System Security @ VU
Past, Present and Future

Herbert Bos

Lorenzo Cavallaro

Andrew S. Tanenbaum

Two Groups

Two Groups

Where is the research?

reliable FS

secure and reliable OS (ERC)

decoupled security

reverse engineering (ERC)

high−speed monitoring

dynamic updates

mobile phones

intrusion recovery

payload execution

static analysis

attack detection

memory corruption

security for legacy binaries

compiler techniques

taint analysis

dynamic analysis

code obfuscation

voting machines

attack + malware analysis

malware collection

honeypots (client+server)

- - - - - = secure and reliable systems
·-·-·-· = systems and networl security
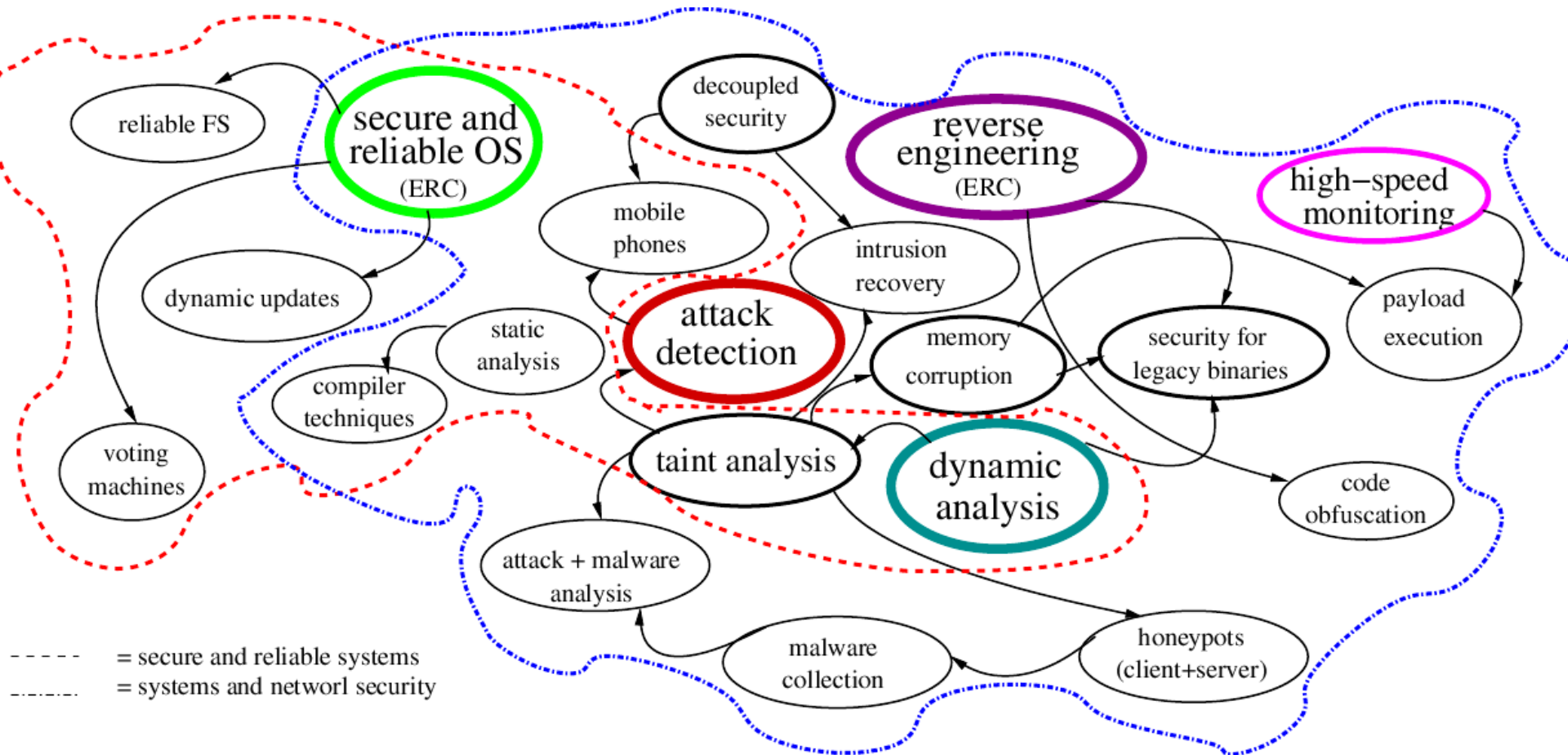
Topics

- Old bugs don't die. They don't even fade away
  - legacy software
  - new variants
- Attacks are stealthy
  - how to detect chameleonic 'stuff'
  - flying under the radar
- Binaries are code!
  - we don't know what they do
  - malware *and* goodware
- Existing solutions often do not work
  - hostile environments
  - resource constrained
- We need to design safe systems!
  - isolate
  - check

reverse engineering!

PAST

PRESENT

FUTURE

parting thoughts
(or what I advise my students)

- stop building stuff that is easy to evade
- stop building yet another network anomaly detector*
- worry about concurrency
- plan for massive complexity
- reach out to other research domains
- build proactive solutions

*Update: or a minor variation of any other detection/analysis technique