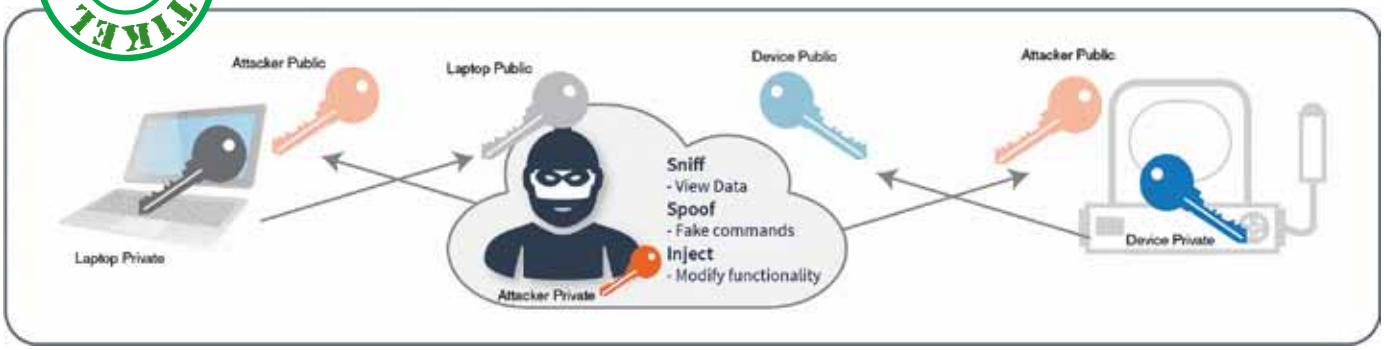
EXPERTARTIKEL



Säkerhet signerad GHS

En autentiseringskedja rotad i hårdvara kan verifiera din produkts integritet

Av Darryl Parisien, Integrity Security Services

Darryl Parisien är Darryl Parisien har 20 års erfarenhet av att leda industriella projekt inom rymd, militär & försvar och mjukvaruutveckling. Han har arbetat med affärsföretag och inbyggnadsföretag med fokus på bland annat säker kommunikation och säkerhet inom sjukvården. Ett patent har han också tagit – på en metod för att autentisera och säkra inbyggnadsenheter.

När man konstruerar för säkerhet måste driftsmiljön bestämma vilken grad av robusthet som krävs. En säkerhetsarkitektur kan inte bara omfatta målenheten, utan alla även ändnoder och användare i det övergripande systemet. Förvisso finns serienummer, MAC-adresser, vitlistning och svartlistning men sådana lösningar är inte idiotsäkra. De flesta intrång på inbyggda system sker genom att man övervakar nätverkstrafik för att rekonstruera kommandon och sedan upprepa samma kommandon eller modifierade versioner, från en annan plats.

I IoT-världen är alla din fiende tills motsatsen bevisats. Även privata nät utsätts för dataintrång och är lika känsliga som Internet. Eftersom inget nät är säkert måste alla fjärranslutna ändnoder autentiseras innan deras kommandon och data går att lita på.

För fri passage från människans till datorns värld används motsvarigheten till det magiska lösenordet: en nyckel. En lösning som bygger på hemliga nycklar duger för mindre sammanhang, men när antalet enheter växer ökar komplexiteten och kostnaden för att skydda dessa nycklar. Om en hemlig nyckel röjs efter intrång i en enda enhet blir samtliga system i miljön öppna för intrång och det går inte längre att skilja vänner och betrodda system från fiender.

MED HJÄLP AV ANVÄNDARNAMN och lösenord går det att dynamiskt generera unika hemliga nycklar, som skrivs in på anmodan och som inte behöver lagras i icke-flyktigt minne, vilket minskar risken för intrång. Även om detta fungerar i vissa system, saknas i andra produkter konceptet ”användare” och de måste kunna fungera med integritet omedelbart när de slås på. Dessa miljöer kräver gemensamma hemliga nycklar mellan båda ändnoderna för autentisering och kryptering.

Men hur kommer dessa nycklar in i systemet? I militära miljöer används speciella handdatorer som kallas nyckelfyllningsenheter (key fill devices) för att fysiskt ladda hemliga nycklar. Systemen är utformade med en ”Fill Port” för att överföra nycklar utan att de exponeras. Nyckelfyllningsenheter och nyckelhanteringssystem skyddar nycklar under distributionen fram till dess att de lagrats innanför enhetens eget säkerhetsstängsel.

Kryptering med hjälp av publika nycklar är mindre komplext än delade nycklar eftersom varje ändnod har ett unikt asymmetriskt nyckelpar för kryptering respektive autentisering – bra säkerhetssystemen använder aldrig samma nyckel för båda. Om en ändnod komprometteras och den privata nyckeln exponeras har skadan begränsats till just det systemet

ASYMMETRISK KRYPTERING tillåter ändnoder att kommunicera säkert utan att behöva dela nycklar på förhand. Men hur kan en enhet veta att den kommunicerar säkert med rätt ändnod? Här används certifikat för att förhindra man-i-mitten-attacker under utbyte av publika nycklar och för att verifiera identiteten på ändnoder. I sin grundläggande form består ett certifikat av metadata som namn, serienummer, utgångsdatum med mera och är kopplat till den publika nyckeln med en digital signatur från en certifieringsmyndighet (Certificate Authority, CA). Ömsesidig autentisering ser till att enheter aldrig svarar på inkommande kommandon om de inte kommer från en giltig källa. Också företagets IoT-tjänster är skyddade genom att de endast svarar på enheter med korrekta behörigheter.

När två system utbyter certifikat kan de publika nycklarna litas på om de båda är certifierade av samma CA. Eftersom båda systemen litar på CA, kan förtroendet utvidgas till hela fjärrsystemet förutsatt att de privata nycklarna inte är komprometterade. När väl programmet är autentiserat och pålitligt kan det läsa certifikatet för att avgöra vilka åtgärder som ska vidtas och vilka systemfunktioner som skall öppnas. Det betyder till exempel att enheter kan skiftas över till felsökningsläge under begränsad tid baserad på teknikerns utbildningsnivå.

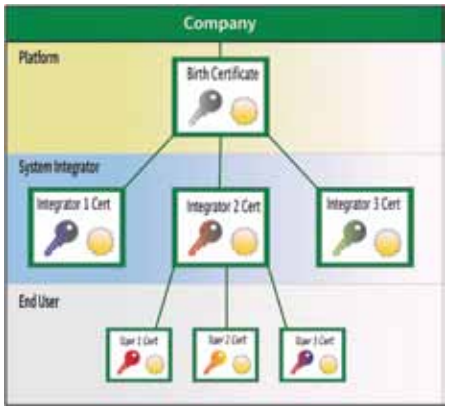
DET FINNS FLERA certifikatgenererings- och hanteringssystem som kan hjälpa utvecklare av inbyggda system att integrera digitala identiteter i sina produkter. Specifikationen IEEE 802.1ar är ett av de som används alltmer i inbyggda produkter som nätverkssystem och industriella styrsystem. 802.1ar berör hanteringen och användningen av ett enskilt iDevID eller flera LDevID-certifikat. iDevID-certifikatet är också känt som ”fö- ▶

delsecertifikat" och används för att identifiera tillverkaren av systemet, kortet eller komponenten. Detta är vanligen systemets primära certifikatet, genererat under tillverkningen. Syftet med LDevID:er varierar beroende på miljön. Exempelvis kan i en produkt ett LDevID-certifikat skapas för att skydda kundprofiler och data. I ett annat exempel kanske ett kort ska säljas till flera integratörer, som alla vill ha kryptografisk separation från sina konkurrenter. Korttillverkaren kanske vill ladda ner säkra mjukvaruuppdateringar och samla in telematik, medan integratörer vill skydda sina immateriella rättigheter. Ett LDevID-certifikat kan genereras för varje integratör så att den kan kommunicera säkert inom sina egna lokala enklaver och skydda sina data utan risk för intrång.

VID INFÖRANDE AV CERTIFIKAT i ett inbyggt system måste utvecklare och tillverkare ta hänsyn till följande:

- Programmera Root CA certifikatet i icke skrivbart minne för att hindra angripare från att ändra innehåll.
- Asymmetrisk nyckelparsgenerering – privata nycklar ska aldrig exponeras utanför enheten under förutsättning att korrekt slumptalsgenerering är möjlig.
- Skydd av privat nyckel – spoofing-attacker är möjliga om privata nycklar kompromitteras.
- Sändning av certifikatsigneringsförfrågningar till CA-systemet – om du använder ett CA-system, hur påverkas produktionen av ett nätverksavbrott?
- Mottagande av certifikat och skyddad lagring – hur skyddas certifikat och nycklar på enheten?
- Hämtning av initiala återkallelselistor – syftar på hela lagringshanteringsprocessen och spårning av behöriga system och RMA:er.

ALLT FLER PRODUKTUTVECKLARE bygger sina egna publika nyckelinfrastrukturer (public key infrastructures, PKI) och genererar certifikat direkt under tillverkningen så att privata nycklar aldrig lämnar sina enheter och produktionen inte påverkas av Internetavbrott. INTEGRITY Security Services, Device Lifecycle Management (DLM) system skyddar företagets CA-nycklar från IT-nätverk som är mottagliga för dataintrång på andra tillverkningsorter och tillverkning hos tredje part för att generera högtillgängliga certifikat. DLM stöder utvecklare som vill integrera certifikat, skräddarsydda för sin konstruktions- och försörjningskedja, utan att behöva bygga och stödja sin egen PKI.



Det viktigaste övervägandet i diskussionen om autentisering är hur kan vi lita på andra om vi inte kan lita på oss själva? Tyvärr är det inte en filosofisk fråga. Om systemprogrammet äventyras är förtroendekedjan bruten från början och inget kan garanteras. Hackad programvara kan hoppa över verifiering, acceptera vilket certifikat som helst och ändra meddelandens innehåll. Nycklar kan äventyras om de inte är ordentligt skyddade och användas för att attackera andra enheter genom att manipulera kommandon och data. Bakdörrar kan öppnas för att samla in och skicka data, vilket gör alla säkerhets- och autentiseringssystem meningslösa.

Innan ett inbyggt system kan lita på sin egen förmåga att autentisera fjärranslutna ändnoder måste det kontrollera att den egna programvaran inte har ändrats. Detta sker genom en process kallad secure boot, där systemprogramvaran verifieras innan den körs. Vid varje strömpåslag kontrolleras autenticiteten i varje mjukvarulager innan det exekveras. Detta garanterar att programmet inte är skadat och att det kommer från en giltig källa. Ett komponent exekveras bara om den är verifierat pålitlig.

HASH:AR OCH CHECKSUMMOR kontrollerar endast programmets integritet, inte dess autenticitet. Så länge en angripare ändrar hash:en tillsammans med koden kan skadlig programvara fortfarande köras oupptäckt. Autentisering åstadkommes genom digital signering av hash:en med en asymmetrisk nyckel. Ett företags säkerhetsinfrastruktur skyddar den privata nyckeln och signerar den aktuella programreleasen. Motsvarande publika nyckel programmeras in i enheten under tillverkning och används under verifiering. Om en angripare ändrar både kod och hash, kan de fortfarande inte uppdatera den digitala signaturen utan att motsvarande privata nyckel återställer den digitala signaturen.

INTEGRITY Security Services arbetar med företag inom alla branscher med att införa secure boot-lösningar, inklusive digitala signeringsinfrastrukturer med nollexponeringsskydd för privata nycklar och integration i de vanligaste mjukvarubyggprocesserna.

Säkerhetsarkitekturen hos dagens uppkopplade IoT-produkter måste kunna hantera fler okända hot än någonsin tidigare. Varje ny enhet som läggs till nätverket adderar ytterligare okända hot och risker för konflikter som orsakar kostnader för utveckling och support. Dessa okända hot motverkas genom att man ser till att kommmunicera endast med ändnoder som verifierats via autentisering. Genom att låta hårdvaran verifiera programvaran innan enheten kopplas upp, bevaras förtroendekedjan. ■