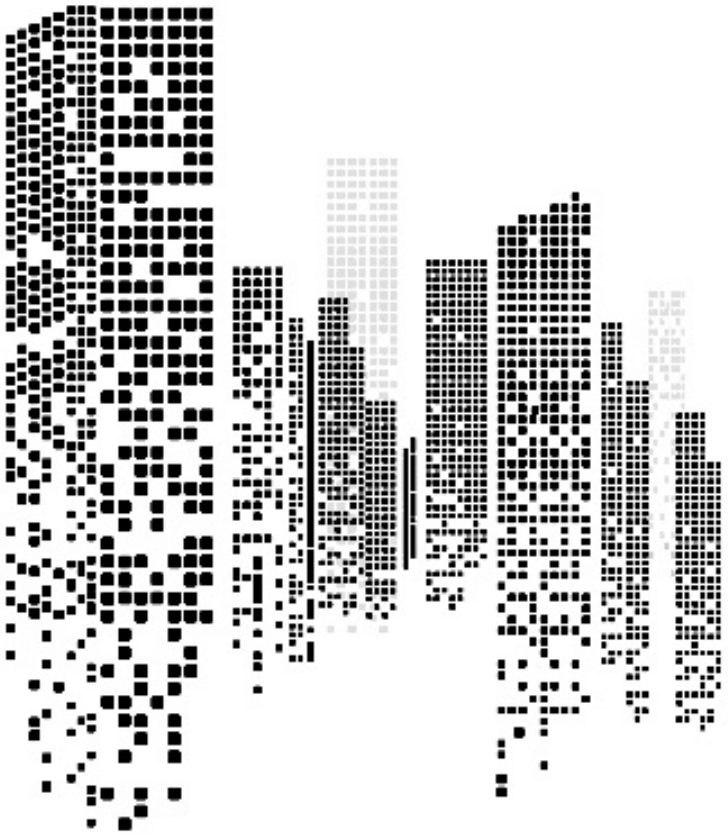


ZDANIA

ZINTEGROWANE SYSTEMY AUTOMATYKI I BEZPIECZEŃSTWA BUDYNKÓW

LOYTEC
COMPETENCE CENTER
IN POLAND

Buildings under Control

Symposium 2018

Kraków 28.02 – 1.03. 2018

Bezpieczeństwo IoT

w systemach automatyki budynków

1. marzec 2018 r., 14:00

Dzień Integratora i Projektanta Automatyki

Autor: Stefan Soucek-Noe, LOYTEC
Tłumaczenie, rozszerzenia i prezentacja:
Grzegorz Hayduk ZDANIA

LOYTEC
A Delta Group Company

Prelegent

- Autor: Dr. Stefan Soucek-Noe
  - Product manager L-INX, L-GATE, L-IOB, L-IP, L-Proxy
- Prelegent: dr inż. Grzegorz Hayduk
  - W ZDANIA od 1996 r
    - Projektowanie i wdrażanie systemów nadrzędnych BMS
    - Protokoły komunikacyjne, serwis, wsparcie specjalistyczne

Teza

- Nadchodzące dziś urządzenia IoT wymagają nowego poziomu dbania o bezpieczeństwo.
- Integracja technologii IoT z usługami budynkowymi staje się nowym wymaganiem.
- Jak zapewnić bezpieczeństwo w instalacjach LOYTEC przy jednoczesnej integracji technologii IoT?

Co to jest IoT

- Definicja jest trudna do uchwycenia
- Połączenie dyscyplin i technologii
  - usieciowione sensory i el.wykonawcze
  - urządzenia wbudowane (ang. embedded), „smart”, sprzęty typowo domowe
  - technologie wywodządze się z www
- Przykłady
  - mikrofalówka „smart”, sieciowy termostat, żarówki
  - usługi Web services, XML, JSON, websockets
- Każde urządzenie IoT jest serwerem www!

Bezpieczeństwo w prasie

- Opublikowano 8000 adresów IP urządzeń IoT
  - tylko 144 z 8233 **nie miało** domyślnych haseł
  - sierpień 2017
- Przeciętne urządzenie Internet of Things miało 25 luki bezpieczeństwa
- Botnet przejmujący rutery
  - malware w ruterach do podsłuchiwania transmitowanych haseł (i ich raportowania)
  - c’t 21, 2013

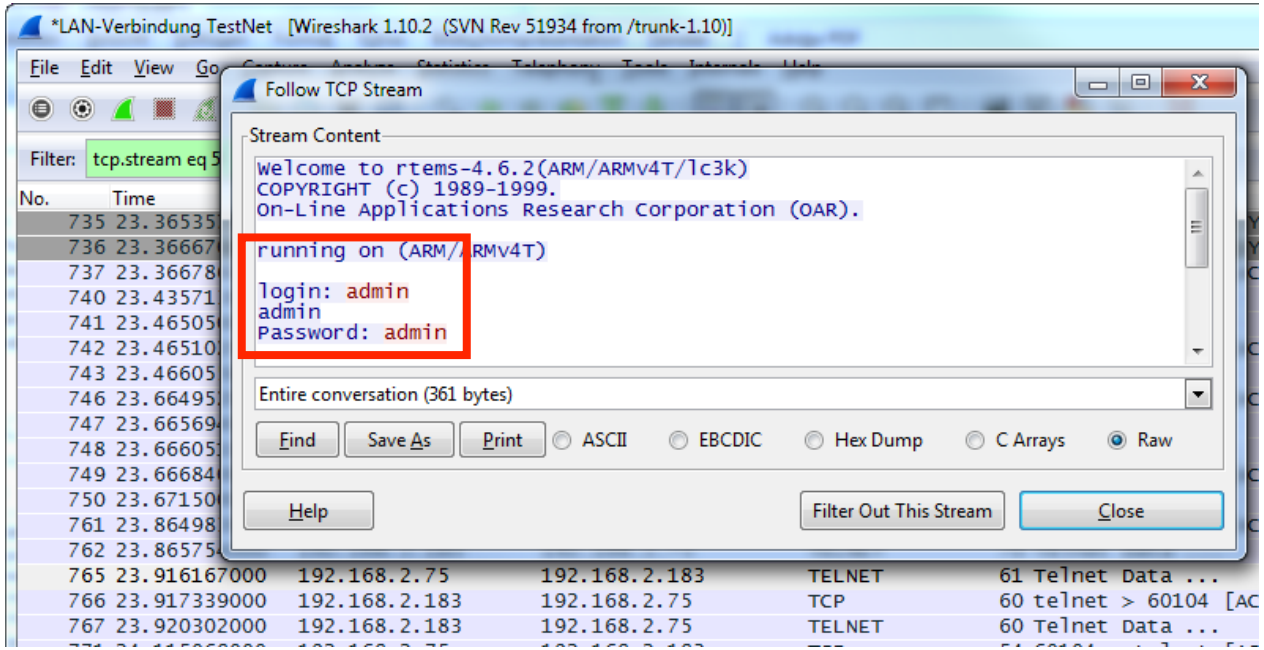
Die Presse

The Telegraph

heise Security

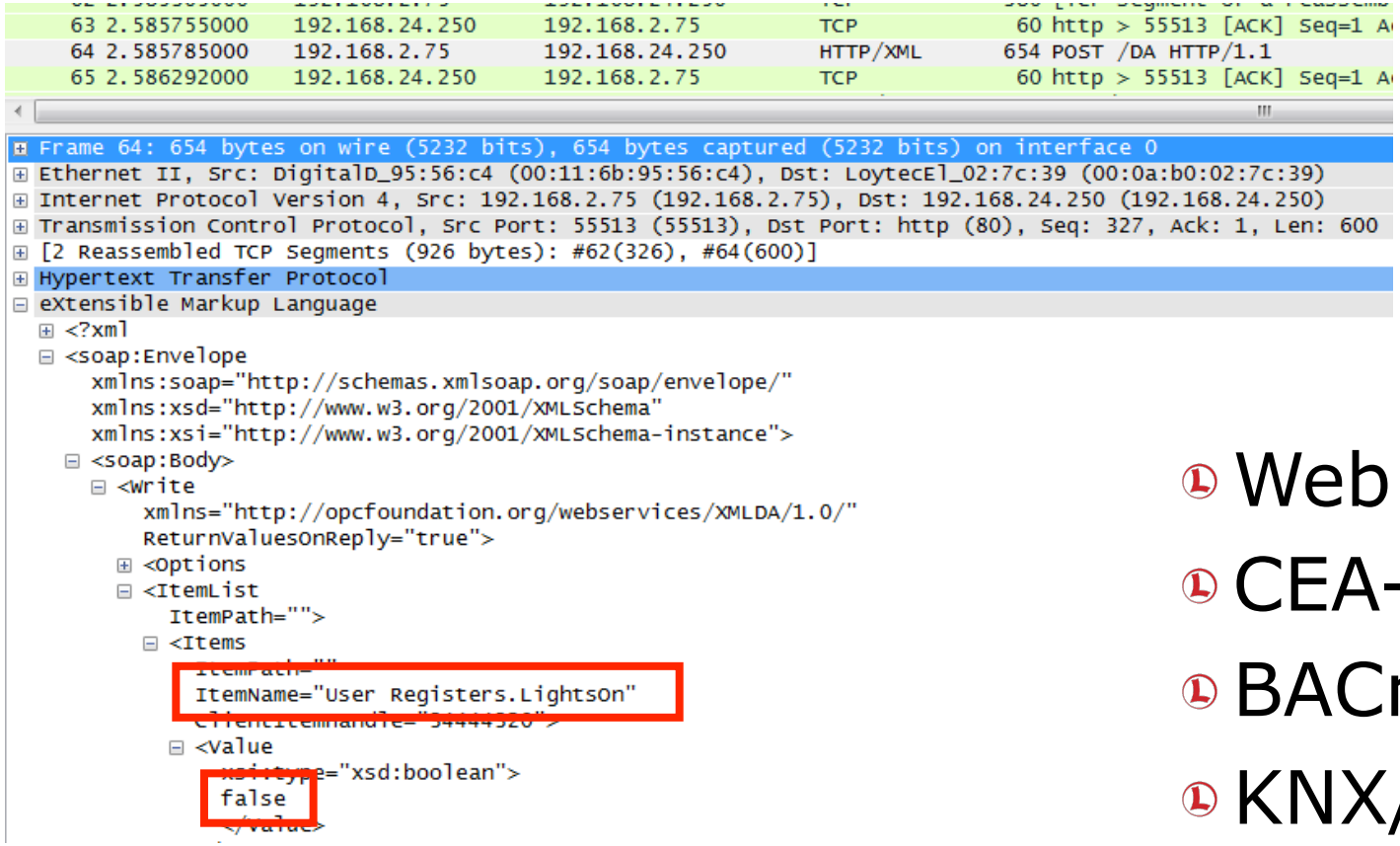
Zagrożenie: Clear-Text – jawnym tekstem

- Transmisja jawnym tekstem: Clear-Text
  - odczyt loginu/hasła (włamanie)
  - zarejestrowanie zachowań użytkowników (ataki, kradzież danych)



Zagrożenie: Odtworzenie transmisji (replay)

- Odtworzenie zarejestrowanych żądań

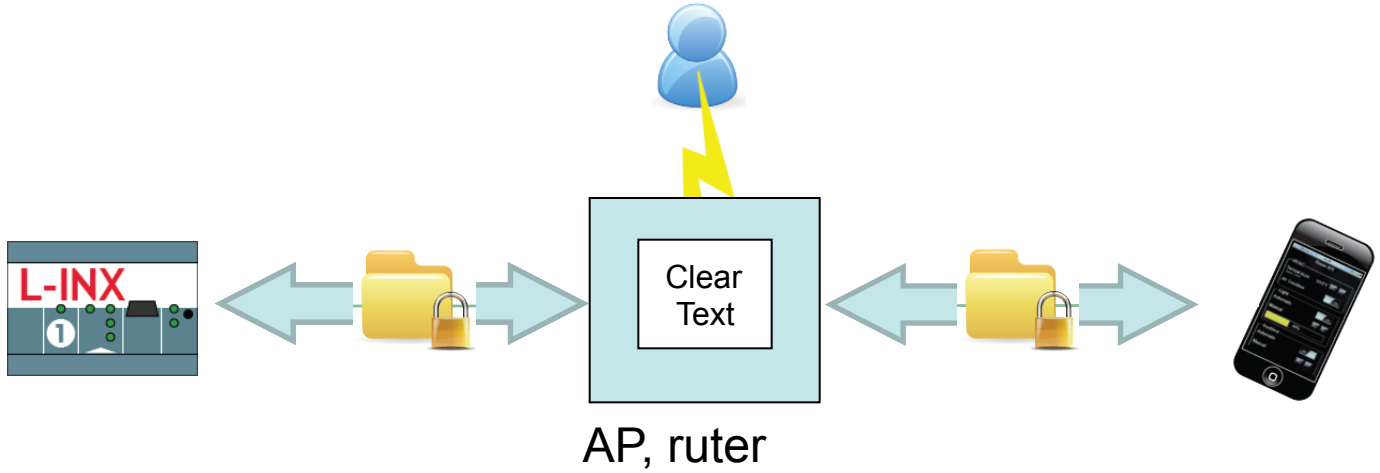


- Web Service
- CEA-852
- BACnet/IP
- KNX/IP

Zagrożenie: Man-In-The-Middle

- Bezpieczna transmisja

- Man-In-The-Middle – bezpieczeństwo złamane



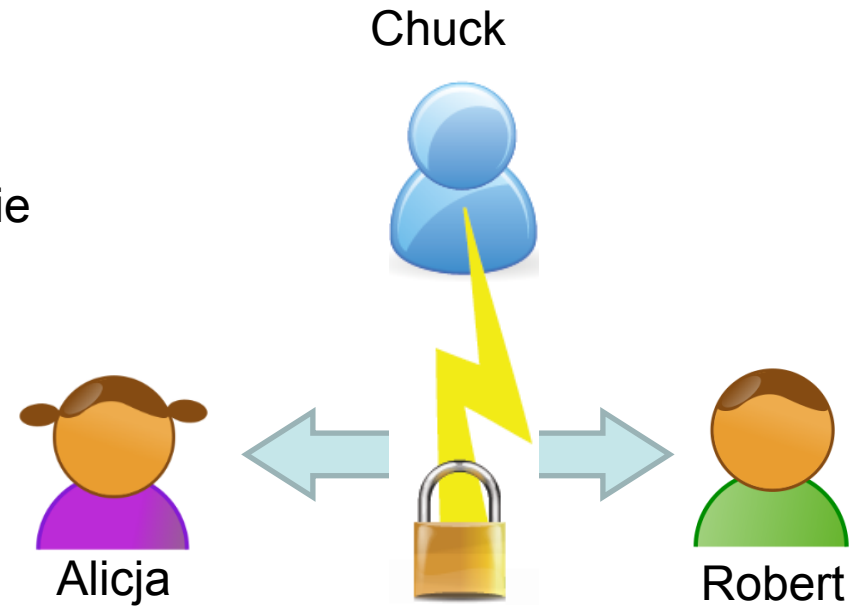
Zagrożenie: Exploit-y

- Atak „Denial of service”
  - uniemożliwienie normalnej pracy urządzeniu
  - użycie otwartych portów
  - podatność na exploit-y (np. restart)
- Włamania
  - tylne drzwi „Back doors”
  - kradzież danych
  - malware

Bezpieczeństwo

- Komunikacja
  - integralność
  - poufność
  - autentyczność
  - niezaprzeczalność

identyfikacja
uwierzytelnianie
autoryzacja



- Ochrona urządzenia
  - silne hasła
  - aktualizacje przeciw lukom w OS
  - ograniczenie fizycznego dostępu

Integralność

- Integralność wiadomości
  - weryfikacja, czy wiadomość nie została zmieniona podczas transmisji od Alicji do Roberta
  - kod MAC - Message Authentication Code
  - nie transmitowanie sekretny kod
  - bezpieczna jednokierunkowa funkcja skrótu: SHA-256
  - sprawdzanie odcisku (Fingerprint)

Poufność

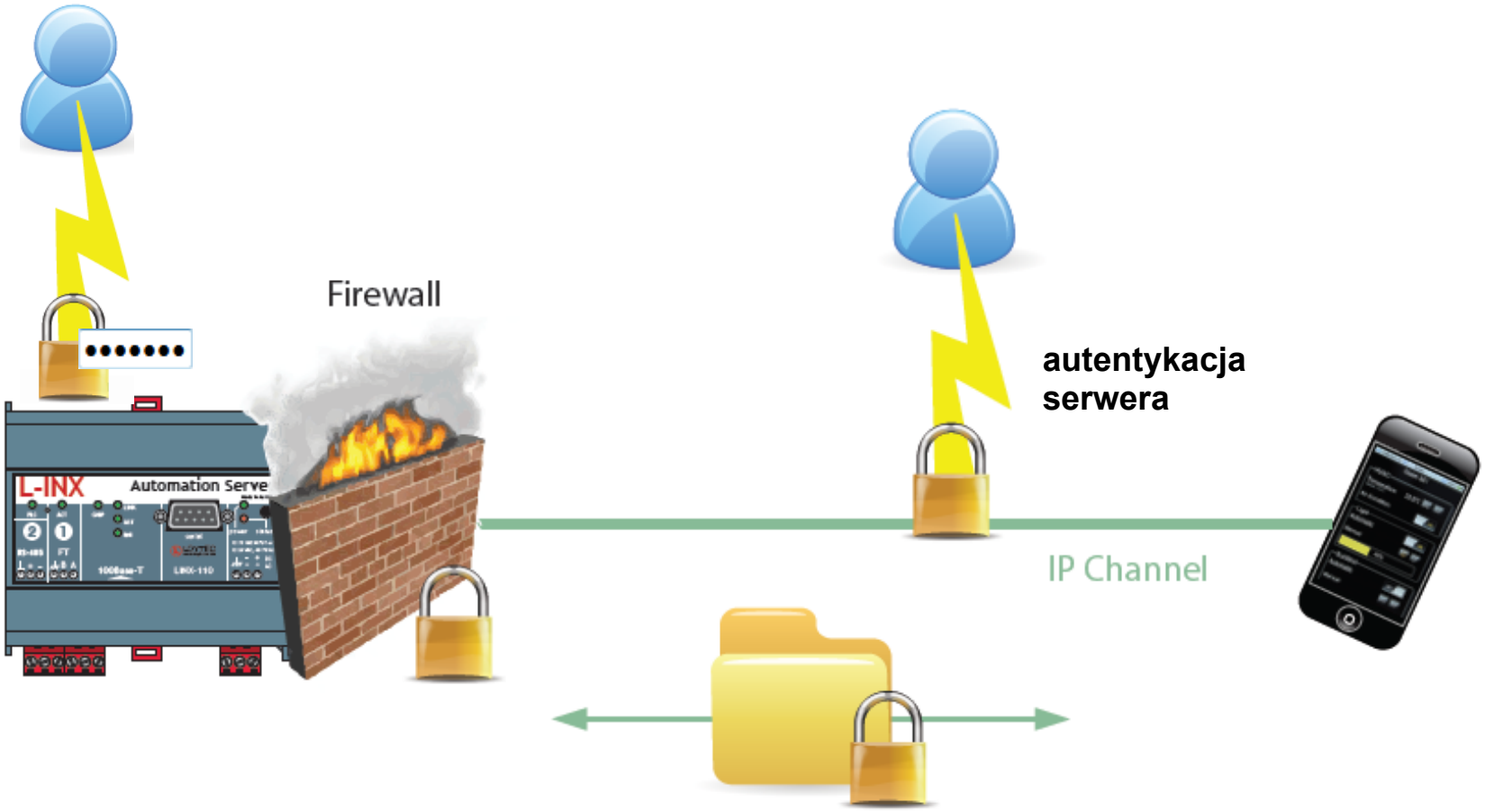
- Kodowanie (encryption)
  - bez przesyłania jawnym tekstem (clear-text): Chuck nie może odczytać transmisji
  - poufność haseł
  - zapobieganie podsłuchiwaniu danych sterujących
- Szyfrowanie strumienia danych
  - kluczem kodującym (symetrycznym)
  - tajnym
  - wstępnie udostępnionym (pre-shared)
  - wymiana klucza pomiędzy Alicją a Robertem

Autentyczność

- Alicja poświadcza tożsamość Roberta
- Poświadczenie - certyfikat
  - dokument z cyfrową sygnaturą
  - auto-podpisany (self-signed) lub podpisany przez CA (Certification Authority)

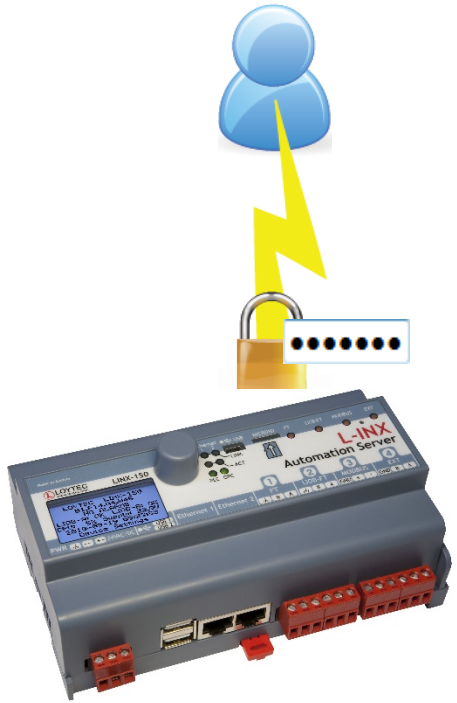
Installed Server certificate (Self-signed)	
RSA Key Size	1024
Validity Start Date	2013-09-17
Validity End Date	2023-09-15
Common Name	loytec.local
Organization Name	LOYTEC electronics GmbH
Organization Unit	Development
City	Vienna
State	Vienna
Country	AT
MD5 Fingerprint	49:B6:4D:79:DD:EF:77:4F:F2:35:BF:6D:47:B3:D8:54
SHA1 Fingerprint	D6:AE:4D:DF:AD:3A:16:2A:57:58:40:3E:8A:55:4F:63:C2:B1:AA:1F

Zwiększanie bezpieczeństwa
Security Hardening



Ochrona urządzenia

- Zmiana haseł (!)
  - użytkownicy Admin/Operator/Guest
  - zabezpieczenie PIN-em dostępu do ekranu LCD
  - użycie silnych haseł
    - nie: admin, 123, asd, yourname1
  - praktyczna wskazówka: zapamiętanie zdania
    - Bezpieczny LINX 0płaci mi się!
    - → BL0ms!



www.defaultpassword.com

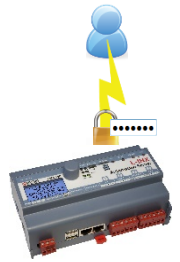
default password list

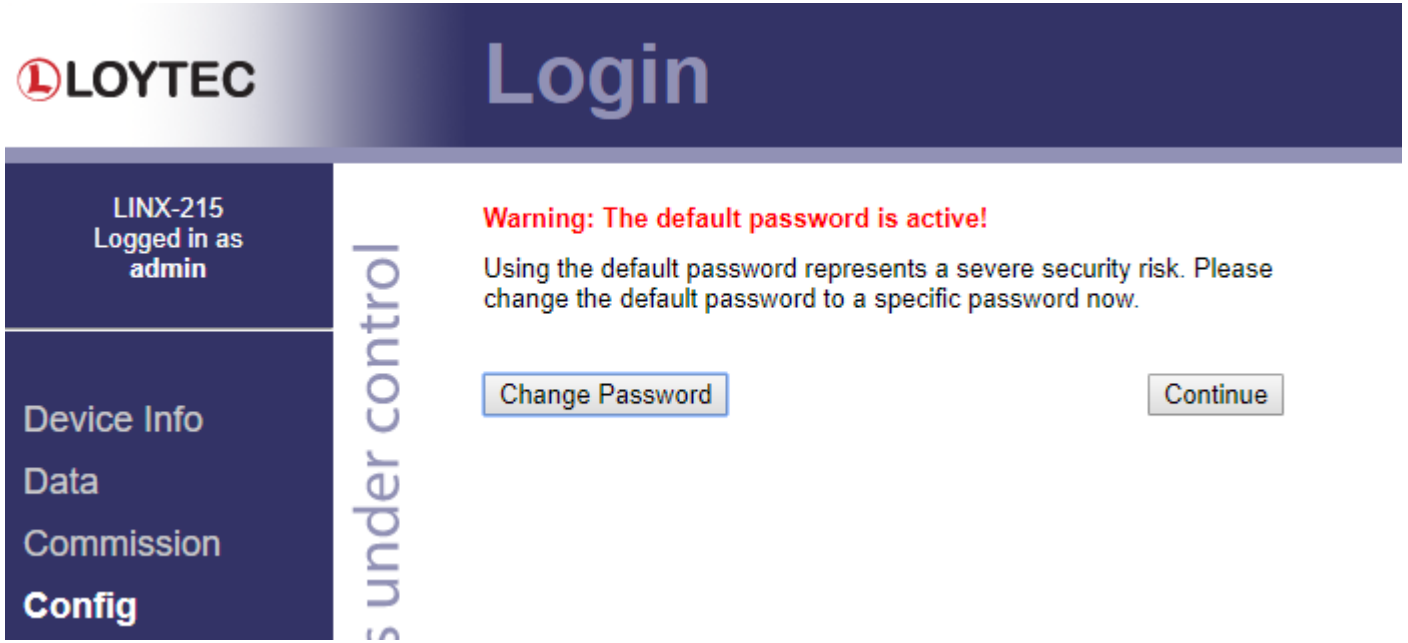
Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9

Displaying 78 passwords of total 1812 entrys.

Manufactor	Product	Revision	Protocol	User	Password
Lanier	5618		Multi	(none)	sysadm
Lantronics	Lantronics Terminal Server		TCP 7000	n/a	access
Lantronics	Lantronics Terminal Server		TCP 7000	n/a	system
Lantronix	Lantronix Terminal		TCP 7000	n/a	lantronix
lawl yo			HTTP	a	b
LdxWXAzNx	xXTGryMUTUScSdRuINI	JetiximZAWXFn		WbvCndpRn	vYetbYhpeyd
Leading Edge	PC BIOS		Console	n/a	MASTER
LeXKceHcgNSOo	ArOpIQXYqsGYTyMIJ	dFhnHHBxm		ljtNZgYHQ	MNhtdCzEregq
LG	mobile handset		Multi	vikram	singh
LgKwakiJHCuGnQg	QCEfjlpLn	wfpkvAiHJl		MALwKkjSQ	PenBZiOJiNngAtNnV
lgwLRDhWeOs	qXIfGICGTSHUdiFu	LGpYMlDRfKdxOadUR	SSH	9688	rK2VV7Ku
LHDDrASZcoahZjVRNBq	XuueWgSUg	DCBIcCtyFLmILNpPgl	SNMP	12728	vhsOPuXl
Linksys	BEFW11S4	1	HTTP	admin	(none)
Linksys	DSL		Telnet	n/a	admin
Linksys	E3000	1.0	HTTP	admin	admin

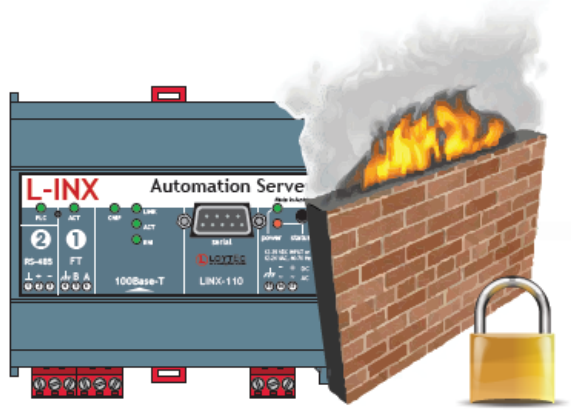
Zmiana haseł



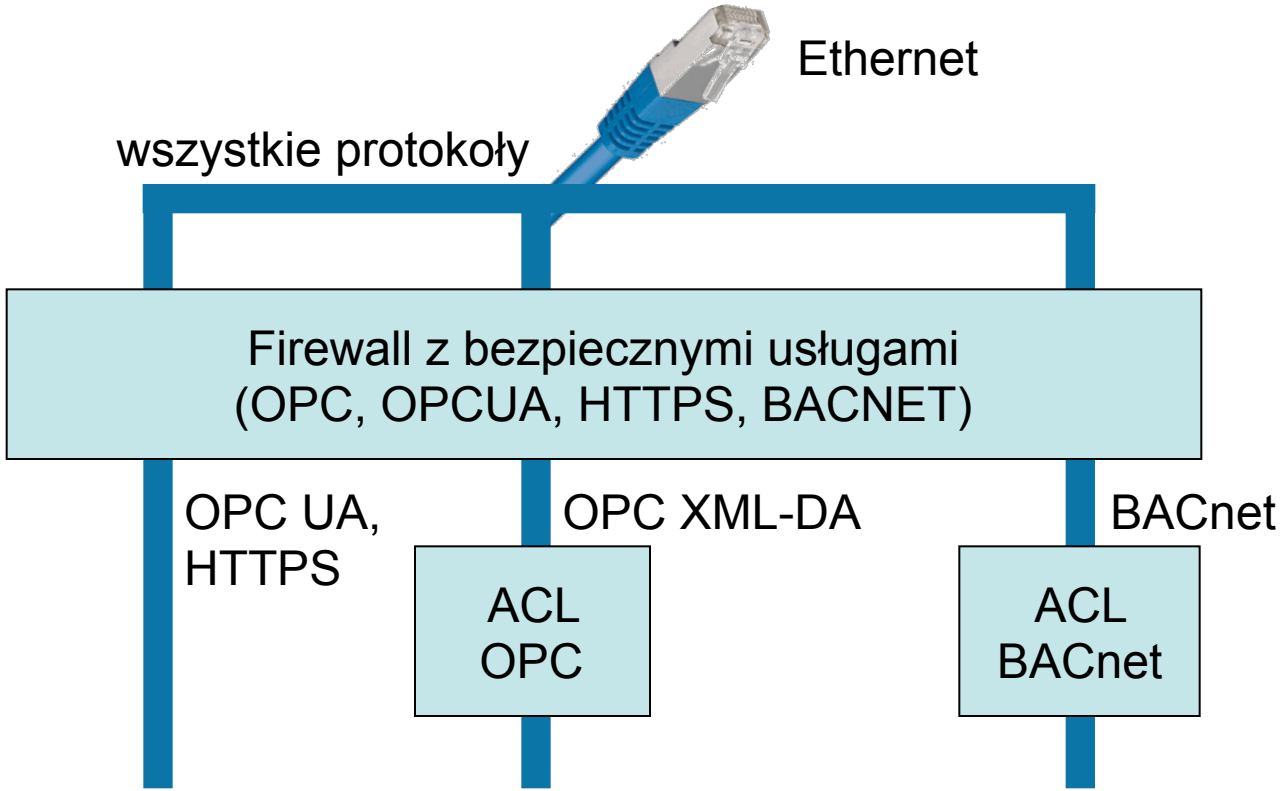


Bezpieczny dostęp

- Firewall (tryb bezpieczny)
  - blokada wszystkich niebezpiecznych portów
  - zezwolenie zdefiniowanych usług
- Listy ACL - Access Control Lists
  - zezwolenie określonych adresów IP
  - BACnet/IP (ACL)
  - LON (lista dostępu do kanału IP852)
  - Web Service (ACL)

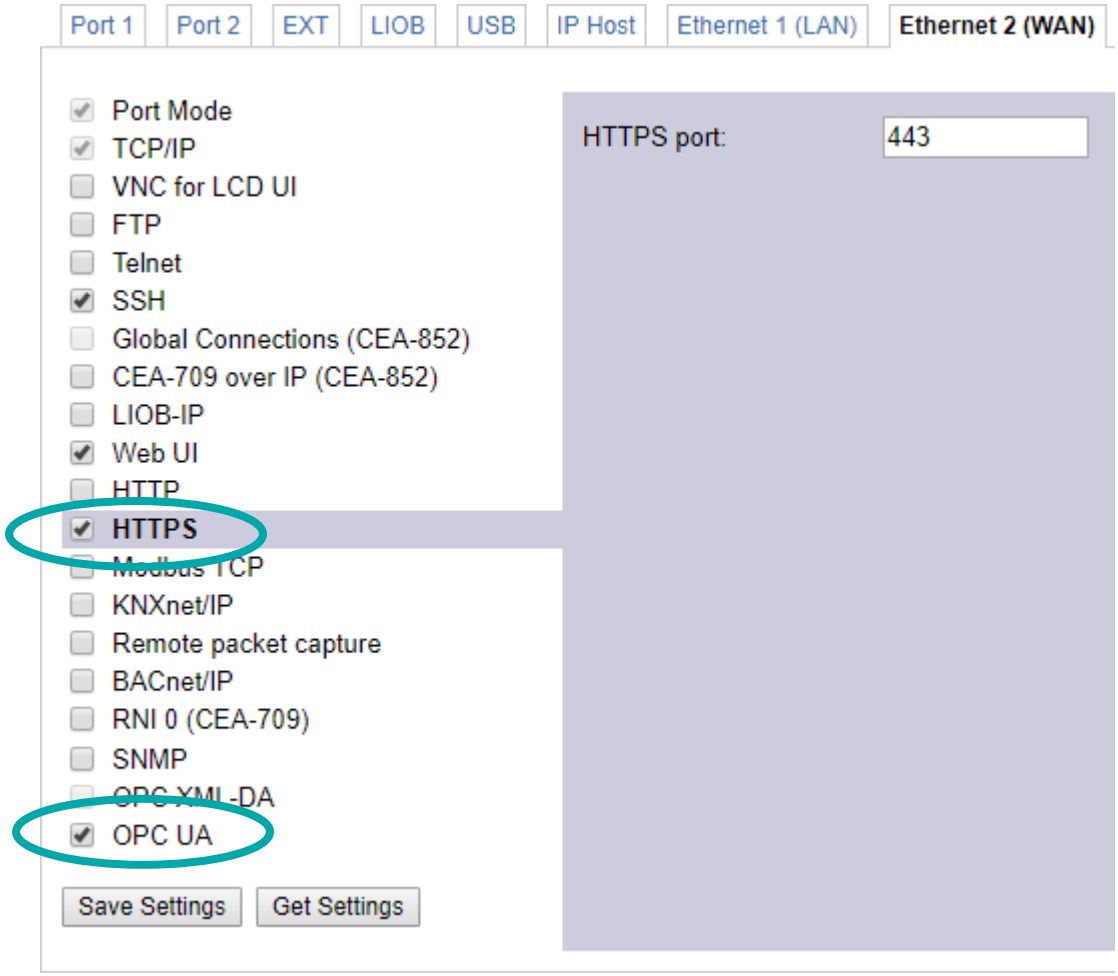


Firewall i listy ACL



Wbudowany Firewall

- Wybór z listy dostępnych protokołów



Listy Access Control Lists (ACL)

- Ograniczenie partnerów komunikacji
  - BACnet/IP
  - OPC XML-DA

BACnet Configuration

Device | Recipients | Time Master | BDT | **ACL** | Slave Proxy

Add | Delete

	IP Address	Subnet Mask	Access
☐	10.101.17.2	255.255.255.255	allow
☐	192.168.0.0	255.255.192.0	allow
☐	0.0.0.0	0.0.0.0	deny

Bezpieczne protokoły

- Szyfrowane
  - HTTPS: Web UI, Web services, konfiguracja
  - OPC UA: BMS, wizualizacja
  - SMTPS: bezpieczna poczta e-mail
  - SSH: diagnostyka i rozw. problemów
  - zarządzanie certyfikatami
- Wyłączyć
  - telnet, FTP

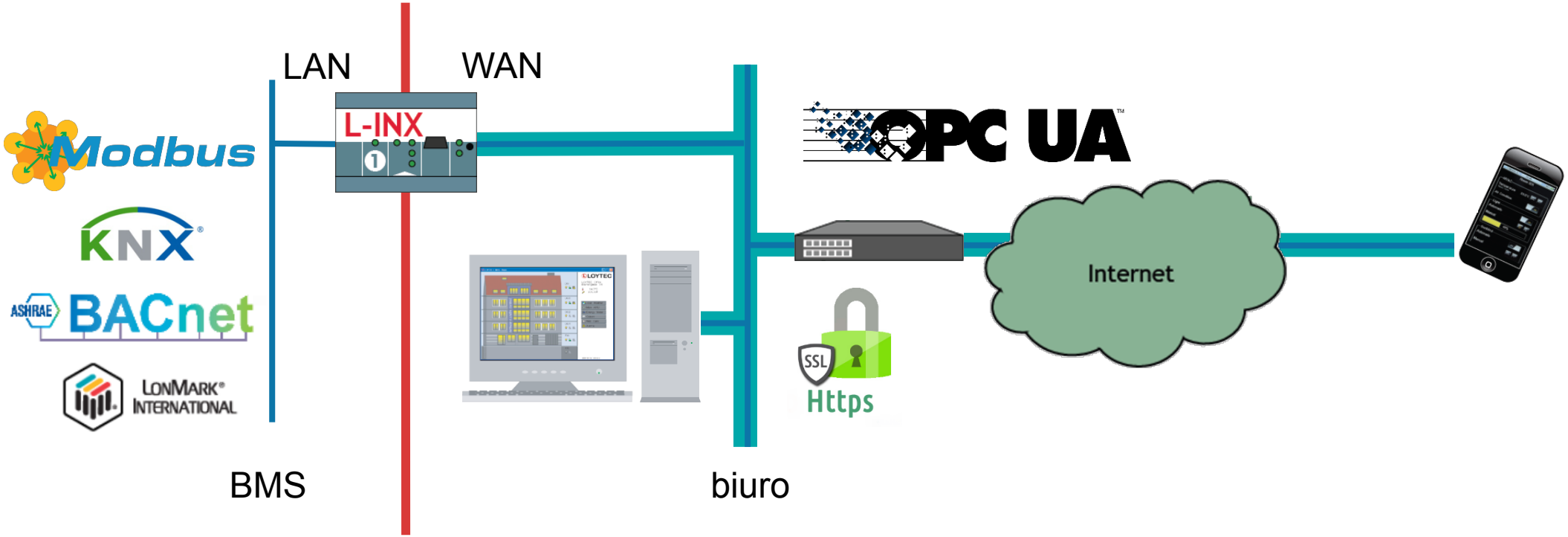
Tryb bezpieczny

- Konfiguracja trybu bezpiecznego
  - aktywacja
  - dodanie bezpiecznych usług
  - dostęp przez www

Secure Mode	input	binary	normal	active
Secure Mode_Set	output	binary	normal	active
Secure Services	input	string	normal	HTTPS OPC
Secure Services_Set	output	string	normal	HTTPS OPC

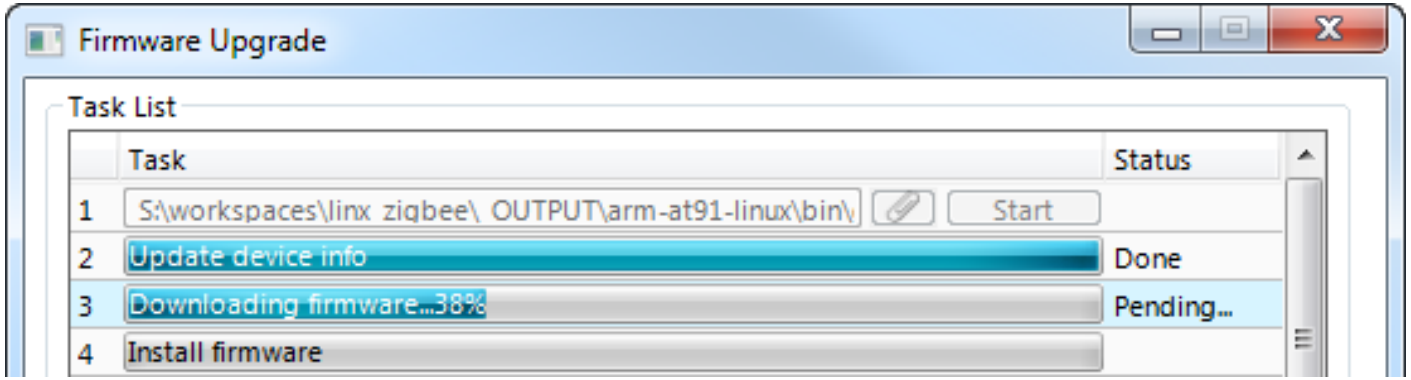
Odrębne rozwiązania sieciowe

- sieć LAN do sprzętu sterującego
- sieć WAN do bezpiecznego dostępu



Bezpieczne aktualizacje

- Aktualizacje firmware-u
  - aktualizacje znanych problemów bezpieczeństwa
  - permanentne testy najnowszymi narzędziami do ataków
  - zabezpieczenie przeciw exploit-om
  - użycie LWEB-900 do aktualizacji wszystkich urządzeń



Integracja LOYTEC z IoT

- Silnik JavaScript w urządzeniu
  - bazuje na node.js
  - model skryptów bazujący na zdarzeniach
  - standardowe moduły dla IoT
- Interfejs punktów danych
  - Skryptowy dostęp punktów danych (dpal.js)

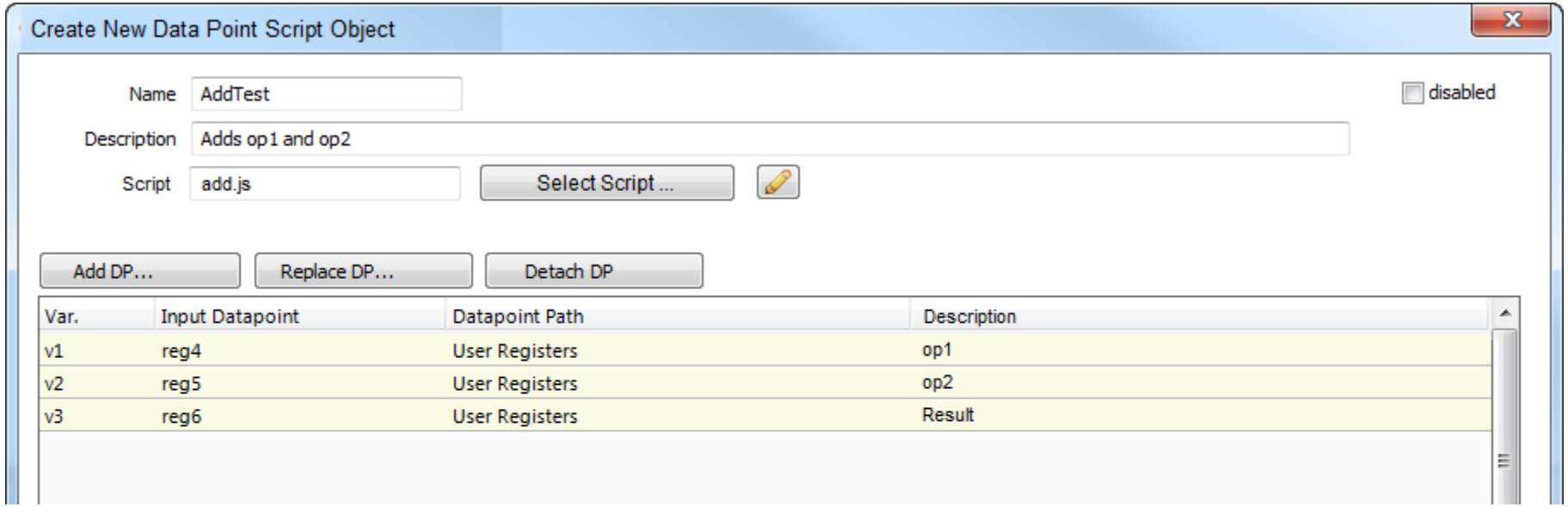
Zasoby skryptowe

- Nowy zasób w konfiguratorze
  - moduły zarządzane przez konfigurator
  - może być wykonywany
  - jawne mapowanie punktów danych (ścieżka/nazwa)

```
1  const dp = require("dpal");
2
3  // create dp objects from supplied dpReferences
4  var v1 = new dp('/User Registers/uptime');
5
6  // uptime of script in seconds
7  var uptime=0;
8  setInterval(function() { uptime++; v1.write(uptime); }, 1000);
9
```

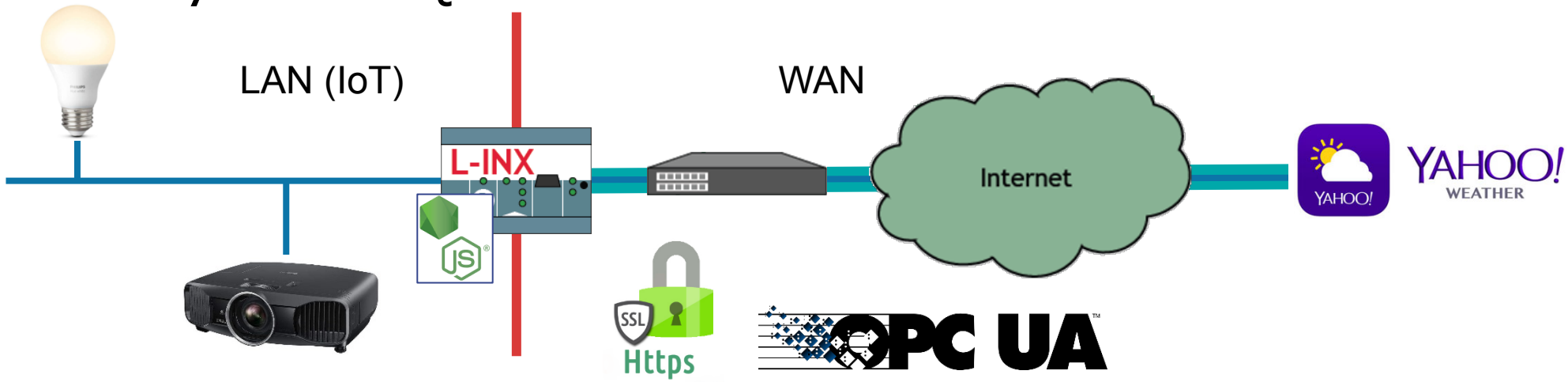
Obiekty skryptu

- Nowa klasa obiektów matematycznych
  - Obiekt odnosi się do zasobu skryptu
  - Utworzenie instancji z referencjami punktów danych



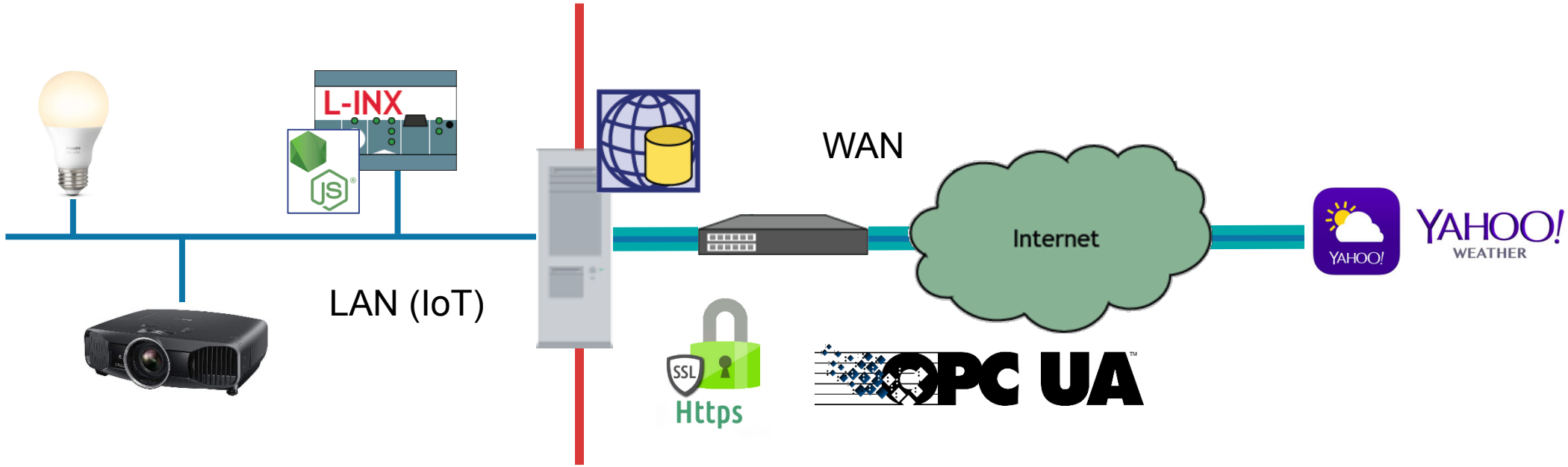
Bezpieczna integracja z IoT

- Podejście z wbudowanym bezpieczeństwem
  - ustawienie bezpiecznego hasła
  - zezwolenie na tryb bezpieczny
  - skonfigurowanie odseparowanych sieci – ukrycie urządzeń IoT



Bezpieczna integracja z IoT – LWEB-900

- Serwer LWEB-900
  - pojedynczy punkt dostępu – aktualizacje zabezpieczeń w jednym miejscu



Przykład 1: Pogoda Yahoo Weather

- Zasób skryptu: weather.js


```
// (1) map data point
var v1 = new dp('/User Registers/temp');

// (2) update weather data every 10 min
setInterval(updateWeather, 600000);

// (3) read weather channel and and write to data points
function updateWeather() {
  getWeather( (channel) => { v1.write(channel.item.condition.temp); });
}

// (4) get the Yahoo weather channel data
function getWeather(callback) {
  const queryUri = `https://query.yahooapis.com/v1/public/yql?q=select * from weather.forecast
  client.get(queryUri).then( (res) => {
    if (res.data.query.results) {
      callback(res.data.query.results.channel);
    }
  });
}
```

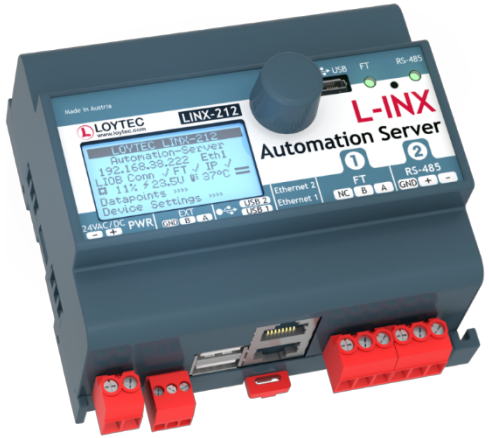
Przykład 2: Inteligentna żarówka

- L-INX uzyskuje dostęp do Philips Hue Bridge
  - LWEB-802 project


```
initHue();

function writeLightState(num, value) {
  try {
    var valobj = JSON.parse(value);
    var state = { on: valobj[0], bri: valobj[1] };
      hue.light(num).setState(state)
    }
  } catch (e) { };
}

var light1 = new dp("/User Registers/hue/lights/1/state");
var light2 = new dp("/User Registers/hue/lights/2/state");

light1.on('value', (value) => { writeLightState(1, value) });
light2.on('value', (value) => { writeLightState(2, value) });
```

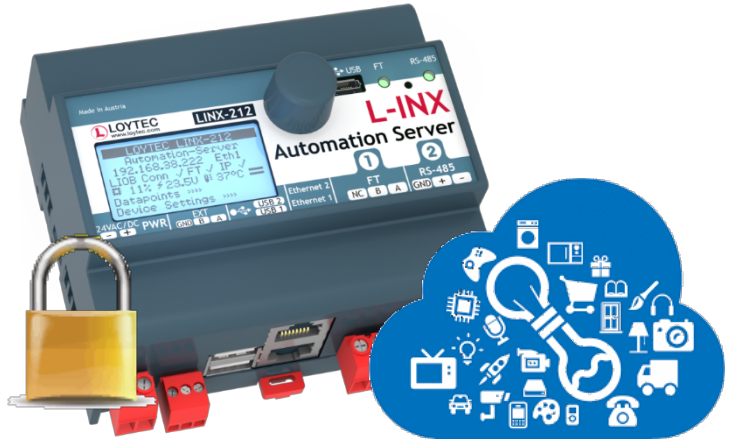
Produkty z obsługą IoT

- Programowalne L-INX-y
  - LINX-112/113/153/154
  - LINX-212/213/215
- LROC-102, LROC-40x
- Sterowniki L-DALI
- LGATE-902/952
- LVIS-3ME
- dostępny w firmware 6.3 (Q1/2018)



Podsumowanie

- LOYTEC integruje IoT
- LOYTEC zapewnia bezpieczeństwo
- rozwiązania LOYTEC dodają bezpieczeństwo do integracji IoT



Pytania?

Buildings under Control
Symposium 2018
Kraków 28.02 – 1.03. 2018

Dziękuję za uwagę

ZDANIA
ZINTEGROWANE SYSTEMY AUTOMATYKI I BEZPIECZEŃSTWA BUDYNKÓW

LOYTEC
COMPETENCE CENTER
IN POLAND

ZDANIA Sp. z o.o.
LOYTEC COMPETENCE CENTER
ul. Królowej Jadwigi 268,
30-218 Kraków
www.zdania.com.pl
office@zdania.com.pl
tel.: +48 12 638 05 67
fax.: +48 12 638 05 77

Presentation

- KISS: Keep It Short and Simple
- 5 ‘statements/issues’ per slide
- Avoid animations
- A picture says more than thousand words.
- Images
  - Minimize image size to keep the file size small.
  - LOYTEC Marketing Team is available for graphics

Logos