FROM DESIGN OF NEW ATTACKS THROUGH ANOMALY DETECTION TO THE DESIGN OF ARTIFICIAL PANCREAS

Krzysztof Szczypiorski
Warsaw University of Technology

Gliwice, 26th of September, 2016

About this talk

- A three level case study:
  - #1: design of new attacks: network steganography
  - #2: design of anomaly detection systems
  - #3: design of artificial pancreas*

* with Prof. **Michał Wszoła**, M.D., Ph.D., D.Sc.
A transplantation surgeon
Foundation for Research and Science Development
MediSpace Sp. z o.o.

Level #1: design of new attacks

Current steganography applications

a carrier – an image
(entitled “the #end of a #season”)

+

a hidden data – an image
(entitled “there is no #spoon”)

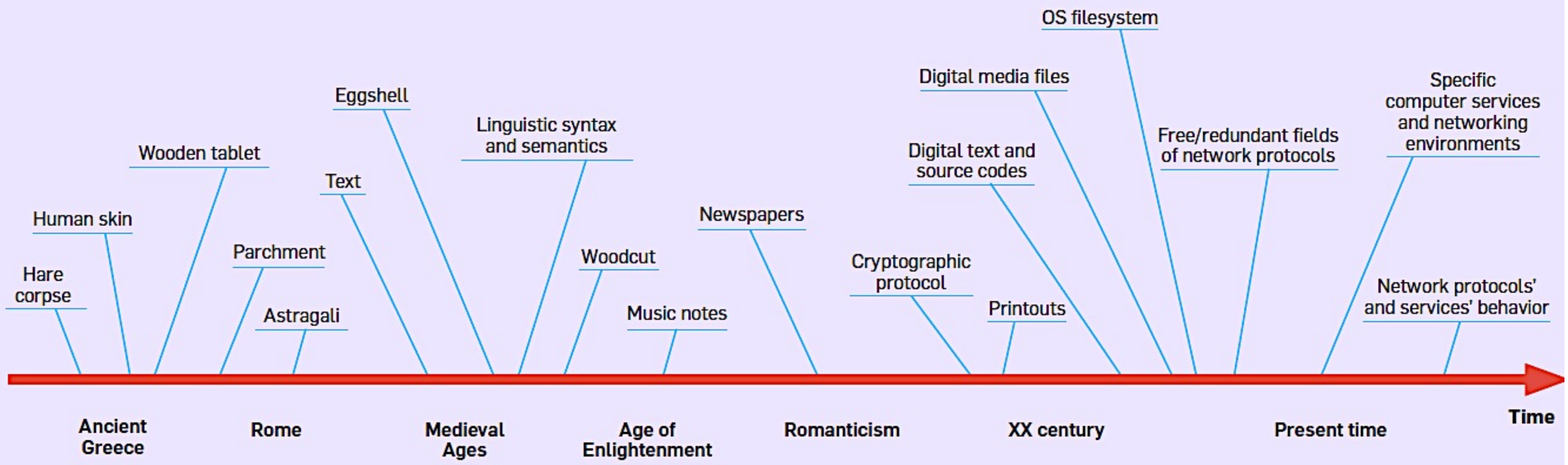
=

a steganogram – an image
(there is no spoon!)

Main hidden data carriers: **images**, voice, and text

Level #1: design of new attacks

Timeline of the evolution of hidden data carrier

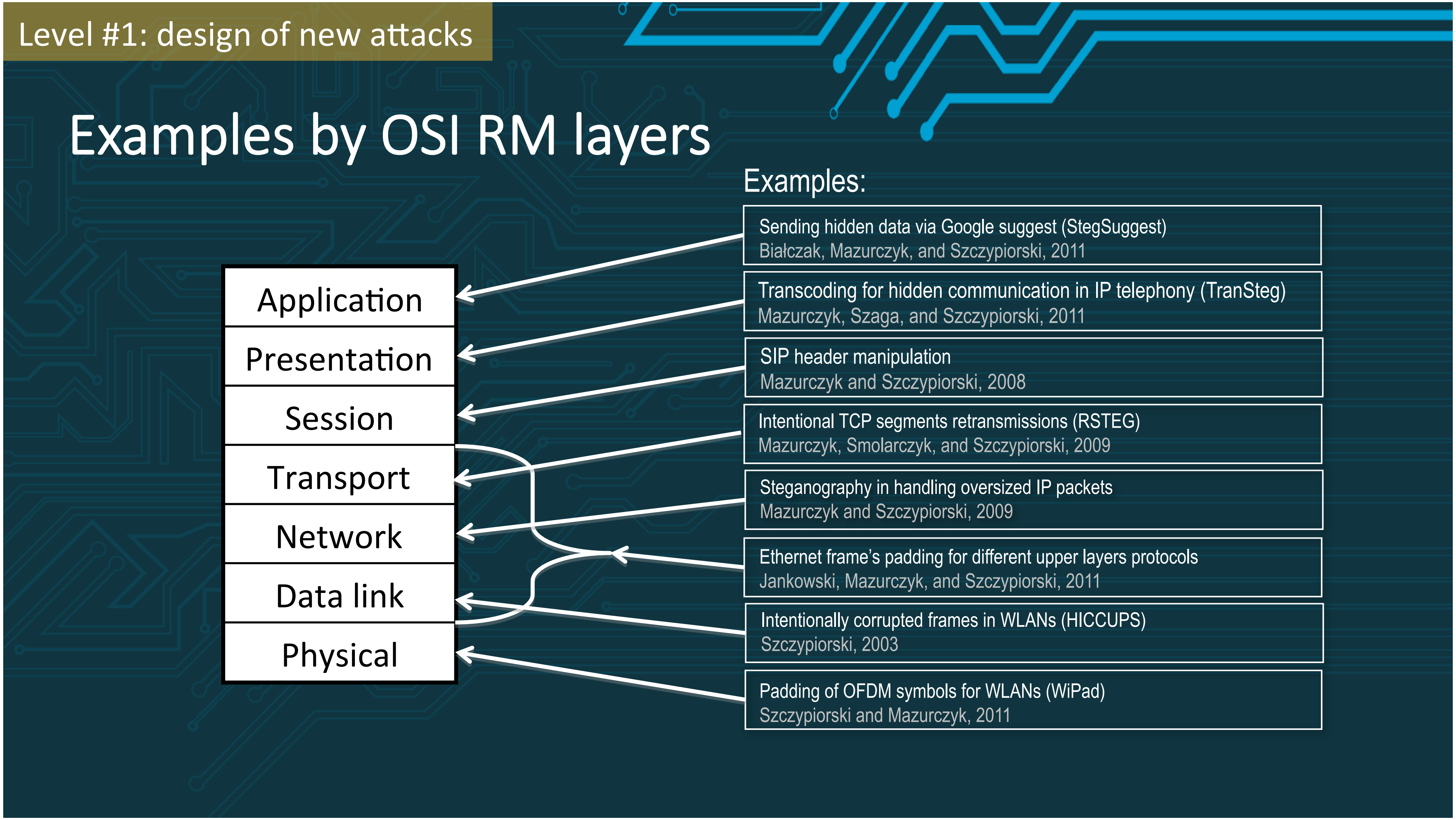


Elżbieta Zielińska, Wojciech Mazurczyk, Krzysztof Szczypiorski: *Trends in Steganography.* Communications of the ACM, Vol. 57 No. 3, pp. 86-95

Level #1: design of new attacks

Network steganography

- First world development was at WUT – 2003 (HICCUPS) – **stegano.net** project
- Definition: information hiding techniques which utilise modifications of the packets to perform hidden communication:
  - **Modification to the structure** of the packet: payload and protocol specific fields
  - **Modification to time relations among packets**: changing the sequence of the packets or inter-packet delays



Level #1: design of new attacks

Examples by OSI RM layers

Examples:

- Sending hidden data via Google suggest (StegSuggest)
  Białczak, Mazurczyk, and Szczypiorski, 2011
- Transcoding for hidden communication in IP telephony (TranSteg)
  Mazurczyk, Szaga, and Szczypiorski, 2011
- SIP header manipulation
  Mazurczyk and Szczypiorski, 2008
- Intentional TCP segments retransmissions (RSTEG)
  Mazurczyk, Smolarczyk, and Szczypiorski, 2009
- Steganography in handling oversized IP packets
  Mazurczyk and Szczypiorski, 2009
- Ethernet frame's padding for different upper layers protocols
  Jankowski, Mazurczyk, and Szczypiorski, 2011
- Intentionally corrupted frames in WLANs (HICCUPS)
  Szczypiorski, 2003
- Padding of OFDM symbols for WLANs (WiPad)
  Szczypiorski and Mazurczyk, 2011

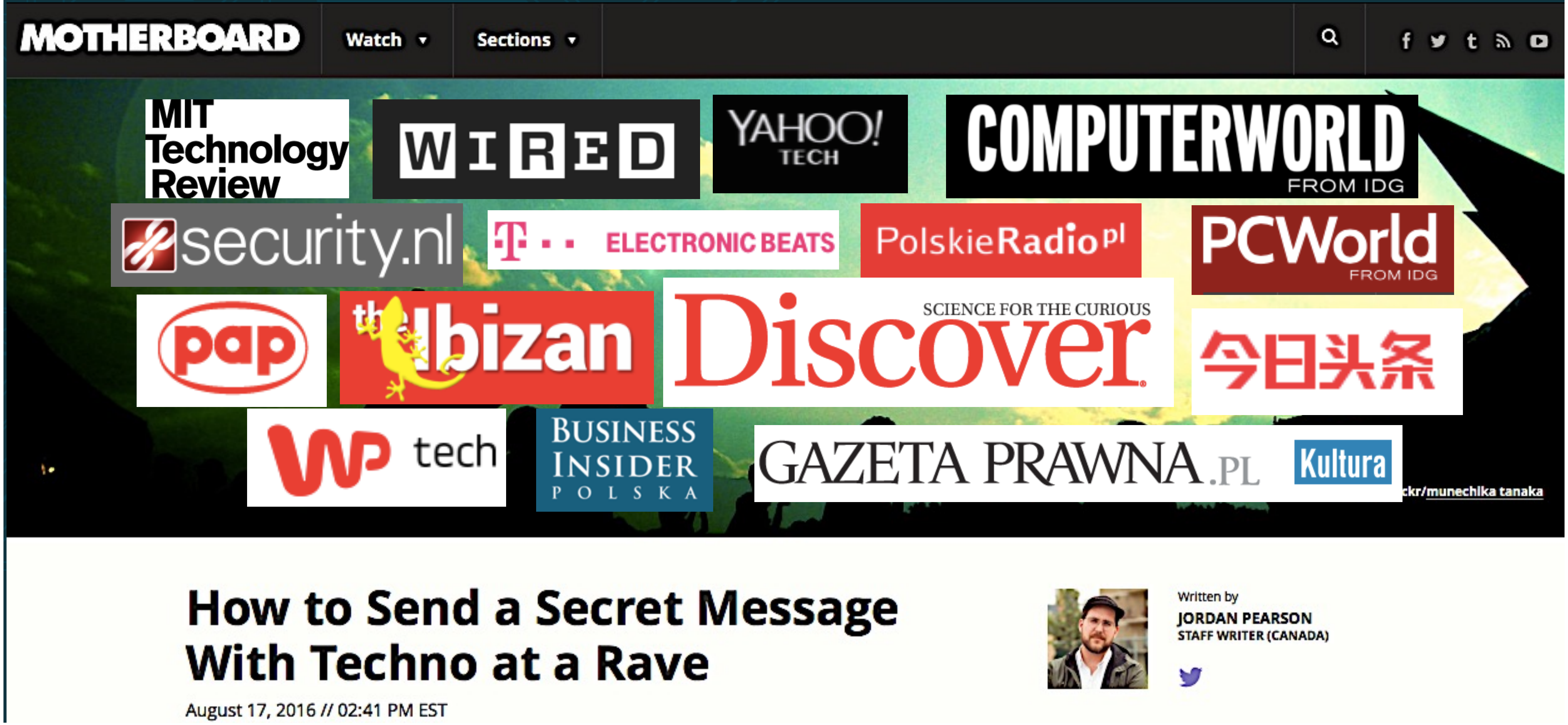
Level #1: design of new attacks

StegIbiza = Steganographic Ibiza

https://www.youtube.com/watch?v=foE1mO2yM04 ↑
http://www.destinationspoint.com/where-is-ibiza-located/ ↗

Level #1: design of new attacks

http://stegano.net/press.html



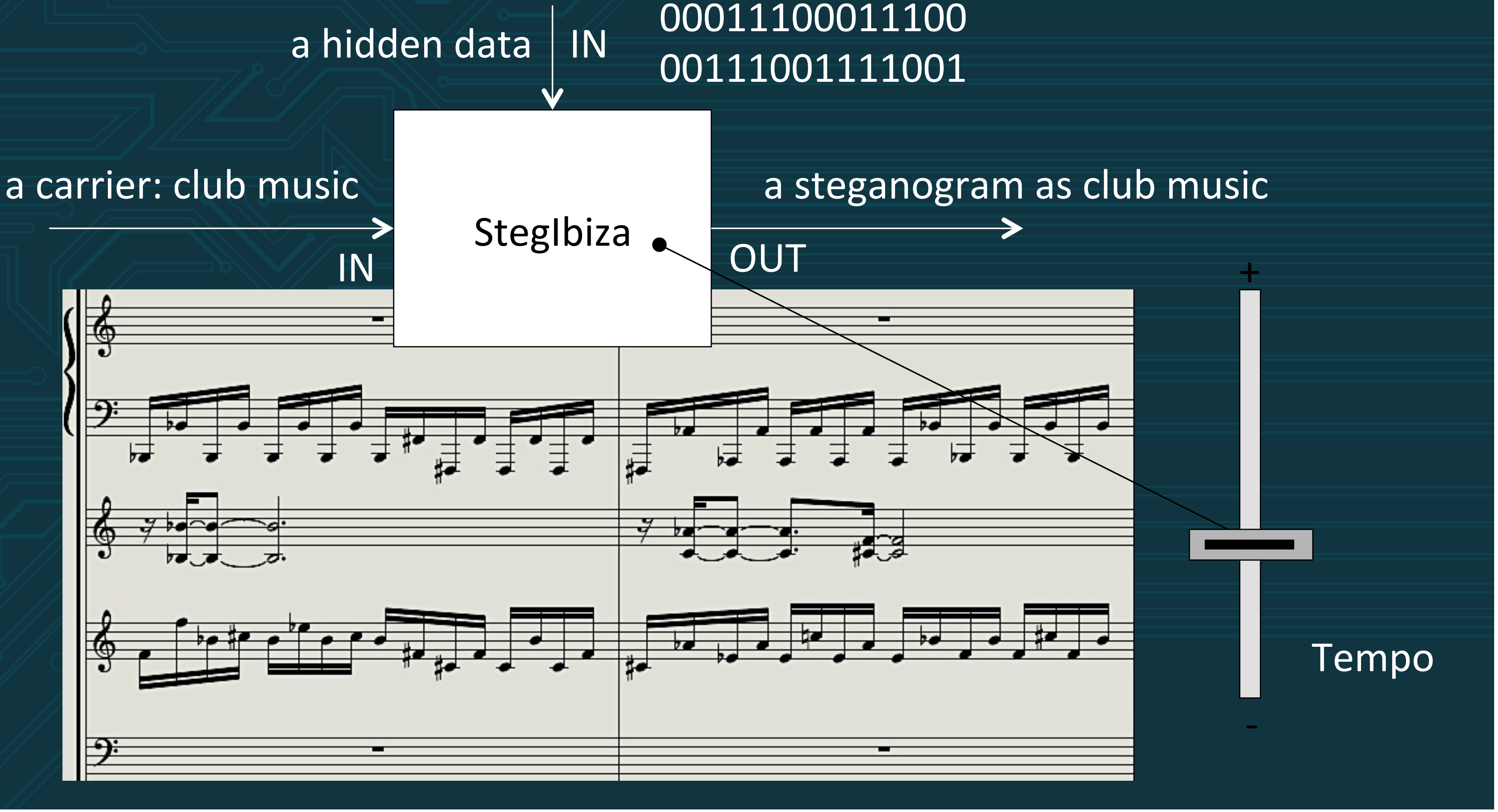
How to Send a Secret Message With Techno at a Rave

August 17, 2016 // 02:41 PM EST

Written by
JORDAN PEARSON
STAFF WRITER (CANADA)

Level #1: design of new attacks

StegIbiza: hiding bits in beats



a hidden data

IN

00011100011100
00111001111001

a carrier: club music

IN

StegIbiza

a steganogram as club music

OUT

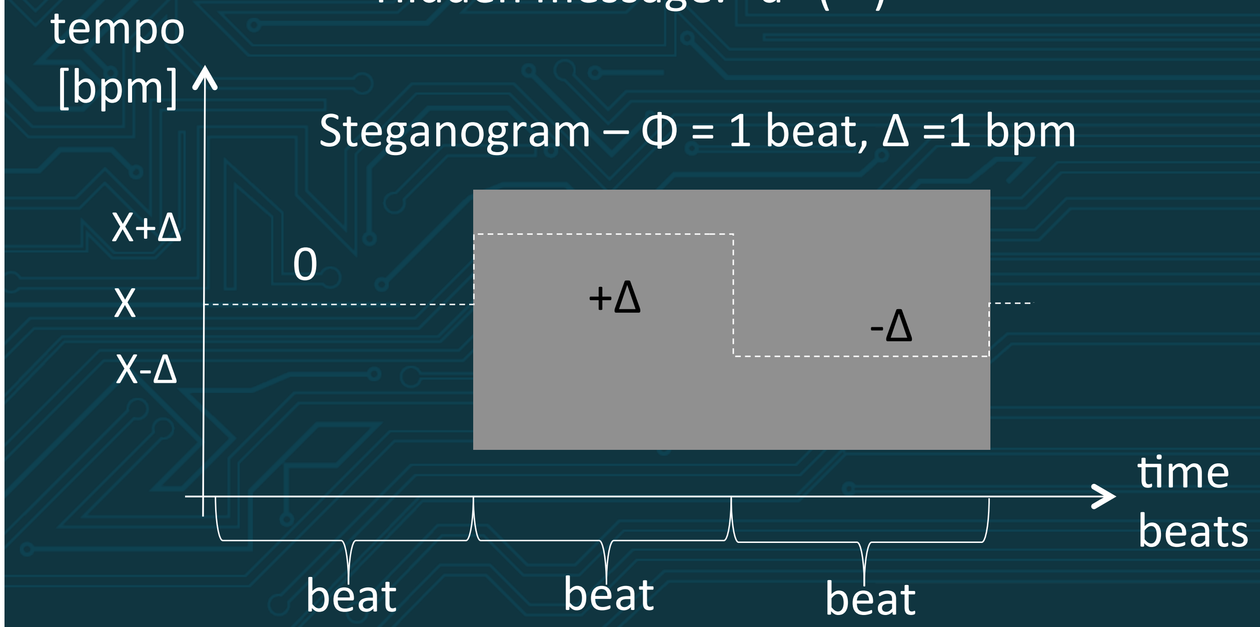
Stegibiza: an idea and results

- Vary the tempo of the beat in a way that encodes information
- A simple Morse-like code was developed in which it is possible to spell out a series of dots and dashes to send messages
- To indicate a dash, the StegIbiza method speeds up the tempo for a single beat; to indicate a dot, it slows it down
- Any changes have to be too subtle for human listeners to notice even for professional musicians; for the worst case scenario, nobody could identify any differences in the audio with a 1% margin of changed tempo
- StegIbized music could be embedded in the payload of a packet and then might be streamed anywhere

Level #1: design of new attacks

StegIbiza: a coding scheme

Hidden message: “a” (+-)



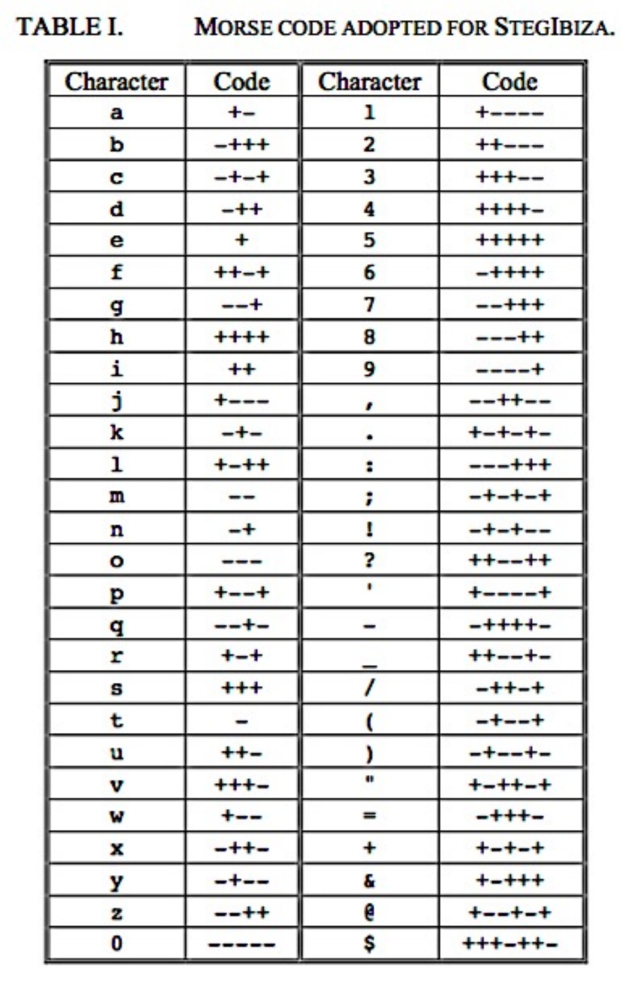
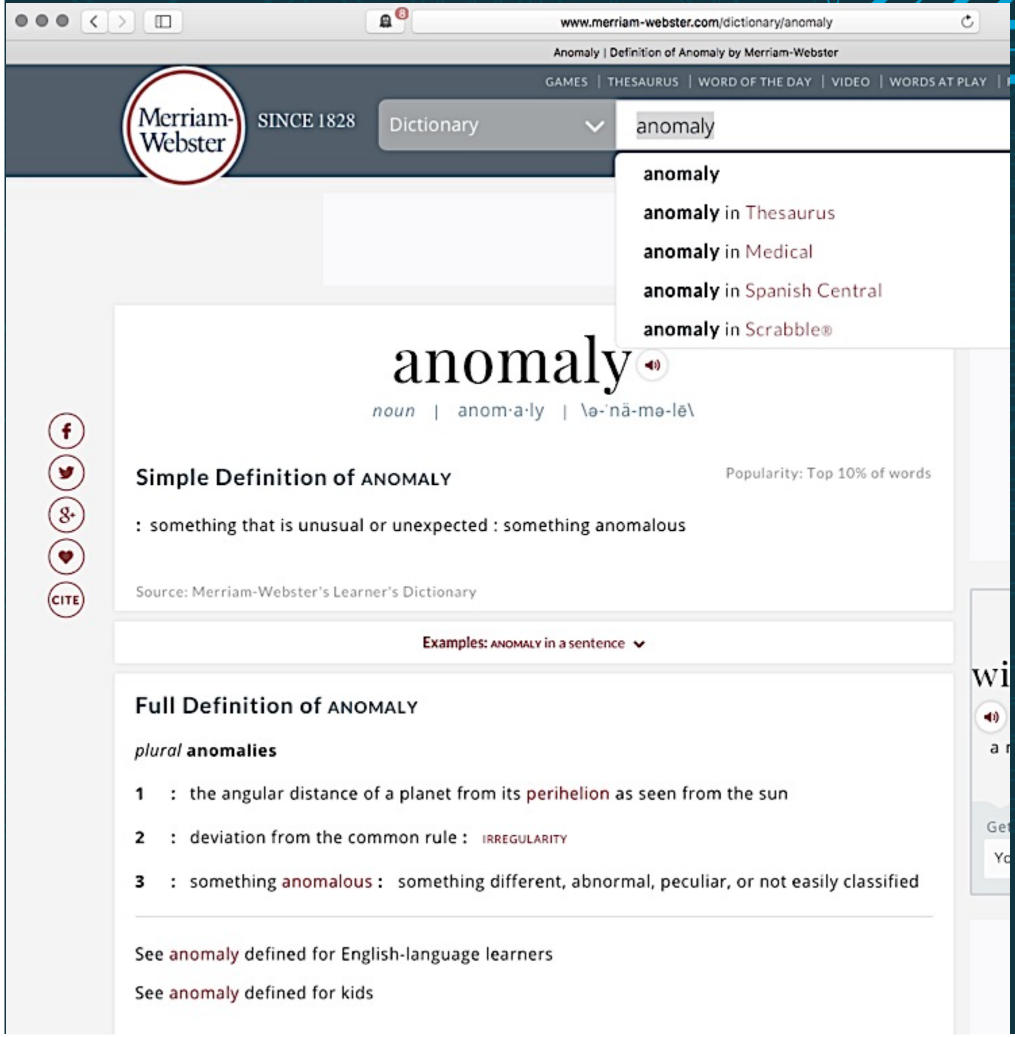


TABLE I. MORSE CODE ADOPTED FOR STEGIBIZA.

Character	Code	Character	Code
a	+-	1	+----
b	-+++	2	++---
c	-+-+	3	+++--
d	-++	4	++++-
e	+	5	+++++
f	++-+	6	-++++
g	--+	7	--+++
h	++++	8	---++
i	++	9	----+
j	+---	,	--++--
k	-+-	.	+-+-+-
l	+-++	:	---+++
m	--	;	-+-+-+
n	-+	!	-+-+--
o	---	?	++--++
p	+--+	'	+----+
q	--+-	-	-++++-
r	+-+	_	++--+-
s	+++	/	-++-+
t	-	(	-+--+
u	++-	)	-+--+-
v	+++-	"	+-++-+
w	+--	=	-+++-
x	-++-	+	+-+-+
y	-+--	&	+-+++
z	--++	@	+--+-+
0	-----	$	+++-++-

Level #2: design of anomaly detection systems



www.merriam-webster.com/dictionary/anomaly

Anomaly | Definition of Anomaly by Merriam-Webster

GAMES | THESAURUS | WORD OF THE DAY | VIDEO | WORDS AT PLAY |

Merriam-Webster SINCE 1828

Dictionary

anomaly

anomaly
anomaly in Thesaurus
anomaly in Medical
anomaly in Spanish Central
anomaly in Scrabble®

anomaly

noun | anom·a·ly | \ə-ˈnä-mə-lē\

Simple Definition of ANOMALY

Popularity: Top 10% of words

: something that is unusual or unexpected : something anomalous

Source: Merriam-Webster's Learner's Dictionary

Examples: ANOMALY in a sentence

Full Definition of ANOMALY

plural **anomalies**

1 : the angular distance of a planet from its perihelion as seen from the sun

2 : deviation from the common rule : IRREGULARITY

3 : something anomalous : something different, abnormal, peculiar, or not easily classified

See anomaly defined for English-language learners

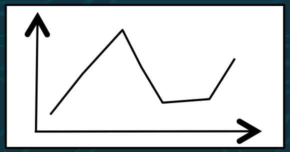
See anomaly defined for kids

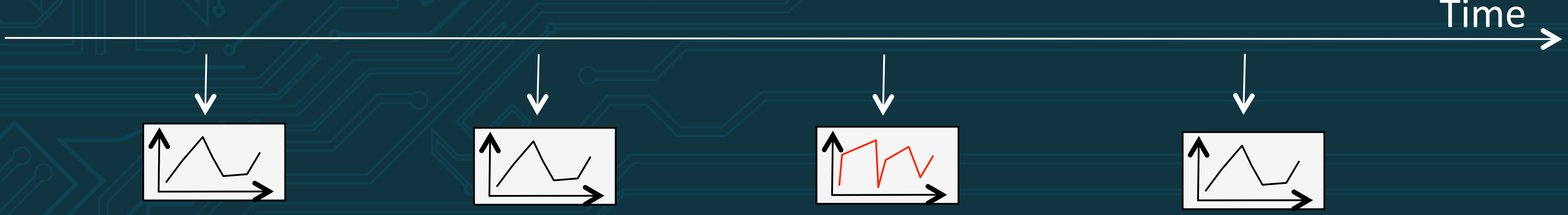
- Steganography is an anomaly
- Detection of steganography is like an anomaly detection
- **Anomalisa.net** project

Tracking unusual and unexpected (2U)

Our knowledge:

Typical behavior





Typical ☺

Typical ☺

Change to 2U ☹

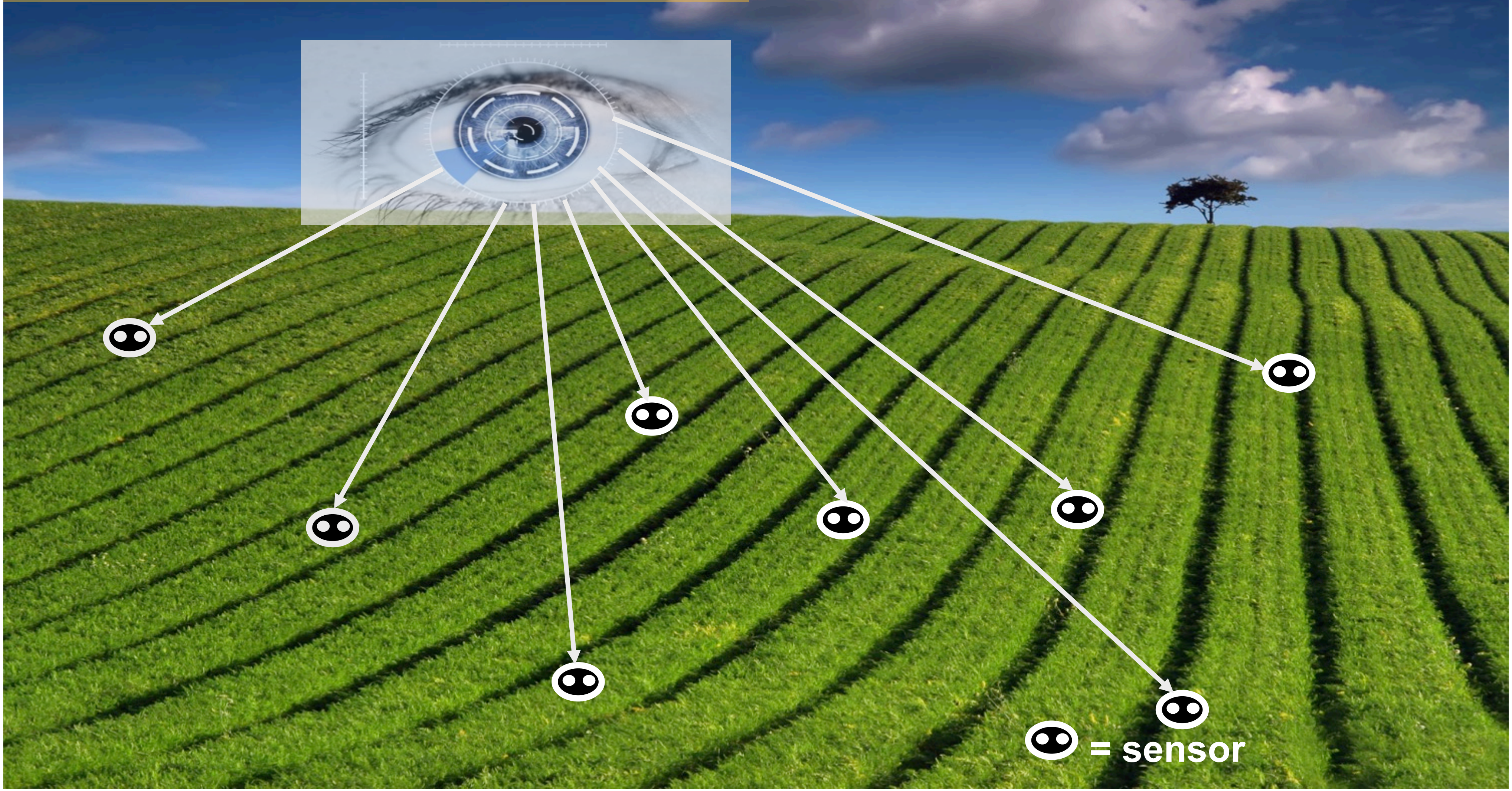
Change to typical ☺

Level #2: design of anomaly detection systems

Research questions

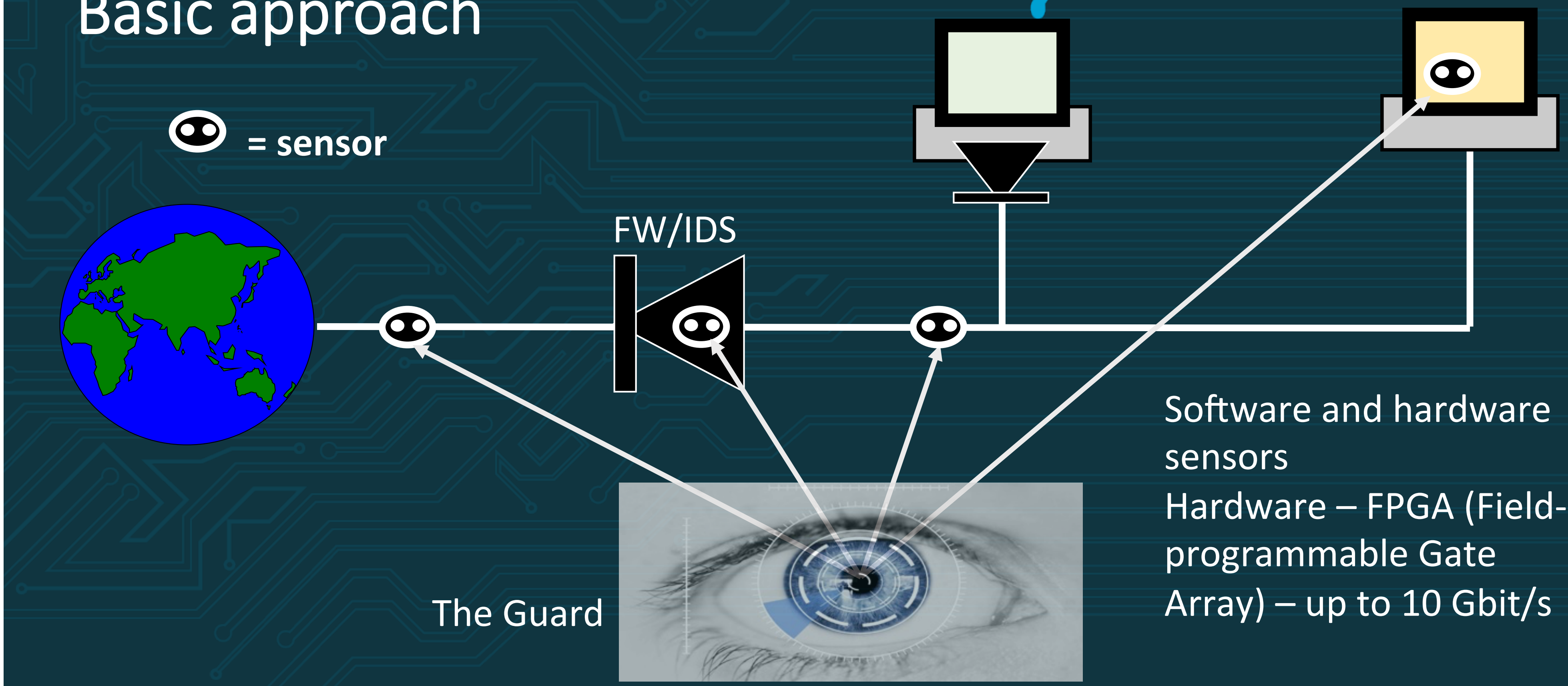
- What to observe?
- How to observe?
- How to build patterns, models, etc.?
- How to validate patterns, models?
- How the observing objects are changing?
- Where to place sensors?
- How to record the past?
- How to predict the future ☺?

Level #2: design of anomaly detection systems



Level #2: design of anomaly detection systems

Basic approach



Software and hardware sensors

Hardware – FPGA (Field-programmable Gate Array) – up to 10 Gbit/s

Detecting known steganographic methods and anomalies in network traffic

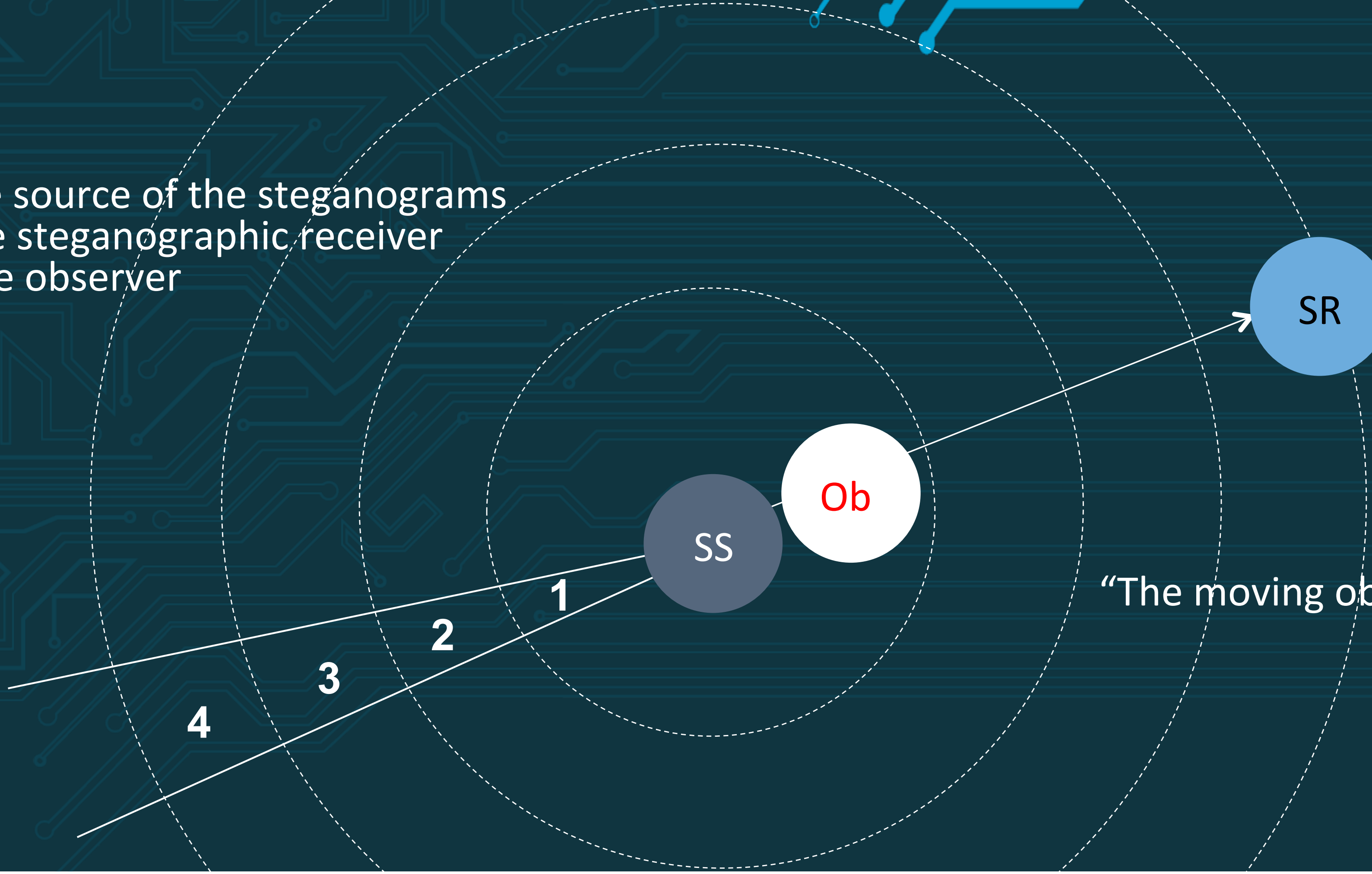
Level #2: design of anomaly detection systems

“The Good, The Bad & The Ugly”

- **“Good”** the observer is unable to detect a hidden communication at the source of the steganograms (SS)
- **“Bad”** the observer is able to detect a hidden communication at the SS, but he/she is unable to detect this communication, when he/she is moved away from the SS
- **“Ugly”** the observer is able to detect a hidden communication anywhere in the network, even at the steganographic receiver (SR)

Level #2: design of anomaly detection systems

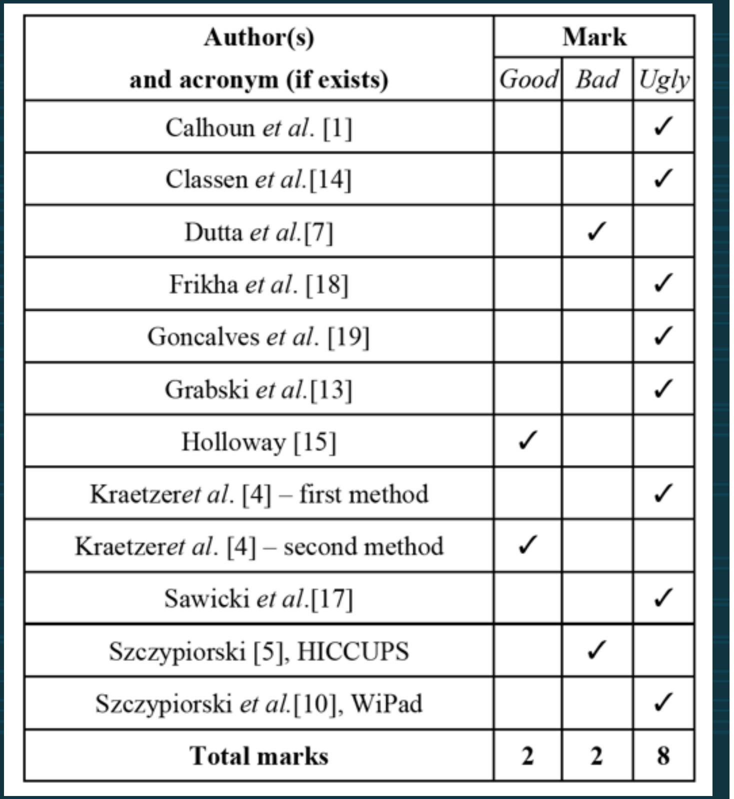
SS – the source of the steganograms
SR – the steganographic receiver
Ob – the observer



“The moving observer”

Evaluation of Wi-Fi Steganography

- Krzysztof Szczypiorski, Artur Janicki, and Steffen Wendzel
  “The Good, The Bad and The Ugly”: Evaluation of Wi-Fi Steganography
- In: Journal of Communications, vol. 10, no. 10, pp. 747-752, 2015
- Presented at ICNIT 2015, Tokyo, Japan
- To be extended to the whole discipline of steganography



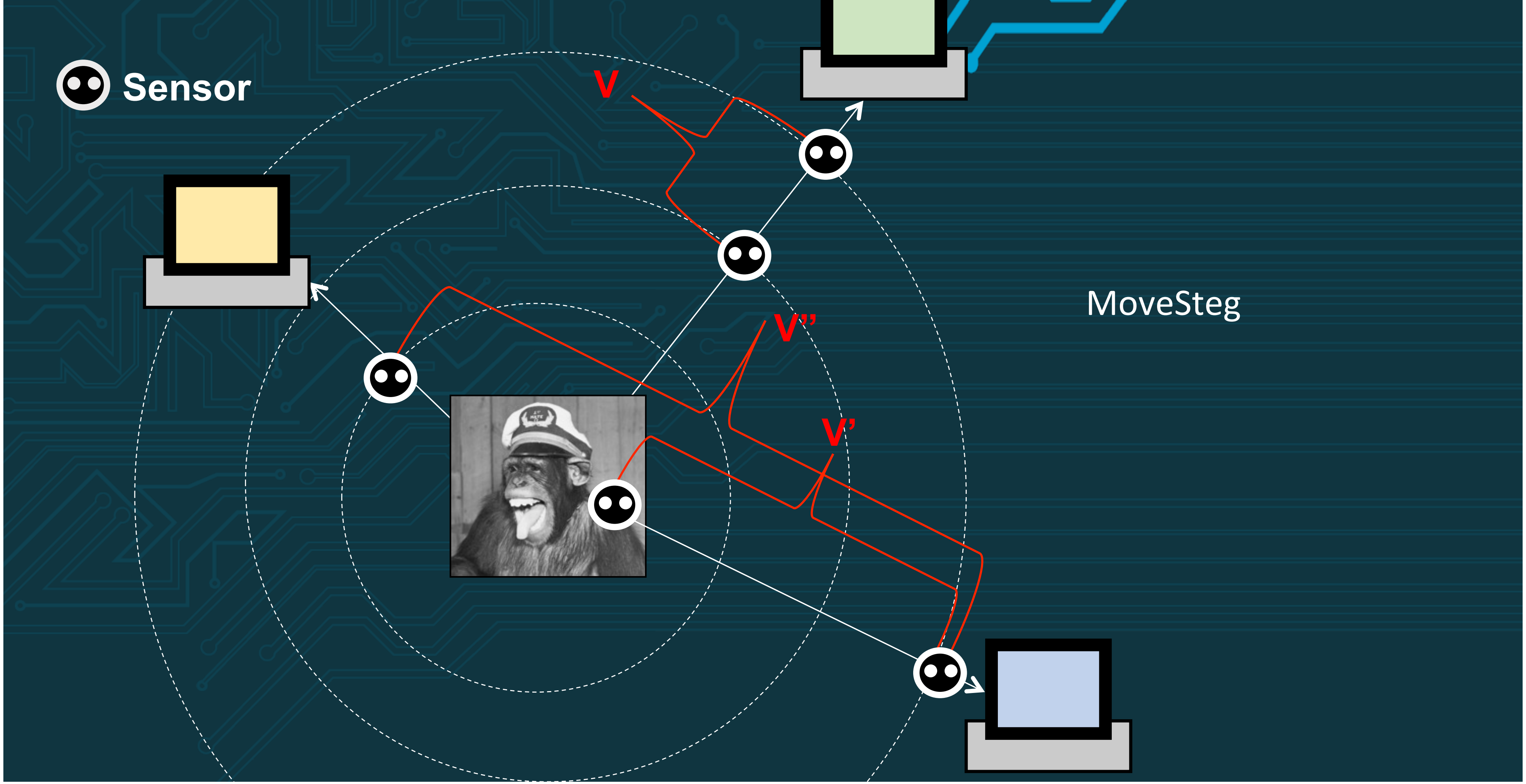
Author(s)	**Mark**		
and acronym (if exists)	*Good*	*Bad*	*Ugly*
Calhoun *et al*. [1]			✓
Classen *et al*.[14]			✓
Dutta *et al*.[7]		✓	
Frikha *et al*. [18]			✓
Goncalves *et al*. [19]			✓
Grabski *et al*.[13]			✓
Holloway [15]	✓		
Kraetzer*et al*. [4] – first method			✓
Kraetzer*et al*. [4] – second method	✓		
Sawicki *et al*.[17]			✓
Szczypiorski [5], HICCUPS		✓	
Szczypiorski *et al*.[10], WiPad			✓
Total marks	**2**	**2**	**8**

Level #2: design of anomaly detection systems

MoveSteg

- “The moving observer” technique:
  - can help not only in the evaluation of steganographic algorithms
  - but also in the design of the fundamentals for the **novel network steganographic detection system**
- The main aim of this system is to detect **“bad”** methods **(“ugly”** could be detected anywhere)
- Is the StegIbiza an “ugly” method ☺?
- Main application: detecting Command and Control (C&C) servers/nodes in botnets

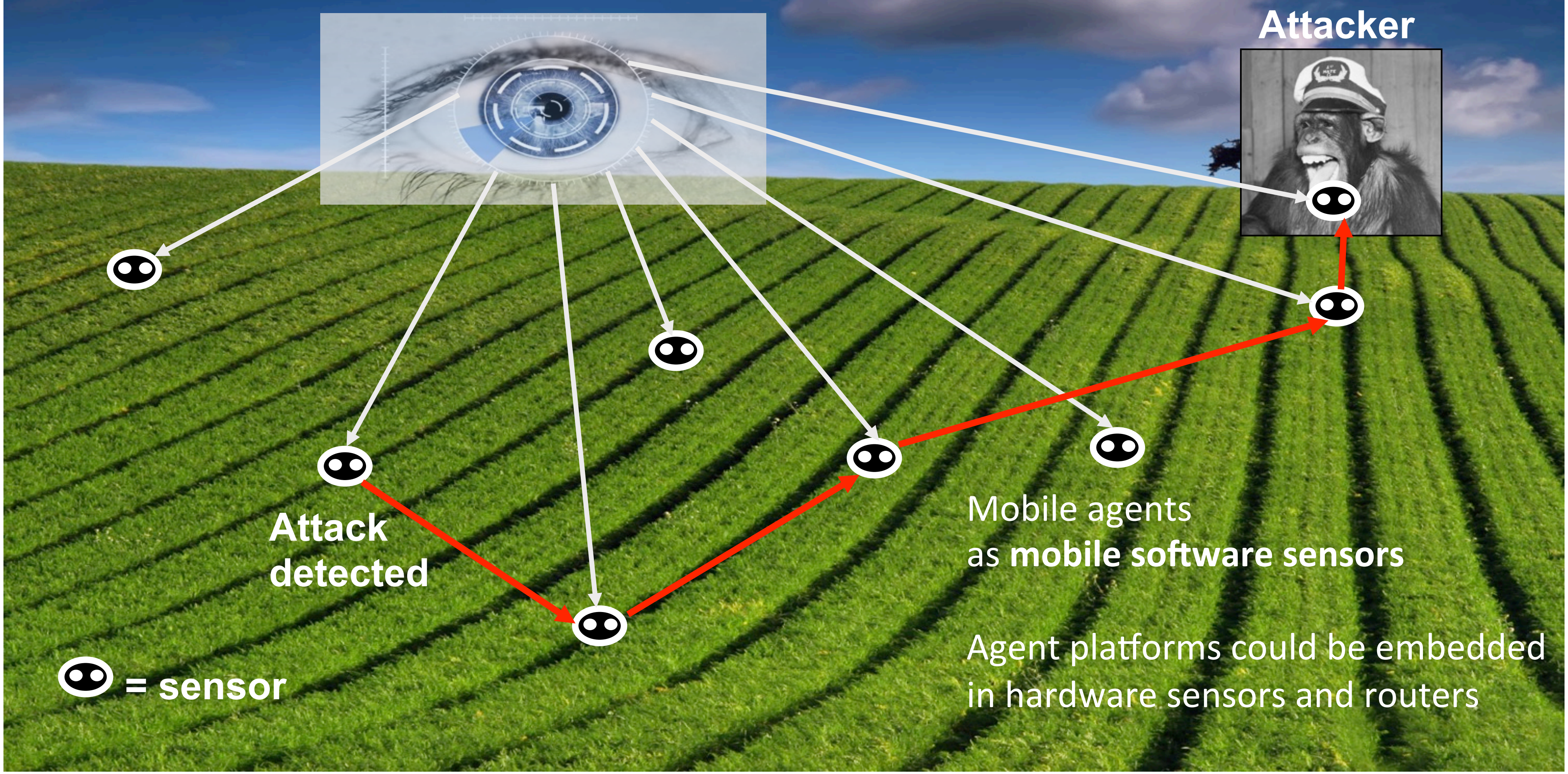
Level #2: design of anomaly detection systems



MoveSteg

Level #2: design of anomaly detection systems

An extension of Movesteg to the network immune system – “healing = killing your enemies”

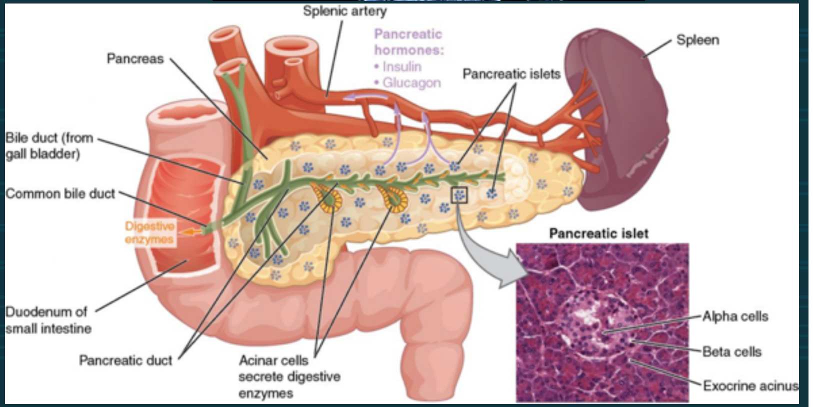


Mobile agents
as **mobile software sensors**

Agent platforms could be embedded
in hardware sensors and routers

The pancreas

- Located behind the stomach
- Large, compound gland consisting of the head, body and tail
- Two functions:
  - Exocrine functions: pancreatic juice contains enzymes for digesting fats, proteins, and carbohydrates; trypsin is the most abundant enzyme
  - Endocrine functions occurs in the islets of Langerhans
    - Beta cells secrete insulin
    - Alpha cells secrete glucagon
    - Delta cells secrete somatostatin



http://www.anatomy-diagram.info/anatomy-of-human-pancreas/human-anatomy-amp-physiology-of-pancreas/

Diabetes

- Diabetes mellitus (DM) is a group of metabolic diseases in which there are high blood sugar levels over a prolonged period
- Three main types of diabetes mellitus:
  - Type 1 DM results from the pancreas's failure to produce enough insulin
  - Type 2 DM begins with insulin resistance, a condition in which cells fail to respond to insulin properly
  - Gestational diabetes occurs when pregnant women without a previous history of diabetes develop high blood-sugar levels

Level #3: design of artificial pancreas

Current approaches

Manual

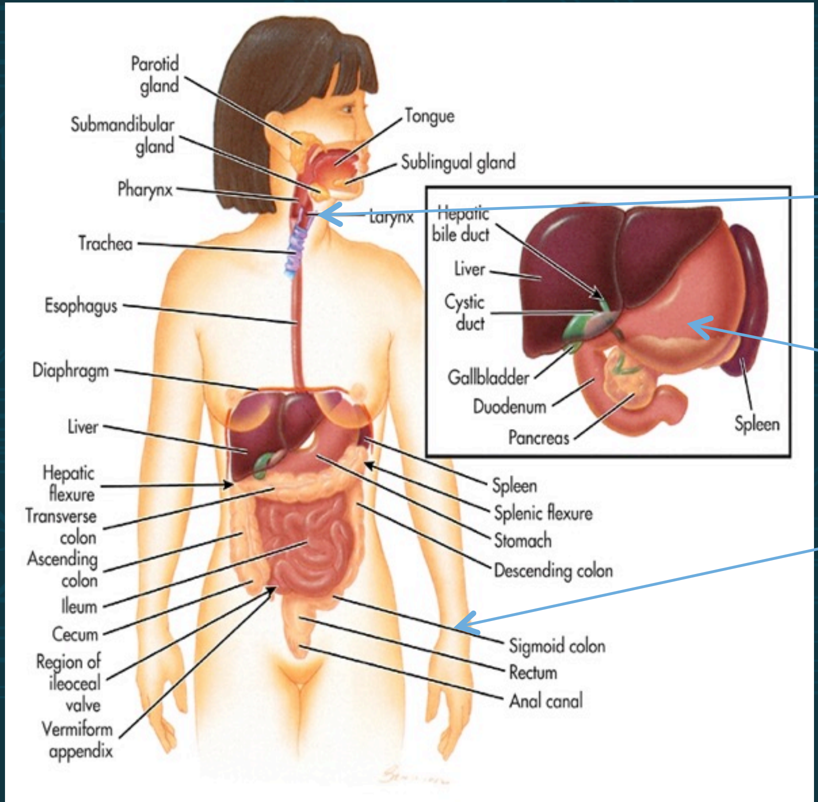
http://zdrowie.gazeta.pl/Zdrowie/1,101580,7044602,Cukrzyca_typu_1_wynikajaca_z_bezwzglednego_braku_insuliny.html
http://www.mojacukrzyca.org/?a=text&id=123

Automatic

https://www.medtronic-diabetes.co.uk/minimed-system/minimed-640g-system
http://insulinnation.com/treatment/artificial-pancreas/is-medtronics-minimed-640g-an-artificial-pancreas/

Level #3: design of artificial pancreas

New placement of sensors



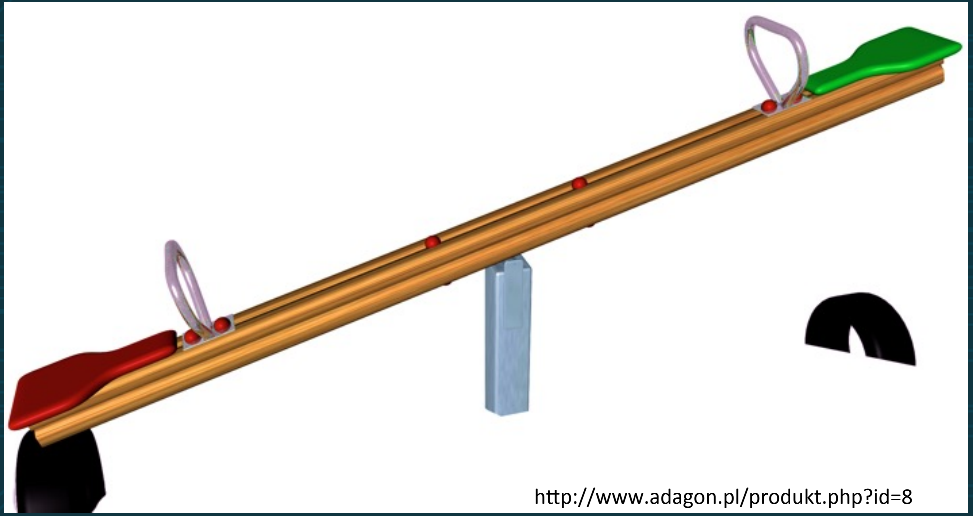
From Thibodeau GA, Patton KT: *Anatomy and physiology*, ed 4, St. Louis, 1999, Mosby.

1. Surroundings of a brain (protecting against low sugar)
2. Stomach (protecting against high sugar)
3. Anywhere else ☺ (just for checking)

Level #3: design of artificial pancreas

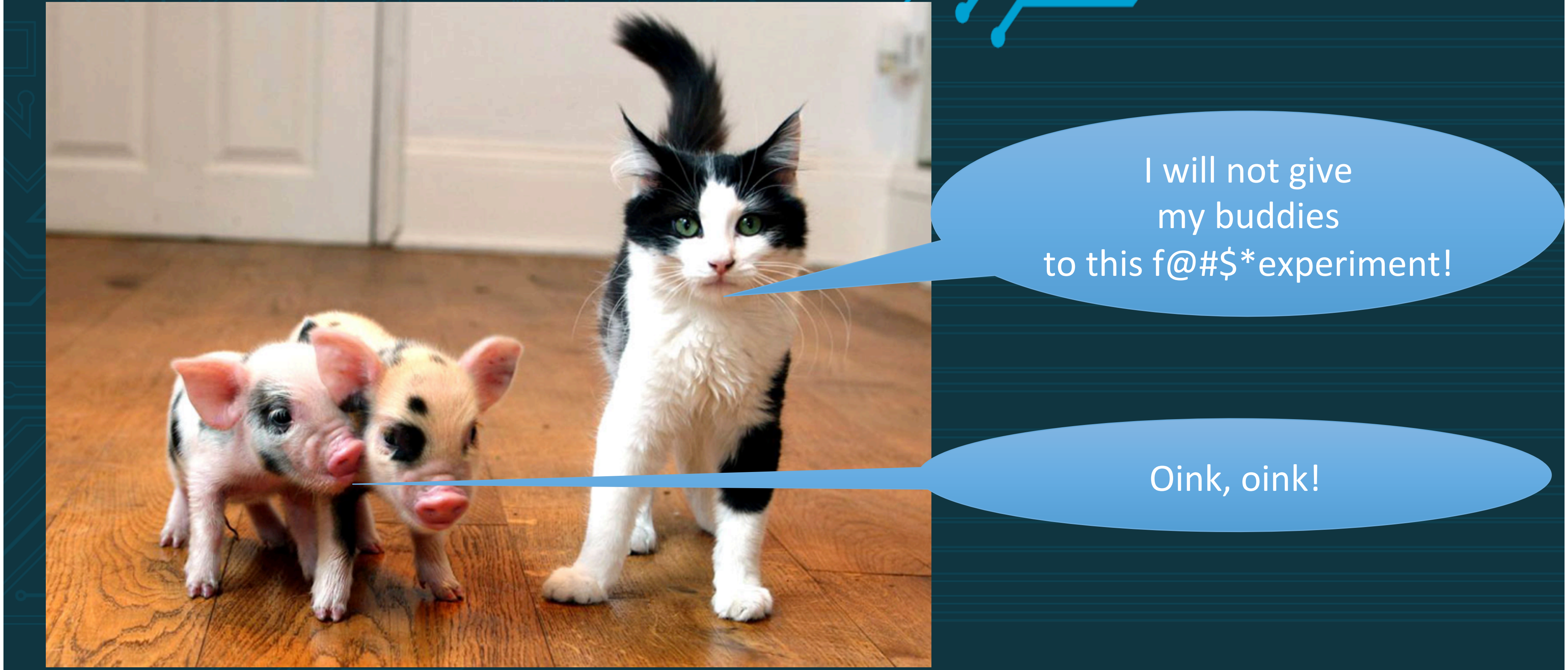
Type of sensors

- Chemical
  - Part of a typical glucometer
  - Very accurate ☺
  - Universal ☺
  - Needs “fuel” ☹
- Fibre-Optic
  - Brand new application for testing the level of sugar
  - Not accurate ☹
  - Depends on a given person ☹
  - Needs frequent calibration ☹
- Both requires power
- Glucose-Level Detection System (GLDS) = IDS ☺
- + IPS: hormone pumps with both insulin (to get glucose down) and glucagon (to get glucose up) – “swing algorithm”



http://www.adagon.pl/produkt.php?id=8

Level #3: design of artificial pancreas



http://wallpaper.imcphoto.net/animals/pigs/funny-pigs-and-cat.jpg

Level #3: design of artificial pancreas

Future of the project

- When we were ready to prepare a grant proposal…
- …our group received fundings for the bionic pancreas based on stem cells
- It is a new challange, but we can still develop and apply our algorithms and learn more than we expected before
- How about running a program on a bionic organ or use a pharmacological support by polymer based drugs as carriers of any chemical compunds?
- Unfortunately, we can’t perform experiments on mothers-in-law, so we still need pigbuddies ☺ for this effort

Almost the end

Conclusions

- Most of steganographic methods are not hard to detect
- Most of them are weak – we called them „bad” or „ugly” – and it is easy to detect them especially at the source of steganograms (SS)
- The SS could be observed from different perspectives
- We used this approach in medicine – to design artificial pancreas

https://www.instagram.com/p/BJlN-sOjZUk/

Thanks!
Any questions!?

krzysztof@szczypiorski.com
http://szczypiorski.com

You can follow me ☺ on:

Instagram: *krisorsky*
Twitter: *k_sz*
Facebook: *szczypiorski*
LinkedIn: *szczypiorski*