Bezpečnosť v priemyselných počítačových sieťach

Security in Industrial Computer Networks

Marek Šimon, Katedra aplikovanej informatiky, FPV UCM v Trnave

Abstract: The role of industrial computer network is to provide automatic transfer of information within the structure of distributed control systems. When designing communication protocols for industrial networks, the main aims were performance and reliability. Components of the industrial networks were designed to be resistant to disruption. But the threat of security vulnerabilities is open to abuse. It is therefore essential within their design to address safety and security.

Key words: security, safety, SCADA, DCS

Abstrakt: Úlohou priemyselnej počítačovej siete je zabezpečiť automatický prenos informácií v rámci štruktúry distribuovaných riadiacich systémov. Pri návrhu komunikačných protokolov v priemyselných sieťach bol hlavným cieľom výkon a spoľahlivosť. Prvky sietí boli navrhované tak, aby boli odolné voči výpadkom. Otvorená je však hrozba zneužitia bezpečnostnej zraniteľnosti. Preto je dôležité pri ich návrhu riešiť zabezpečenie (safety) aj ochranu (security).

Kľúčové slová: ochrana, bezpečnosť, SCADA, DCS

1. Úvod

V súčasnosti sú už v prostredí riadiacich systémov bežne implementované technológie doteraz používané v dátových počítačových sieťach. Komunikačné štandardy ako Ethernet, protokoly TCP/IP a ďalšie sa stávajú kritickými komponentami riadiacich systémov.

Zatiaľ čo sieťové technológie umožňujú výrazne znižovať náklady a spriehľadňujú prostredie, v ktorom prebiehajú technologické procesy, je dôležité uvedomiť si ich pôvod. Ethernet, TCP/IP a ďalšie totiž pochádzajú z úplne odlišného prostredia. Ako príklad je možné uviesť vyžadovanú dostupnosť. V Internete/intranete sú problémy s dostupnosťou služieb časté a do

určitej miery akceptovateľné, od riadiacich systémov sa naopak očakáva vysoká spoľahlivosť.(1)

Úlohou priemyselnej počítačovej siete je zabezpečiť automatický prenos informácií v rámci štruktúry automatických riadiacich systémov (ARS) technologických procesov. Vďaka tomu je možné realizovať požadované funkčné prepojenia (v čase a priestore) podsystémov a prvkov ARS na získavanie, spracovanie a využitie informácií na automatické a operatívne riadenie. Komunikáciu v štruktúre ARS možno definovať ako proces obojsmerného prenosu informácií medzi dvomi alebo viacerými prvkami riadiaceho systému. (2)

2. Ochrana a zabezpečenie – Security a Safety

Pri návrhu komunikačných protokolov v priemyselných sieťach bolo hlavných cieľom výkon a spoľahlivosť. Prvky sietí boli navrhované tak, aby boli odolné voči výpadkom. Otvorená je však hrozba zneužitia bezpečnostnej zraniteľnosti. Preto je dôležité pri ich návrhu riešiť zabezpečenie (safety) aj ochranu (security).

Priemyselné podniky majú vo všeobecnosti dobre vyriešenú fyzickú bezpečnosť. Trend pripájania priemyselných počítačových sietí do firemných počítačových sietí však zvyšuje dôležitosť riešenia otázky informačnej ochrany priemyselných počítačových sietí. Dôležité je uvedomiť si, že pri súčasných technológiách počítačových sietí, do každej siete existuje spravidla viacero prístupových bodov. Fyzická izolácia teda nezaručuje ochranu siete. Vždy je možnosť existencie pripojenia lokálnej siete do sveta (typicky Internetu) cez modem, intranet, sieť obchodného partnera, alebo užívateľom pripojeného AP[1] wifi siete. Potencionálny útočník môže zneužiť ktorékoľvek z týchto pripojení a získať tak prístup až na stroje v priemyselných počítačových sieťach.

Ďalší faktor ovplyvňujúci úroveň ochrany je používanie COTS[2] hardvéru a softvéru pri budovaní priemyselných sietí. Dizajn postavený na COTS produktoch síce znižuje cenu a zvyšuje rýchlosť vybudovania siete, ale zároveň vyvoláva obavy o celkovú bezpečnosť konečného produktu. COTS softvér má zvyčajne nízku úroveň bezpečnosti a je teda lákavým cieľom pre útočníka. Zariadenia určené pre prácu v kritickom prostredí sú síce zvyčajne

1 AP – Access Point, prístupový bod cez ktorý sa klientske stanice pripájajú do bezdrôtovej siete

2 COTS – Comercial Off-The-Shelf produkt, jednoducho použiteľný (implementovateľný) produkt bez možnosti/nutnosti ďalších úprav

navrhnuté s vysokou odolnosťou voči chybám (fail-safe design), ale útočník môže zneužiť bezpečnostnú chybu a vypnúť mechanizmus odolnosti voči chybám. Tieto zariadenia teda musia byť navrhnuté nielen ako odolné voči chybám, ale aj ako bezpečné.

Častejšie používanie COTS zariadení vedie k vývoju priemyselných komunikačných protokolov, ktoré sú schopné pracovať v tradičných ethernetových sieťach s TCP/IP. Tieto protokoly často vytvárajú spojenie cez sériovú linku pričom toto spojenie je zapuzdrované do štandardných TCP segmentov. Toto vedie k opúšťaniu striktného vzťahu master - slave, ktorý bol tradičný v priemyselných sieťach. Zariadenia pre tieto nové priemyselné siete často pridávajú doplňujúcu aplikačnú vrstvu. Toto môže zahŕňať prvky webrozhrania, ktoré umožňuje zbierať informácie o výrobe pre najvyššie úrovne manažmentu. Samozrejme, implementácia týchto funkcií do prvkov priemyselných sietí robí tieto zariadenia zraniteľné na bežné typy útokov známe z prostredia TCP/IP sietí.(3),(4),(5)

3. Hrozba – útočník a jeho motivácia

Súčasné prieskumy ukazujú nárast počtu útokov na riadiace systémy (či už DCS alebo SCADA). V British Columbia Institute of Technology (BCIT) v Kanade vytvorili databázu bezpečnostných incidentov v SCADA (a DCS). Databáza bola naplnená informáciami o útokoch na priemyselné počítačové siete. Analýza týchto informácií ukázala znepokojivý trend. Do roku 2000 viac ako 70 % oznámených incidentov bolo spôsobených neúmyselnou nehodou alebo chybou vlastných pracovníkov spoločnosti, ktorá udalosť oznámila. Od roku 2001 sa pomer otočil a v súčastnosti viac ako 70 % incidentov je spôsobených útočníkmi z vonku.(6)

Útočník, ktorý získa neoprávnený prístup do priemyselnej siete, môže v podstate neobmedzene útočiť na zdroje tejto siete. Pritom tieto útoky môžu viesť k výpadkom vo výrobe a tým aj k finančným stratám. V extrémnych prípadoch môže útok viesť až k stratám na životoch.

Útočníci sa môžu pokúsiť kompromitovať bezpečnostné vlastnosti priemyselnej siete ako je integrita, dôvernosť, autentifikácia alebo dostupnosť. Odpočúvanie komunikácie na sieti je príkladom ako sa útočník môže pokúsiť získať prístup k dôverným informáciám. Keďže šifrovanie komunikácie v priemyselných sieťach je skôr výnimočné, odpočúvanie je možné ak sa útočníkovi podarí preniknúť do priemyselnej siete. Útočník potom už len pasívne zachytáva a analyzuje komunikáciu a na základe toho potom môže vytvoriť falošnú správu. Alebo môže zasahovať do prenášaných správ a tak narúšať ich integritu. Útočník môže

napríklad zmeniť riadiace signály a tým znefunkčniť zariadenie, čo môže viesť k zastaveniu výrobného procesu. Prípadne môže získať neoprávnený prístup k zariadeniu a priamo zmeniť jeho konfiguráciu (zasiahnuť do jeho programu), alebo zmeniť uložené dáta o priebehu výrobného procesu. Čo zase môže viesť k výrazným škodám. Ďalšia možnosť je, že potom čo útočník získa neoprávnený prístup k zariadeniu, zmení zobrazované hodnoty na HMI[3]. Takže namiesto zobrazenia varovania pri kritických stavoch technologického procesu, sa zobrazia normálne hodnoty. Toto môže viesť obsluhu technologických procesov k nesprávnym reakciám. Útočník taktiež môže jednoducho zablokovať akúkoľvek komunikáciu a vykonať tak DoS útok. Keďže mnohé zariadenia nemajú bezpečný operačný systém, útočník sa môže pokúsiť zaviesť do pamäte zariadenia svoj vlastný zlomyseľný program, ktorý mu umožní lepšiu kontrolu zariadenia, ukryť svoju prítomnosť v systému, prípadne znásobiť účinnosť ďalšej zlomyseľnej aktivity.(5)

Obrázok 1: Odtajené video DHS

3 Human Machine Interface, typicky dotykový displej zobrazujúci informácie a umožňujúci zadávanie príkazov operátorom

27. septembra 2007 bola odvysielaná (7) reportáž o experimentálnom kybernetickom útoku v dôsledku ktorého bol zničený elektrický generátor. Experiment preukázal reálnu hrozbu takýchto útokov. Ministerstvo vnútornej bezpečnosti (Department
of Homeland Security – DHS
) zverejnil len odtajené video z priebehu experimentu bez ďalších podrobností.

4. Záver

Tri problémové oblasti musia byť riešené pri ochrane priemyselných sietí. Prvou je zlepšiť kontrolu prístupu do priemyselných sietí (DCS a SCADA). Riešenie by malo sťažiť prístup útočníka do priemyselnej siete. Druhou je zlepšiť bezpečnosť a ochranu vo vnútri samotných priemyselných sieťach a vyvinúť efektívne nástroje na monitorovanie bezpečnosti. Bezpečnostné mechanizmy vyvinuté na pokrytie tejto výzvy zaručia, že aj keď sa útočník dostane do priemyselnej siete, bude pre neho obtiažne vykonať ľubovolný typ útoku. Monitorovacie nástroje pomôžu pri detekovaní prieniku a iných podozrivých aktivít na sieti. Treťou je zlepšenie riadenia bezpečnosti v priemyselných sieťach.(5)

5. Zoznam bibliografických odkazov

(1) Byres, Eric – Franz, Matthew – Miller, Darrin: The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems, International Infrastructure Survivability Workshop (IISW'04), IEEE, Lisbon, Portugal, 4. decembra 2004, 9 s.

(2) Georgiev, Boris – Jurišica, Ladislav: Prevádzkové riadiace systémy 2, In:AT&P Journal 2/2006, s. 46 - 48, ISSN 1335-2237

(3) Byres, Eric – Lowe, Justin: The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, VDE Congress, Berlin, október 2004, 5 s.

(4) Byres, Eric et al.: Worlds in Collision - Ethernet and Factory Floor, ISA Emerging Techonlogies Conference, október 2002, on-line [http://www.isa.org/link/WCollisionpdf], [cit.:9.12.2010]

(5) Igure, Vinay – Laughter, Sean – Williams, Ronald: Security issues in SCADA networks. In Computers & SecurityVolume 25, Issue 7, október 2006, strana 498-506.

(6) Byres, Eric: SECURITY INCIDENTS AND TRENDS IN SCADA AND PROCESS INDUSTRIES, máj 2007,
on-line [http://ethernet.industrial-networking.com/articles/articleprint.asp], [cit.:9.12.2010]

(7) Reportáž CNN z 27.9.2007: Mouse click could plunge city into darkness, experts say, on-line [http://www.cnn.com/2007/US/09/27/power.at.risk/index.html#cnnSTCText], [cit.:9.12.2010]

6. Adresa autora:

Marek Šimon, Ing.
Katedra aplikovanej informatiky FPV UCM
Nám. J. Herdu 2
917 01 Trnava
marek.simon@ucm.sk