EXPERTARTIKEL

Azure Sphere ger dig trygga rötter i en otrygg IoT-värld

Av Leif Wartacz, Elfa Distrelec

Leif Wartacz är regional säljchef på Elfa Distrelec för norra Europa. Han har en elektronikutbildning i grunden och utnyttjar sin erfarenhet från elektronikindustrin till att göra verklig skillnad när det gäller utvecklingen av Elfa Distrelecs verksamhet i regionen.

Beteckningen IoT, Internet of Things, kan vara svår att få grepp om. Det är ett paraplybegrepp som väsentligen omfattar alla elektroniska komponenter som kan anslutas, samverka eller utbyta data. Det smarta hemmet och smart hälsovård är bara två av oräkneliga exempel på tillämpningar som presenterats för IoT. Men bortsett från den smarta marknadsföringen och de allomfattande begreppen finns en aspekt som de flesta kan hålla med om: att produkterna typiskt har stora brister när det handlar om cybersäkerhet.

Säkerheten hos komponenter och system anslutna till Internet är en evig utmaning eftersom nya sårbarheter sprids och exploateras dagligen. Smart Home-produkter med undermålig säkerhet, nu senast babymonitorer, har skapat oönskade rubriker under de senaste åren. Att koppla upp en simpel styrkretsbaserad produkt till Internet på ett tillförlitligt och säkert sätt känns nästan omöjligt, i alla fall vid första anblicken. Microsoft har dock utvecklat en ny strategi tillsammans med sin hårdvarupartner MediaTek, där de inte bara tillhandahåller hårdvara och ett IoT-ekosystem, utan också har säkerheten inbyggd och dessutom på ett sätt som går att uppgradera.

MICROSOFTS PLATTFORM Azure Sphere sätter Internet-säkerheten i fokus. Lösningen står på tre ben: en säkrad mikrokontroller (MCU), ett säkrat operativsystem (OS) och en nyckelfärdig säkerhetsfunktion.

Den säkrade MCU:n innehåller en IP-kärna kallad Pluton Security Subsystem, som implementerar en så kallad root-of-trust. Härifrån utförs autentisering mot molntjänsten och här exekveras kryptografiska funktioner på säkert lagrade privata lösenord. Stöd erbjuds också för programuppdateringar over-the-air (OTA). Genom att dessa funktioner lyfts bort kan övriga kärnor fokusera på realtidsbearbetning, på tillämpningens funktion och på datakommunikationen.

Det säkrade operativsystemet är baserat på en anpassad Linux-kärna med en säkerhetsmonitor som skyddar åtkomst till kritiska resurser. Det här är en lösning som ger ökad stabilitet. Den tillhandahåller containers som medel för programmerarna att dela upp tillämpningskoden i separata bitar.

Den tredje benet i säkerhetsplattformen är Azure Sphere Security Service. Denna molnlösning erbjuder en kontinuerlig övervakning av eventuella hot och är den som förmedlar den ”trust” som utgår från root-of-trust, mellan de enheter som använder Azure-tjänsten. Säkrade firmware-uppdateringar kan skickas ut till IoT-noder och autentisering ser till att endast genuin maskinvara kan laddas med utvecklarens applikationskod. Också fel som uppstår i fält eller indikationer på missbruk kan upptäckas med plattformen.

En av de första komponenter som erbjöd åtkomst till Azure Sphere-ekosystemet var MediaTek MT3620 MCU, en styrkrets med trippelkärna, integrerat wifi-block och Pluton Security Subsystem. Här finns en Arm Cortex-A7 som kan köras i upp till 500 MHz och dessutom två Arm Cortex-M4F på upp till 200 MHz. Alla tre kan köra tillämpningskod. A7-kärnan lämpar sig bäst för tillämpningskod på hög nivå, medan M4F-dubbelkärnan kan ta hand om realtid och annan lågnivåkod. Kringutrustning kan kopplas till alla tre kärnorna.

Wifi-delsystemet kontrolleras av en fjärde processor med en 32-bitars RISC-kärna (N9), dual-band 802.11a/b/g/n, basband och MAC. Den här uppdelningen är utformad för att ge låg strömförbrukning och ser till att den trådlösa anslutningen får hög kapacitet utan att belasta prestandan i övriga systemet.

SLUTLIGEN, en femte processor, också den med en Cortex-M4F-kärna, levererar cybersäkerhet och robust strömhantering för hela MCU:n. Här finns root-of-trust, en slumptalsgenerator med entropiövervakning och motåtgärder mot fysisk manipulering och sidokanalsattacker.

Totalt har MCU:n omkring 5 MB inbäddad SRAM och 16 MB seriellt flashminne (SiP). Efter att operativsystemet Linux har laddats finns det fortfarande kvar omkring 512 KB SRAM för binärkoden till en Azure Sphere-tillämpning, med 256 KB tillgängligt under exekvering. Enligt dokumentationen kan det i en del fall finnas en viss flexibilitet i dessa begränsningar.

Låg effekt är givetvis en nyckelfaktor när du överväger olika plattformar för IoT-tillämpningar. MT3620 drar mellan 0,01 mA

och 0,02 mA på lägsta effekt då endast realtidsklocka (RTC) är i drift. Den högre effektförbrukningen gäller för fall där den interna strömhanterings-IC:n (PMIC) används. Väckning från detta lågeffektläge kräver bara 24 ms, inklusive PLL-lås och uppstart av kristalloscillator. Med wifi i lätt viloläge ligger effektförbrukningen på 220 mA (i värsta fall 380 mA) och upp till 520 mA (i värsta fall 750 mA) med allting i drift.

Att komma igång är enkelt eftersom tillverkarna följt trenden att bygga små enkortsdatorer (SBC) med enkla anslutningar i form av plug-on-sköldar. Azure Sphere MT3620 Development Kit har två inbyggda wifi-antenner, samt två kontakter för externa antenner. Åtkomst till kringutrustning på chipet fås via två rader med dubbla kontaktdon. Kortet inkluderar även tryckknappar, en knapp för systemåterställning, LED:s för användare och status samt en strömmatande mikro-USB-kontakt som också används som debug-gränssnitt.

Enheten programmeras och felsöks med Microsofts integrerade utvecklingsmiljö Visual Studio, tillsammans med Azure Sphere SDK. Runtime-miljön baseras på en delmängd ur POSIX-standarden och består av bibliotek som ger tillgång till kringutrustningen och annan funktionalitet via körtidstjänster. Generisk I/O eller interprocesskommunikation (IPC) är blockerad på grund av säkerhetskonfigurationen. Men efter autentisering med Azure Sphere kan applikationskoden samverka med molntjänster och utnyttja de http(s)-bibliotek som tillhandahålls.

Tillvägagångssättet för programvaruutveckling fungerar lite annorlunda än det för en MCU utan operativsystem. Utvecklaren måste skaffa ett Microsoft Azure-konto och paxa enheten för sig själv (claim), vilket innebär att enheten kopplas till Azure Sphere-innehavaren. Åtgärden är därefter oåterkallelig. Därefter rekommenderas du att konfigurera wifi-anslutningen eftersom det är via denna länk som uppdateringarna till Azure Sphere OS kommer att laddas ned för installation. Detta sker sedan var 24:e timme för att hålla systemet uppdaterat.

KORTET LEVERERAS i låst tillstånd, vilket innebär att ingen kod kan laddas upp till kortet. Utvecklingsmiljön tillhandahåller ett kommandoradsgränssnitt för att låsa upp och programmera kortet, varefter kodutvecklingen fortsätter på ungefär samma sätt som vid typisk utveckling av inbyggda system. Programvarubiblioteken innehåller också en omfattande loggfunktion för att stödja felsökning och felanalys.

För snabb prototyputveckling krävs en lösning för att snabbt kunna sätta upp maskinvara runt en programmerbar plattform som implementerar ens idé. Azure Sphere Grove Starter Kit erbjuder en lösning för dessa situationer. I paketet ingår en skärm med sex kontakter för att underlätta anslutningen av den medföljande sensorn samt ingångs- och utgångskorten. Dessa består av sju kort och inkluderar produkter som en OLED-display, ljussensor, ett relä, en tryckknapp och en temperatursensor. Allt är snyggt förpackat och det ingår en anslutningskabel samt en beskrivning av modulens funktioner och de elektriska specifikationerna.

Efter åratal av uppståndelse runt IoT och prat om användningsområden och marknadssegment som kommer att gynnas, tycks det äntligen finnas en plattform som förenklar den mest komplexa aspekten: säkerheten. Azure Sphere bakar in säkerheten i maskinvaran och länkar detta till en säker molnlösning, vilket säkerställer att den vanliga kompromissen – programmets funktionalitet kontra dess säkerhet – inte längre är föremål för diskussion. Genom att lägga ut upptäckten av hot till en plattform som hanterar dem dagligen, kan utvecklare och produkttillverkare fokusera på produktdifferentieringen med vetskapen om att säkerheten är tryggad. ■