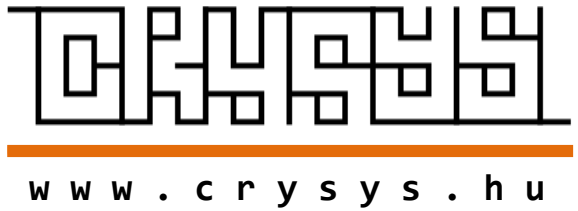


Malware Protection for IoT Devices

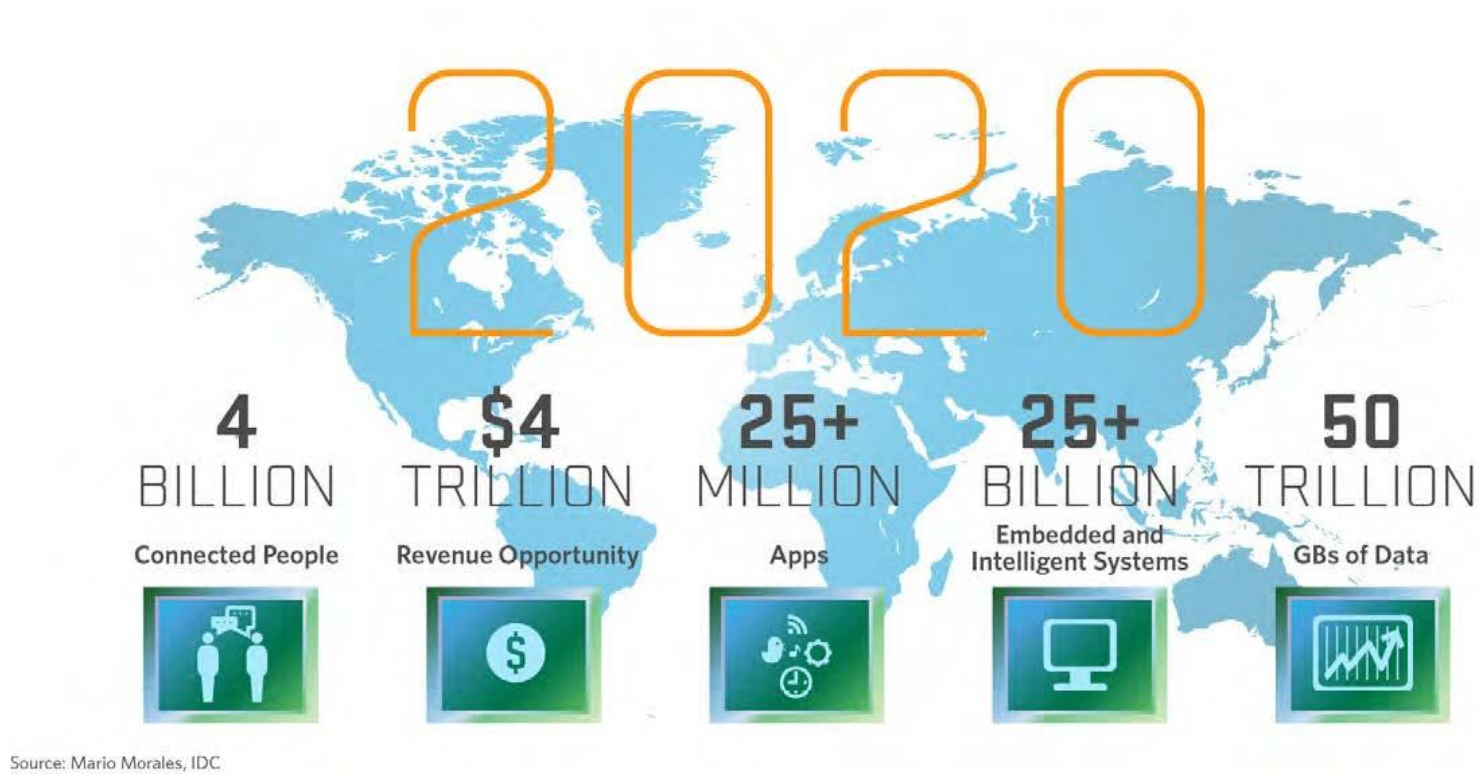
Dorottya Futóné Papp

CrySyS Lab, BME Ukatemi Technologies

dpapp@crysys.hu

Internet of Things

- On-going evolution of the Internet
- More connected devices than connected people

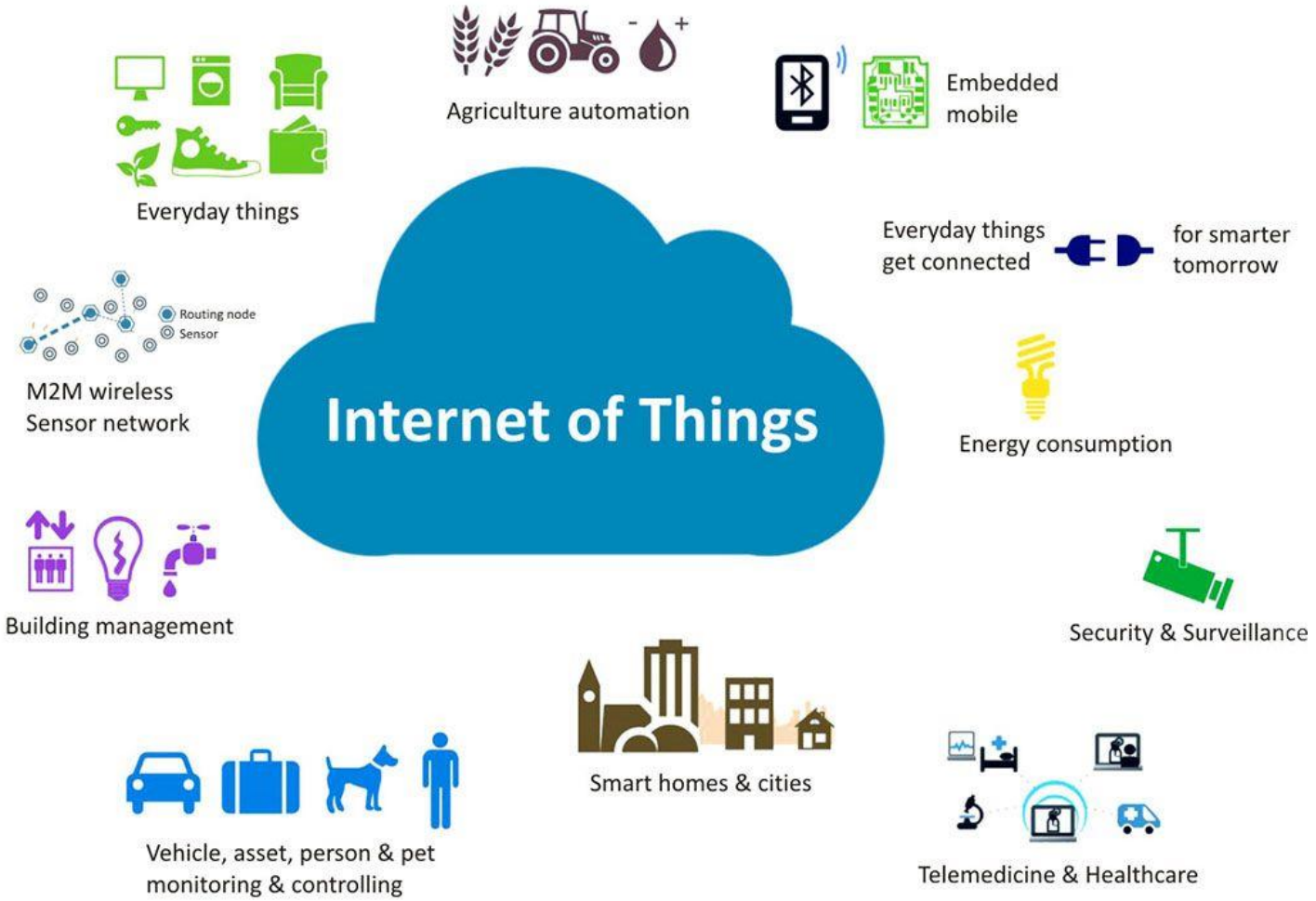


IoT ”smart” devices

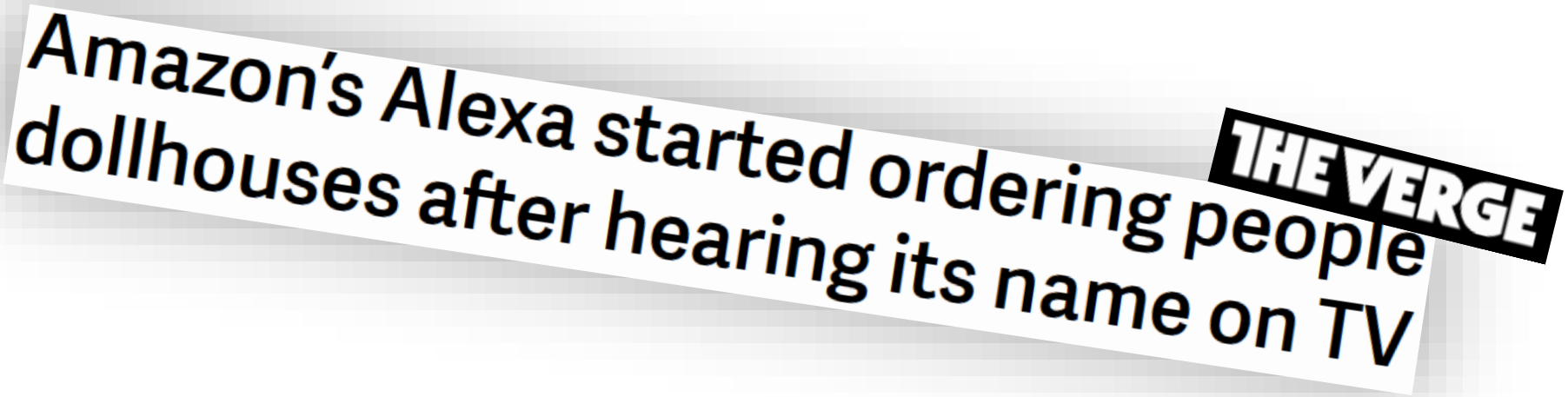
- Internet connection
- Embedded device: developed to perform a specific task
  - Sensors, actuators

- → Machine-to-machine interaction
- → Monitoring, Automation and control

IoT applications



”Smart” devices can be tricked



”Smart” devices can be tricked

”Smart” devices can be tricked

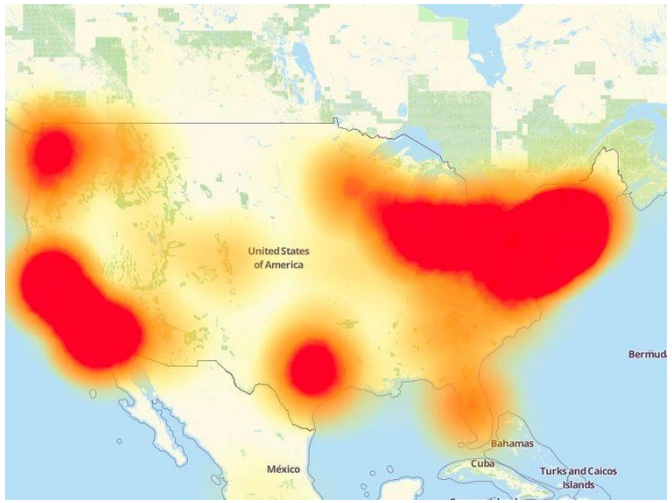
”Smart” devices can be tricked

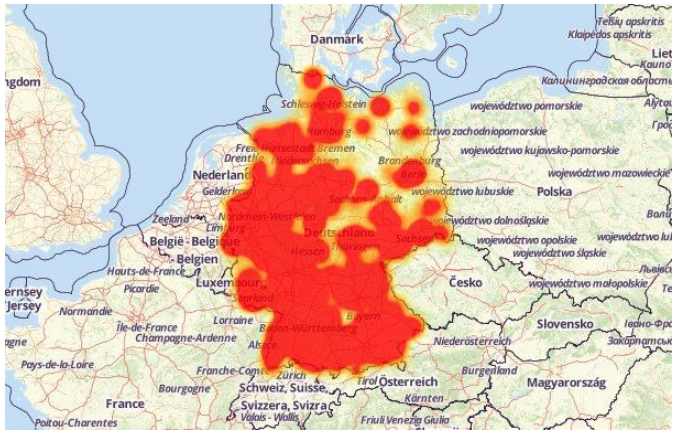
”Smart” devices can be tricked

IoT targeted by malware

- Malware = **mal**icious soft**ware**
  - Generic term, encompasses viruses, worms, trojans, etc.
  - Installed without user consent
  - Performs unintended operations

- Example: Mirai botnet (2016)
  - DDoS attack against DNS servers
    → Many websites unreachable
  - Magnitude: 1.2 Tbps





Security issues of IoT devices

- Insecure open ports for communication
  - No authentication necessary for privileged access
- Weak passwords
  - Default passwords can be collected in dictionaries
  - Hard-coded passwords can be found in firmware images
  - Guessable passwords
- Vulnerable software
  - Vulnerabilities in the firmware/OS and the applications
    → Infection, privilege escalation
  - Exploitation may begin before patch is available

Protection is challenging

- Traditional protection: antivirus scanners
  - Scan individual files for signs of malware, called signatures
  - Signatures are stored in the signature database (GBs of RAM/HDD)

Protection is challenging

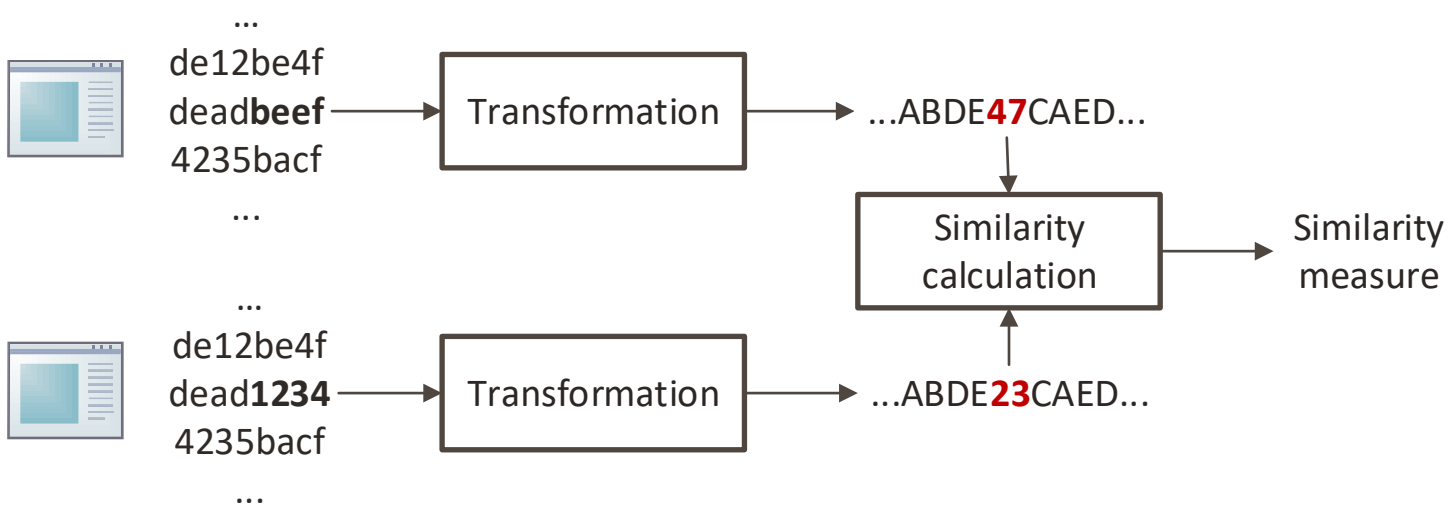
- Traditional protection: antivirus scanners
  - Scan individual files for signs of malware, called signatures
  - Signatures are stored in the signature database (GBs of RAM/HDD)

- IoT devices are resource constrained
  - Less computing power
  - Less memory
  - Less storage
  - In many cases, battery-powered
- → IoT devices cannot handle existing signature databases!

Antivirus scanner for IoT devices

- Goal: create a smaller signature database

- Binary similarity measure

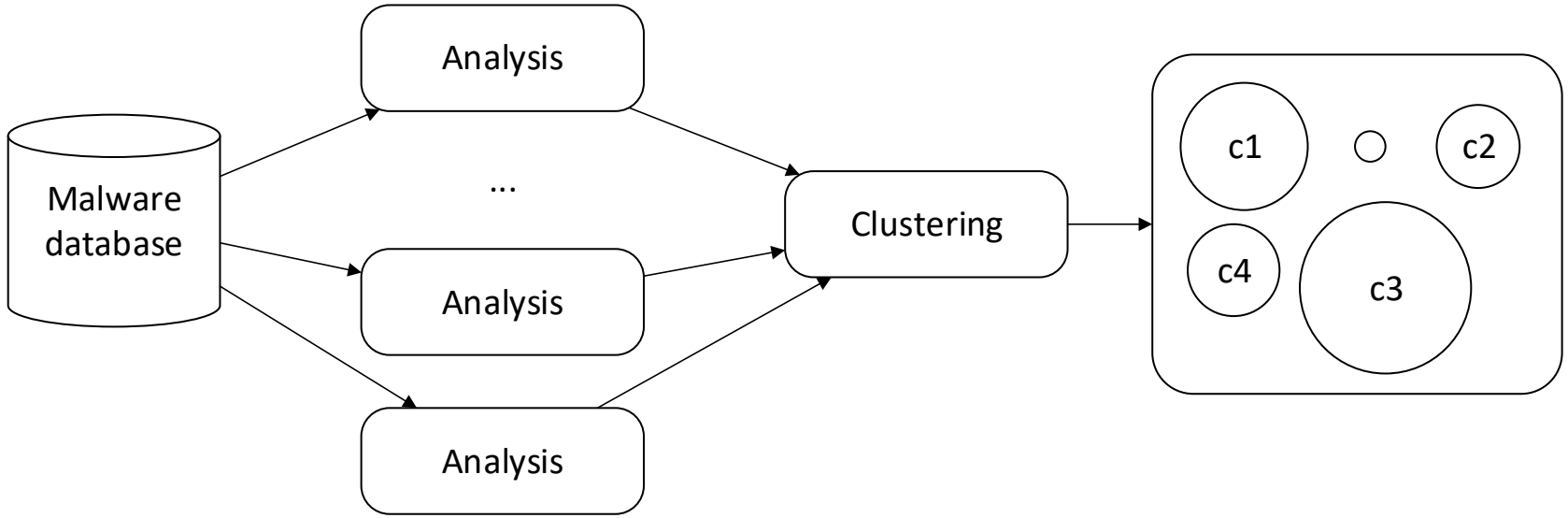


  - Transformation and similarity calculation is fast (milliseconds)
  - Result of transformation is tens of bytes

Antivirus scanner for IoT devices

- Goal: create a smaller signature database

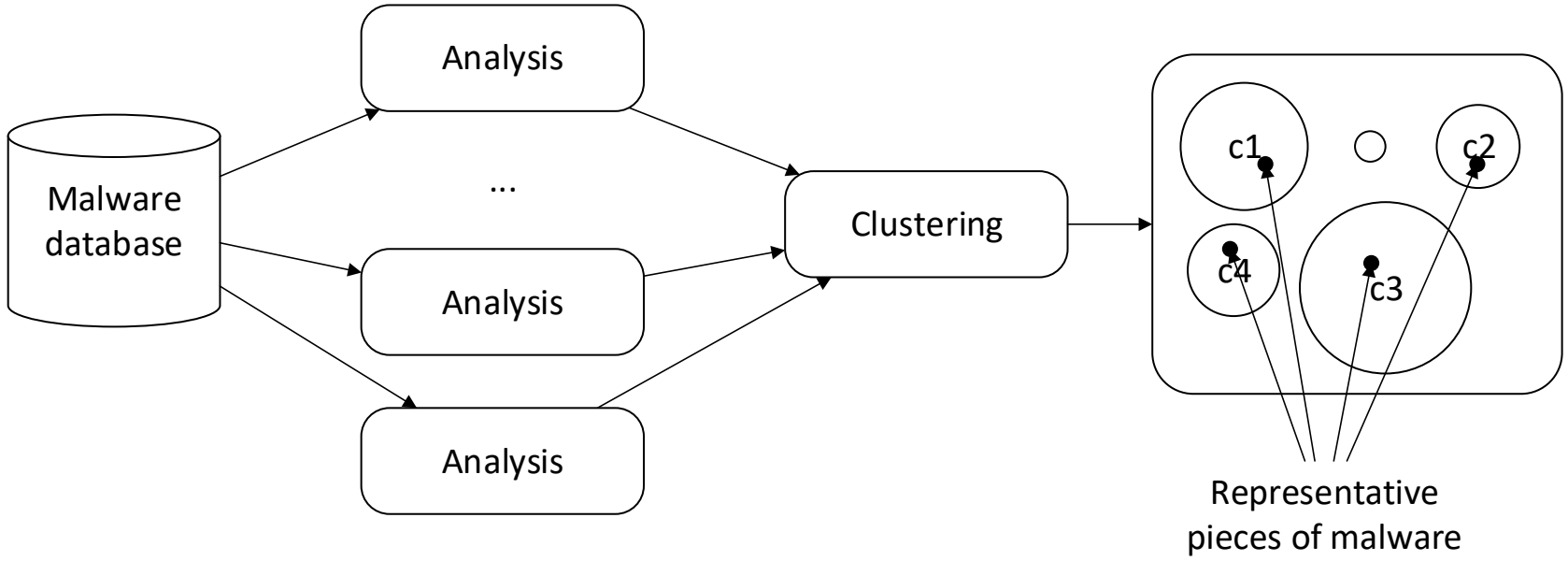
- Binary similarity measure
- Malware clustering



Antivirus scanner for IoT devices

- Goal: create a smaller signature database

- Binary similarity measure
- Malware clustering



Takeaway messages

- Internet of Things enables new and innovative applications but devices face many threats
- Traditional security measures are hard to apply due to resource constraints
- CrySyS Lab and Ukatemi developed new, innovative antivirus scanner for IoT devices
  - Orders of magnitude smaller signature database
  - Computation tailored for resource-constrained embedded devices

Acknowledgement

This work was supported by the SETIT project (no. 2018-1.2.1-NKP-2018-00004), which has been implemented with the support provided by the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme.