Hétpecsét Egyesület
LXXXIII. Szakmai Fórum

IoT szenzorok biztonsági kérdései és megoldásuk

Budapesti Műszaki és Gazdaságtudományi Egyetem

Távközlési és Médiainformatikai Tanszék

Pal Varga, PhD

Áttekintés

- Internet of Things, Cyber-Physical Systems,...
  - átfedések a buzzword-ök között
- Internet of HACKABLE Things
  - esettanulmányok
- Smart & Intelligens szenzorok
- Az IoT architektúra rétegei
  - más-más biztonsági kihívások
- Biztonsági megoldások a szenzor rétegben

Pókerparti?

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Sunday April 15, 2018 Wang Wei

Share 9.13k Share Tweet Share

A hackereknek sikerült kihasználni a kaszinó előterében lévő akvárium (netre kapcsolt) termosztátjának sérülékenységét. Amint bejutottak, hozzáfértek a „high roller” adatbázishoz, és a termosztáton keresztül kijuttatták a publikus internetre az adataikat.

From Prof. Nicola Dragoni, @ ETFA 2018

Welcome to the smart home ... of horror!

By Glenn McDonald, InfoWorld | June 4, 2015

Security issues are darkening the future of home automation and the Internet of things.

December 21, 2015 7:00 pm

Cyber security: Attack of the health hackers

Kara Scannell and Gina Chon

Share | Author alerts | Print | Clip | Comments

Breach of Anthem database, probably from China, is part of a 2015 wave of 100m hacked medical records

TODAY'S TOP STORIES

Despite reports of hacking, baby monitors remain woefully insecure

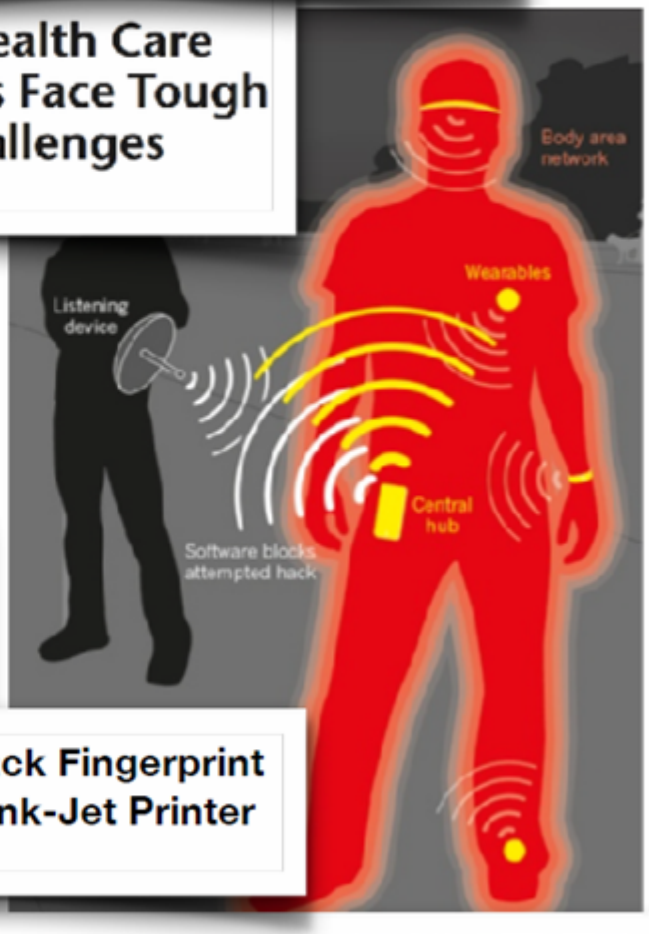
Researchers from Rapid7 found serious vulnerabilities in nine video baby monitor devices

MORE GOOD READS

Welcome to the

Pervasive Health Care Applications Face Tough Security Challenges

Vince Stanford



...It's Actually Worse Than You Think...

NATURE | NEWS FEATURE

What could derail the wearables revolution?

Electronic gadgets on — and in — our bodies are multiplying fast, but transmitting all their data safely will be a challenge.

Researchers Hack Fingerprint Sensors Using Ink-Jet Printer

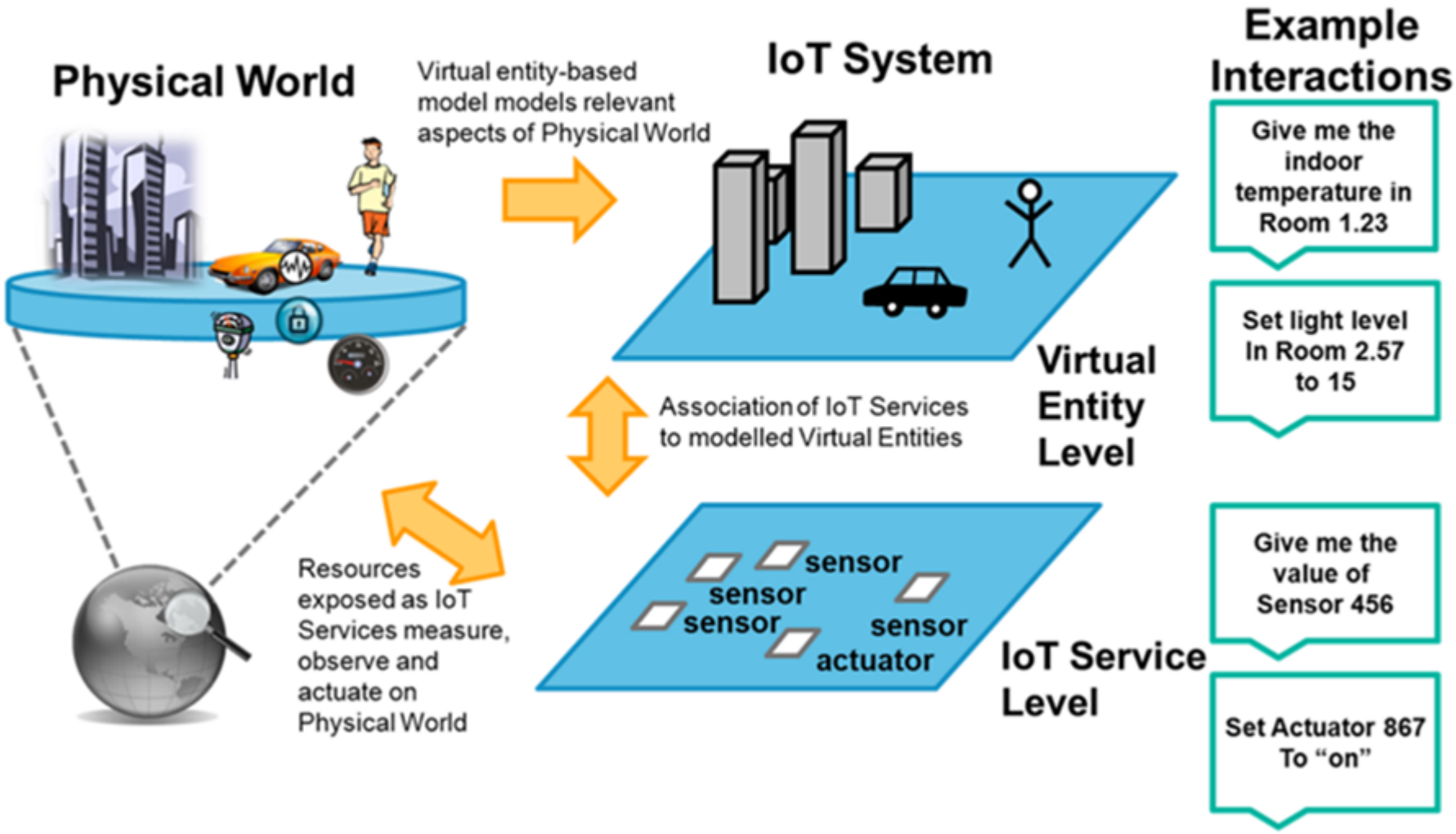
Author: SecureWorld

Hackers Killed a Simulated Human By Turning Off Its Pacemaker

September 7, 2015 // 11:45 AM EST

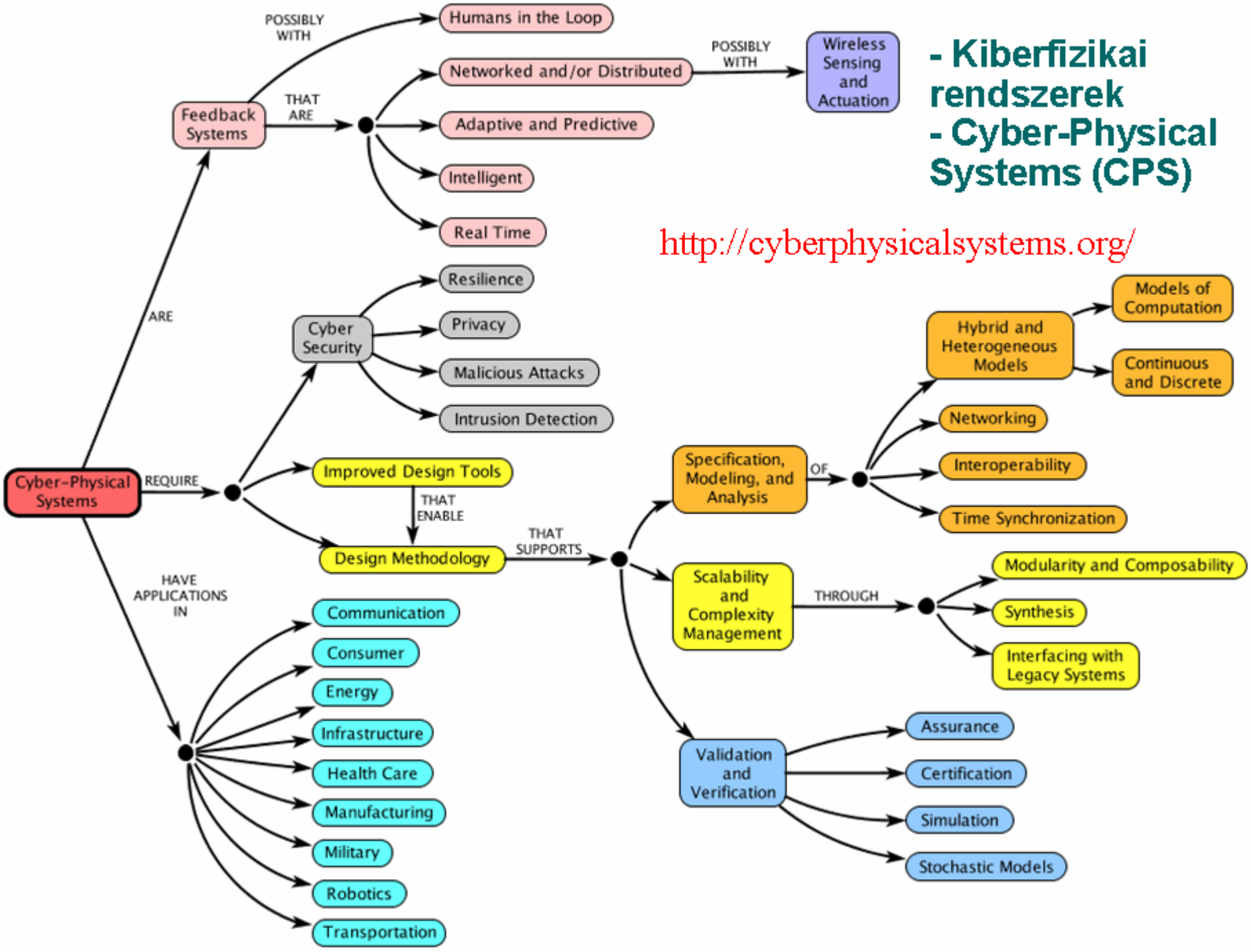
Hackers Love the Internet of Things

Egy tipikus IoT architektúra

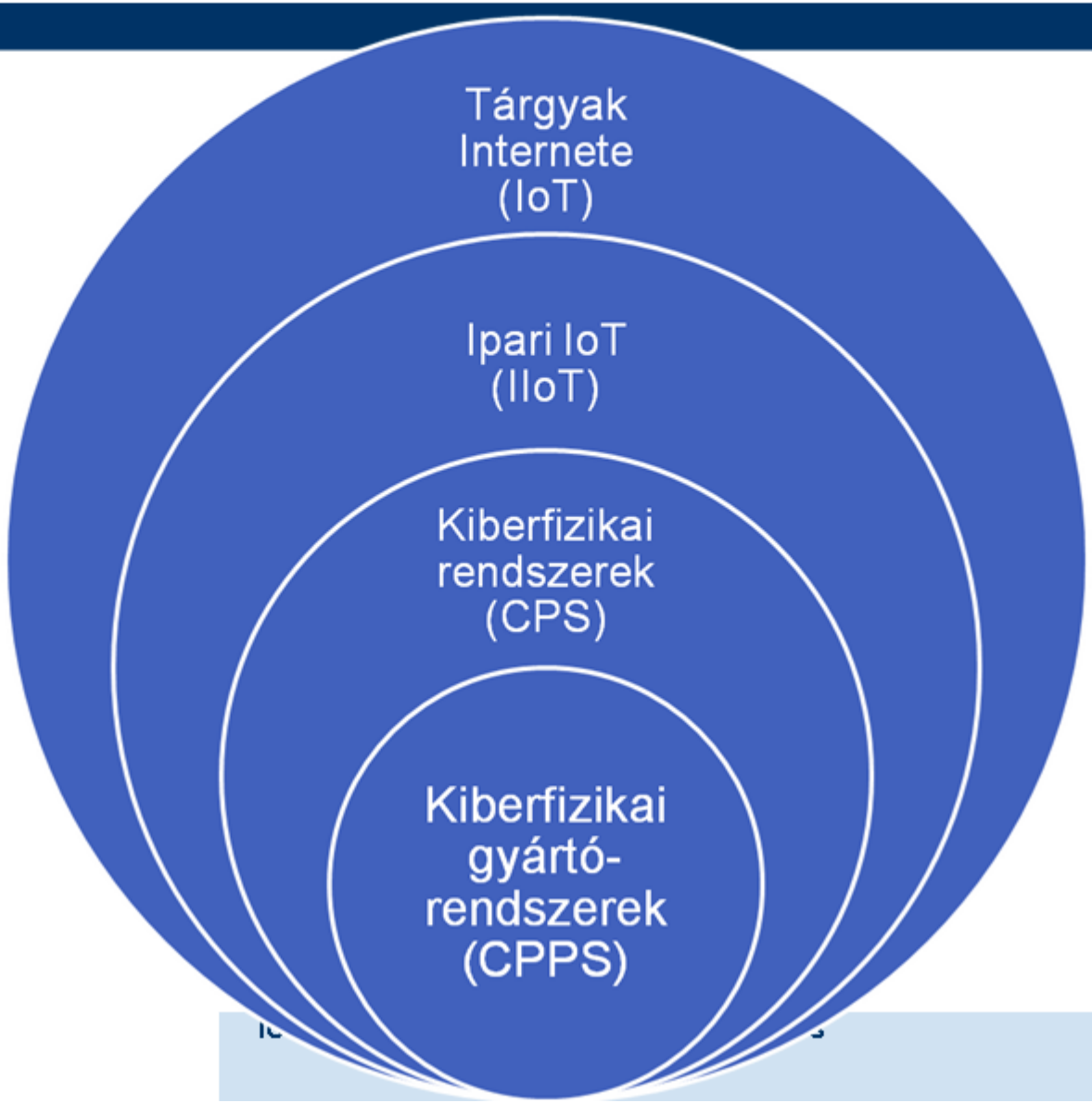


- Kiberfizikai rendszerek
- Cyber-Physical Systems (CPS)

http://cyberphysicalsystems.org/



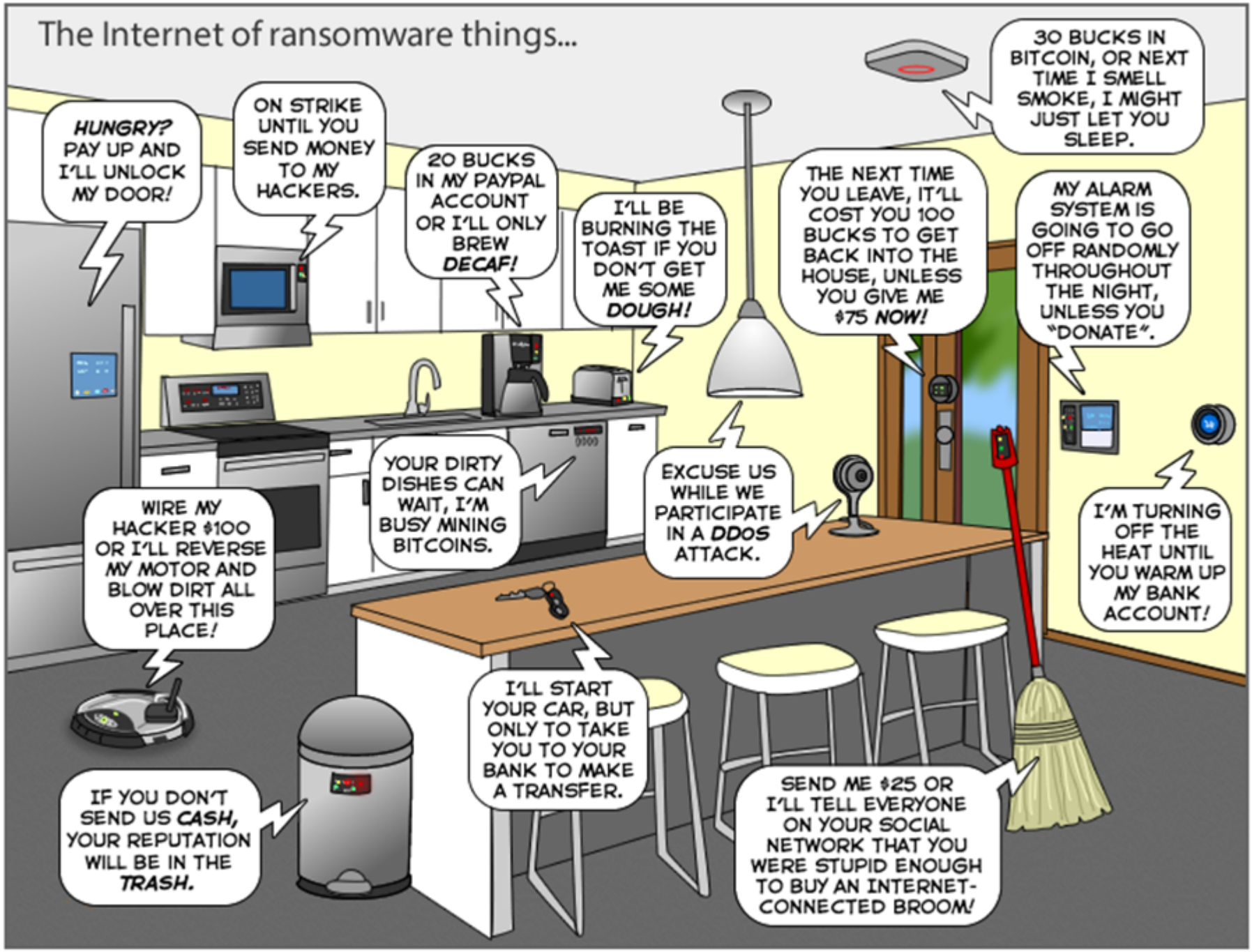
Alkalmazási területek átfedései



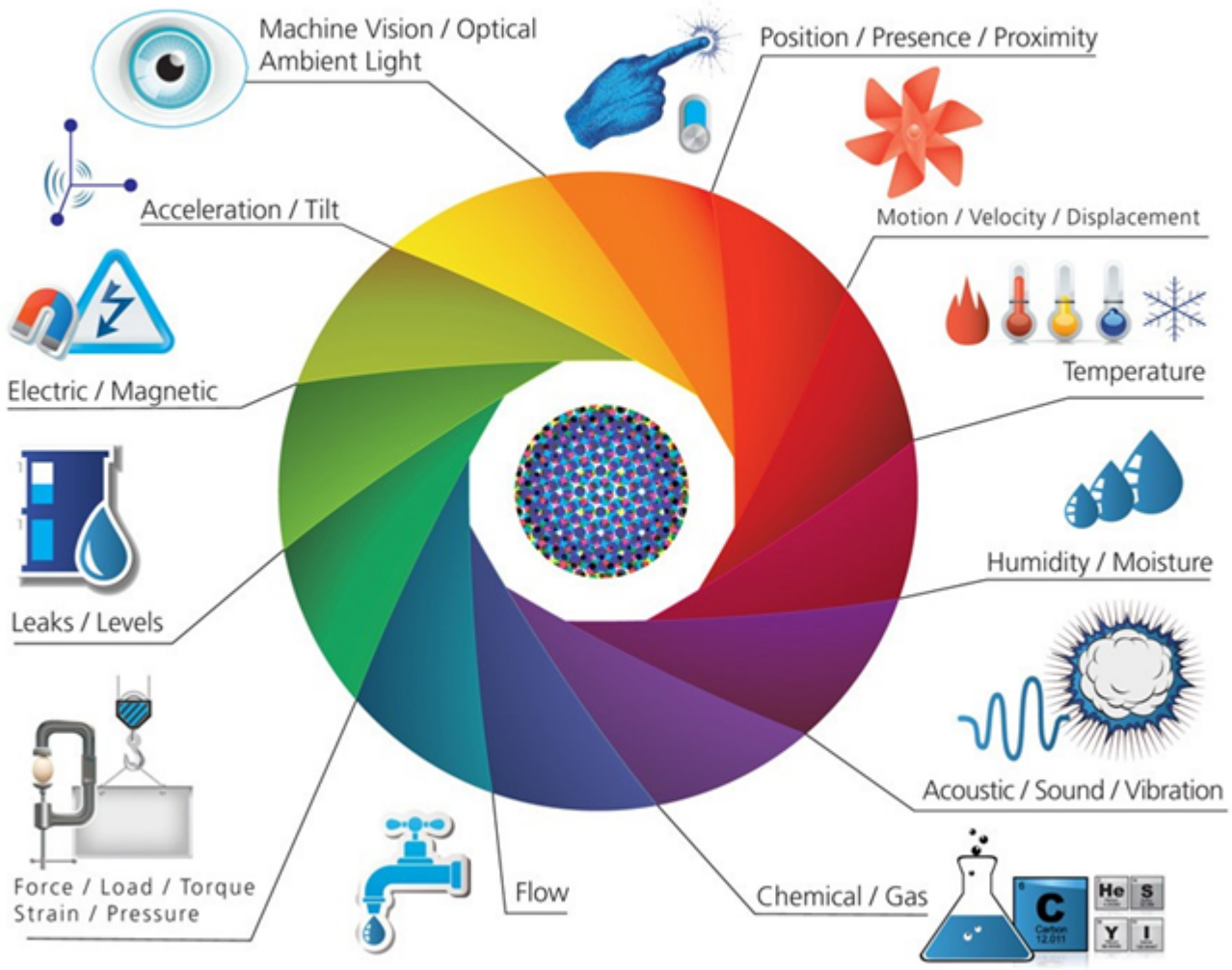
Internet of Hackable Things – Proven

- Okos otthon
  - Vasaló, vízforraló

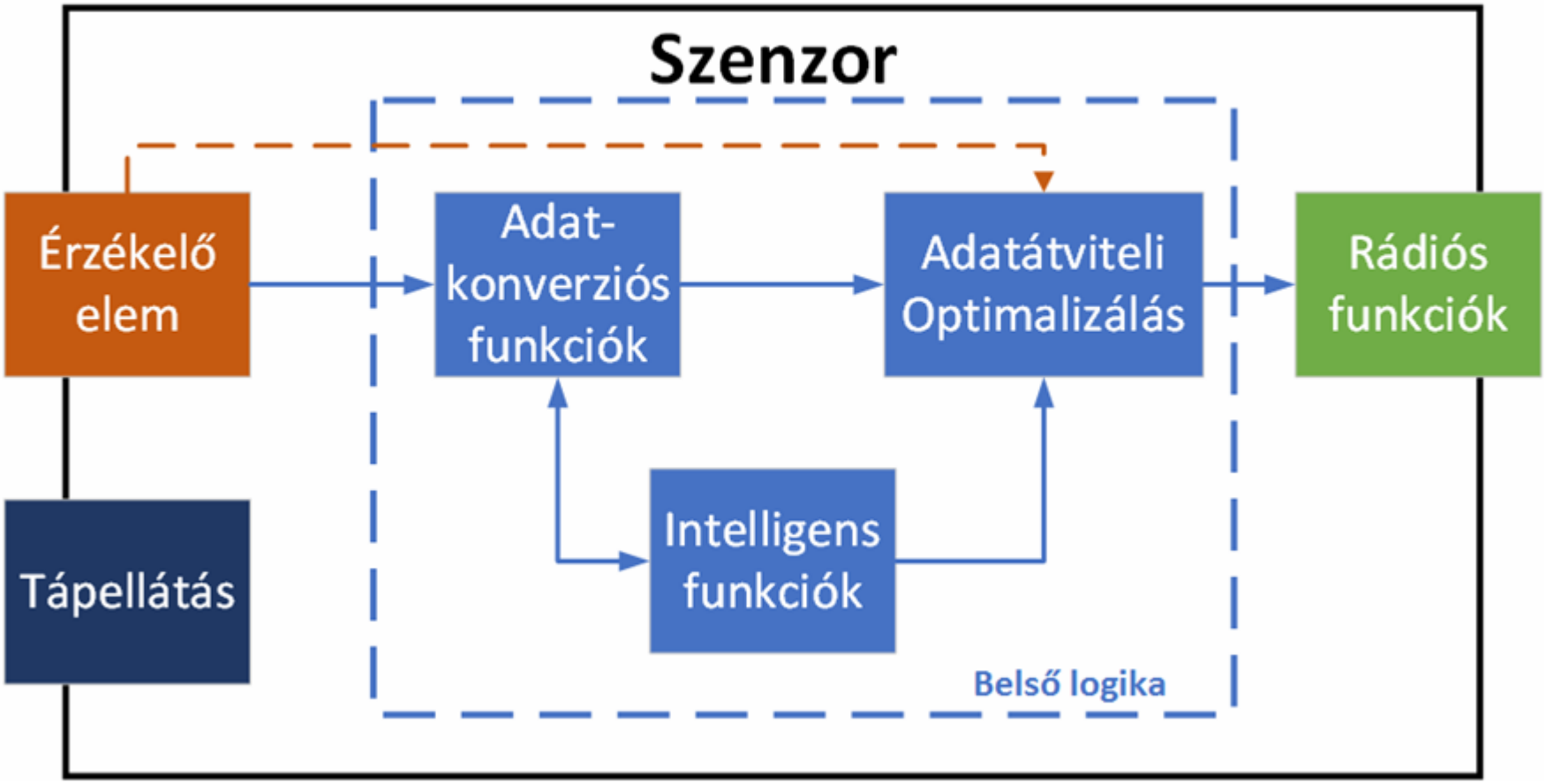
  - Égők
  - TV, rádió, kommunikációs eszközök
  - Bébifigyelő
  - Plüssjátékok (4.8M szülő, 6.4M gyerek személyes adata, 2 millió hangfelvétel szivárgott ki …eddig ismert módon)
  - Termosztát
  - Konyhai gépek
  - Víztisztítók
  - Okosórák, kamerák


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

Szenzor típusok

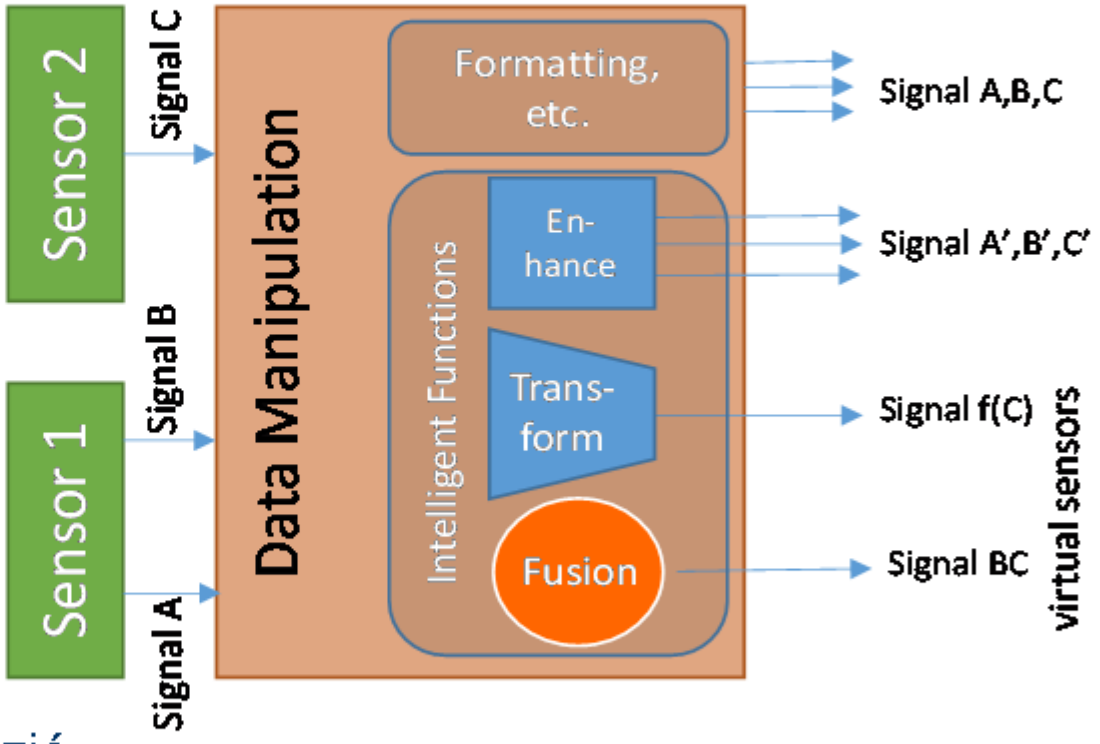


Általános szenzor modell



Smart szenzorok

- Adatmanipuláció típusa
  - Formázás
  - Gazdagítás
  - Transzformáció
  - Fúzió
  - Intelligents funkció
  - Szoft Szensor
- Soft szenzor
  - Virtuális szenzor
  - Transzformáció + Fúzió



Intelligens szenzorok

- Self-identification – képes azonosítani magát
- Self-testing – képes teszteket végrehajtani magán
- Self-validation – képes validálni a működését, vagy validálni a kimenetét
  - Pl. pontosság-mércét adni a kimenethez:

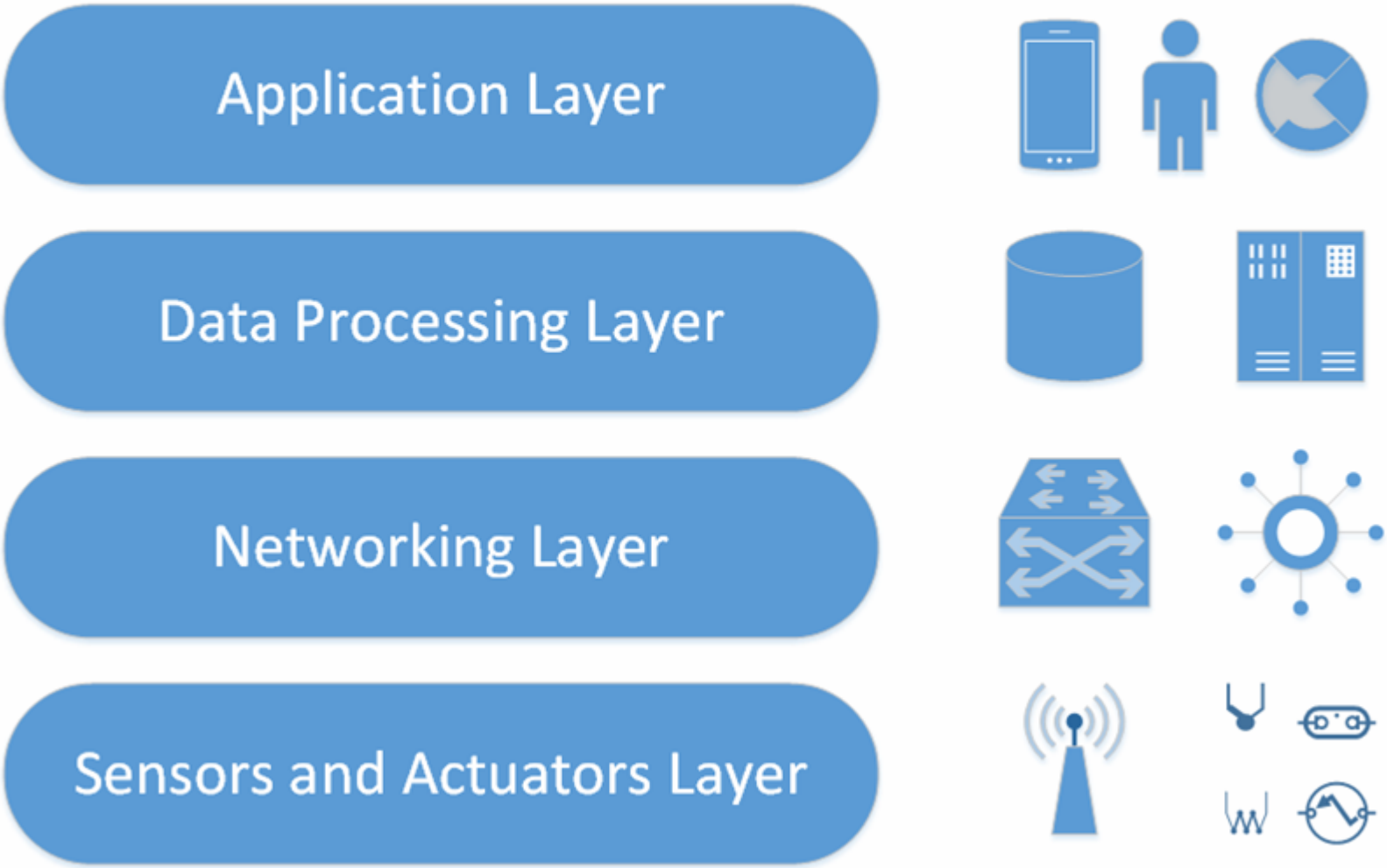
```
2015-10-01T00:00:02+00:00 , temp=12.3 C
2015-10-01T00:00:03+00:00 , temp=12.3 C
2015-10-01T00:00:04+00:00 , temp=1222.3 C
2015-10-01T00:00:05+00:00 , temp=12.4 C

2015-10-01T00:00:02+00:00, temp=12.3 C,accuracy= +-0.2 C,confidence=99,errorflag=0
2015-10-01T00:00:03+00:00, temp=12.3 C,accuracy= +-0.2 C,confidence=99,errorflag=0
2015-10-01T00:00:04+00:00, temp=1222.3 C,accuracy= +-100 C,confidence=0,errorflag=1
2015-10-01T00:00:05+00:00, temp=12.4 C,accuracy= +-10 C,confidence=10,errorflag=1
```

- Self-adaptation – alkalmazkodás a kondíciókhoz (pl. skála)
- Intelligent firmware update

IoT: Biztonság és Titkosság (Security, Safety and Privacy)

- Az IoT rendszerek titoktartási és biztonsági sajátosságai
- Azonosítási (Identification and Authentication) kérdések
- Vezetéknélküli szenzorhálózatok IoT biztonsági kérdései
- Behatolásvédelem az IoT területen
- Kriptográfia, adatbiztonság, AAA és CIA az IoT területen
- Fizikai/MAC/Hálózati támadások a Tárgyak Internete ellen
- Csatornatitkosítás a szenzorhálózatokban
- Rétegeken átívelő támadások az IoT területen
- Biztonsági, emberi biztonsági (Security and Safety), valamint QoS kérdések együttes kezelése
- Big Data és Információ-integritási kérdések IoT
- Kommunikáció-biztonság az IoT területen
- IoT biztonsági szabványok

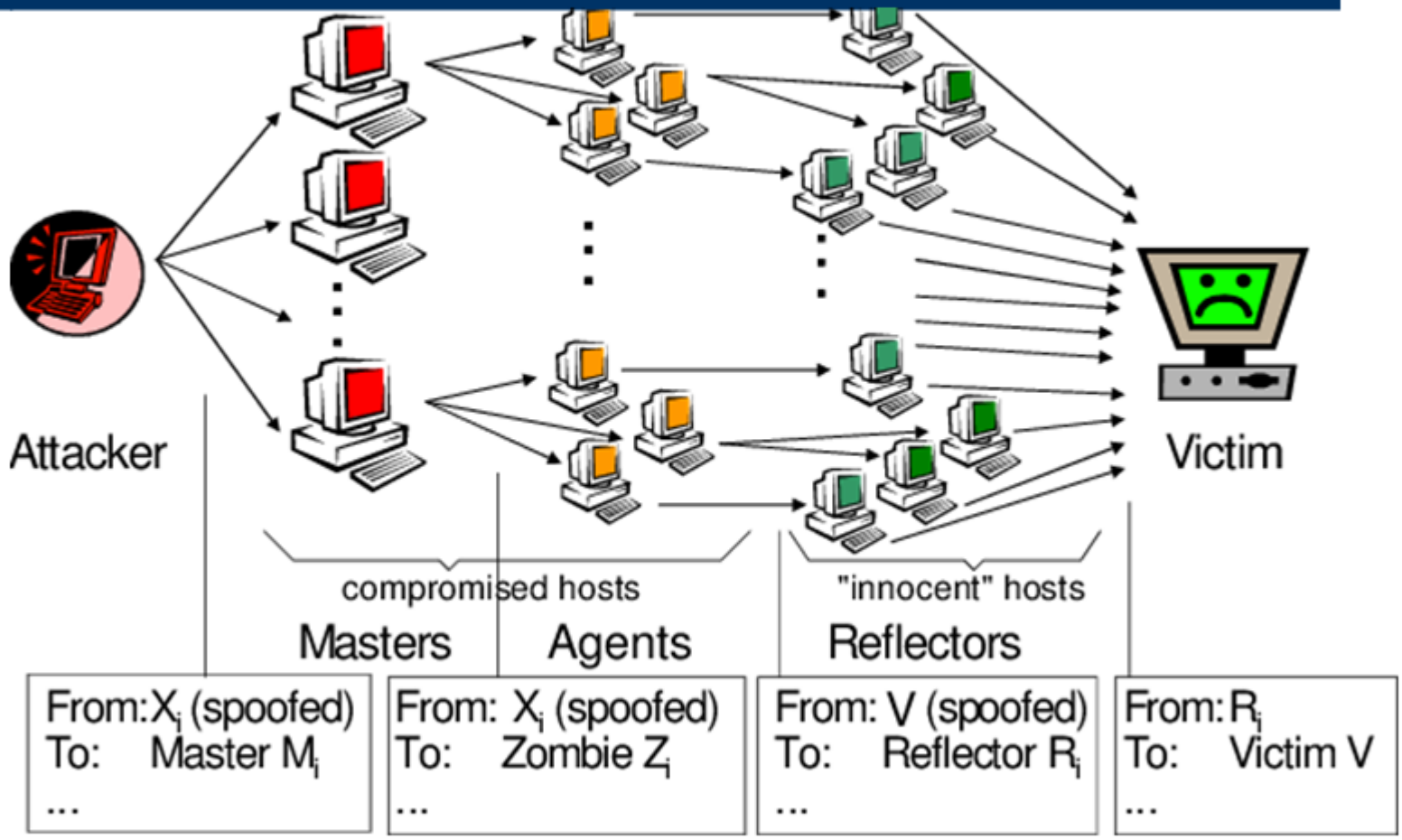
Az IoT-rendszerek rétegei – egy „vélemény” a sok közül



Szenzor-réteg támadás-típusai

- Tampering
  - fizikai módosítások
    - az eszközön
    - a kommunikációs csatornán
  - hozzáférés, ID lopás/csere
- Eavesdropping – lehallgatás
- Denial of Service
  - Jeltorzítás, jamming, (szélessávú?) rádiózaj
- A szenzor mint a DDoS támadás eszköze

Elosztott, reflektált támadások szereplői

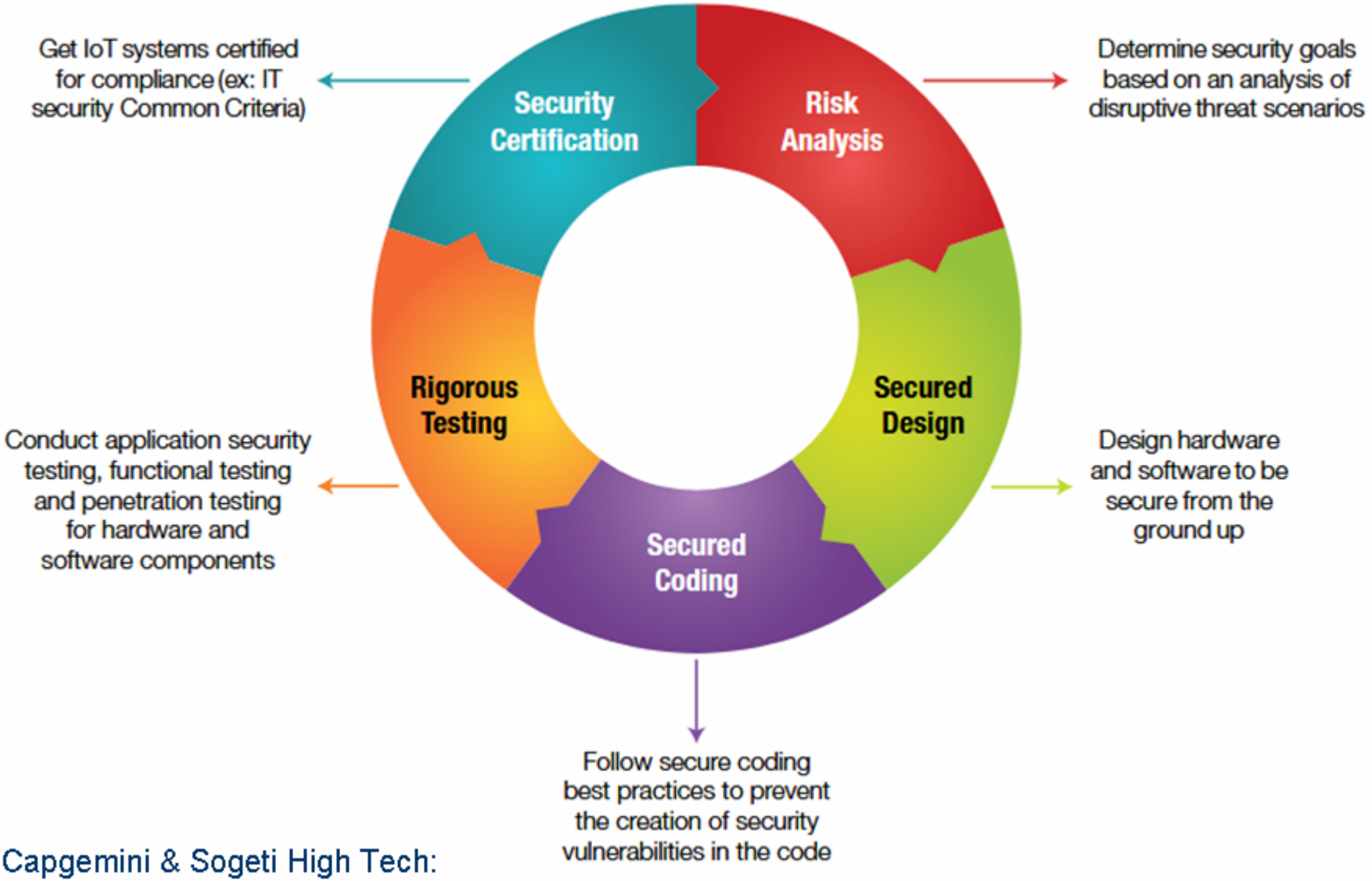


T. Dübendorfer et. al., 2005.,
Adaptive Distributed Traffic Control Service for DDoS Attack Mitigation

Fenyegetések és védelmi stratégiáik

Layer	Threat type	Mitigation
Physical	Tampering	tamper-resistant packaging
	Eavesdropping	encryption, authorization
	Denial of Service	spread-spectrum techniques
Networking	Exhaustion	active firewalls, passive monitoring (probing), traffic admission control, bi-directional link autentication
	Collision	
	Unfairness	
	Spoofing	
	Selective forwarding	
	Sinkhole	
	Wormhole	
	Sybil	
	Flooding	
Data processing	Exhaustion	traffic monitoring
	Malware	malware detection
Application	Client app.	anti-virus filtering
	Communication	
	Integrity	testing
	Modifications	validation
	Multi-user access	process planning and design
	Data access	Traceability

Javasolt hozzáállás



Capgemini & Sogeti High Tech: Securing the Internet of Things Opportunity

Köszönöm a figyelmet!

Dr. Varga Pál

BME

Távközlési és
Médiainformatikai Tanszék