# Skydda det smarta hemm

*Det finns goda skäl att oroa sig eftersom IoT-system utsätts för cyberattacker.*


## Av Hal Kurkowski och Scott Jones, Maxim Integrated

**Hal Kurkowski** är chef över affärsenheten Micros & Security på Maxim Integrated där han har varit engagerad i säkerhetsrelaterade produkter i över 30 år, om man räknar in hans år på Dallas Semiconductor, som Maxim köpte 2001. Han har en magisterexamen i elektroteknik från University of Illinois i Urbana-Champaign.

**Scott Jones** leder en grupp på Maxim Integrated som jobbar med produkter för säker autentisering. Med 15 års erfarenhet på Maxim hanterar han produktlinjer och ansvarar för slutkunders affärsutveckling. Innan han kom till Maxim tillbringade han 15 år dels som applikationsingenjör, dels i olika konstruktörsroller inom hårdvara/mjukvara på Dallas Semiconductor och andra teknikföretag.


Halvvägs till jobbet börjar du tvivla på om du verkligen släckte ljuset i sovrummet. Men du behöver inte åka tillbaka – lampan kan du numera släcka från en mobilapp.

Smarta hem-enheter för belysning, säkerhet, temperaturkontroll och andra tillämpningar gör livet enklare. Men det finns en oro över vad som kan hända om dessa till synes oskyldiga IoT-tjänster blir hackade. Det kan leda till potentiellt farliga situationer.

Många Internetanslutna barnmonitorer saknar grundläggande säkerhetsfunktioner och är sårbara. Det rapporterade Rapid7, en cybersäkerhetsfirma i Boston, i fjol. Bland bristerna fanns dolda lösenord som inte gick att ändra, enkel åtkomst av kontonummer samt okrypterade dataströmmar. Inkräktare kunde inte bara titta på andras barn över live-videoströmen, utan dessutom sända sina egen röst och video över systemet.

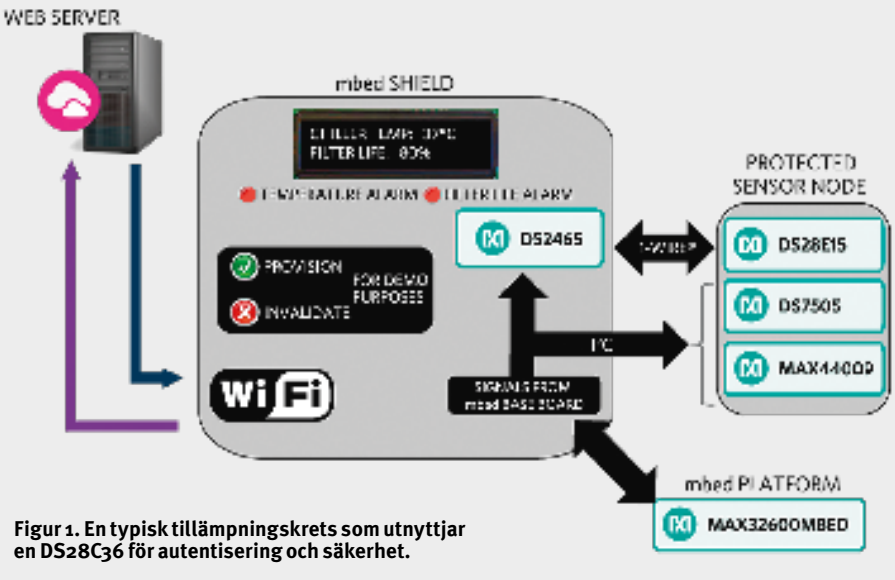
I höstas användes hackade övervakningskameror i en storskalig DDoS-attack (Distributed Denial of Service) som fick många populära webbplatser att gå offline, inklusive Amazon, Tumblr, PayPal och Reddit.

Uppenbarligen finns det goda grunder för konsumenter att oroa sig. Också företag har motsvarande bekymmer, med kloning, förfalskning, reverse engineering och de skador på varumärket som sådana angrepp kan medföra.

Därför måste säkerheten alltid sättas i främsta rummet i designprocessen, och detta tidigt, när det handlar om smarta uppkopplade produkter i hemmet.

**GARTNER RÄKNAR MED** att det kommer att finnas 20,8 miljarder uppkopplade ting i världen år 2020, jämfört med 6,4 miljarder i år.

Det är en stor ökning på väldigt kort tid, och en stor marknadsmöjlighet som inga företag vill missa.




**Figur 1. En typisk tillämpningskrets som utnyttjar en DS28C36 för autentisering och säkerhet.**

Men, som Gavin Kenny konstaterar på IBM-bloggen Security Intelligence, ”I tävlingen om att bli först på marknaden och svara upp mot behovet av lättkonfigurerade produkter, har säkerheten på många IoT-produkter blivit sorgligt lidande” [1]

Vad skulle det krävas för att konstruera in mer säkerhet i smarta hem-produkter?

För det första måste man hantera det faktum att många IoT-enheter är integrerade i nätverk och att komprometterad säkerhet i en enda enhet därmed potentiellt kan utsätta också andra enheter för angrepp.

För det andra måste man integrera säkerhet tidigt i processen och på alla nivåer, från sensornod och chips till hela systemet, och ända upp i molnet.

I sitt blogginlägg argumenterar Gavin Kenny för att säkerheten i sig måste vara intelligent, ”den måste vara automatiserad, självunderhållande, adaptiv och kanske till och med kognitiv”.

**UR KONSTRUKTIONSSYNPUNKT** är det viktigt att verifiera att anslutningar och gränssnitt uppfyller alla relevanta standarder. Kvalitetskontrollerande test ska användas för att undanröja potentiella problem.

Metoder som säker boot, säker nyckelförvaring, kryptering och autentisering är centrala.

Säker boot innebär att elektronikenheten endast kan exekvera autentiserad (det vill säga betrodd) programvara. Styrkretsen innehåller programvara som inte kan ändras. Det kallas för en ”root-of-trust”. När styrkretsen startas körs först denna programkod. Alla tillämpningsprogram är signerade och startas inte förrän deras signatur verifierats, vilket sker med hjälp av en offentlig nyckel som är installerad i styr-

# et från säkerhetsintrång


**Figur 2. Den här ARM mbed-baserade IoT-referenskonstruktionen kan användas för att autentisera IoT-noder, skydda industriella tillämpningar från förfalskning, spåra produktlivslängd, leverera smarta meddelanden och invalidera osäkra industriella sensornoder.**

kretsen. Den säkrade styrkretsen garanterar att systemet startar i en känd och trygg miljö och lagrar dessutom krypteringsnycklar on-chip. Utöver det, kan den användas på normalt sätt – köra program, ta emot sensoravlösningar och annan indata, och styra utsignaler.

Säker tvåvägsautentisering – att två enheter båda bevisar sin identitet mot den andra – skyddar mot attacker. För ändamålet används kryptoalgoritmer med symmetriska nycklar, som SHA-x (Secure Hash Algorithm). Här använder värd och slav samma hemliga nyckel och båda måste hålla den säker mot röjande attacker.

**TVÅ UTMANINGAR** med symmetriska nycklar är (1) distribution och administration av nycklar, och (2) att skydda den hemliga nyckeln hos både värd och slav. Eftersom värd och slav använder samma unika hemliga nyckel, måste man använda en metod för att etablera och härleda nycklar, för att förhindra att antalet nycklar växer ohanterligt.

För att slippa dessa problem kan man använda asymmetriska nycklar istället, till exempel ECDSA (Elliptic Curve Digital Signature Algorithm).

Asymmetriska nycklar har olika värden, men de är relaterade matematiskt. Värden använder en öppen nyckel (som inte behöver hållas hemlig) och slaven använder motsvarande privata nyckel (som måste hållas hemlig).

ECDSA är att föredra eftersom den som administrerar autentiseringen av perferienheterna då inte behöver lagra en hemlighet; tvärtom kan nyckeln distribueras helt öppet. Asymmetriska algoritmer löser både nyckeldistributionsproblemet och behovet av att säkra nyckeln i värdsystemet.

I vissa system kan det finnas behov av att gå bortom att bara autentisera periferienheter, sensorer och förbrukningsmateriel mot värdsystemet. Det kan behöva säkerställas att data som övervakas och skickas från sensor till aggregerings- eller beslutspunkt inte har modifierats. Eller att styrsignaler som skickas till en ventil eller manöverdon inte komprometterats. En verifierad datakedja från sensornod till webbserver eller från webbserver till system och styrdon kan vara en central faktor i att ett system kan betraktas som säkert.

**DET ÄR DEN UNDERLIGGANDE** tekniken som är grunden för säkra IoT-konstruktioner. Styrkretsar med integrerad avancerad kryptografi och integrerad fysisk säkerhet kan ge ett starkt skydd mot både fysisk manipulering och piratkopiering och sidokanalsattacker.

En säkerhetslösning kallad DeepCover används i styrkretsar från Maxim bland annat i form av integrerad säker NVSRAM som omedelbart raderas när intrång upptäcks.

Dessa lågeffektskretsar innehåller FIPS-certifierade kryptomotorer i hårdvara med stöd för standardalgoritmer, och patenterad realtidskryptering av kod och data för att fullt ut skydda externa minnen.

En DeepCover Secure Authenticator från Maxim skyddar kvalitet och säkerhet, stoppar förfalskning, ger säker boot, kontrollerar användningen, säkrar upp GPIO och autentiserar periferienheter. De har också en sofistikerad form av fysiskt skydd (Figur 1).

**FÖR ATT SKYDDA** känsliga data från fysisk manipulering eller manipulering av miljön erbjuder Maxim DeepCover Security Managers. De kombinerar sofistikerad fysisk säkerhet med non-imprinting memory.

Maxim erbjuder en ARM mbed-baserad referenskonstruktion för cybersäkerhet kallad MAXREFDES143# IoT. Den underlättar processen att utveckla smarta och säkra uppkopplade produkter (Figur 2).

Konstruktionen säkrar industriella sensorer och sensornoder via autentisering och via meddelanden som skickas över Wifi mellan noden och en webbserver hos Maxim. Det här visar möjligheten att slippa lagra säkra nycklar i processorminnet.

Algoritmen SHA-256 används för symmetriska nycklar och du kan snabbt integrera din egen tillämpning. Du hittar konstruktionen på mbeds webbplats.

**SAMMANFATTNING.** I tävlingen om att komma först till marknaden med nästa smarta, uppkopplade produkt för hemmet – som alla måste ha – har ingen råd att försumma säkerheten. Teknik som säker boot, säker nyckellagring, autentisering och kryptering kan hjälpa dig att göra hemmet smartare och säkrare. Dessutom ger integrerade kretsar med inbyggd säkerhet dig ett försprång och en stark grund att bygga vidare på. ■

**KÄLLOR:** [1] https://securityintelligence.com/smart-homes-need-smart-security/