25 Excel@FIT 2018

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Bezpečnost' SCADA systémov a protokol DLMS

Ján Pristaš
Faculty of Information Technology, Brno University of Technology
xprist06@stud.fit.vutbr.cz

Abstrakt práce

SCADA (Supervisory Control And Data Acquisition) systém je typ architektúry riadiaceho systému využívaný na vzdialené riadenie a zber dát. Vo všeobecnosti systém obsahuje riadiacu stanicu a niekoľko vzdialených staníc, ku ktorým sú pripojené rôzne riadené objekty. Ako u väčšiny odvetví počítačových sietí ani tieto systémy sa nevyhnú hrozbe rôznych útokov, ktoré môžu systému spôsobit' veľké škody. Táto práca sa zaoberá vytváraním/simuláciou rôznych druhov útokov na testovacie siete a zist'ovaním reakcií systému na ne. Výstupom práce je datová sada vo formáte .pcap, ktorá obsahuje jednotlivé útoky spolu s popisom reakcií systému a možnost'ami detekcie.

SCADA systém

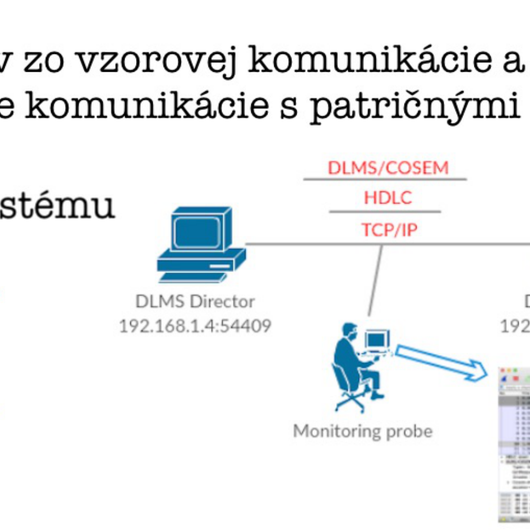
SCADA systémy slúžia na vzdialenú kontrolu a zber údajov. Skladajú sa z dvoch častí: strany klienta a strany serveru.

Klient
- riadiaca stanica
- vzdialene monitoruje a riadi pripojené prvky

Server
- vzdialená stanica
- riadená klientom
- má pripojené rôzne inteligentné meracie zariadenia (snímače, teplomery, elektromery ap.)

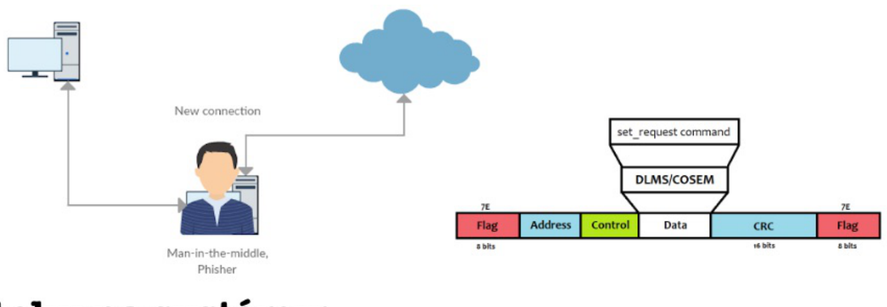
Protokoly: DLMS/COSEM, IEC 104, MQTT, ...

Využitie:
- hlavne energetické a výrobné závody
- v ČR využívané spoločnost'ami RWE, E.ON a skupinou ČEZ



Bezpečnost'

Hlavné dôvody ohrozenia SCADA:
- postupný prechod nad IP vrstvu
- rozrastanie sytémov a nemožnost' komunikácie iba na fyzickej vrstve



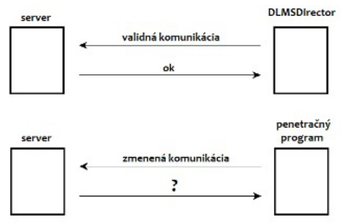
Útoky na systémy:
- neberie sa do úvahy väčšina bežných počítačových útokov
  - predpoklad dostatočného zebezpečenia
  - firewally konfigurované na prepúšt'anie iba najdôležitejšej komunikácie
- man-in-the-middle útoky, šírenie malware do systému
- útoky často spočívajú v odchytení komunikácie, zmene v paketoch a následnom zaslaní nesprávnych údajov jednotlivým staniciam

Prienik do systému:
- pomocou platných autentizačných údajov (z oddchytenej komunikácie)
- pripojenie vlastného meracieho zariadenia

Testovanie

Testovanie pozostáva z niekoľkých fáz:

1. Vytvorenie simulačného prostredia, ktoré sa chová ako reálny systém
2. Vygenerovanie (validnej) komunikácie, ktorá slúži ako vzorová
3. Pozmenenie príkazov zo vzorovej komunikácie a opätovné vygenerovanie komunikácie s patričnými zmenami
4. Sledovanie reakcií systému



Výsledky testov:
- zistenie reakcií systému na rôzne typy narušení
- systém reagoval rôznymi spôsobmi:
  - na zmenu odpovedal štandardne
  - na zmenu sa pokúsil odpovedat', ale nemal potrebné dáta (napr. dotaz na neexistujúci atribút, objekt)
  - na zmenu nevedel reagovat' a preto neodpovedal
  - ukončil komunikáciu, ak príkaz neodpovedal štandardu

Prínos práce

Táto práca môže pomoct' mnohým spoločnostiam predíst' nežiadúcim ohrozeniam ich systémov a efektívne sa bránit' väčšine typov známych útokov na ich siete. Výsledky práca sú tiež súčast'ou projektu IRONSTONE vo výzkumnej skupine NES@FIT.