Bezpečnosť v automatizácii
Možnosti uplatnenia a špeciálne požiadavky

Stefan Heiss
Oliver Puls

Prednosti neobmedzenej komunikácie procesných dát prostredníctvom štandardného ethernetového protokolu cez komplexné siete (intranet a internet) a spracovanie týchto dát v štandardných IT produktoch ako Windows CE sú všeobecne uznávané a akceptované, a to vďaka tomu, že:

- ethernet je všeobecný a otvorený štandard, ktorý zaisťuje homogénne sieťové prostredie a komunikáciu rôznych typov zariadení,
- všeobecne používanie jedinej sieťovej zbernice uľahčuje programovanie, konfiguráciu a monitorovanie zariadení na úrovni prevádzky „cez celú sieť“,
- štandard je bežne rozšírený v kancelárskom prostredí, možno na ďalšie spracovanie dát využívať (monitoring, SCADA ap.) aj pomerne lacné komponenty.

Z hľadiska bezpečnosti informačných technológií však tieto výhody skrývajú niektoré riziká:

- Prítomnosť ethernetu a ethernetových protokolov TCP/IP alebo UDP/IP dáva potenciálnym útočníkom pomerne ľahký prístup do siete. Znalosti potrebné na poškodenie sú všade k dispozícii a z internetu si možno stiahnuť príslušné nástroje.
- Neúmyselná chybná konfigurácia komponentov (napríklad zadanie zlej IP adresy) môže viesť k poruchám stroja alebo zariadenia.
- Pri štandardnom hardvéri a softvéri nie je pre útočníka ťažké využiť známe slabé miesta, napríklad v podobe „pretečenia vyrovnávacej pamäte“.

Celkovo platí, že technológie, ktoré sa dnes používajú v kancelárskom prostredí, majú okrem uvedených predností aj svoje špecifické nedostatky. V kancelárskom prostredí treba teda používať zároveň osvedčené bezpečnostné riešenia. Pritom musíme mať na zreteli špeciálne požiadavky na automatizačnú techniku, ako je odolnosť a jednoduchá konfigurovateľnosť.

Zabezpečenie verzus bezpečnosť informačných technológií

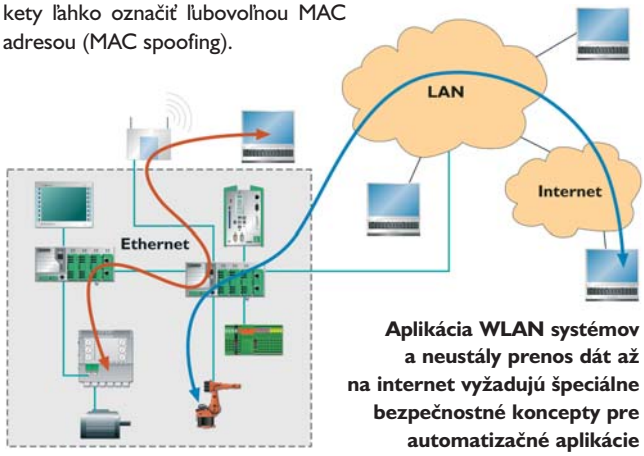
Zabezpečenie informačných technológií rieši predovšetkým ohrozenie, ktorému sú vystavené informačné systémy a v nich prítomné dáta. Toto ohrozenie pramení predovšetkým z možného aktívneho prieniku útočníka, ktorý má prístup do systému alebo ho dokáže v prípade úspechu získať. Ako príklad možno uviesť sabotáž alebo špionáž. Pojem sabotáž tu budeme používať v širokom význame a budeme do neho zahrnovať aj nešpecifické DoS útoky, ktoré napríklad pri zaútočení na firemný intranet pomocou malwaru, vírusu alebo červov môžu mať vplyv aj na integrovanú automatizačnú sieť.

Aspekty ako odolnosť proti výpadkom a riziko spôsobené chybnou obsluhou patria do kategórie bezpečnosť. Medzi obidvoma kategóriami neexistuje zreteľná hranica. Odolnosť komponentov proti výpadkom ako klasické kritérium bezpečnosti informačných technológií sa vzhľadom na požiadavky na vysokú dostupnosť systémov v prípade niektorých typov útokov stáva skôr aspektom zabezpečenia informačných technológií. Typickým mechanizmom zaisťujúcim bezpečnosť informačných technológií je ochrana pred chybnými krokmi obsluhou formou autentifikácie a autorizácie používateľov.

Riziko prameniace z pripojenia infikovaného notebooku k firemnej sieti patrí do oblasti zabezpečenia informačných technológií, pretože nebezpečenstvo tu predstavuje malware. Tento príklad ukazuje na potrebu predchádzať bezpečnostným rizikám v IT (často v prvom rade) vhodnými organizačnými opatreniami (napr. zavedenie a používanie bezpečnostnej politiky). Technické opatrenia na ochranu technológií možno zmysluplne aplikovať až na základe pravidiel stanovených bezpečnostnou politikou.

Riešenia z oblasti kancelárskych aplikácií

V zásade platí, že je nevyhnutné kontrolovať prístup ku kritickým sieťovým segmentom. Pri použití v kancelárskom prostredí sa ponúkajú osvedčené riešenia v podobe firewallu a VPN (Virtual Private Network – virtuálna súkromná sieť). Firewally chránia sieťové segmenty, ktoré nie sú určené pre aplikácie bežiace v danom segmente, pred nadbytočnou dátovou prevádzkou. Zároveň možno vykonávať hrubé filtrovanie pokusov o prístup podľa IP adresy alebo MAC adresy. Pritom nesmieme zabúdať, že filtrovanie MAC adries, nazývané často ako zabezpečenie portov (port security), nepredstavuje žiadne zabezpečenie z hľadiska IT. Útočník môže dátové pakety ľahko označiť ľubovoľnou MAC adresou (MAC spoofing).



Aplikácia WLAN systémov a neustály prenos dát až na internet vyžadujú špeciálne bezpečnostné koncepty pre automatizačné aplikácie

Špecifické požiadavky na priemyselný ethernet

Technická správa ISA [1] podáva prehľad o bežných zabezpečovacích riešeniach v oblasti informačných technológií. Okrem všeobecného opisu jednotlivých technológií uvádza ich slabé stránky a aplikačný potenciál pre automatizačnú a procesnú techniku. Pod pojmom VPN technológia sa rozumie zabezpečenie dátovej prevádzky na úrovni IP (vrstva 3) pomocou IPsec protokolu i aplikácie SSL/TLS (vrstva 4) a SSH (Secure Shell). Je to nezvyčajné, pretože ako VPN sa spravidla označuje len zabezpečenie siete na úrovni IP.

Pri hodnotení VPN riešení v priemyselnom prostredí sa zohľadňujú nasledujúce body: vzájomná komunikácia zariadení, nastavenia (konfigurácie), podpora a údržba, špeciálne riešenia na zabezpečenie inej ako IP prevádzky (Profinet, Ethernet/IP), (ne)dostupnosť VPN riešení pre zabudované (embedded) operačné systémy, reakcia v prevádzke a počas vytvorenia spojenia, nedostatok skúseností s návrhom a manažmentom pri zostavovaní a prevádzky VPN pri veľkých automatizačných sieťach alebo delených SCADA aplikáciách.

Ako príklad koncepcie zabezpečenia informačných technológií pre ethernetové komunikačné siete v automatizačnej technike uvedieme Profinet Security Guidelines (bezpečnostné smernice Profinet) [2], presadenie aplikácií tzv. zabezpečovacích modulov s kombinovanou funkciou firewall a VPN. Koncepcia Profinet počíta s nasadením jedného zabezpečovacieho modulu na vstupe každej automatizačnej bunky. Prostredníctvom modulu je pritom vylúčená dátová prevádzka v reálnom čase. Smernice neuvádzajú žiadnu presnú špecifikáciu protokolov na ochranu dátovej prevádzky. Treba vychádzať z toho, že produkty rôznych výrobcov, ktoré realizujú koncepciu bezpečnostných smerníc Profinet, nedokážu vzájomne spolupracovať. Okrem toho je diskutabilné, či bezpečnostné smernice reprezentujú všetky aplikačné prípady a či spĺňajú rôzne, v praxi oprávnené bezpečnostné požiadavky. Ešte väčšie rozšírenie má dokument Profil systémovej ochrany – Priemyselné riadiace systémy [3], vydaný fórom PCSRF, ktorý opisuje koncepciu

zabezpečenia jednotlivých komponentov až na úroveň akčných členov a snímačov.

Komplexná povaha protokolu IP security (IPsec)

Protokol IPsec, ktorý je štandardom VPN, zahŕňa tri rôzne definície protokolu:

- AH (Authenticated Header, autentifikovaná hlavička),
- ESP (Encapsulation Security Payload, zapuzdrený bezpečnostný priestor) na samotné zabezpečenie dátovej prevádzky na sieťovej vrstve 3 (vrstva IP),
- IKE (Internet Key Exchange, medzisieťová výmena kľúčov) na výmenu kľúčov potrebných pre oba uvedené protokoly.

Protokoly možno využiť pre rôzne konfigurácie (sieť – sieť, hostiteľ – sieť, hostiteľ – hostiteľ) a v dvoch rôznych režimoch (transportný a tunelový). Ďalej si môže používateľ zvoliť medzi rôznymi kryptografickými protokolmi a mechanizmami.

Vzhľadom na komplexnosť IPsec protokolov treba zohľadniť nasledujúce problémy: nemožno prvoplánovo počítať s interoperabilitou rôznych implementácií Ipsec, konfigurácia pre nasadenie IPsec býva nákladná, uspokojivá bezpečnostná analýza celého radu protokolov je viac-menej nemožná.

Na poslednú spomínanú skutočnosť upozorňovali bezpečnostní odborníci Nils Ferguson a Bruce Schneier v rozsiahlom hodnotení IPsec [4] už v roku 1999. Na podporenie ich tézy vydalo pred nedávnom NISCC (National Infrastructure Security Co-ordination Centre, Národné koordinačné centrum pre bezpečnosť infraštruktúry) správu o závažných bezpečnostných nedostatkoch v špeciálnych prípadoch aplikácie IPsec [5]. Nedosiahnuteľnosť absolútneho zabezpečenia informačných technológií dokresľujú tiež súčasné útoky na hash algoritmy [6], ktoré sa nachádzajú aj v protokoloch IPsec. Zatiaľ majú také útoky akademický charakter. Ukazujú však, že protokoly alebo ich implementácie musia reagovať na slabé miesta algoritmov.

Bezpečnosť v automatizácii

Obmedzenie potenciálnych možností je dôležité vzhľadom na požiadavky, ktoré na využitie IPsec kladie automatizačná technika. Spočíva v zostavovaní pevne daných profilov. Pomocou profilov sa dosahuje bezpečná sieťová štruktúra s minimálnou konfiguračnou náročnosťou. Dlhodobý problém zabezpečovania siete v automatizačnej technike predstavuje identifikáciu a zabezpečenie inej ako IP dátovej prevádzky. Zvyčajnou metódou je tunelovanie príslušných paketov pomocou paketov vyššej sieťovej vrstvy, napríklad UDP. Naďalej zostáva otvorená problematika procedúr a operácií v reálnom čase, ktoré možno ešte pri takýchto zabezpečených spojeniach garantovať. Prepojenie rôznych sietí, predovšetkým integrácia WLAN systémov, vedie nakoniec k nutnosti jednotnej bezpečnosti infraštruktúry informačných technológií. Aplikáciou IPsec možno dosiahnuť komplexné bezpečnostné riešenie aj pri heterogénnych sieťach.

Referencie

[1] ISA-TR99.00.01-2004 Security Technologies for Manufacturing and Control Systems, ISA – The Instrumentation, Systems, and Automation Society, 2004.

[2] Profinet Security Guideline, verzia 1.0. Organizácia používateľov Profibus (PNO), 2005.

[3] System Protection Profile – Industrial Contorl Systems, Ver. 1.0, Process Control Security Requirements Forum, 2004.

[4] FERGUSON, N., SCHNEIER, B.: A Cryptographic Evaluation of Ipsec. (http://www.schneier.com/paper-ipsec.pdf).

[5] National Infrastructure Security Coordination Center, Vulnerability Advisor IPsec-004033, 9. 5. 2005.

[6] WANG, X., YIN, Y. L., YU, H.: Finding Collisions in the Full SHA-1, Advances in Cryptology, Crypto '05.

Fenix SK, s. r. o.

http://www.fenixsk.sk