

# Options to Secure PCs

## Against Phishing and Espionage

A report from the EU-project „Open Trusted Computing“

*Arnd Weber*

ITAS:

Institute for Technology Assessment and Systems Analysis  
Partner of ETAG (EP) and TAB (Bundestag)



# Problems

## Malicious code

- Leading to data leakages
  - Homebanking
  - Economic espionage
- Fake digitally signed documents
- Costs



# Securing MS Windows

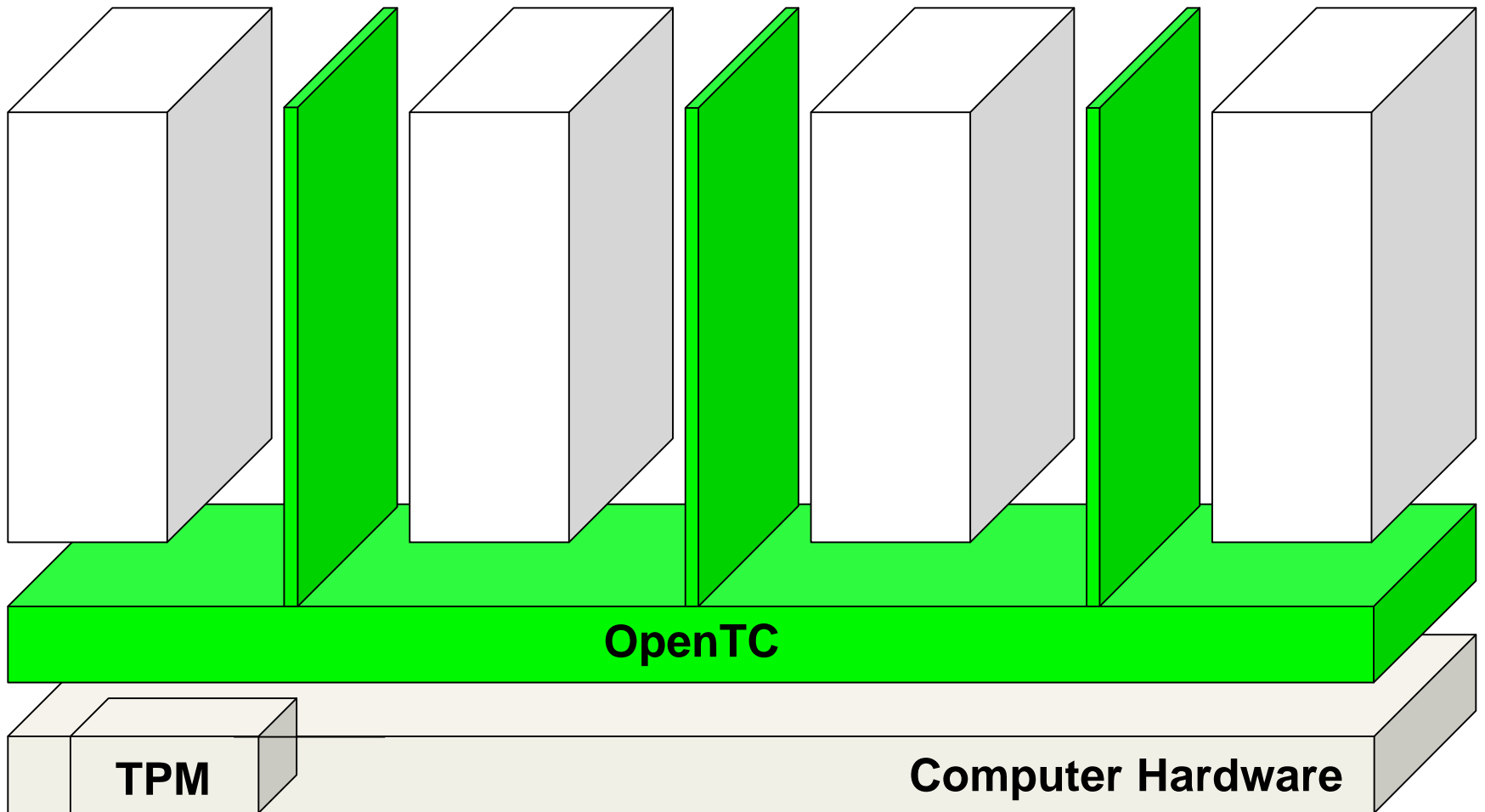
„Isn't going to work“

Paul England, Microsoft

# Redesign Computers

Useless for everyday use

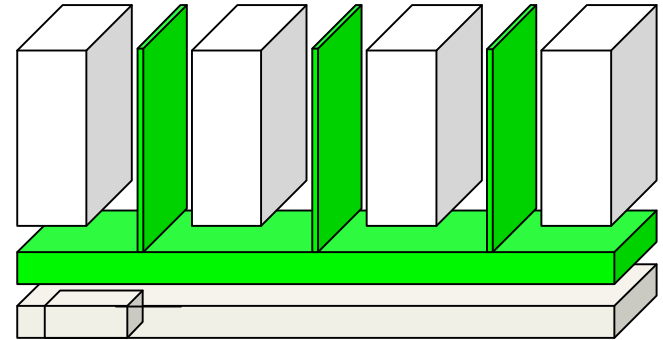
# A Secure Hypervisor



# „Silver Bullet“

## Sandboxes with

- Windows
  - Corporate
  - Private
- Risky apps
- Secure apps



# Progress towards a secure hypervisor

OpenTC project 2005-2009

- Several prototypes
  - Open source HV works with Windows
- Several modules evaluated and error-free
- More work needed



# PC hardware

- Intel and AMD work on „curtaining“  
„Mainframe security for everybody“  
David Grawrock, Intel
- Error-free?
- Will future hardware contain backdoors?

*Same principles can be applied to  
servers,  
cloud computing, mobile phones...*

# Messages

- If you want to protect data on PCs, you need a secure hypervisor
- Hypervisors might become mainstream
  - Look for
    - Openness of source code
    - Evaluation

# Thanks

Dirk Kuhlmann, HP; Matthias Schunter, IBM;  
Armand Puccetti, CEA; Dirk Weber, ITAS

and all others from our 23 OpenTC-partners

# Next steps and info

- Check [opentc.net](http://opentc.net), e.g., for
  - Next newsletter
  - Chris Dalton: A hypervisor against ferrying away data. Interview by Franco Furger and Arnd Weber. OpenTC Newsletter April 2009
- New dialogue-oriented website
- Contact [arnd.weber@kit.edu](mailto:arnd.weber@kit.edu)