TECHNISCHE UNIVERSITÄT DRESDEN

Professur Datenschutz und Datensicherheit

Department of Computer Science, Institute for Systems Architecture, Chair of Privacy and Data Security

Security & *Privacy* by Design – Introduction to Topics at the Chair of Privacy & Data Security TU Dresden

dud.inf.tu-dresden.de

Stefan Köpsell (stefan.koepsell@tu-dresden.de)

Job Offer (SHK/WHK)

Tasks:

- Support the Chair regarding IT-infrastructure realted tasks
- Administration of Machines and Users
- Develop Web-Application
- Support our IoT-Lab
- Help with developing skill for our robot
- Support the research….

Skills:

- broad knowledge in IT
- ability to program
- responsible
- selforganising

Master/Diplom topic

Topic: Holistic View on Secure Software Updates for IoT Devices

Problem:

- IoT devices will need updates over their whole lifetime
- IoT device lifetime >> lifetime of producer

Task:

- Think about supporting pre-conditions like componentized software architecture, common (secure) operating system etc.
- How to organise software updates if company is not longer available
  - Open Source community
  - Governmental agency?
- How to protect intellectual property of produces and at the same time ensuring access to the source code
- Economic, legal implications?
- How can IT-security support all this?

Master/Diplom, INF-PM-FPA, Großer Beleg, maybe bachelor topic (also chained)

Topic: Fingerprinting / detecting hypervisors and possibly countermeasures

Problem:

- Virtualisation based environments are used for malware analysis
- How could malware detect this?
- (How) can we prevent this detection?

Task:

- State-of-the-Art literature review related to the topic
- Analysis of exemplary hypervisor
  - SuperNOVA – hypervisor by Cyberus Technologies (Dresden)
  - In co-operation with that company
- Proposals for countermeasures

Topic: Mixe on Trusted Execution Environment (TEE)

Problem:

- Operating Mix in Cloud
  - On has to trust the cloud provider
- Solution: Trusted Execution Environment
  - Intel SGX (assumption: secure)

Task:

- port the existing Mix implementation so that it can run in a TEE
  - Utilise the SCONE runtime/compile framework developed by Prof. Fetzer
- Decompose the current design so that only necessary parts run in TEE
  - Reduced trusted execution base (TCB)
- Think about remaining problems (e.g. observation of memory access patterns), their influence on anonymity and how to solve that

Topic: Mixe on network card

Problem:

- Enhance the performance of anonymous communication

Task:

- Port the existing Mix implementation so to that the main message loop can run directly on a programmable network card
  - Programming languages: P4 / C

Topic: Mixe using DPDK/QAT

Problem:

- Enhance the performance of anonymous communication

Task:

- Port the existing Mix implementation so to it can utilise DPDK/QAT
  - Technologies which allow very fast network packet processing
  - Technologies which include hardware assisted cryptograhpie

TECHNISCHE UNIVERSITÄT DRESDEN

Master/Diplom, INF-PM-FPA, Großer Beleg, maybe bachelor topic

Topic: Analysing Malicious Software despite of TEEs

Problem:

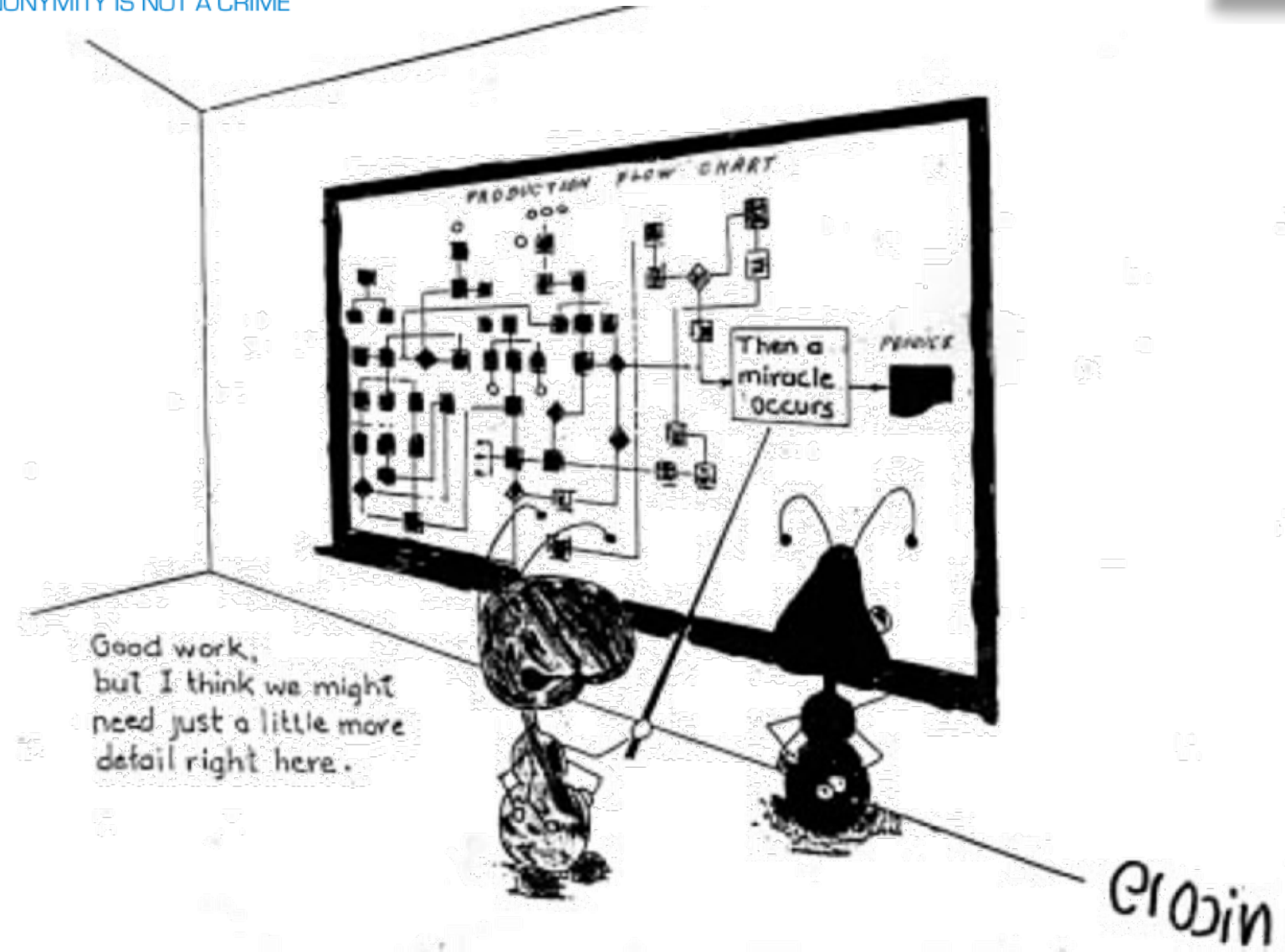
- Trusted Execution Environments (TEEs) can be utilised by malicious software (malware, bots, command&control server) to hinder their analysis/reverse engineering

Task:

- Think about if and how the fundamental conflict can be solved between:
  - TEE: no outsider should be able to tamper with
  - Analysing malicious software: outsider wants to get access/reverse engineer
- State-of-the-Art literature review
- Proposal for system/security architecture balancing the different interessts

Questions?


low
fair
high
Anonymity


PRODUCTION FLOW CHART
Then a miracle occurs
Good work, but I think we might need just a little more detail right here.
Robin