Priemyselné systémy potrebujú dodatočnú ochranu pomocou bezpečnostných integrovaných obvodov

Donedávna sa väčšina priemyselných riadiacich systémov (ICS – Industrial Control System) vyvíjala s dôrazom na vysokú spoľahlivosť, bezpečnosť a maximálnu prevádzkyschopnosť. Desaťročia sa priemysel zameriaval na plnenie týchto požiadaviek bez akéhokoľvek dôrazu na digitálnu bezpečnosť. Až v roku 1990 začali vládne agentúry utajene skúmať kybernetickú bezpečnosť pre kritické infraštruktúry (napr. distribúcia elektrickej energie). S príchodom Stuxnetu sa však kybernetické útoky namierené na priemyselné riadiace systémy stali kľúčovou témou všetkých zainteresovaných.

Ohrozenie priemyselných riadiacich systémov

Pripúšťam, že diskusia o všetkých ICS náchylných na útoky by si zaslúžila oveľa viac priestoru. Musíme však obmedziť článok na niekoľko dôležitých ICS. V tomto článku budú spomínané tri rôzny typy:

- Programovateľné logické automaty (PLC), ktoré sa plošne používajú na automatizáciu výrobných procesov alebo riadenie subsystémov. PLC sú často pripojené ako súčasť širšej infraštruktúry.
- SCADA systémy, ktoré monitorujú a riadia geograficky distribuovanú kritickú infraštruktúru (rozvod vody alebo systémy distribúcie elektrickej energie).
- Distribuované riadiace systémy (DCS), ktoré riadia výrobné procesy (chemická výroba a výroba elektrickej energie) všeobecne obsahujú niekoľko automatizovaných subsystémov.

Implementácia týchto systémov sa značne líši na základne konečného priemyselného použitia. Niektoré systémy sú fyzicky koncentrované s obmedzením na definované výrobné zariadenia alebo sa nachádzajú na rozľahnej geografickej oblasti. Všetky systémy však pracujú na základe osobitných výkonnostných očakávaní alebo obmedzení. Napríklad SCADA systém musí mať vysokú úroveň prevádzkyschopnosti – ideálne „päť 9s“ alebo „šesť 9s“ („päť 9s“ znamená 99,999% dostupnosť, ktorá je ekvivalentná 5 minútam prestojov ročne). Pri iných ICS sú najväčším obmedzením systému reakčné časy.

Priemyselné riadiace systémy môžu byť veľmi podobné, ale aj veľmi odlišné. V súčasnosti vidíme dva hlavné trendy. ICS sú čoraz viac prepojené a používajú štandardizované komponenty ako pracovné stanice, ktoré sa môžu spoľahnúť na štandardný softvér (napríklad operačný systém Microsoft Windows®) alebo komunikáciu cez IP. Tieto trendy otvárajú nové nebezpečné možnosti pre kybernetické útoky.

Použitie IT technológie v priemyselnom prostredí nie je vždy ideálne

ICS systém, ktorý musí fungovať v rámci svojich konkrétnych výkonnostných cieľov alebo obmedzení, začal čoraz častejšie využívať technológie z IT oblasti. Bezprostredným dôsledkom konvergencie týchto technógií je, že niektoré hrozby pre štandardné IT komponenty sa vzťahujú aj na ICS. Lenže kvôli rozdielnym výkonnostným cieľom a pracovnému prostrediu, nie sú bezpečnostné prostriedky používané v IT svete nevyhnutne využiteľné v ICS.

Ešte predtým než sa ponorím do problematiky, uvediem jednoduchý príklad. SCADA systém monitoruje tlak chladenej vody v priemyselnom zariadení. Ak zistí stratu tlaku, spustí alarm. V takomto potenciálne-núdzovom stave sa očakáva od operátora okamžitá reakcia.

Teraz si predstavte odozvu operátora v klasickej IT infraštruktúre. Po niekoľkých minútach nečinnosti sa PC stanica pravdepodobne sama uzamkne. Operátor musí zadať svoje prihlasovacie meno a heslo, zvyčajne po troch neúspešných pokusoch sa stanica uzamkne opäť. IT operátor musí kontaktovať administrátora a ten mu heslo zresetuje. Čas beží... Podobný postup by bol v priemyselnom prostredí devastujúci. Operátor ICS by mal reagovať okamžite, akékoľvek otáľanie predstavuje kritickú stratu častu. Čiže tento štandardný IT postup nie je použiteľný v ICS.

Hrozby pre priemyselné riadiace systémy

Človek sa nemôže spoliehať len na vlastnú architektúru ICS, ktorá by ho chránila pred elektronickými hrozbami. Historicky dané, kybernetické útoky neboli považované za závažné ohrozenie riadiacich systémov, pretože ICS siete boli buď izolované alebo nekopírovali štandardy IT. Môžeme z toho toho vyvodiť tri závery:

1. Riadiace a automatizačné siete musia komunikovať s inými systémami, a preto sú čoraz viac prepojené so štandardnými a otvorenými sieťami.
2. Pomocou reverzného inžinierstva je možné priemyselný proprietárny protokol relatívne ľahko (za primeranú cenu) „napadnúť a ovládnuť“. Prípadné nedostatky protokolu nemusia byť preskúmané, pochopené a ani odstránené. Je nebezpečné sa domnievať, že proprietárny protokol ponúka istotu len preto, že informácie nie sú voľne dostupné. Prístup „bezpečnosť cez nezrozumiteľnosť“ je zavádzajúci a zlý, riziko je obrovské.[1] Slabé miesta nezabezpečených proprietárnych protokolov ostro kontrastuje s otvorenými protokolmi, ktorých hrozby a obmedzenia sú dobre známe.
3. Siete nepredstavujú jedinú cestu pre kybernetické útoky. Izolovaný ICS môže byť ohrozený útokom z USB disku alebo z konzoly údržby.

Rovnako ako priemyselné siete nepoužívajú zdokumentované a známe protokoly, takisto aj proprietárna architektúra PLC zvyčajne neponúka bezpečnú ochranu. Dobrou ukážkou je bohužiaľ Stuxnet. Stuxnet totiž útočil len na proprietárny softvér a na PLC s konkrétnou konfiguráciou. Tento malware by sa nepodarilo navhrnúť bez dôverného pochopenia špeficického cieľového systému. „Systémová bezpečnosť by nemala byť závislá na utajení realizácii alebo implementácii jej komponentov.“[2] Tento prístup ohrozuje hardvér – v tomto prípade PLC. Takže znova: človek sa nemôže spoliehať na ochranu pred elektronickými hrozbami pomocou vlastnej architektúry ICS.

Aj keď majú ICS odlišnú architektúru od typickej IT infraštruktúry a plnia aj iné úlohy, hrozby pre IT sektor môžu ovplyvniť aj ICS. Zoznam týchto hrozieb je bohužiaľ dlhý a znepokojúci: malware, vírusy, softvérové alebo hardvérové zmeny, falošné správy alebo príkazy od útočníka, krádež identity alebo neoprávnené monitorovanie. Sme vo veľmi náročnej situácii. Bezpečnostné hrozby pre ICS sú podobné tým z IT oblasti, ale špecifické požiadavky pre operácie v priemysle neumožňujú používať známe bezpečnostné protiopatrenia!

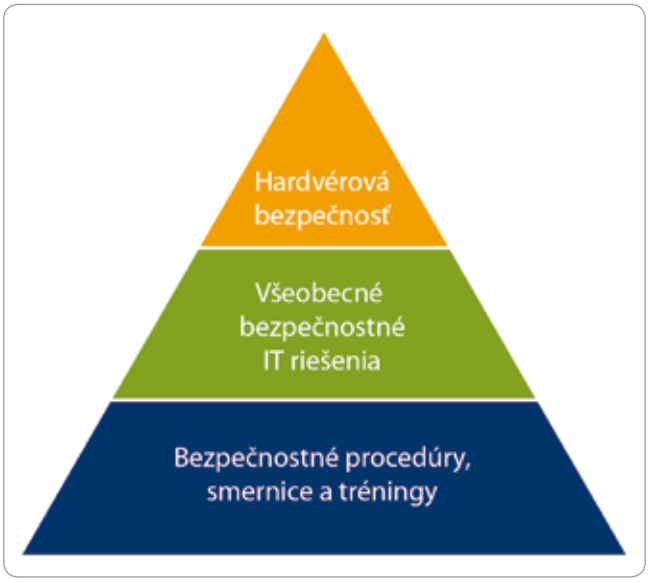
Implementujte najvyššiu úroveň protiopatrení priamo do ICS

Čoraz častejšie sa kvôli obavám o bezpečnosť priemyselných a automatizačných aplikácií implementujú protiopatrenia a zmierňujúce akcie. Doteraz bola väčšina týchto obranných opatrení

zahrnutá v bezpečnostných postupoch, prostredníctvom fyzickej ochrany a vo vzdelávaní obsluhy. ICS však zostával zraniteľný. Predtým, ako sa prikloním ku kritike priemyselnej komunite kvôli týmto bezpečnostným opatreniam, musím pripomenúť, že podobne začala starostlivosť o bezpečnosť v tradičnej IT oblasti. Toto je skutočne prvý stupeň ochrany – základ, ktorým sa naštartuje celý proces.

Tradičné obranné taktiky v žiadnom prípade neposkytujú maximálnu úroveň ochrany potrebnej pre ICS. Pravidelne kontrolované postupy sa nedodržiavajú na 100%, fyzická ochrana – zamykanie dverí sa dá obísť a nedá sa použiť vo všetkých prípadoch. Je dôležité si uvedomiť, že manuálne obranné postupy nepokrývajú útoky uskutočnené vysoko kvalifikovanými ľudmi s časom a finančným pozadím potrebným na vypracovanie najnáročnejších scenárov. Existujú ešte horšie prípady, kedy podplatení operátori ICS cielene obchádzali postupy.

Odpoveď na bezpečnosť je už v hardvéri ICS. Vyššie úrovne bezpečnostných protiopatrení obsahujú všeobecné IT prvky zabezpečenia, ako je kryptografia a hardvérové zabezpečenie (obr 1.)



Obr. 1

Všeobecné bezpečnostné riešenia IT sú už niekedy implementované priamo v softvéri. Niektoré infraštruktúry sú chránené firewallom, iné používajú zabezpečené protokoly ako TLS/SSL. Hoci sú všetky stupne pyramídy nevyhnutné, my si teraz popíšeme ako prináša hardvérová bezpečnosť najvyššiu úroveň ochrany.

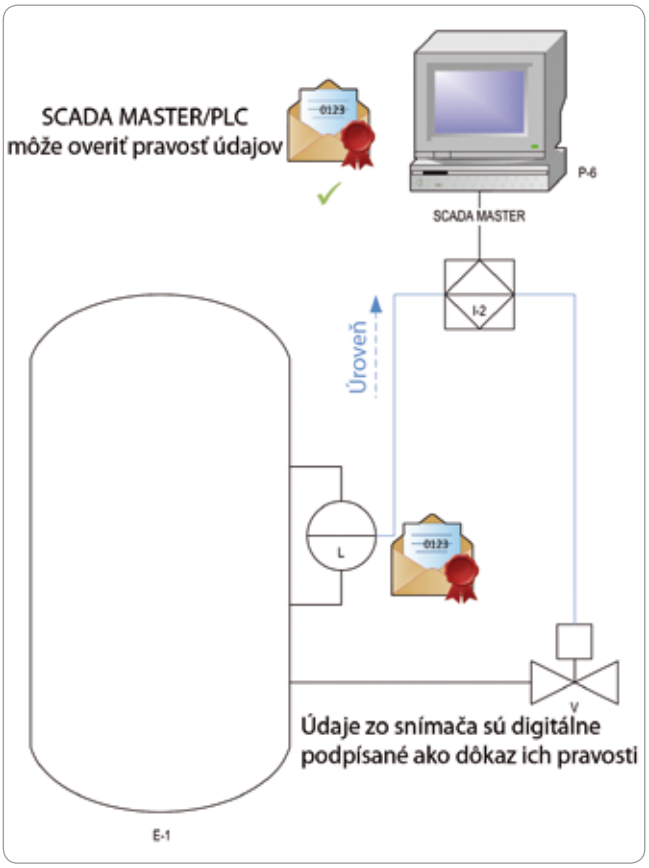
Chráňte ICS integrovanou kryptografiou

Všeobecné IT spôsoby nemôžu byť systematicky aplikované na rôzne ICS v priemysle. Jedna technológia, často používaná v IT svete, však realizovateľná je: šifrovanie.

Kryptografia chráni pred väčšinou vyššie uvedených hrozieb. Napriek tomu to nie je kúzelná palička, jej využitie nemôže vyzerať ako „Pridám šifrovanie do môjho ICS a hneď bude zabezpečený“. Šifrovacie algoritmy a protokoly sú stavebné kamene, ktoré by mali byť implementované od prípadu k prípadu, po dôkladnej analýze hrozieb pre každý subsystém. Šifrovanie je spoločný nástroj pre ICS a IT infraštruktúru, ale implementácia v ICS musí byť prispôsobená konkrétnemu systému. Poznáme veľa kryptografických techník, no pre ICS sú najdôležitejšie dve: digitálny podpis a šifrovanie. Preskúmame opodstatnenosť obidvoch techník v ICS prostredí.

Digitálny podpis. Táto technika sa používa na overenie správ, objednávok alebo softvérových komponentov. Uvažujeme o dvoch prípadoch pre ICS:

1. V SCADA systéme musíte dôverovať informáciám prichádzajúcim z prevádzkového snímača. Musíte vedieť, že informácie prišli zo skutočného snímača (z jeho fyzickej reprezentácie), a nie sú to informácie od útočníka, ktorý chce narušiť systém. RTU (Remote Terminal Unit) najprv overí, či informácie zaslané digitálnym snímačom skutočne prichádzajú z reálneho a povoleného zariadenia (obr. 2). Tento postup funguje aj opačným smerom, t.j. aj v zostupnom poradí ku aktuátoru a je podpísaný jeho pôvodcom. Rovnaký prístup môže byť použitý na komunikáciu medzi RTU, PLC a hlavným SCADA systémom.



Obr. 2 Digitálny podpis aplikovaný na výstup snímača

2. Digitálne podpisy umožňujú systému kontrolovať, či softvér alebo aktualizácia softvéru pochádza z dôveryhodného zdroja. Ako príklad opäť použijeme Stuxnet. Škodlivý kód bol aplikovaný do PLC a pohonov pri predvídanej rýchlosti. To spôsobilo, že PLC spustil nesprávny výrobný proces.[3] Ak je však softvér a aktualizácia sofvéru digitálne podpísaná ešte pred stiahnutím do PLC, ten overí pravosť softvéru pred jeho vykonaním.

Rovnaký princíp môže chrániť systém proti zmene v konfigurácii hardvéru. Útočník by mohol zmeniť kalibračné údaje snímačov - nesprávne nakonfigurované snímače by mohli poslať chybné informácie do hlavného systému, ktorý následne narušil priemyselné procesy. Zvlášť náchylné sú rozsiahle systémy rozprestierajúce sa na veľkých geografických oblastiach (napr. distribúcia vody), v ktorých sa nedá zabezpečiť fyzický prístup ku každému snímaču v prevádzke. Tento problém rieši digitálny podpis. Pred odoslaním nameraných informácií nadradenému systému, môže snímač súčasne poslať aj „podpísané“ kalibračné údaje. Prípadne si môže nadradený systém vyžiadať podpísanú odpoveď s kalibračnými alebo konfiguračnými údajmi.

Digitálny podpis sa môže použiť aj na overenie hardvéru, čo je výhodné, ak je RTU pripojené k SCADA sieti. Samozrejme, že nikto nechce, aby neznámy (t.j. neoverený) hardvér prijímal a odosielal dôležité informácie. Na vybudovanie kritických ICS sa preto používa iba originálny hardvér. Digitálny podpis tento hardvér overuje a tým vytvára dôveru.

Šifrovanie je užitočná a často používaná obranná technika pred zverejnením informácií. Pre podnik sú najdrahšie výrobné „recepty“, keďže môžu obsahovať know-how potrebný na výrobu produktov. Monitorovaním parametrov z aktuátorov alebo údajov zo snímačov by sa dali získať cenné informácie o výrobnom procese, či dokonca aj osobné údaje. Na trhu je mnoho publikácii o útočníkoch, ktorí zistili

správanie užívateľov pomocou sledovania ich spotreby elektrickej energie cez Smart Grid. Šifrovanie údajov v ICS sieťach by takýmto útokom mohlo zabrániť rovnako ako v klasickej IT infraštruktúre.

Prečo bezpečnostné integrované obvody podporujú kryptografiu?

Zatiaľ sme sa zaoberali iba aplikáciami kryptografie na zabezpečenie ICS. Kryptografia je často implementovaná priamo v softvéri, tak prečo by sa mali používať bezpečnostné integrované obvody v ICS? Existuje mnoho dôvodov prečo bezpečnostné integrované obvody ponúkajú výhody: bezpečné uskladnenie kľúčov, ochrana pred odhalením kľúča prostredníctvom špeciálnych útokov, bezchybná a jednoduchá implementácia šifrovania, zrýchlenie výpočtov, kvalita náhodných čísel a nahrávanie dôveryhodného softvéru prostredníctvom zabezpečeného zavedenia systému.

Bezpečné uskladnenie kľúčov

Táto koncepcia je bez preháňania dôležitá: akákoľvek bezpečnostná implementácia musí používať štandardné šifrovacie algoritmy (napr. AES, Triple DES pre symetrické šifrovanie, RSA, ECDSA pre šifrovanie s verejným kľúčom). V rámci šifrovacích systémov sú najcennejšie kľúče. Čiže ak je šifrovanie zavedené pomocou softvéru a štandardného procesora, potom sa šifrovacie kľúče nachádzajú vo všeobecnej systémovej pamäti a sú ľahko získateľné pomocou malwaru, ladiaceho portu JTAG alebo fyzického vniknutia. Bezpečnostné systémy výrazne znižujú tieto zraniteľnosti.

- Bezpečnostné mikroprocesory majú integrovanú logickú ochranu. Bezpečné zavedenie systému a jednotka správy pamäte (Memory Management Unit) chráni pred infikovaním malwarom. Prot JTAG je možné zakázať.
- Bezpečnostné integrované obvody majú vstavané ochranné prvky, ako je kovové krytie, snímače okolitého prostredia alebo vonkajšie snímače proti fyzickému vniknutiu. Okrem toho môžu mať zakódovanú nielen vnútornú, ale aj vonkajšiu pamäť. Najvyššia úroveň ochrany predstavuje automatické zničenie kľúčov pri neoprávnenej manipulácii.

Ochrana pred odhalením kľúčov pomocou špeciálnych útokov

Spotreba elektrickej energie v mikrokontroléri je úmerná jeho aktivite. Sledovaním spotreby energie počas šifrovania je možné získať šifrovacie kľúče. Iné špeciálne útoky sú založené na elektromagnetickom žiarení (EMA).

Najvyspelejšie bezpečnostné systémy však majú ochranu pred špeciálnymi útokmi a kľúče nie je možné týmto spôsobom získať.

Implementácia dôveryhodnej a bezchybnej kryptografie

Spoločnou slabinou v systémoch integrujúcich kryptografiu je čiastočná alebo „falošná“ implementácia algoritmu. Chybný algoritmus spôsobuje zraniteľnosť ICS a môže umožniť úspešné útoky už niekoľko mesiacov po predstavení produktu.

Ale ak projektant ICS používa bezpečnostné integrované obvody už od systémového návrhu, môže si byť istý, že implementácia algoritmov bude bez chýb. Táto úroveň bezpečnosti sa ďalej zvyšuje certifikáciou podľa noriem a testovaním tretími stranami.

Zrýchlenie výpočtov

U ICS je často rozhodujúcim faktorom doba odozvy. Na zaslanie nameraných údajov zo snímača do RTU v SCADA systéme je napríklad zadefinovaný určitý časový interval. Bezpečnostné integrované obvody ponúkajú vyšší výkon ako softvérové riešenia – hlavne kvôli implementovanému hardvérovému šifrovaniu. Snímače môžu získať digitálny „podpis“ ešte pred odoslaním aj napriek tomu, že radič snímača má obmedzený výpočtový výkon. Bezpečnostné integrované obvody môžu odľahčiť aplikačný procesor aj keď má obmedzené výpočtové prostriedky.

V najmenších – najviac obmedzených systémoch (moduly snímačov zvyčajne obsahujú 8bitový mikrokontrolér) je nedostatočný výpočtový výkon na realizáciu sofistikovaných matematických operácií. V týchto situáciách je jedinou možnosťou pridanie bezpečnostného integrovaného obvodu, inak by sa musel celý systém prepracovať.

Bezpečnostné mikrokontroléry môžu pridať aj kompletné bezpečnostné riešenia, ako je napríklad podpora protokolov TLS/SSL.

Kvalita náhodných čísel

Bežne používaný útok proti systémom chráneným kryptografiou sa nazýva opakovaný útok. Koncept je pomerne jednoduchý: útočník zaznamenáva šifrované alebo podpísané správy (aj keď ich nemôže dešifrovať alebo pochopiť) a zachytenú správu pošle o chvíľu neskôr. Náš príklad s digitálnym podpisom snímača dobre ilustruje spomínaný problém. Prepodkladajme, že tlak vody vo vzdialenom potrubí je v rámci predpísaných hodnôt. Snímač hlási normálny tlak v potrubí a zašle túto správu do SCADA systému. Útočník túto správu zaznamená. Keď neskôr snímač zistí neštandardný tlak, útočník zasiahne. Pošle správu nahranú skôr a systém sa tvári, že pracuje v štandardnom režime. Klasickou ochranou proti takémuto typu útoku je zavedenie náhodných čísel do prenosu, čo zabraňuje spätnému využitiu predchádzajúceho prenosu.

Nie všetky generátory náhodných čísel sú rovnakej kvality. Existujú prípady, kedy útočník získal tajný kľúč zo systému s nekvalitným generátorom náhodných čísel. To je najhoršia situácia, akú si môžete predstaviť. Kryptografia sa stávy zbytočnou.[4] Ako sa to stalo? Generátor náhodných čísel v bezpečnostných integrovaných obvodoch spĺňa náročné kritéria v podmienkach entropie a je testovaný použitím štandardizovaných metód.

Dôveryhodný softvér cez bezpečné zavedenie systému

Brilantným predstaviteľom tejto témy je bohužial opäť Stuxnet. Systémoví operátori a projektanti musia zabezpečiť, aby všetko vybavenie SCADA alebo DCS systému malo identifikovateľný originálny kus softvéru. Bezpečné zavedenie systému a manažment bezpečnostných aktualizácií sú spôsobom ako chrániť zariadenie pred malware alebo pred implementovaním nedôveryhodného softvéru. Bezpečné zavedenie systému a manažment bezpečnostných aktualizácií sú implementované do najnovších a najmodernejších bezpečnostných mikrokontrolérov.

Bezpečnostné integrované obvody sú hlavné ochranné zariadenia dneška

Dnešné bezpečnostné integrované obvody obsahujú mnoho funkcií s cieľom zaistiť bezpečnosť ICS alebo iného kritického systému pracujúceho 24/7.

Autentifikačné integrované obvody, ako je DS28E15 umožňujú silné šifrovanú autentifikáciu subsystému z alebo do hlavného systému. Ich súčasťou je autentifikačný protokol SHA-2 a obvod dokáže autentifikovať rozširovacie I/O moduly PLC. Môžu bezpečne ukladať a digitálne podpisovať konfiguračné alebo kalibračné údaje zo snímacieho modulu a brániu útočníkom nahradiť zariadenia alebo meniť kľúčové parametre.

Bezpečnostní manažéri bezpečne ukladajú tajné kľúče. DS3654 dokáže v prípade detekcie prieniku zničiť všetky kľúče. Bezpečnostný manažér MAX36025 podporuje AES autentifikáciu a šifrovanie. Bezpečnostní manažéri sa môžu pridať do existujúceho mikrokontroléra a odbúrajú portovanie softvéru z predchádzajúcich verzií.

Bezpečnostné mikrokontroléry poskytujú bezpečné ukladanie kľúčov, umožňujú bezpečné spúšťanie systému, aktivujú softvérovú logickú ochranu a ponúkaju väčšiu flexibilitu kryptografie až do úrovne PKCS#11. Taktiež podporujú sieťové protokoly a môžu odbremeniť hlavný systémový procesor od kryptografických operácií. Nový ARM926 mikrokontrolér MAX32590 s operačným systémom Linux®BSP je jednočipové riešenie slúžiace na zabezpečenú komunikáciu zariadení.

Záver

Povedali sme mnoho a núka sa jedna otázka: „Takže pred kybernetickými útokmi sme chránení používaním bezpečnostných integrovaných obvodov?“ Odpoveď však nie je jednoduchá. Kompletný bezpečnostný systém vyžaduje dôkladnú identifikáciu a hĺbkovú analýzu hrozieb ešte pred praktickým nasadením akéhokoľvek riešenia. Efektívna bezpečnosť do značnej miery závisí od realizácie mnohých kryptografických opatrení, ktoré spájajú softvér a hardvér.

O AUTOROVI

Christophe Tremlet je bezpečnostný segmentový manažér v Maxim Integrated vo francúzskom La Ciotat. Pracoval 13 rokov v divízii inteligentných kariet STMicroelectronics – 10 rokov ako produktový inžinier a produktový manažér a tri roky ako aplikačný manažér. Následne dva roky pracoval ako hlavný technologický šéf pre Innova Card, ktorú neskôr akvizovala spoločnosť Maxim Integrated Products. Je držiteľom magisterského titulu v odbore elektrotechnika z INSA Lyon vo Francúzsku.

Referencie

1. Scarfone, Karen, Jansen, Wayne, a Tracy, Miles, NIST Special Publication 800-123, Sprievodca základnou bezpečnosťou serverov, júl 2008, http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
2. Ibid
3. Správa Symantecu o Stuxnet, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
4. Viac informácií o DSA požiadavkách na náhodné hodnoty, pozri Lawson, Nate, „DSA požiadavky na náhodné hodnoty K,“ root labs rdist, 10. november, 2010, http://rdist.root.org/2010/11/19/dsa-requirements-for-random-k-value /.

Prvýkrát publikované v EE Times, Industrial Control Design Line. Publikované so súhlasom autora.

-mk-