# Intro to IoT Security



Ivan Marković Ethical Hacker





## Hello, I'm ...

- Somebody who like to know how things works
- Somebody who broke into things for fun and profit
- and somebody who like to share knowledge



## and from my experience



# it's time to get serious

## What is OWASP



https://www.owasp.org/index.php/Category:OWASP\_Project#tab=Project\_Inventory

## What is OWASP



https://www.owasp.org/index.php/OWASP\_Internet\_of\_Things\_Project

## What is KALI Linux



https://www.kali.org/

## What we will learn today

- What is the Internet of Things (IoT)
- Why is so important to take care about security and privacy
- What are the main threats
- How to do basic security overview of your IoT system

# What is the Internet of Things (IoT)

- The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.
- Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental and user contexts.

# What is the Internet of Things (IoT)



# What is the Internet of Things (IoT)



- Smart home control (lighting, security, comfort)
- Optimized energy use
- Maintenance

#### 🗂 Retail

- Product tracking
- Inventory control
- Focused marketing

#### 🕀 Medical

- Wearable devices
- Implanted devices
- Telehealth services

#### Military

- Resource allocation
- Threat analysis
- Troop monitoring



#### Industrial

- SmartMeters
- Wear-out sensing
- Manufacturing control
- Climate control

#### Automotive

- Parking
- Traffic flow
- Anti-theft location

#### Environmental

- Species tracking
- Weather prediction
- Resource management

#### Agriculture

- Crop management
- Soil analysis

## Our Laboratory for today (1)



Logic Analyzer, Serial/UART interface, Bus Pirate v4, Set-Top Box

## Our Laboratory for today (1)

BOOTSPI BIST0\_OK \_OK!decomp \_done done

Hello U-Boot

U-Boot 1.1.6 (Aug 22 2016 - 16:45:10)

Board: MSTAR KRITI (CPU Speed 576 MHz) DRAM: 64 X 0 MBytes U-Boot is running at DRAM 0x87610000 Module: USB FAT FLASH SPI LOGO OSD ENV=SERIAL Flash is detected (0x0C02, 0xC8, 0x40, 0x16) In: serial **Out:** serial Err: serial MSVC00B000100100208768TH0000000T MDrv PNL Init u32PnlRiuBaseAddr = BF200000 MDrv PNL Init u32PMRiuBaseAddr = BF000000 DAC eTiming =6 HDMITx eTiming =7 HDMITx eTiming =7 Create Dolby single part name task failed!! [Hal VE EnableDI][1430] bEnable = 0, blsDNR2VE = 0 u32ReadBuffVirAddr = A0000000, u32IntBuffVirAddr = A0100000, u32OutBuffVirAddr = A0730000 verJPD SetStatus >>>>>> w:720, h:576, p:720

[GOP3, PID 0, TID 0x-1][Driver Version]: 0089, BuildNum: 0002, ChangeList: 00524916 keypad\_pressed is [0] ir\_pressed is [0] << MStar >>#

## Our Laboratory for today (2)



WiFi/LAN Router, 2 x Raspberry Pi 3, 2 x Temperature/Humidity Sensors, 2 x BLE Plugs + Fan's, USB WebCam, 3 x LEDs

## Our Laboratory for today (2)

mt:s ψ	<b>∦ .,,  </b> 95% <b>►</b> +	11:47	mt:s <b>* </b> 95% <b></b> 11:43
E Devices sto	P SCANNING	÷	Smart Lab PoC
SCANNER BONDED	ADVERTISER		CONNECT
No filter		•	LIGHTS ON
N/A (iBeacon) EA:DF:8E:F6:2B:1A NOT BONDED -68 d	CONNECT Bm ↔ 207 ms	:	LIGHTS OFF
Crown (iBeacon) C7:F1:D3:E0:75:25 NOT BONDED -56 d	CONNECT Bm ↔ 317 ms	•	PRO. VERSION Hello World!
SmartLab B8:27:EB:C6:B9:E4 NOT BONDED -59 d	CONNECT Bm ↔ 94 ms	:	👿 Web page not available
			The web page at http://smart.lab/password.txt? username=admin&password=admin&token=1234 could not be loaded because:
			net::ERR_NAME_NOT_RESOLVED

Wireless by Nordic

## Our Laboratory for today (3)

•••	OWASP T	OP TEN	× +			
← →	۵	i http://192.16	8.0.12/owasptopten/?	🔽 🏠 🔍 Search	>>	Ξ

[	User	name:		
[	Pass	word:		
l	Open	Sesame		
	Groups () j	for this user!		
Select image to upload:	Browse	No file selected.	Upload Image	]

DEBUG SQL: SELECT \* FROM users WHERE username = "' AND password = " LIMIT 1 ERROR DESCRIPTION: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near "" AND password = " LIMIT 1' at line 1 Content here!



• IoT is all about data and control

- No One's Telling You Your Data Is Valuable
- Limit on Power / Control / Manipulation

• Regulatory compliance





Za opseg vašeg posla Što je za to zadužena treća strana Što ste nasledili taj sistem Što je "komplikovano implementirati zakrpu" Za vaš zastareli windows Za vaš budžet Što ste to uvek tako radili Za datum izlaska vaše finalne verzije Što je to samo primer realizacije Za vaše ugovore o poverljivosti Što to nije bio zahtev ugovora Što je to vaš interni sistem Što je baš teško da se to promeni Što će to uskoro da se zameni Što niste sigurni kako da to popravite Što je to u Oblaku Za vaše procene rizika Što proizvođač ne podržava tu konfiguraciju Što je to privremeno rešenje Što je enkriptovano na disku Što se ne uklapa u novčane benefite Što "Niko drugi to nije uspeo da uradi" Što ne možete da objasnite rizik nadleženima Što imate druge prioritete Što nemate poslovno opravdanje Što ne možete da prikažete povratak investicija Što ste izbacili mogućnost tog rizika

#### WHY HACKERS HACK WHO'S BEHIND DATA BREACHES? MOTIVES BEHIND CYBERATTACKS GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES GLOBAL STUDY OF LARGE ORGANISATIONS THAT WERE VICTIMS TO A CYBERATTACK Outsiders .c∰D Organised Ē <u>×Ĥ×</u> criminal groups Internal actors State-affiliated actors 41% 27% 26% 26% 24% 11% 20% **Multiple parties** Political Ransom Insider Competition Cyberwar Angry user Motive Partners threat unknown Radware 2017 0% 20% 40% 60% 80% Verizon 2017 DATA BREACHES, BY PATTERN AND MOTIVE GLOBAL STUDY OF ALMOST 2,000 DATA BREACHES 61-100 101+ 1-10 11-30 31-60 PATTERN Financial Fun, ideology, grudge Espionage Lost and Point Miscellaneous Web app at-Payment card Everything Denial Privilege misstolen MOTIVE\* of service use assets of sale error tacks Crimeware skimmers Espionage else ACCOMMODATION AND FOOD SERVICES EDUCATIONAL SERVICES FINANCIAL AND INSURANCE HEALTHCARE INFORMATION MANUFACTURING PUBLIC ADMINISTRATION RETAIL 0% 20% 40% 60% 80% \*Some motives were unknown so not included in this data Verizon 2017

RACONTEUR

100%

100%

HACKING TOOLS & SERVICES									
Account Hacking Program	\$12.99 (See more details on page 10)								
Hacked Instagram Accounts in Bulk	1,000 - 10,000 accounts <b>\$15 - \$60</b>								
Botnet: Blow-Bot Banking Botnet	Monthly Basic Rental <b>\$750   M</b> onthly Full Rental <b>\$1,200  </b> Monthly Support <b>\$150</b>								
Disdain Exploit Kit	Day <b>\$80</b> , Week <b>\$500</b> , Month <b>\$1,400</b>								
Stegano Exploit Kit: Chrome , FireFox, Internet Explorer, Opera, Edge	Unlimited Traffic, Day <b>\$2,000</b> Unlimited Traffic, Month <b>\$15,000</b>								
Microsoft Office Exploit Builder	Lite exploit builder <b>\$650</b> Full Version <b>\$1,000</b>								
WordPress Exploit	\$100								
Password Stealer	\$50								
Android Malware Loader	\$1,500								
Western Union Hacking Bug For World Wide Transfer	\$300								
DDoS Attacks	Week long attack <b>\$500 - \$1,200</b>								
ATM Skimmers: Wincor, Slimm, NCR, Diebold	\$700 - \$1,500								
Hacking Tutorials	Multiple Tutorials <b>\$5 - \$50</b>								

🔏 Ѕнос	DAN schr	neider device -ubiquiti		۹ 🕷	Explore	Downloads	Reports	Developer Pricing	Enterprise Access		
8 Exploits	🐔 Maps	Share Search	🛓 Download Results	Lul Creat	e Report						
TOTAL RESUL	TS		46.14.182.52								
1 621			52.182.14.46.static.wline	e.lns.sme.cust.swi	sscom.ch	Unit ID: 0					
1,021			Added on 2018-03-18 17	ed on 2018-03-18 17:08:26 GMT			Device Identification: Schneider Electric SAS TSXETY4103 V4.3				
TOP COUNTR	IES		Switzerland, Gase Details	el		Unit ID: 1					
	The second		Details			Device Ide	ntification:	Schneider Electric SAS	5 TSXETY4103 V4.3		
	AV- C	and the second s									
						Unit ID: 2					
		A STA				Device Ide	ntification:	Schneider Electric SAS	TSXETY4103 V4.3		
		0				Unit ID: 3					
	6.					Device Ide	ntification:	Schneider Electric SAS	TSX		
France		279									
Spain		202									
Brazil		168	166.155.236.2	24							
Turkey		129	Verizon Wireless	/zw.com		Instance ID: 100					
			Added on 2018-03-18 17	7:07:36 GMT		Vendor ID: 0	Sillar LS LT UXUN	e controller i			
TOP SERVICES	5		Details			Vendor Name:	Schneider				
Modbus		1,481	ics			Application Software: 0.5.2					
503		70				Firmware: 2.2	0.1.4				
EtherNetiP		45				Model Name: S	MantStruxure				
HTTPS		2				beschiption.	nanager				
						Foreign Devic	e Table (FDT	):			
TOP ORGANIZ	ZATIONS					166.155.2	36.26:47808:	ttl=60:timeout=38			
Orange		244									
Vivo		121	102 249 120	14							
Turkcell		113	LPuteaux-657-1-96-14.w	14 /193-248.abo.wan	adoo.fr	Unit ID: 0					
Verizon Wireles	\$\$	107	Orange	-54-20 GMT		Device Ide	ntification:	Schneider Electric BMX	NOE 0100 V2.90		
Vodafone Rom	ania	33	France, Cluses	NOTION OFFICE		CPU module	: BMX P34 20	20			
TODODED			Details			Memory car	d: BMXRMS008	MP			
TOP OPERATI	NG SYSTEMS		ics			Project in	formation: P	rojet - V8.0 PA101708			
Windows 7 or 8	8	7				Project la	st modified	2018-03-12 11.31.30			
						in officer in	et mourreu.	2010 00 12 11101100			

Autosploit marries Shodan, Metasploit, puts IoT devices at risk



Autosploit marries Shodan, Metasploit, puts IoT devices at risk scmagazine.com

Car Backdoor Maker v1.0											×	
<u>F</u> ile	<u>T</u> ools <u>H</u> e	elp										Car Backdoor Maker v1.0 By @UnaPibaGeek - @holesec
Basic	Setup											Status
	ID 60D	DLC	#1	#2	#3	#4	#5	#6	#7	#8	SMS	
2	60D	8	46	16	00	00	43	4F 4F	02	00	LBON	
3 4 5	651	2	04	FO							CNON	40
AdvaA	Advanced Setup Frame Ø GPS    Attacker's Tel-Number Filter Inject the previously defined frame (1-5):   You'll send the SMS commands from: Inject the previously defined frame (1-5):										GPS 🌍	
When the target passes near the following coordinates: STOP Enable SMS "STOP" Command?										Device		
	24%											

- Common IoT Architecture -



### IoT Attack Surface Areas





#### **Ecosystem**

#### Interoperability standards Data governance System wide failure Individual stakeholder risks Implicit trust between components Access procedures



#### Health checks Heartbeats Ecosystem commands De-provisioning Pushing updates

**Ecosystem Communication** 



# IoT Ecosystem Example

#### The Healthcare Internet of Things (IoT) Market Map



www.cbinsights.com

### IoT Ecosystem services providers



### This is also a part of IoT Ecosystem



### This is also a part of IoT Ecosystem



### Hardware / Device

Sensors

Device Physical Interfaces

Device Memory

**Device Firmware** 

Device Web Interface

**Device Network Services** 

Update Mechanism

#### **Sensors**

Sensing Environment Manipulation Tampering (Physically) Damage (Physically)





## Sensors in Smart Home



# Sensors in your Car

#### Automotive Sensors



#### **Device Physical Interfaces**

Device ID / Serial number exposure Firmware extraction User CLI Admin CLI Privilege escalation Reset to insecure state Removal of storage media Tamper resistance UART (Serial) JTAG / SWD
## Device Physical Interfaces in MSTAR / Vivax Set-up Box



## Device Physical Interfaces in HUAWEI / Telekom ADSL routers



## Device Physical Interfaces in TP-LINK router



## Device Physical Interfaces in Crownstone smart power plugs



## **Device Physical Interfaces**



#### **Device Memory**

Sensitive data Cleartext usernames Cleartext passwords Third-party credentials Encryption keys PIN codes

#### **Device Firmware**

Sensitive data exposure Backdoor accounts Hardcoded credentials Encryption keys Vulnerable services and software versions Security related function API exposure Firmware downgrade possibility

**Device Firmware** 

## Hard-coded password exposes up to 46,000 video surveillance DVRs to hacking

Hackers can log into DVRs from RaySharp and six other vendors using a six-digit hard-coded root password

## Internet cameras have hard-coded password that can't be changed

Cameras with multiple brand names are wide open to remote hacking.

## **Vulnerable Device Firmware**

The following devices are known to be vulnerable:

Model Name	System Firmware Version	Application Firmware Version
Opticam i5	1.5.2.11	2.21.1.128
Foscam C2	1.11.1.8	2.72.1.32



Tens of thousands of potentially vulnerable devices are exposed to the internet around the world.

#### **Device Network Services**

Information disclosure User or Administrative CLI Command Injection Denial of Service Unencrypted Services Test / Development Services Credential management vulnerabilities Buffer Overflow UPnP

## Huawei HG532 UPNP Botnet



#### **Update Mechanism**

Update sent without encryption Updates not signed Update location writable Update verification Update authentication Malicious update Missing update mechanism No manual update mechanism

## USB firmware update

- auto\_update / bin / zip / ...
- auto\_upgrade / bin / zip / ...

HARCHER CONTRACTOR

## General USB attacks



USBee attack 2016

28

### **Network Traffic**

Wireless (WiFi, Z-wave, XBee, Zigbee, Bluetooth, LoRA) LAN, LAN to Internet Non-standard, Protocol fuzzing





### **Network Traffic**

Rough Devices, MiTM



### **Network Traffic**



#### **Device Web Interface**

Standard set of web application vulnerabilities, see: OWASP Web Top 10 OWASP ASVS OWASP Testing guide

> Credential management vulnerabilities: Username enumeration Weak passwords Account lockout Known default credentials Insecure password recovery mechanism

## **OWASP WEB TOP 10**

OWASP Top 10 - 2013		OWASP Top 10 - 2017	
A1 – Injection	<b>→</b>	A1:2017-Injection	
A2 – Broken Authentication and Session Management		A2:2017-Broken Authentication	
A3 – Cross-Site Scripting (XSS)	3	A3:2017-Sensitive Data Exposure	
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]	
A5 – Security Misconfiguration	3	A5:2017-Broken Access Control [Merged]	
A6 – Sensitive Data Exposure	7	A6:2017-Security Misconfiguration	
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)	
A8 – Cross-Site Request Forgery (CSRF)	×	A8:2017-Insecure Deserialization [NEW, Community]	
A9 – Using Components with Known Vulnerabilities		A9:2017-Using Components with Known Vulnerabilities	
A10 – Unvalidated Redirects and Forwards		A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]	

#### **Mobile Applications**

- M1 Improper Platform Usage
- M2 Insecure Data Storage
- M3 Insecure Communication
- M4 Insecure Authentication
- M5 Insufficient Cryptography
- M6 Insecure Authorization
- M7 Client code Quality
- M8 Code Tampering
- M9 Reverse Engineering
- M10 Extraneous Functionality

### **Cloud Services**



# How to do basic security overview of your IoT system

- Information gathering
- Hardware
- Communications / Network
- Software

## Read the documentation :)



#### Pokazivači maksimuma

Standardno, dva maksimuma 15-minutne srednje snage (1.6.1 i 1.6.2) se beleže za prvu i drugu tarifi 

ija moregi -reninismu andrani raponaj on natima nasovranja so se more iskatsum za jiji moregi praktimu ao dovrini ana punog sun. Io 1021 pokazaje akode i tidade merejie srednje 15-minuma aktivne srage (bela kazajika), videti narastivo ao 1082, DEMA DONGT.

Usodjuji je elektronska oprema koja po prestanka uporsche podlaže obavezi odlaganja etgala trze dostapne slazene za prikujijanje i odlaganje otgada koga čisi elektronska eprema. Dradjuja se re ume bucati u umore iz domastimošta. X

GARANCLIA

FABRIČKI BROJ

Digitalno brojilo DB2 proizvedeno od starse "ENEL" d.o.c. Bosgrad, ima garancjiu za muterijsl, i fankcimisnije prema specifikaciji prekordaka u tajanja od tri gudine od tranuka igorake. da posednje veličacija o igoracu za na za faktiko brojere brojila. U taku garancije, proizved će u služaju neispravnesti bili popera/jan ili zamanjen novim o trasku dose.

reizvedab, Ked tanja proizveda na sorvisinaje u toku gamecije, korinik snosi truškeve noetaže, mentate i služu proizveda, dek truškod imagota u obnuzon inese padaju na tere produceša Gamecija se u odnosi na dokička izovare o reprovišnom mentakon, potroben i redižavanjem nebaja od zame kapes, Gamecija se e odnosi na du nedaju izva uslava specificinatih a orona apatriva. Drzeg zameli, osim ved nava udostih, se ne podrazmenjeni du, u.

"ENEL" d.o.o. Beograd, Petrovaradinska 26, 11000 Beograd Phone: ++381 11 285 0 582 Fax: ++381 11 285 0 580 enel@EUnet.rs http://www.enel.co.rs V2 RO

#### Ostale funkcije brojila DB2

Contact summaple networks of the status heads heads heads and the status and t

ri za listanje Benjiko na displeju pokazuje tri setu podruka u modovimu rada displeju A, M, O (A-automatica) Benjiko na displeju pokazuje tri setu podruka u da konzeditočki radi.

Brijflam, nifopije pokonjet in sten politika u modovim mla displad A, M, O (Austomatia, mulk, Orbitalisti, Turoglari karne yakanje nad i lonen finoji niti. Gornji uster služi na izbor moda nak displat, a dotji na littanje numer oklarasne unok Pitikkom su gornji uster u dijinju objero skundi petensis zi znadi A u ma M i obratus. Ako do M gornji uster di če stakata, prelazi su a na O. Pitikako na gornji uster v najju o djeto skundi petensis v diversite i kon do moda na poslati se najju o djeto skundi petensisti petensisti solju peter v najju o djeto skundi petensisti mo olnarava se pickazi i djetjej nazavlja neomala na. Pritiska ko dogi petensisti i djetjej nazavlja neomala na. Pritiska ko dogi peter v ingiju o djet v skundo v dve ja priticika jeda da staka zameta o kone tremto nadi, lo važi za svaki nod. U bilo som nodi nadi pritiskom ma goriji natar u trajnite ud čatit skalanda ačivira se mod na politika staka najju na jeti na priti naj na naj na politika skala na zameta na oka staka na politika skano na djetaje politika na jeti na najju na politika politika na okolativati na politika na politika politika na okolativati na politika politika politika politika politika politika politika politika na politika po

elaltaçla modul Brojiko DB2 ima mogućost priključenja-trofaznog prekidarkog modulu PM1 sa kojim komunicim preko Mbas-

Tip Nerrinalei napon V.	DB2 3x230/400V (+15%, -20%)	Funkcija trofaznog brojila aktivne energije klase 1, 2		
Nominalita frekvencija f <sub>6</sub> Bazna straja I <sub>8</sub>	50 Hz 5A, 10A	Klasa talnosti Konstanta brojila	JUS IEC 1036 klasa 1, 2 1000 impulsa/kWh, opti2k	
Prag merenja Divaž intralsa:	<20mA po fazi ontokonievan. 90. IEC 62053-31.	Impulsni izlaz brojila	(300 impulsación, econer 1 Wh/impuls (2Wh/impuls)	
	Class B, 2Wh/impulsu	Funkcijo uklaman čas	sanika	
napon impulsa(max) struja (max)	15V 15mA	Tačnost časovnika Rezervní hod	±1 minut/mesec >15 godim	
Botoshier	Jones	Funkcija pokazivača maksimuma klase 1		
nzponsko kolo pri V, strujno kolo	<1W(9VA) po fazi <0.5VA po fazi	Klasa tačnosti	MUSJF-4/2 kizzi 1 IEC 211 kizzi 1	
lspitti napon Preturonska zaštita	4kV, 50Hz, 1 minut 6kV, 1.2/50us	Memi period	programljiv početra vrednost: 15min/9	
Temperaturski opsog rada Relativna vlažnost ambilenta	-25°C, +70°C	Relejni izlaz	3A/230Vac	
Dimmzije kućištu 327,5 x 170,0 x 65 mm Otvor za novoduk na stezalici 6.5 mm		Relejna priključnica		
Tetira	1,05 kg	Struia	3x230/400V 3x100A	
Opiaka port	RS232/485 protokol DLMS	Ručno isključanje		
zien pur		Detalji dati u "Uputstvu za prikljačenje brojila DB2 sa relejnom prikljužnicam"		

+ ENEL d.o.o. Beograd DIREKTNO TROFAZNO BROJILO

adlms DB2 CORN

Brojilo zadovoljava specifikaciju Tehničkog saveta EPS-a donetu 11.12.2013. godine Korisnik je obavezao do pre upotrebe proveri da li se fabrički broj brojila DB2 slaže sa fabričkim brojem na garanciji. Uputotvo je važeće samo ako su fabrički brojevi isti.

Detaljni podaci o urođaju se nalaze u dokumente "Korisničko uputstvo za DB2, DB2M, DMG2 " koje je nametjeno za projektante i tehničke rukovodioce u distributivnom preduzniku.

Funkcije Doctore predsomo bregilo DB2 meri aktivnu energiju u klasti 1, 2 i makeimam enednje 15-minutose aktivne anage a klasti 1, u sistemu su česin provodnika u direktanji vezi su do četiri tarifa. Bregilo meri i prikazaje snagu, najove i straje po fazaran. Bregilo meri zavati oprikli po naj si straj a sogrammenje i odhavanje brojila i ugrađenih ukopnih

razu. Breijila,DB2 izu i évožítni RS 485 port. Breijila,DB2 izu upaden DLMS postol za konsurikaciju su spoljnim svetem. Pretokol Kreijule podo žičnog port. Preko opriklog porta, DLMS komunikacija funicionije preto protokolu 6 200-21 Mode E.

21 Moder E. lo DB2 ima uguden akkopni časovnik taji služi za registaciju događaju i za prebacivanje tacifa. Tarifa se na distan konvedan sko korstifu alze T12 slobođan. Ako je na tarifu ulaz T12 brojila politjučena

Prinnea. Prinnea. Do 1001 je semenjeno za meneje deleto energije i mikelomma sange u titokaj poznataj i naj ilegije je predstavan za diestara teneretivist priljeksk sa nepozon 3x300000 i mikratikom spojim 3663/1036, zama meng 5x100. Rogile DRZ je sretikene u kolčitu od usengaviseg polikeherara. Septivem akkepta naprese polita je imeđena u kosm kazam priljužnice. Kazedovi a priljužnej sojisnje oklopne naprese, MelUS, RS465 i rele gaspe trolita se nalaze u denom kazenu peljužnice.



Composition of the second second

Thick 1. Thick 1. In this case of the second secon rementsko-uklopne naprave. Icentsk 2 predstavlja vezu sa naponom faze 1.1, 5 sa 1.2, 8 sa 1.3. maju faza i mala za persocine rappianje, koristi se žica debljine do 1,5mm<sup>2</sup>.

Kada se uz

Redosled faza kod priključenja brojila nije bitan. Smor toka onergije se mora poštovati . Dolazak sa mreže kontakti 1, 4 i 7. Odlazak ka potrošača kontakti 3, 6 i 9.

Prikljuženje brojila DB2 sa relejnom prikljužnicom je detaljno opisana u "Uputstvu za montažn DB2 sa relejnom prikljužnicom" NAPOMENA: Also sin a displeju pojavi ponda greške FF XXXXXXX urskji tetis vniši preisveliča, mim Jaža prakravnja greška FF B100000, sak krvisti MORA PRVO DA PROVERI do I postaji preiskažki usodi j reje škole posena. Also predkladi modul obstan. Moje moda prisnar jedno postaji preiska pos retimja da je prakladi modu obstan. Moje moda prisnar i dobe povezan, and postaje postaje algeška je jedno post na i zmani predkladi modul obstan. Moje moda prisnar i dobe povezan, and postaje postaje algeška je jedno post na i zmani predkladi modul. Jose za moste predkladi postaji postaji postaji postaji postaji postaji postaji post postaji posta

masevia, Izno hojilo DB2 mole du se koristi u monofaznej vezi bez izmena sofvera ili hardvera, tako štu se a fazu L2 i L3 ne povenuju. Takvo hrojilo se utole postaviti na monofazu trijine prikljednica koju jedav sele na fazi L1. Opis monofazue reliejne refikiljednice je da u "Upatstva za monetažu hrojili. DRj

Stretytene pro-limpolsni idzi Impolsni idzi 15m. Urajać in pravla i offans. Konstanta impolsa je 2% filmpolsa. Udza se uzima sa igličastog konstazara koji se nakać u dosnom buzara i to između konstanta 11.2 za dstove energija, sika 7. Ugrađena LED-disola 1 dige vedlosne impolse za impolsni izdra zdrivog benjita.

VAŽNO: U slučaju da je brojilo povezano tako da je smer proteka energije suprotan od impulsni izlaz se ne generšie, kao ni svetlosni impulsi, kada brojilo ima kočalcu Tarifa

Tarifa Kah knjih DR2 pilasoje rajskar prve tarife za slebne energiju, ra LCD indianes se pokazaje vodeta condu IAI X0XXXXX Kah hnjih DR2 pikazje rajskar engiar druga, teris i červre tarife za altriven energije, ra LCD indianes se pokazaje vodet carda kaj IXXXXXXXX, tali SXXXXXXXX, tali Artikazi Artikazi IXXXXXXX, radje se pokazaje u otoko na se obchines u ISXX Tarifa ta slogi po pokažnej vodeto rada kaj IXXXXXXX za slovanje se na LCD indiastre karectera sa leve donje stane LCD dingin, Promen tarika se vrši preko matratajn ili pieko aplikajne donje na parace. Ja sloven kaj in stani kaj IXXX piekova pokazaje se na LCD indiastre karectera sa leve donje stane LCD dingin, Promen tarika se vrši preko matratajn ili pieko aplikajne donje na parace.

ju uklopen anprava ima prioritet nad unstatujion uklopnom napravom. Unstrašnja uklopna raprava može vojik ili MTK prioritik.
omena tarifa preko spoljačnja uklopne naprava se izvodi preko relea vremensko-uklopne naprave tisko ita se šor raprom 2009 prema tabeli ili slici 2.





#### **BUS PIRATE / ANY UART DEVICE / RASPBERRY PI / LOGIC ANALYZER**











## **Dump Firmware**



## Check communications









## Check communications



A new attack vector exposes almost every connected device.

## Check communications





#### bleno

#### gitter join chat

A Node.js module for implementing BLE (Bluetooth Low Energy) peripherals.

Need a BLE central module? See noble.



## Analyze firmware





## Check network services









# Analyze web applications and services











Nikto

## Analyze mobile applications



## drozer

## FЯIDA

#### QARK

build passing

Quick Android Review Kit
## **DEMO TIME**



## QUESTIONS



## Thank you for your time!

You can contact me via e-mail:

ivanm@security-net.biz

"If you think you are too small to make a difference, try sleeping with a mosquito." - Dalai Lama XIV