Salaus ja tietoturva teollisen internetin ratkaisuissa

Teknologia 2015

Tietoiskut 6.-8.2015

Tomi Engdahl

Teollinen Internet

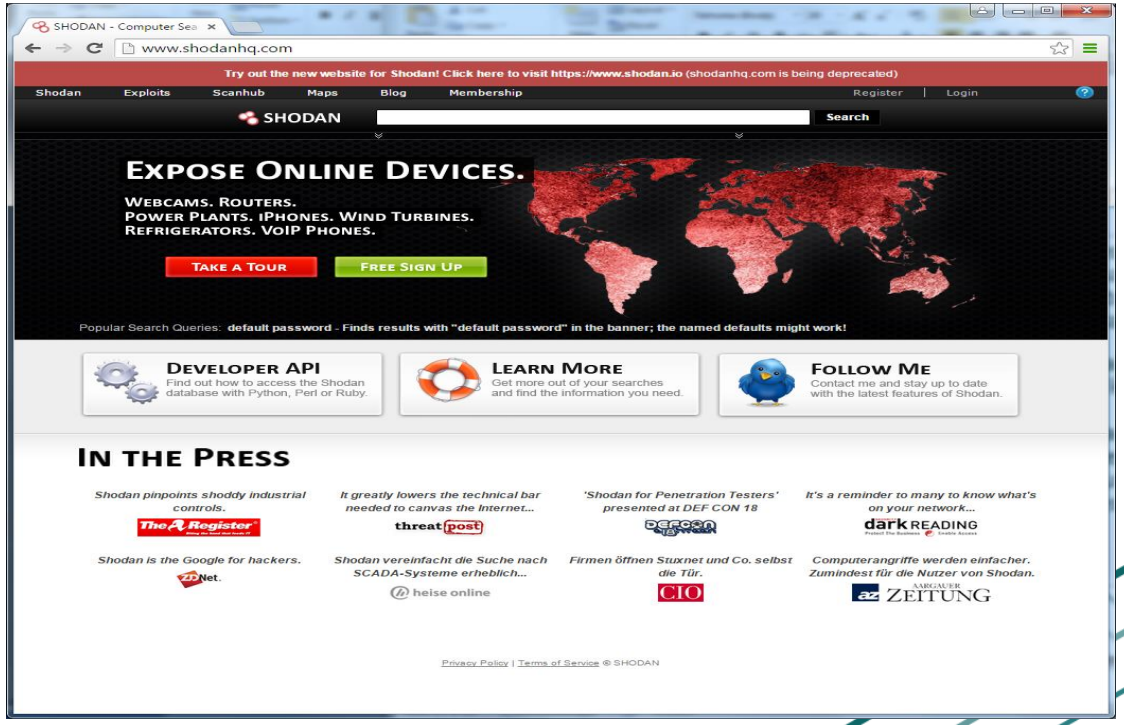
- Suuri joukko erilaisia tekniikoita
- Yhteisenä nimittäjänä TCP/IP-tietoliikenteen käyttö
- SCADA/M2M (Supervisory Control And Data Acquisition/Machine-to-Machine) -maailman tekniikoita Internet-maailmaan sovitettuna ja markkinoituna
- Lisäksi mukana Internet- ja kuluttaja-IoT-tekniikoita

Tietoturvan tarpeita

- IoT-laitteiden integriteetti
- IoT-laitteiden identiteetti
- IoT-laitteessa olevien tietojen suojaus
- Tiedon suojaaminen laitteessa, verkossa ja pilvessä
- Verkkoturvallisuus
- Jos verkossa kiinni oleva laite ohjaa prosessia niin ulkopuoliset eivät saa häiritä sitä (väärä ohjaus, DoS häiritsee prosessin ohjausta)

Suojaamattoman laitteen riskit

- Mitä tapahtuisi jos kuka vaan pääsisi ohjaamaan automaatiojärjestelmää?
- Maailmassa on paljon järjestelmiä joita kuka tahansa pääsisi ohjaamaan.
- Suomessa tuhansia suojaamattomia automaatiojärjestelmiä!
- Haavoittuvia laitteita voi etsiä hakukoneella: http://www.shodanhq.com/



Mitä haavoittuva IoT-laite voi tehdä

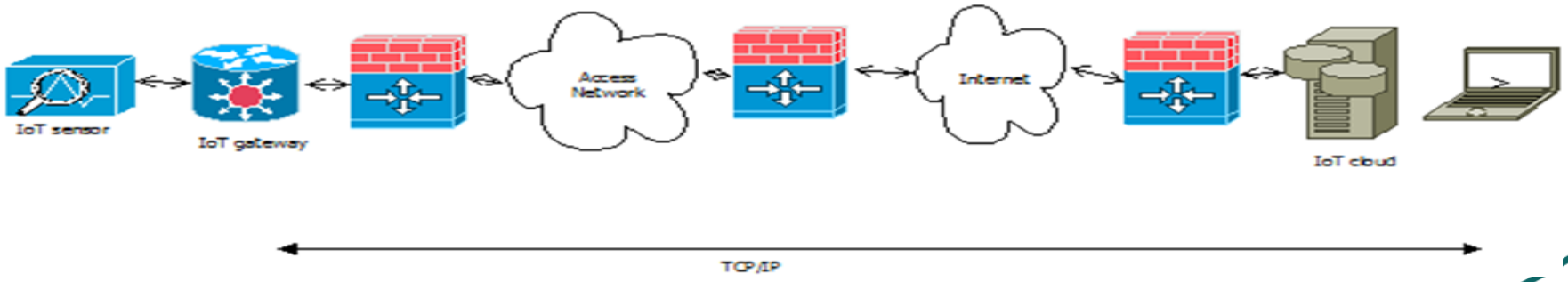
- Lähettää väärää dataa
- Aiheuttaa haittaa verkossa: Verkon salakuuntelu, DoS-hyökkäys, tietoliikennelasku tai haavoittuvien laitteiden etsintä
- Tunkeutumisreitti yritysverkkoon: Target-kauppa ja sairaalat
- Tehdä vaarallisia ohjauksia suoraan tai välillisesti:
  - Kytkee autosta jarrut pois ajon aikana (http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ ja **http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/)**
  - Muuttaa lääkepumpun toimintaa (http://www.cnbc.com/2015/08/03/citing-hacking-risk-fda-says-hospira-pump-shouldnt-be-used.html)

Suojaamattomia yhteystekniikoita

- Suojaamattomia joissa tieto kulkee ”paljaana verkossa”
  - HTTP
  - FTP
  - Telnet
  - Modbus TCP jne. SCADA- ja automaatioprotokollat
  - Suurin osa etäsarjaporteista (sarjaliikenne "raakana" TCP:n yli)
- Universal Plug and Play (UPnP): UDP + HTTP – käytössä mm. Belkin WeMo, Philips Hue
- Helposti kuunneltavissa (esim. Wireshark)
- Käytä näitä kriittisessä sovelluksissa vain luotettavasti
- Internetistä erotetussa verkossa!

Kuluttajalähtöinen IoT

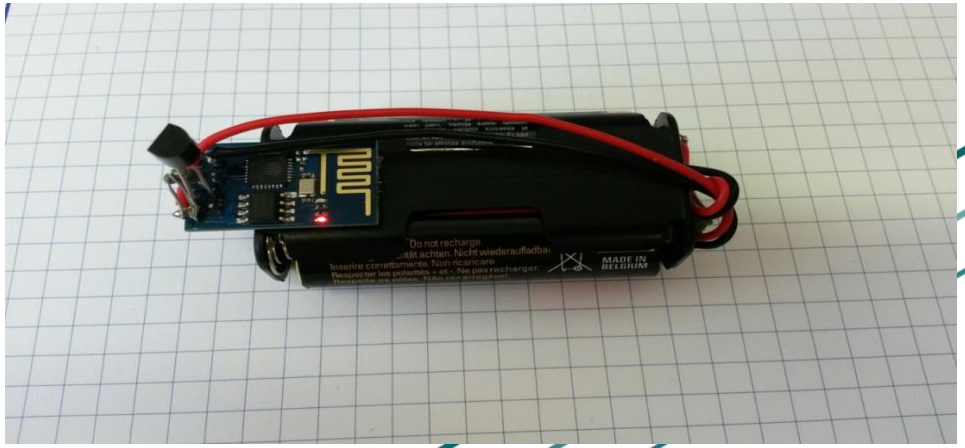
- Kuluttajakäyttöön alun perin suunniteltu tekniikka voi soveltua tai päätyä teollisuussovelluksiin
- Se voi olla yksinkertainen anturi, joka lähettää mittauksia pilveen tai kauko-ohjattava pistorasia
- Connected Device <-> Internet of Things
- Tyypillisesti hallitaan ja data kuljetetaan HTTP/HTTPS- yhteyksien kautta IPv4-verkossa



Tee se itse IoT-esimerkki: NodeMcu

- ESP8266 NodeMCU-pohjainen lämpömittari
- Kommunikoi WLAN-yhteydellä (WPA2 salattu)
- Lähettää data HTTP-yhteydellä ThingSpeak-palveluun laitenumeron ja tiedot salaamattomana
- Yhteys pilvestä päätelaitteeseen voi olla salattu tai salaamaton
    1. http://www.epanorama.net/newepa/2015/06/19/iot-temperature-meter/

1. http://www.epanorama.net/newepa/2015/06/25/battery-powered-iot-temperature-logger-testing/



Suojattuja yhteystekniikoita

- Suojattuja tyhteystekniikoita
  - HTTPS (SSL/TLS) -suojattu HTTP-liikenne
  - MQTT over HTTPS
  - VPN (esim. OpenVPN)
  - SSH /SCP
  - WSS (Web Socket Secure)
- Käytä suojattuja yhteyksiä aina kun voit!
- Päästä päähän suojaus on paras valinta!
- Pelkkä suojaustekniikan valinta ei ratkaise mitään – laitteiden tunnistuksen, avainten hallinnan yms. pitää olla kunnossa

Transport Layer Security (TLS)

UUSI TEKNOLOGIA.fi

- **Transport Layer Security (TLS) on eniten käytetty** salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli. Tavallisin käyttötapa on suojata WWW-sivujen siirtoa HTTPS-protokollalla, mutta sillä voidaan suojata myös Websocket (wss://), VPN:n (OpenVPN), SMTP, FTP, NNTP, XMPP ja MQTT
- Perusperiaatteiltaan TLS on yksinkertainen, toteutukseltaan monimutkainen (suuri joukko salausmenetelmiä joiden käytöstä neuvotellaan) – oikein käytettynä TLS 1.0 ja uudemmat kohtuullisen turvallisia.
- Web selauksen (HTTPS) turvallisuus perustuu varmenteisiin, joita myöntävät varmennusyritykset (CA): Yhteys avataan varmennusavainparilla (esim. 2048 bitin RSA key) ja data salataan symmetrisellä salauksella (esim. 256 bittinen AES)
- **OpenSSL** on hyvin laajasti käytetty toteutus.

Tietoliikenteen salauksen haasteita

- Suojaus lisää monimutkaisuutta: prosessoriteho- ja muistivaatimukset, avainten hallinta, mahdollisesti heikompi järjestelmän luotettavuus
- Salattua tietoliikennettä on mahdotonta tai vaikeaa tutkia yrityksen palomuurissa!
- VPN-tekniikat (TCP-over-TCP) ovat arkoja yhteyden laadulle
- Älä yritä keksiä itse omia tietoturva-algoritmeja – niistä tulee huonoja!
- Muista sipuli-malli: Monta päälleikkäistä suojauskerrosta!

IoT-laitepään suojaus

- Internettiin kytketty laite ei pysy salassa, joten valmistaudu että laitteitasi kohtaan hyökätään käyttäen tunnettuja haavoittuvuuksia ja oletussalasanoja
- Kunnolla toteutetut suojatut protokollat, joissa ei aukkoja
- Eri kriittisten toimintojen luotettava erottaminen (eri prosessorit, eri prosessit, virtualisointi)
- Ohjelmiston turvallinen etäpäivitettävyys ja etähallinta
- Testaa turvan taso (nmap, Metasploit, Kali Linux, Wireshark)
- Palomuuri: Älä paljasta ylimääräisiä turvattomia palveluita verkon suuntaan!

HUOM! Avoimia Telnet-yhteyksiä laitteen hallintaan on löytynyt droneista, turvakameroista, NAS-palvelimista jne...

Palvelimen suojaus

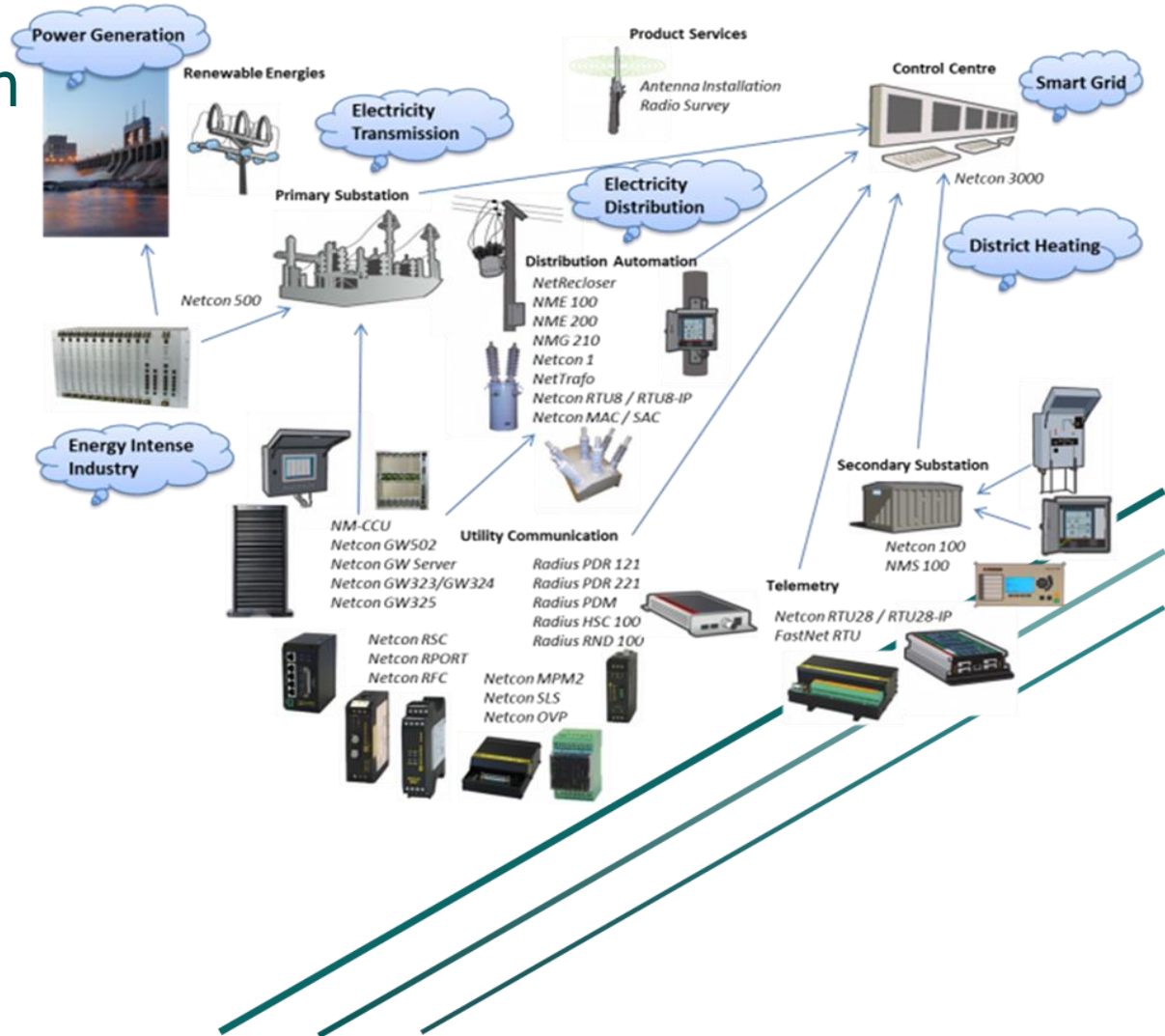
- HTTP:tä käyttävä prokollan palvelinpäään ylläpito vastaa pitkälle web-serverin ylläpitoa
- Varaudu että joutuu päivittämään
- Palomuuri (sisäinen tai ulkoinen)
- IDS, Honeypot
- Logitukset
- Varmuuskopiointi
- Virtualisointi
- Pidä Internet-palvelin ja tietoturva-avainten/sertifikaattien luominen erillään!

Internet Trust Framework suosituksia (otalliance.org)

- Tietoturvapolitiikka dokumentoitu
- Sensitiivinen tieto talletettava ja siirrettävä salatussa muodossa
- Oletussalasana vaihdettava!
- Vastauskyky haavoittuvuuksiin
- Tietovuotoihin vastaaminen ja tiedotus
- Laitteet ilmaisevat toiminnon kun liikennöivät
- Päivitykset varmennettuja
- Prosessit: katoaminen, siirto, virhetoiminta, tunnusten unohtaminen, omistajan vaihto
- Turvallisuus- ja yksityisyystaso säädettävissä
- Mikä toimii ja ei toimi kun ”äly” kytketään pois

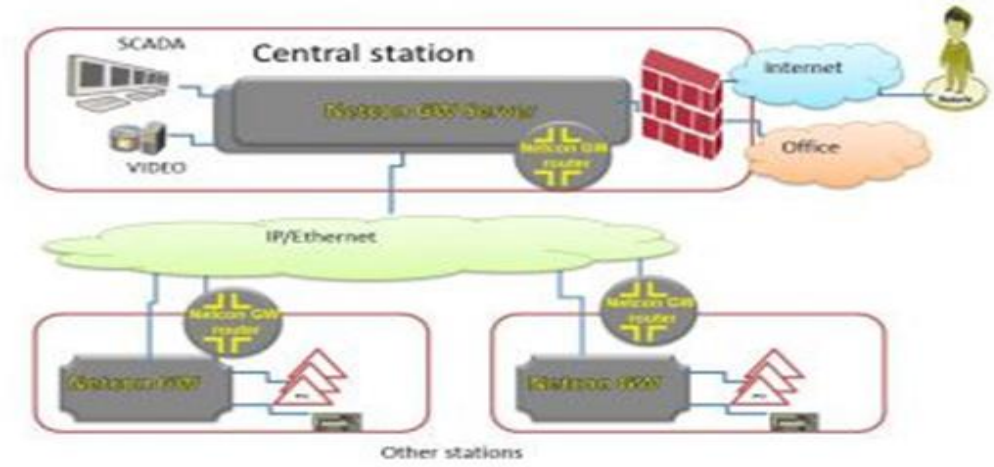
Teollinen Internet - SCADA maailman erityisominaisuuksia

- Turvallisuus tärkeä asia koska virhetoiminto voi tulla kalliiksi ja johtaa henkilövahinkoihin
- Perinteisesti toimineet erotetuissa verkoissa – nykyisin yhä enevässä määrin kiinni Internetissä
- Järjestelmän käytettävyys on tärkeä ominaisuus – liittyy rahaan ja prosessiturvallisuuteen
- Tavoitteena käytettävyys ja turvallisuus – joskus tilanteita joissa käytettävyys vastaan turvallisuus (IT vs OT)



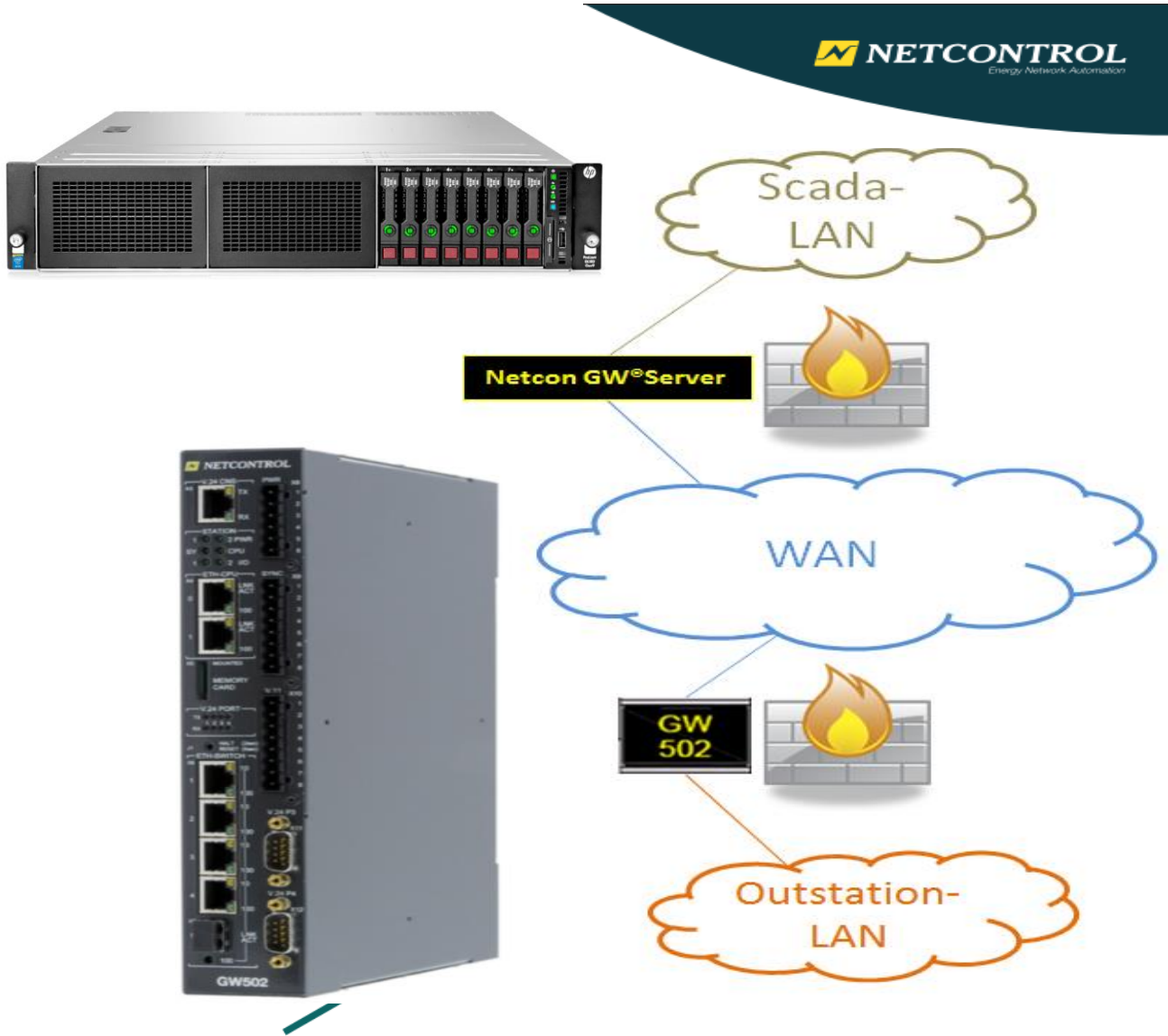
Industrial IoT: SCADA/M2M

- Perinteiset TCP/IP:n päällä toimivat kaukokäyttöprotokollat (esim. IEC 60870-5-104, Modbus TCP, IEC 60870-5-101) eivät tarjoa salausta tai muuta tehokasta suojausta itse
- Perinteisesti SCADA-protokolla avaavat yhteyden valvomosta kentällä olevaan laitteeseen
- Nämä käytännöt eivät sovi kuin julkisesta verkosta tiukasti erotettuihin verkkoihin joihin ulkopuoliset eivät pääse käsiksi – onko sellaisia enää?



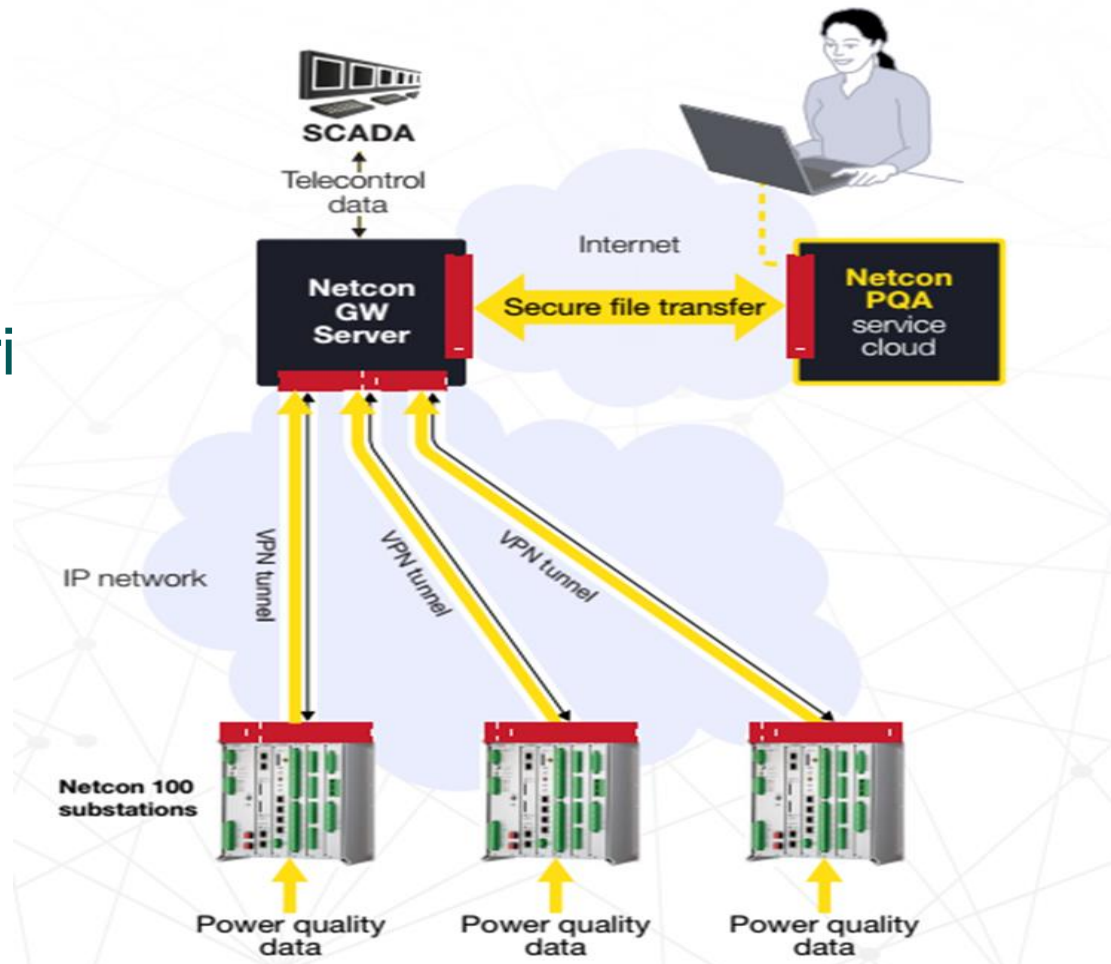
Vanhojen SCADA-protokollien suojaus

- Vanhat suojaamattomat prokotollat voi suojata kuljettamalla ne salatun tiedonsiirtokanavan yli (VPN) – etälaite avaa VPN-putken palvelimelle ja SCADA-valvomo saa tätä kautta turvallisen yhteyden kenttälaitteeseen
- Gateway-laite on turvallinen verkkoon päin, tarjoaa salauksen ja autentikoinnin ja juttelee vanhaan laitteeseen päin vanhaa protokollaa



Teollisuusverkon tehokas suojaus

- Laitteet toimivat Internetissä erotetussa IP-verkossa
- Jokaisessa laitteessa palomuuri
- Teollisuusprotokollat kuljetetaan salattuna VPN-yhteyden läpi – palomuuri käytössä myös VPN-yhteyden sisällä
- Ylläpitoyhteyksiin SCP ja SSH
- Keskitetty laitteiden hallinta: konfigurointi, avaimet, tunnisteet, IP-osoitteet ja päivitykset



IPv6 on tulossa

- IPV6 on tulossa vääjäämättä – se on jo käytössä
- IPV6 sisältää Internetin tietoturva-arkkitehtuuri IPsec:n
- IPV6:n haasteet:
  - IPV6-tietoturvaosaamisessa puutteita
  - IPV6-tunnelointitekniikat mahdollistaa uudenlaisia hyökkäyksiä
  - Puutteellinen IPV6-tuki laiteissa ja operaattoreilla
  - IPv6-koodi uudempaa -> bugeja vielä löytymättä
  - Ei NAT:ia (ollut monen IPV4-käyttäjän turvana)
  - Ajatus on väärä, että IPV6-tietoturva on samanlainen

Miltä tulevaisuus näyttää?

UUSI TEKNOLOGIA.fi

- IPv4 ja IPv6 tulevat olemaan pitkään rinnakkain (10 vuotta?) -> monessa laittessa tulee olemaan molempien tuki ja molempien tietoturvahaasteet
- IoT-laitteiden määrä verkossa kasvaa voimakkaasti
- Rikolliset kiinnostuvat IoT-laitteista yhä enemmän
- Verkossa on ja tulee olemaan suuri joukko laitteita joissa on tietoturva-aukkoja, sen kanssa pitää vain elää
- Raudanlujan tietoturvan tarve on jo tunnistettu pilvidatakeskuksissa – kun pilvilaskennasta tulee sumulaskentaa (sovellus voi pyöriä missä tahansa), nämä turvallisuusvaatimukset laajenevat solmuihin ja lopulta julkiseen verkkoon

KIITOS

tomi.engdahl@netcontrol.fi

www.netcontrol.fi, www.epanorama.net ja www.uusiteknologia.fi