GREYCORTEX

New approaches to detection of SCADA threats

Vladimír Sedláček, CTO, GREYCORTEX s.r.o.

WHAT DOES SCADA MEAN TO YOU?

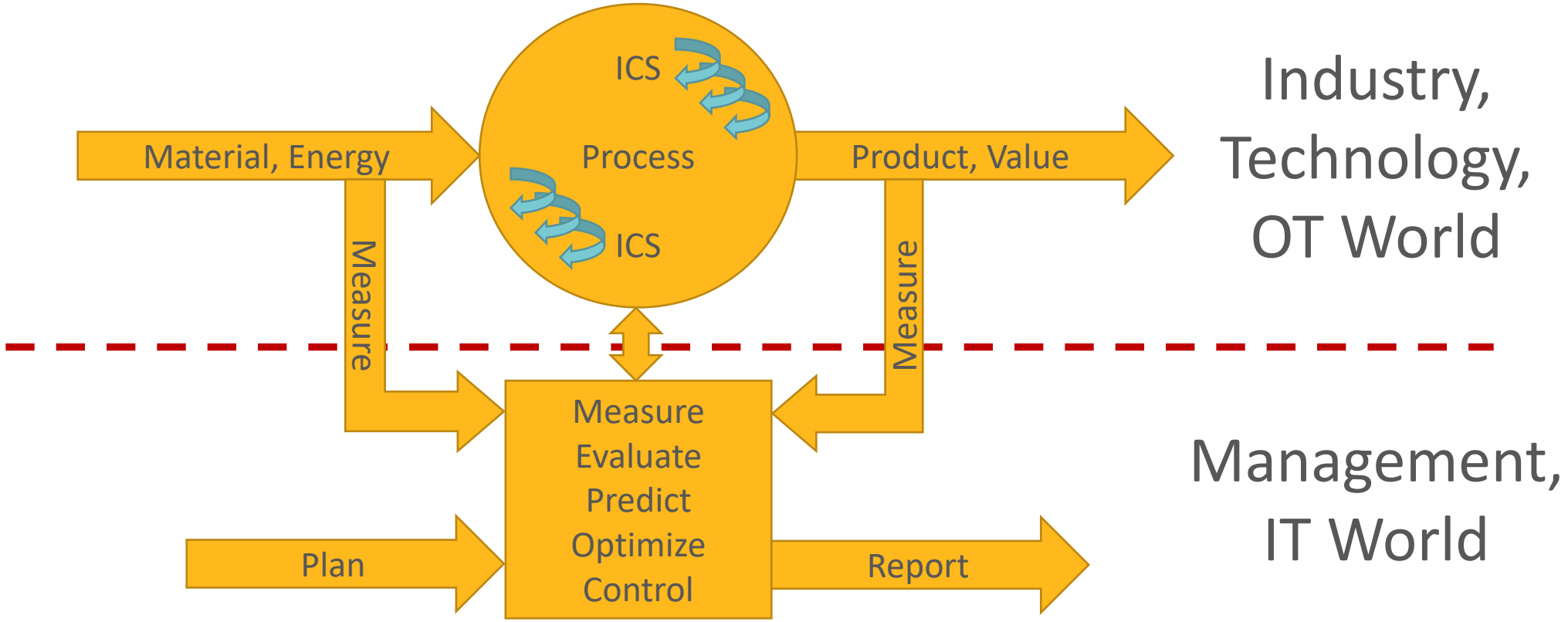
- Supervisory control and data acquisition
  - Dohledové řízení a sběr dat

- Industry? Control System?
- Energy and Utilities?
- Critical Infrastructure?
- Smart Meters? Smart Building? Smart City?
- Surveilance?
- IoT? 5G?

GREYCORTEX

SCADA IS ABOUT CONTROL!

SCADA is not a technology, it‘s about controlling processes. But not acting in!



GREYCORTEX

INDUSTRIAL SYSTEMS IN THE PAST

Control Loop is bound inside the system

Isolated, not connected together

Used and maintained by trained engineers

GREYCORTEX

MODERN INDUSTRIAL SYSTEMS

Control Loop is outside the system, includes a connected computer.

Used by trained operators, maintained by others

GREYCORTEX

BUT THERE IS NO PROBLEM. OR?

The modern industrial systems are perfectly safe. By design and process (*) they include safeguards. Computers inside may not cause harm!

GREYCORTEX

PLAGUE: OT AND IT CONVERGE

OT: islands in the past

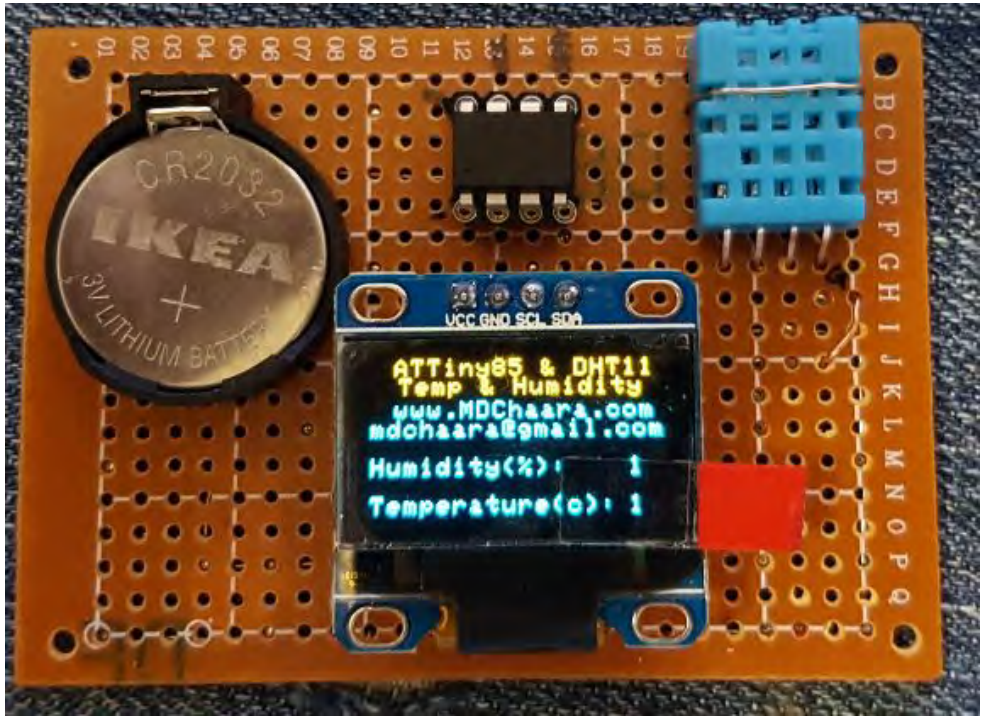
- Starts reporting telemetry
- Tries building sophisticated solutions (expensive), created cheap sensors
- Adopts the (cheap) IT commodity ecosystem and deploy it widely (wildly)
- Inherited serious security issues
- Talks about Industry 4.0 (connected, intelligent, and „Smart“)

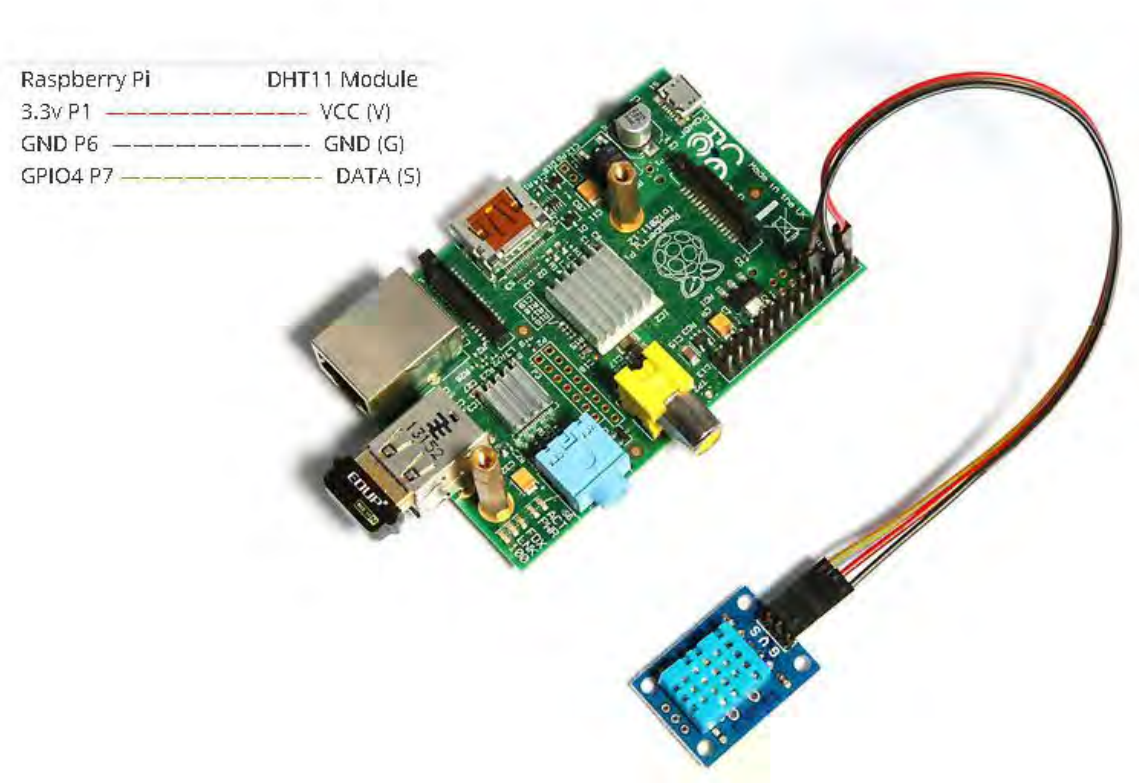
IT: islands in the past

- Starts connecting together
- Builds up commodity in networking (Ethernet, WiFi) and MCUs
- Discovers cheap sensors (made for OT) and starts IoT wave (madness)
- Has serious security issues in its DNA
- Makes everything cloud-connected, intelligent, and „Smart“

GREYCORTEX

EXAMPLE





GREYCORTEX

ONE-TIME DEVELOPMENT PROJECTS

Problematic maintenane and upgradeability

- IT‘s agile MVP (Functionality First)
- No actual sustainment over long lifespan of device
- Adopting changes after release vs. continuity and replaceability

Limited resources in computing and power

GREYCORTEX

INHERITED VULNERABILITY?

A „Standardized Exploitable Flaw“ in IEEE 802.11 (WiFi): **KRACK (CVE-2017-13082)**

Existing since 2008, introduced into 802.11r by support for fast BSS Transition (envisioning SIP IP roaming)

From Wikipedia, the free encyclopedia [2017-11-05, https://en.wikipedia.org/wiki/KRACK]:

*“KRACK (Key Reinstallation AttaCK) is a severe replay attack (a type of exploitable flaw) on the Wi-Fi Protected Access protocol that secures Wi-Fi connections. … discovered in 2016 by the Belgian researchers … published details of the attack in October 2017. By repeatedly resetting the **nonce** transmitted in the **third step of the WPA2** handshake, an attacker can gradually match encrypted packets seen before and learn the full keychain used to encrypt the traffic.”*

The **weakness is in** the Wi-Fi **standard itself**, … any **correct implementation** of WPA2 is likely **to be vulnerable** … **all major software platforms** …

The widely used **open-source** … wpa_supplicant, … Linux and Android, is especially susceptible as it can be manipulated to install an all-zeros encryption key, effectively nullifying WPA2 protection in a man-in-the-middle attack.

GREYCORTEX

SO, WHERE IS SCADA NOW?

IT entered OT domain and interacts directly with control busses, sensors, and actuators inside industrial systems

IT replaced analogue loops and signaling with digital processing

IT-based control systems replaced traditional control systems in all areas (services, utilities, public and private operations, government, etc.)

IT increased capabilities of all operational control technology, replaced analogue processing and transfer of data (telematics, grids, etc.)

IT created new ways of gathering information, processing and applying the knowledge (surveilance and social score, interconnected vehicles, etc.)

GREYCORTEX

GREYCORTEX

SCADA = IT + Legacy OT

GREYCORTEX

SCADA Threats =
IT Threats + OT Threats

GREYCORTEX

ISLANDS OR NETWORKED FOREVER?

OT and IT are connected to **one** network

Network is switching packets, **everything** is connected all the time

Disconnecting does not help, we need things to **remain** connected

Threats come in person, physical (mobile) device, or in data over **network**

Threat agents almost always **communicate**

Any **security** arrangement (isolation) and device (firewall) can be **bypassed**

We need the current security **provisions** AND added **oversight** layer

GREYCORTEX

THE THREAT LANDSCAPE

Threats come from network, communicate over network

SCADA is connected to the network, inherits IT vulnerabilities, adds its own

Protection: Let‘s detect the threats in the network communications

- In the IT layer (local intranet, WiFi, …)
  - ~ 50k known signatures + detecting the unknown by anomal behavior
- In the OT layer (SCADA protocols over serial and Ethernet – DNP, IEC 101/104, …)
  - 400+ known signatures + detecting the unknown by anomal behavior

GREYCORTEX

HOW TO DETECT THREATS?

Network Traffic Analysis (NTA) - an automated, 24/7 all seeing eye on your network

- Advanced statistical models, dynamic prediction
- Protocol and application data analysis, incl. SCADA anomaly detection
- Deep content analysis and signature detection, harmonic analysis
- Network visibility, Hosts inventory, Communication matrices
- Anomaly detection and forensic capture, assisted ML for reporting improvement

Advanced Persistent Threats communicate over network in a specific, anomalous way. Our product MENDEL discovers the threats hiding in your network and even in your security devices.

GREYCORTEX

MENDEL: Shine on network!

Full network visibility

Designed primarily for security oversight in IT and OT networks

GREYCORTEX

DISCOVER: ENLIST AND MODEL

Network

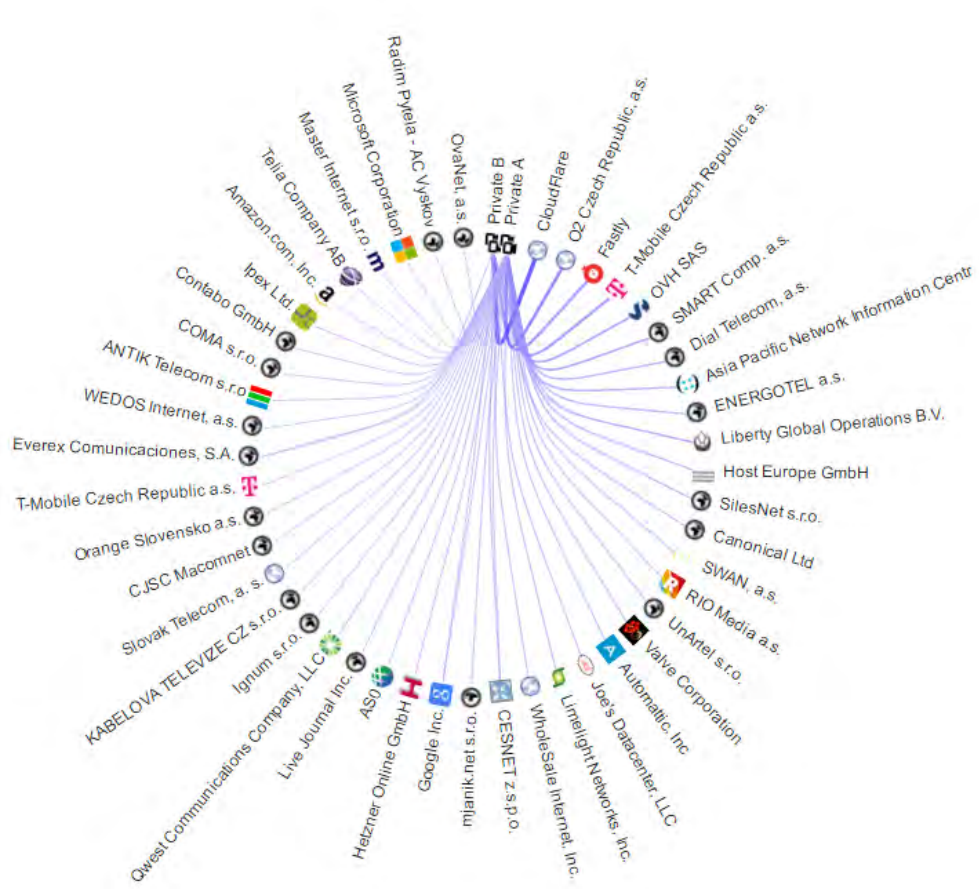
- Inventory: Locality, Address, ASN, Location
- Model: Time, Networks, Services, Metrics

Endpoint

- Inventory: Locality, Address, Services, Protocols
- Model: Time, Networks, Services, Protocols, Metrics

Automated discovery of new devices and services

- by listening and learning



GREYCORTEX

DETECT: ANOMALY, THREAT, DROPOUT

Prediction of metrics based on the past

- Unusually high or low actual value,
- Periodic analysis

Deep packet inpection

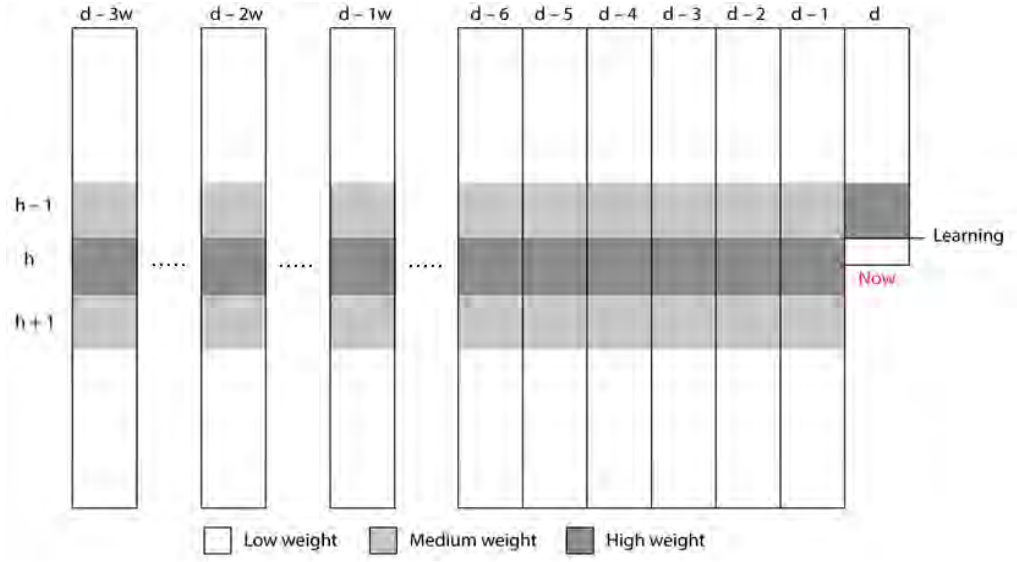
- Signature based detection
- Incidence correlation

Application dialogue timing

- Performance dropouts, saturation and latency

Semi-supervised machine learning

- Adjust sensitivity to anomaly in model data input feed

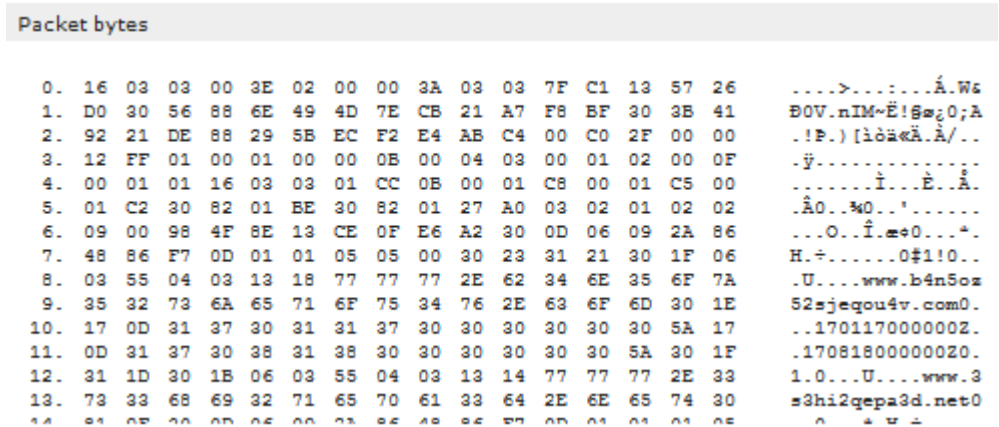


GREYCORTEX

DOCUMENT: FORENSIC EVIDENCE

Collecting L3 to L7 content and metadata

- Flag combinations
- Application
- Request filename
- Response status
- Headers and content signatures
- Tunnel indices
- etc.



GREYCORTEX

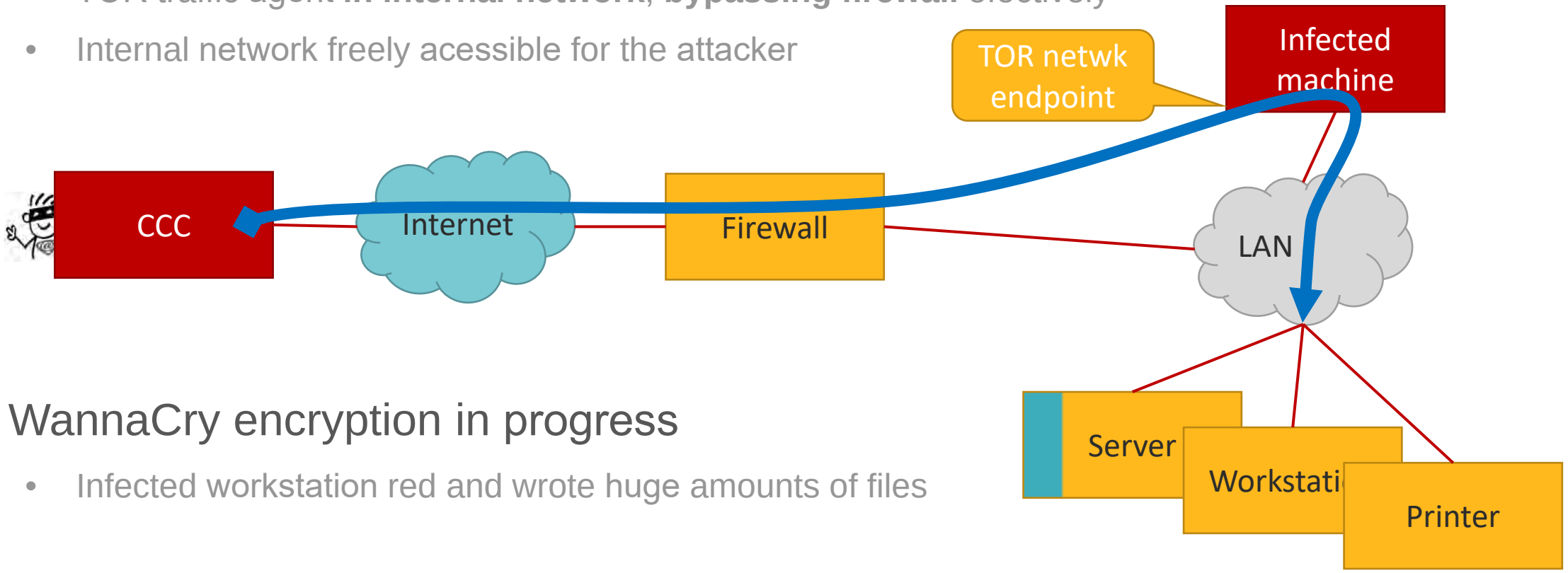
What MENDEL saw

Easy examples of discovered real network issues discovered within 1 hour of deployment

GREYCORTEX

RESIDENT MALWARE SUCCESS

- Malware VPN Filter
  - TOR traffic agent **in internal network**, **bypassing firewall** efectively
  - Internal network freely acessible for the attacker



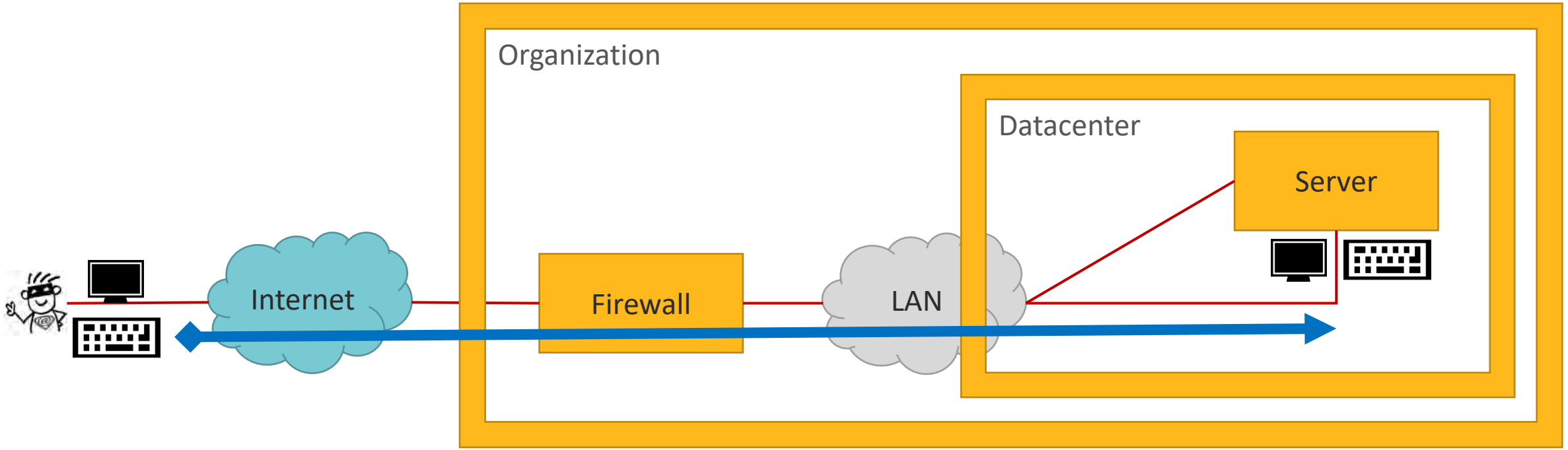
- WannaCry encryption in progress
  - Infected workstation red and wrote huge amounts of files

GREYCORTEX

SERVER CONSOLE FREELY ACCESSIBLE FROM THE INTERNET

Firewall open for access, forwarding public address to a server console with default password

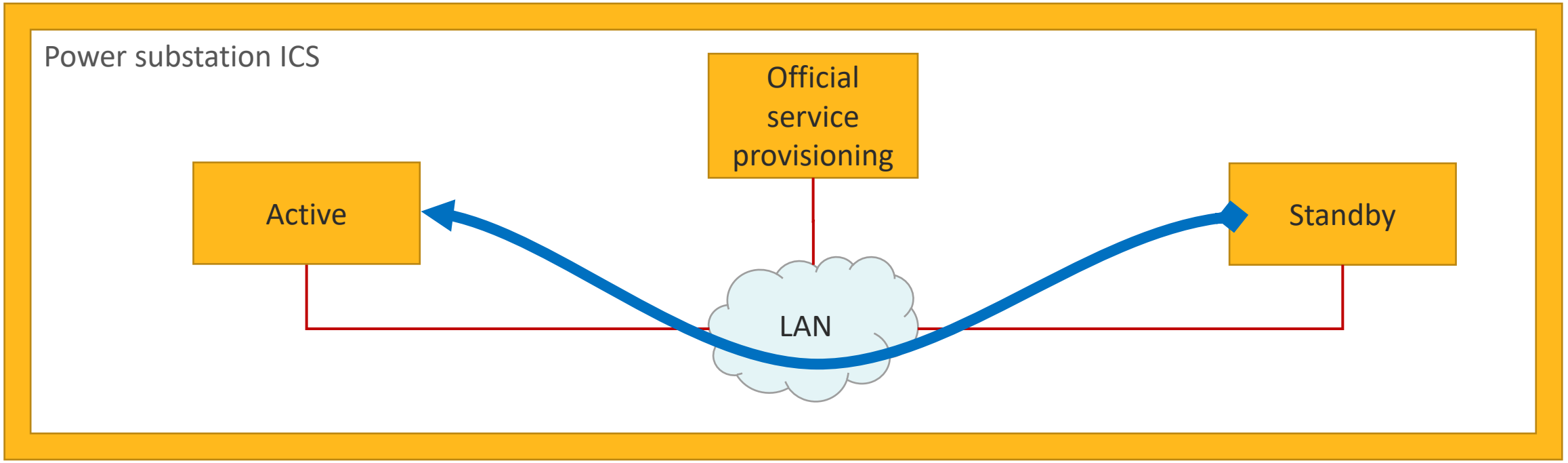
Unrestricted access to screen, keyboard, CD, USB and diagnostic utilities of a private server behind two locked doors



GREYCORTEX

OT MISCONFIGURATION

- Active and standby systems used a service in P2P fashion instead of the assigned service provider. They also talked across geographically spread substations, possibly harming the energy flow stability.



GREYCORTEX

TYPES OF OUR CUSTOMERS

- Research and production factory
- Bank, finance corporation
- Web service
- Private healthcare
- Law office
- Office, ministry, prefecture
- State agency, armed force
- Municipal infrastructure service
- Transfer grid operator
- SoC provider
- YOU?

GREYCORTEX

Final …

Questions?

GREYCORTEX

USE GREYCORTEX MENDEL FOR A BETTER SLEEP!

Tato fotka , unknown author, 2019-09-16 20:09

Memes courtesy of: http://weknowmemes.com/generator/generator/

GREYCORTEX

It can‘t happen to us…

Polemic

GREYCORTEX

There are 10 types of ICT users:

- Those, who were hacked, and
  - Those, who will be

Are you the next target?

GREYCORTEX

THE SURVEY

My office/company/industry is not interesting for attackers	☑ Yes	☒ No
I have anti-virus solution and it will keep me safe	☑ Yes	☒ No
The guards at entrance will recognize an attacker and deny entry	☑ Yes	☒ No
It is the responsibility of IT department to protect us	☑ Yes	☒ No
Our Wi-Fi is ultimately secured by password and no outsiders can connect	☑ Yes	☒ No
I will immediately recognize my computer got infected	☑ Yes	☒ No
We trust our employees and personal devices do not need to be secured for work	☑ Yes	☒ No
Our cybersecurity coverage is complete and there is nothing to improve	☑ Yes	☒ No
I don‘t need to see what‘s happening in my network	☑ Yes	☒ No

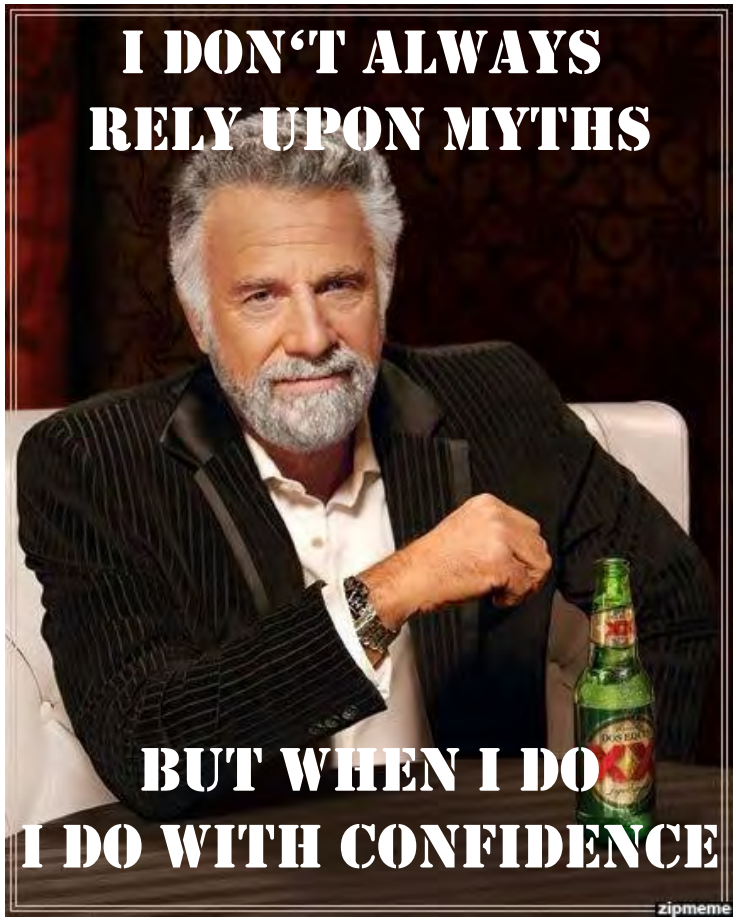
GREYCORTEX

SURVEY RESULT

If you replied any question with yes,

you are about to be …

HACKED SOON!



GREYCORTEX

Use GREYCORTEX Mendel and have a better sleep!

www.greycortex.com – look at whitepapers, use cases, insights, scenarios

vladimir.sedlacek@greycortex.com – blame author

info@greycortex.com – ask for a demo or 30 day PoC

www.youtube.com/greycortex – watch our videos

GREYCORTEX