Hochschule Konstanz
Fakultät Informatik

Introduction to IT Security

WIN+AIN

Hanno Langweg

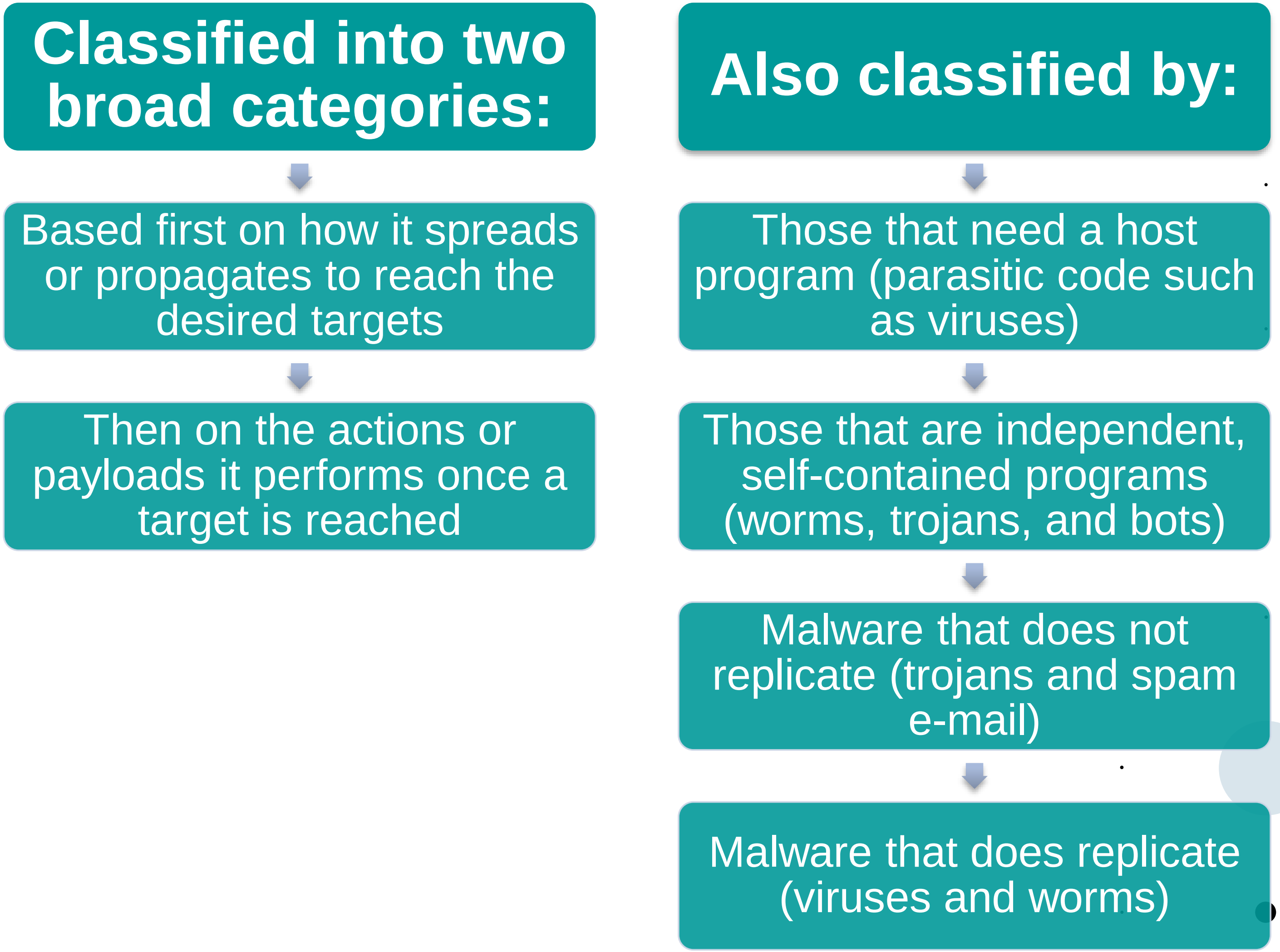
04d Secure Operating Environments - Malware

Secure Operating Environments

- Security of operating systems
- Trusted Computing
- Access control
- Malware

Malware and Antivirus

Classification of Malware



Classified into two broad categories:

Based first on how it spreads or propagates to reach the desired targets

Then on the actions or payloads it performs once a target is reached

Also classified by:

Those that need a host program (parasitic code such as viruses)

Those that are independent, self-contained programs (worms, trojans, and bots)

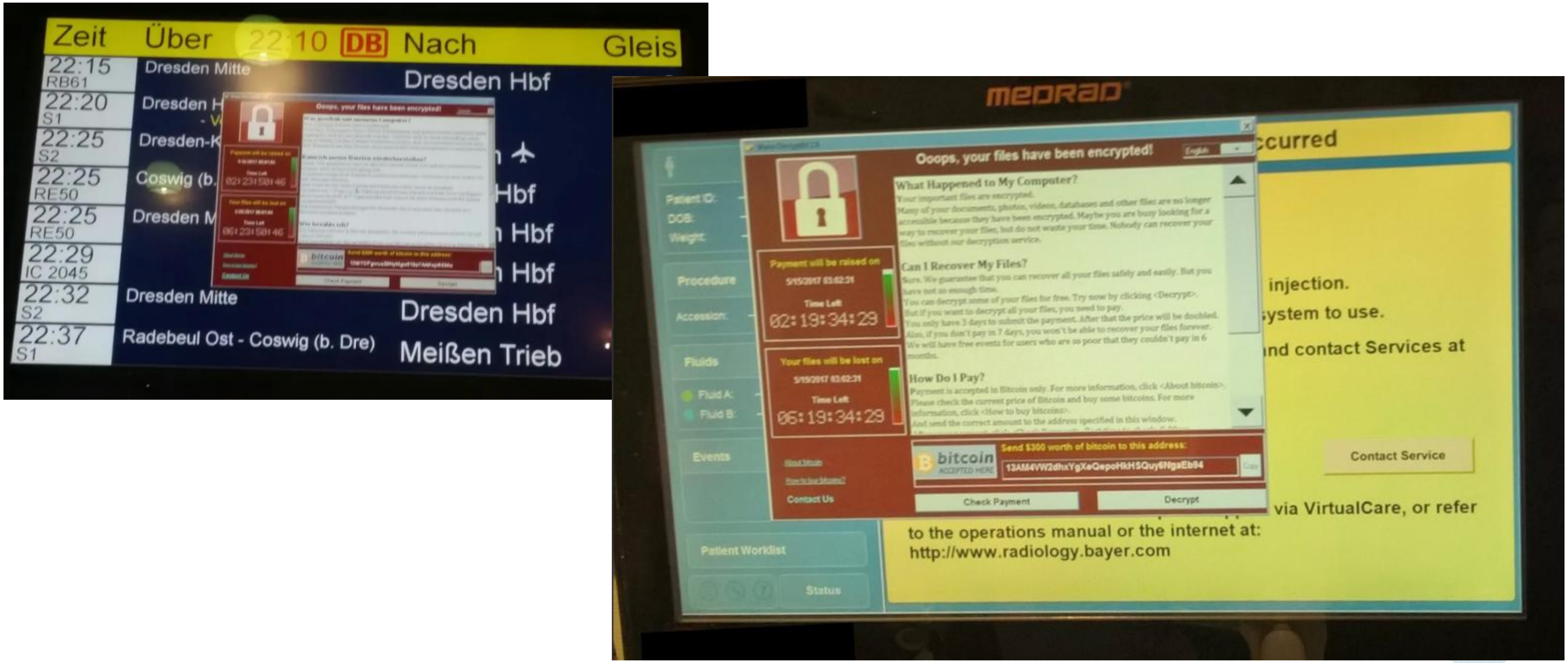
Malware that does not replicate (trojans and spam e-mail)

Malware that does replicate (viruses and worms)

Types of Malicious Software (Malware)

- Propagation mechanisms
  - Infection of existing content (binaries, macros)
  - Exploitation of software vulnerabilities, e.g. by worms
  - Social engineering to convince users to bypass security mechanisms; often used by Trojan horse programs or phishing attacks
- Payload actions
  - Anything that is allowed for the user account the malware is executed under (i.e. browser, logged on user)
  - Examples: transfer personal data to remote system, corrupt local files, encrypt files on network share, record keystrokes

Ransomware


Zeit Über 22:10 DB Nach Gleis
22:15 RB61 Dresden Mitte Dresden Hbf
22:20 S1
22:25 S2
22:25 RE50 Coswig (b.
22:25 RE50
22:29 IC 2045
22:32 S2 Dresden Mitte Dresden Hbf
22:37 S1 Radebeul Ost - Coswig (b. Dre) Meißen Trieb
MEDRAD
Ooops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
Payment will be raised on
Time Left
02:19:34:29
Your files will be lost on
06:19:34:29
bitcoin
Send $300 worth of bitcoin to this address:
Check Payment
Decrypt
Contact Us
Patient ID:
DOB:
Weight:
Procedure
Fluids
Events
Patient Worklist
Status
injection.
system to use.
and contact Services at
Contact Service
via VirtualCare, or refer
to the operations manual or the internet at:
http://www.radiology.bayer.com

https://www.heise.de/newsticker/meldung/Ransomware-WannaCry-befaellt-Rechner-der-Deutschen-Bahn-3713426.html (2017-05-13)

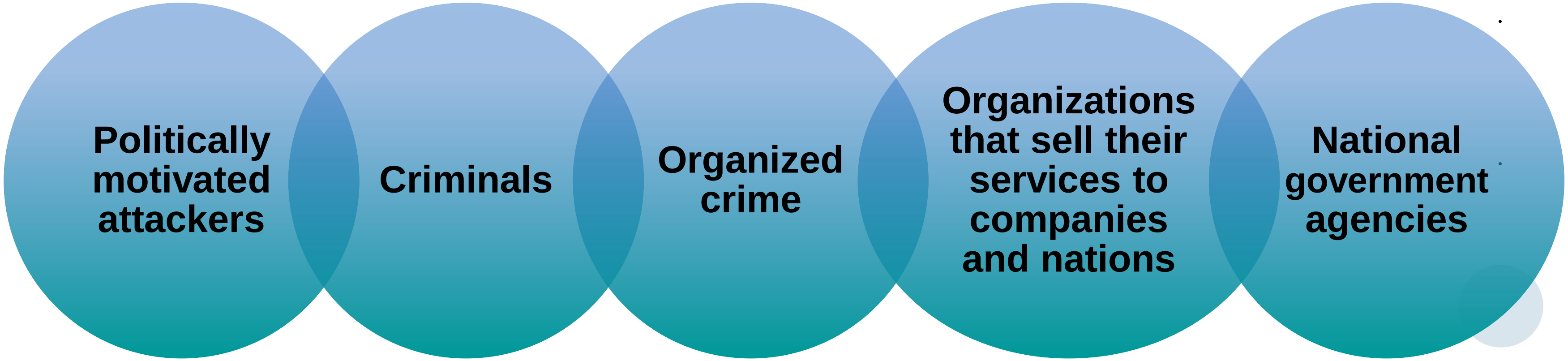
https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/ (2017-05-17)

Attack Kits

- Development and deployment of malware required considerable technical skill
  - Development of virus-creation toolkits in early 1990s and more general attack kits in the 2000s greatly assisted in development and deployment of malware
- Toolkits often known as “crimeware”
  - Include variety of propagation mechanisms and payload
  - Generated variants pose problem for defenders 1,000's of new malware variants per day
- Widely used toolkits include e.g.
  - Zeus, Blackhole, Sakura, Phoenix

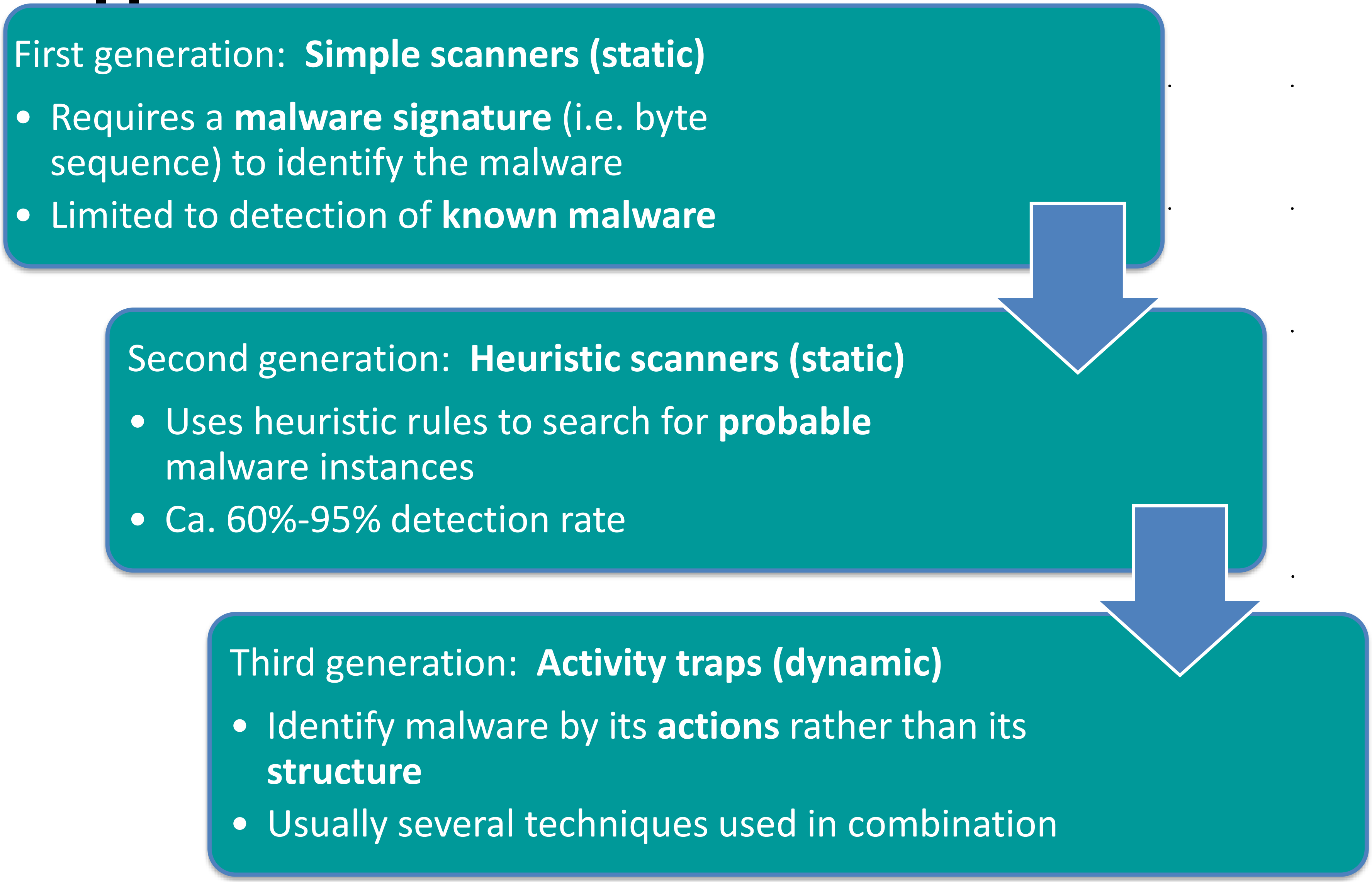
Attack Sources

- Change from individual attackers often motivated to demonstrate technical competence to peers to more organized and dangerous attack sources e.g.:


Politically motivated attackers
Criminals
Organized crime
Organizations that sell their services to companies and nations
National government agencies

- This has changed available resources and motivation behind rise of malware and led to development of large underground economy involving sale of attack kits, access to compromised hosts, and to stolen information

Approaches of Anti-Virus Software



First generation: **Simple scanners (static)**

- Requires a **malware signature** (i.e. byte sequence) to identify the malware
- Limited to detection of **known malware**

Second generation: **Heuristic scanners (static)**

- Uses heuristic rules to search for **probable** malware instances
- Ca. 60%-95% detection rate

Third generation: **Activity traps (dynamic)**

- Identify malware by its **actions** rather than its **structure**
- Usually several techniques used in combination

Summary

- Security of operating systems
  - Hardening, i.e. configuration with reduced attack surface and least privilege
- Trusted Computing
  - Bind access to cryptographic keys to system configuration
  - Remote attestation of system state
- Access control
  - Discretionary access control, role-based access control
  - Assignment+revocation of rights
- Malware: Detection is hard (in theory: impossible)
  - Effect can be limited by access control