertrouwensmodel waarbij één ondertekenaar van software vertrouwd wordt, maar ook voor complexere gedistribueerde systemen waarin meerdere partijen kunnen ondertekenen en, bijvoorbeeld, reboots op regelmatige basis georkestreerd kunnen worden. De TBM hardware bevat een klok waarmee de TBM op regelmatige tijdsintervallen een harde reset van het moederbord kan forceren.

De TBM software en hardware is volledig open source en aan te passen naar wens. De componenten zijn eenvoudige *off-the-shelf* componenten waaronder een microcontroller unit (MCU) en SPI-flash memory. Het moederbord heeft alleen een *read-only* geheugen nodig waarin de vertrouwde software wordt opgeslagen die als eerste opstart. In veel systemen (zoals de Raspberry Pi) is hiervoor reeds een speciaal soort flashgeheugen zoals SPI-NOR aanwezig. De vertrouwde software communiceert met de Trusted Boot Module om informatie zoals de (gevalideerde) softwareversie door te geven vóórdat deze (onvertrouwde) software wordt opgestart, om te kunnen voorkomen dat het systeem later misleid kan worden om alsnog verouderde, onveilige software te draaien. Doordat de boot management software en de trusted boot module software niet gemodificeerd kunnen worden, wordt voorkomen dat compromittering van software die op het systeem draait een blijvend effect op de integriteit van het systeem kan hebben.

Het voorkomen van permanente compromitering van een device is van belang voor de Whitebox, maar ook voor veel andere gedistribueerde systemen, die in toenemende mate gevoelige gegevens verwerken en die door de complexiteit van de software die zij draaien gevoelig zijn en blijven voor compromittering. Zo draagt het systeem bij aan een veiliger internet.

De *blueprints* van de TBM alsmede de software die op de TBM draait zijn vrij beschikbaar via https://opensource.whiteboxsystems.nl/ en interessant voor alle ontwikkelaars van gedistribueerde systemen die gebruik maken van ARM-gebaseerde of andere gedistribueerde hardware. Het systeem is eenvoudig en goedkoop en door zijn opzet – in tegenstelling tot andere systemen die *trusted boot* mogelijk maken, zoals de Trusted Platform Module (TPM) of UEFI – eenvoudig te controleren op correctheid.

Ontwikkelaars die direct met een TBM aan de slag willen, kunnen de hardware bij Whitebox Systems bestellen. Het project is mede mogelijk gemaakt door een subsidie van Stichting NLnet.