ERNW
providing security.

TROOPERS 11

Opening Remarks

Enno Rey

Welcome!

TROOPERS: Maximize your personal development.

Opening Remarks

- Announcements
- What is TROOPERS?
- Why TROOPERS is important

Announcements

Some organizational stuff

- Tracks
  - Attack & Research: Auditorium (→ here ;-)
  - Defense & Management: 3rd floor
- Breaks
  - Lunch: 12:30 PM, 2nd floor
- Badge Challenge
  - Hey, it's just an iPad2… relax ;-)
- Shared Dinner
  - 6:30 PM, "Weisser Bock" (Old Town)
    - We'll provide detailed information how to get there.
- PacketWars
  - After the dinner, same location
- TROOPERS 10k run
  - 7:00 AM, Marriott lobby + stopover @Qube

For those who don’t know me

Enno Rey

- Old-school network security guy
- Founder of ERNW, in 2001
- Your TROOPERS host

ERNW GmbH

Heidelberg based security consulting and assessment company.

- Independent
- We understand corporate
- Deep technical knowledge
- Structured (assessment) approach
- Business reasonable recommendations

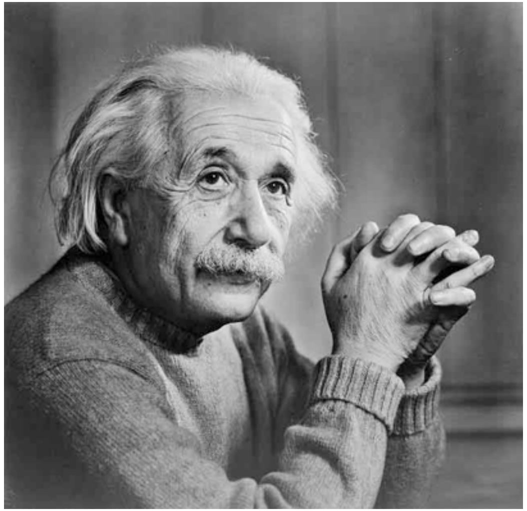
ERNW
providing security.

ERNW

Our Mission

- The evident part: help our customers perform their business.
  - And, of course, thereby enable our employees to feed their families ;-)
- Contribute to public security research & debate.
- → Make the world a better place.
  - Yes, I'm aware this might sound pathetic. Still, I'm fully serious here.

From Theory to Reality



- Some of you might remember the old L0pht slogan:
- *Making the theoretical practical*
  - *We carry on this heritage.*
  - This is quite important for our understanding of our research.
- It will play a role for these opening remarks, too ;-)

Talking about research

I‘d like to introduce two research projects we‘re involved with.

SPONSORED BY THE

Federal Ministry
of Education
and Research

ASMONIA

Attack analysis and **S**ecurity concepts for **MO**bile **N**etwork infrastructures, supported by collaborative **I**nformation exch**A**nge

www.asmonia.de

Trust Evidence

Bridging the Policy Gap in Trust Evidence

- How can enterprises today proof trust to regulators, external business partners, and: themselves?

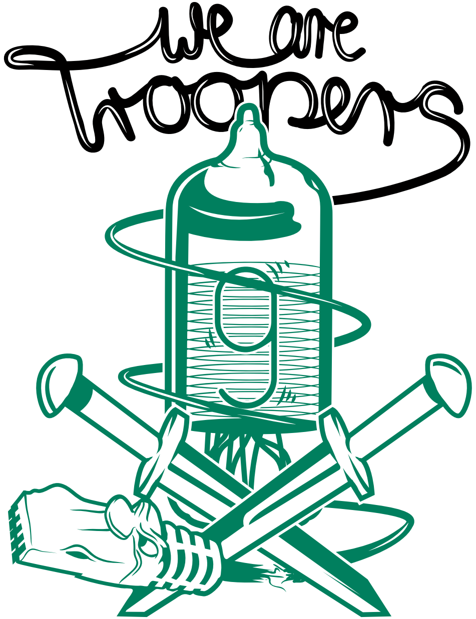
- Together with

Dartmouth
COMPUTER SCIENCE

Tuck School of Business
at Dartmouth

ERNW & TROOPERS

What’s the link?



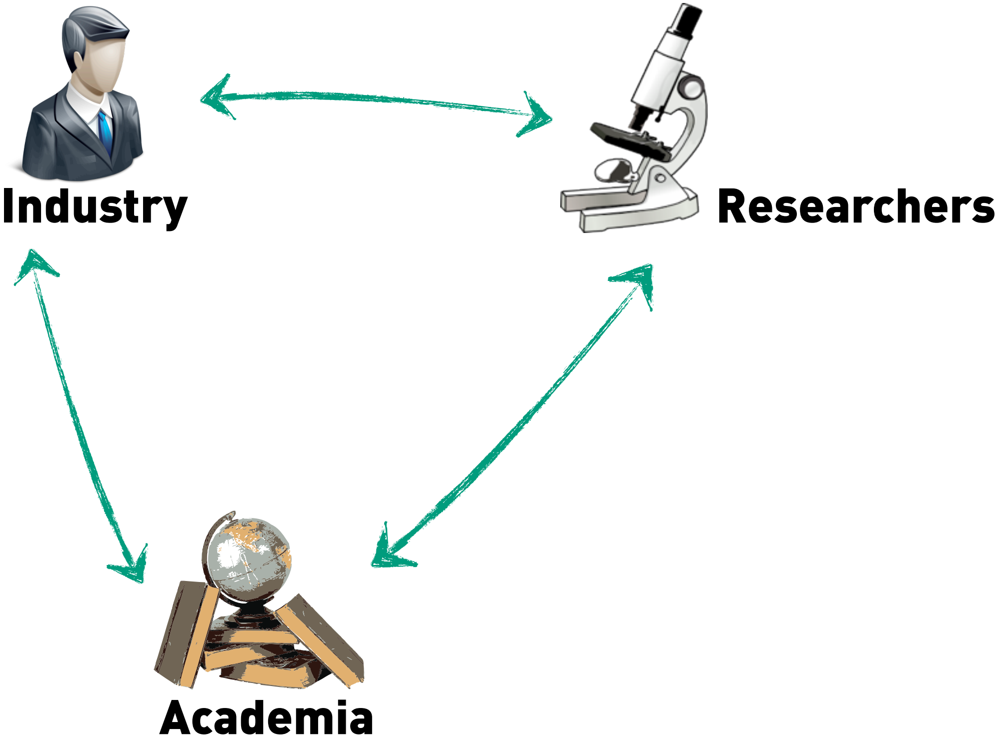
- TROOPERS is our (ERNW’s) contribution to the public security debate. And public sec knowledge.

The Mission

Why TROOPERS?

- Bring the right people together
  - Industry & Academia & Hacker/ Research Community
- Have them interact and learn

WE ARE TROOPERS



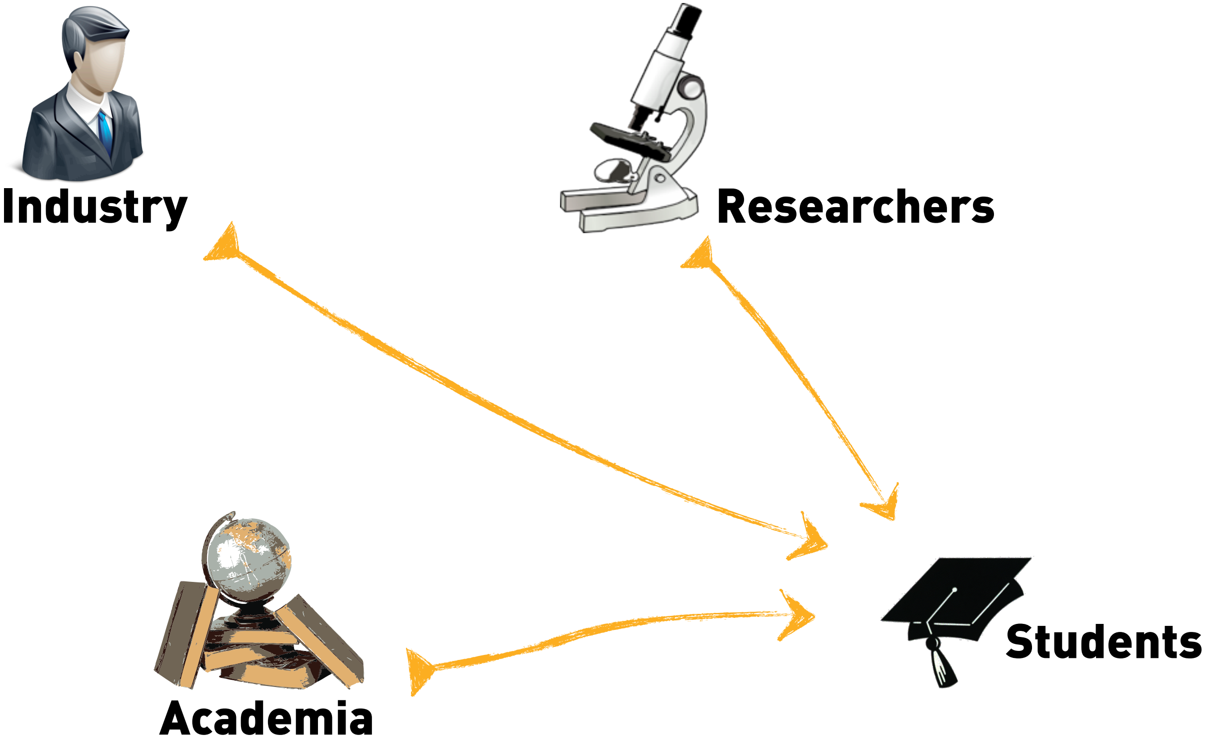
Industry

Researchers

Academia

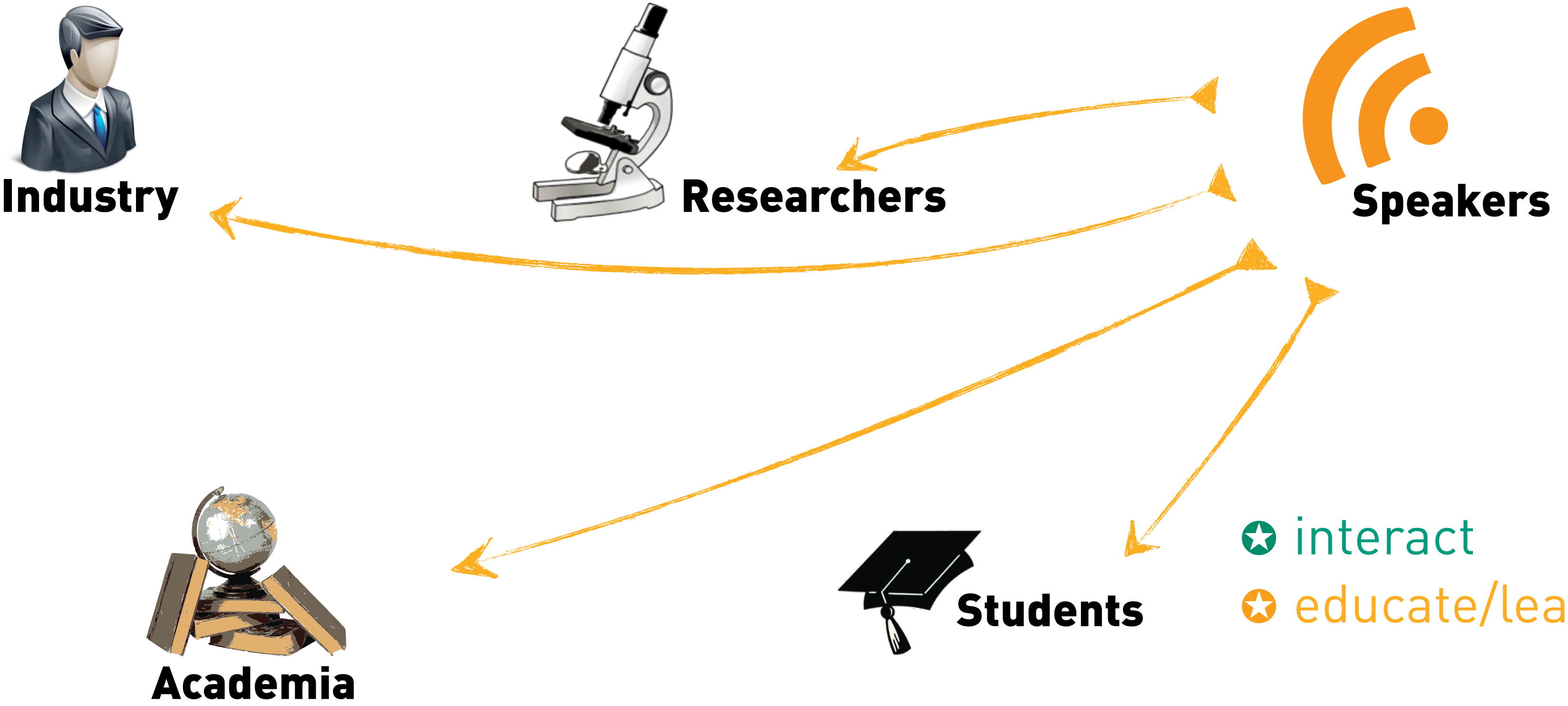
- interact

WE ARE TROOPERS



- ✪ interact
- ✪ educate/learn

WE ARE TROOPERS



Industry

Researchers

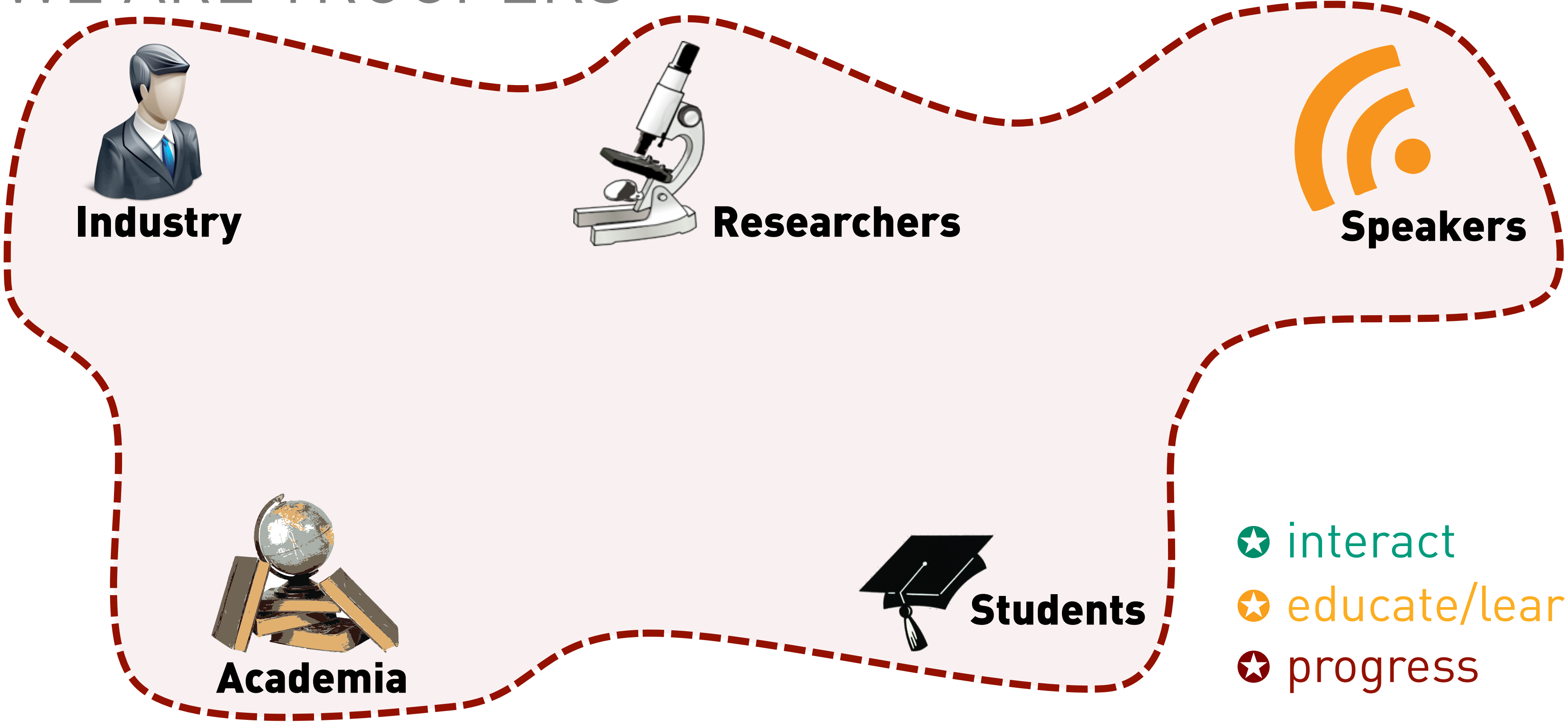
Speakers

Academia

Students

- ✪ interact
- ✪ educate/learn

WE ARE TROOPERS



Industry

Researchers

Speakers

Academia

Students

- interact
- educate/learn
- progress

TROOPERS – We get bigger every year

- This is based on the numbers
  - .. and, of course, on personal perception too ;-)
  - like the Christmas turkey that, in every year, is "the best we ever had".
  - and the Christmas tree that in every year is "the (biggest|most elegantly decorated|sth.) we ever had ;-)
- Why do I mention Christmas?
- Simple answer: Giving this keynote I feel like a kid on Christmas eve.
[Pls don't tell my wife ;-)]

WE ARE TROOPERS

60 %

Industry

10%

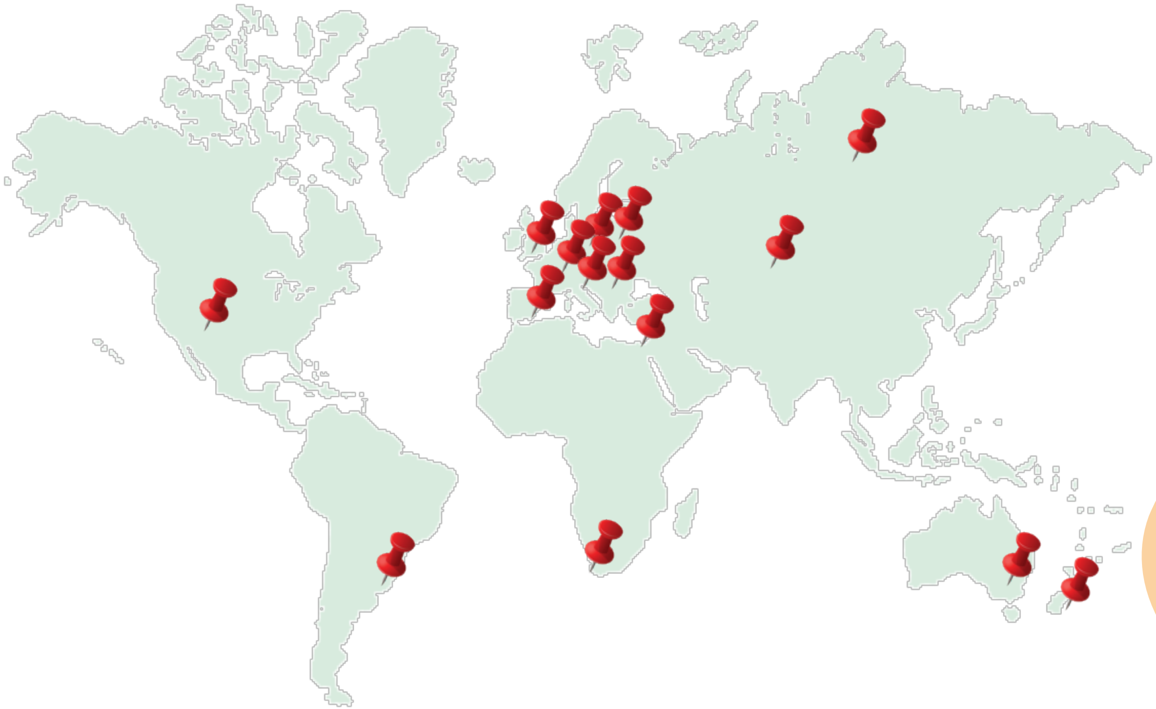
Researchers
from Hacker community

The formula

15 %

Academia

Students 15%



TROOPERS

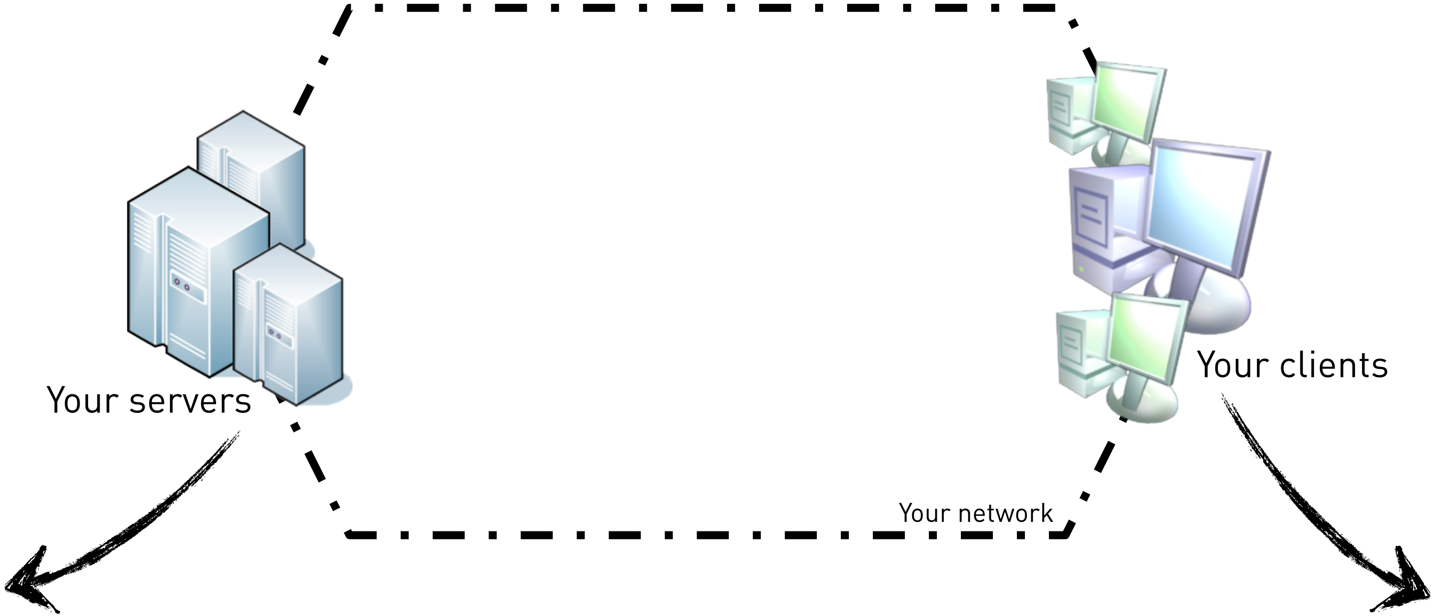
From 15 countries on six continents.

Why TROOPERS is important

- Infosec world ever evolving
- Currently heavy IT paradigm change
  - Ok, here's the buzzword you might have been waiting for: THE CLOUD
- Your area of responsibility is growing
  - Internet of Things
- Nature of threats changes

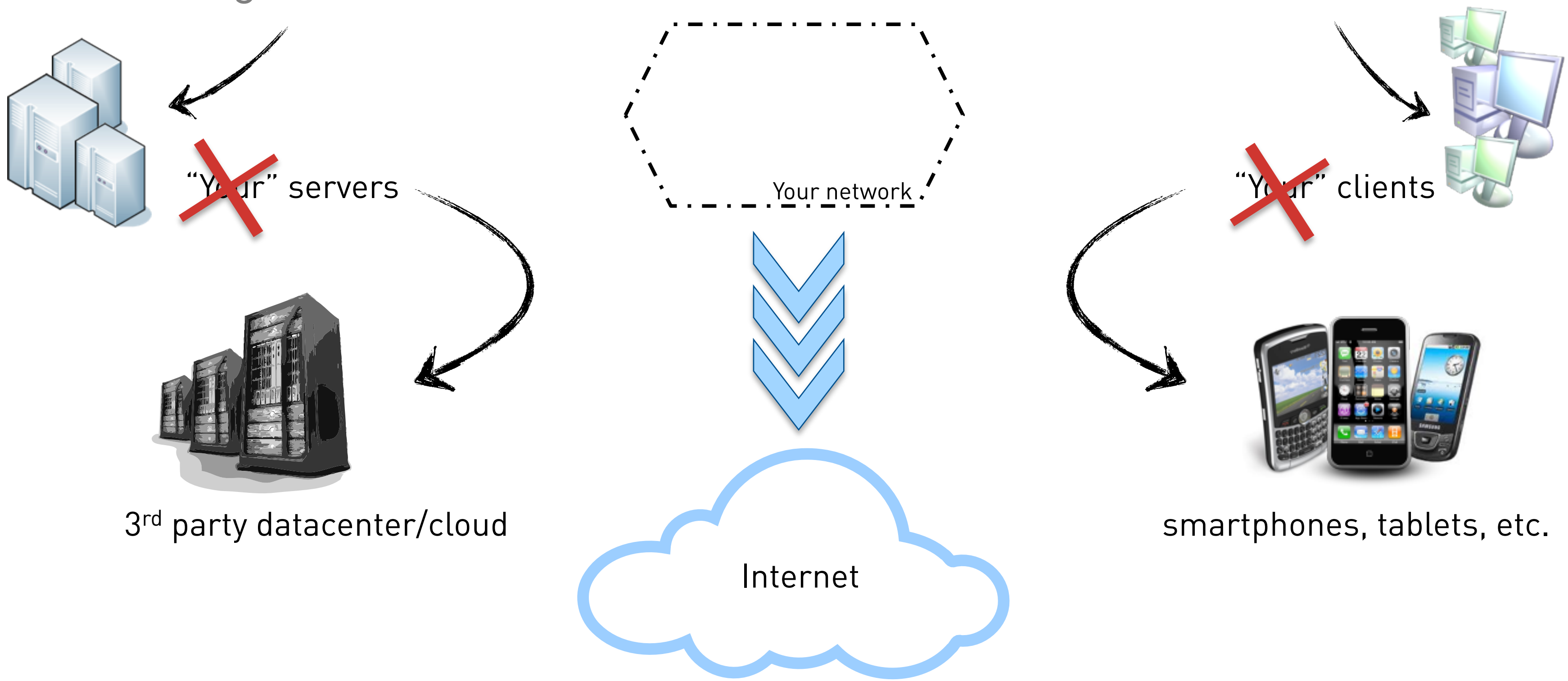
IT paradigm change

How networks looked in the past



How this will look in the future

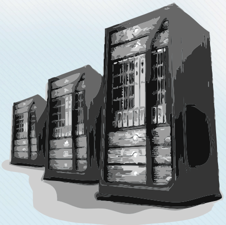
The emergence of mobile devices and the cloud



It's not only a technology change

… but affects fundamental security principles as well.

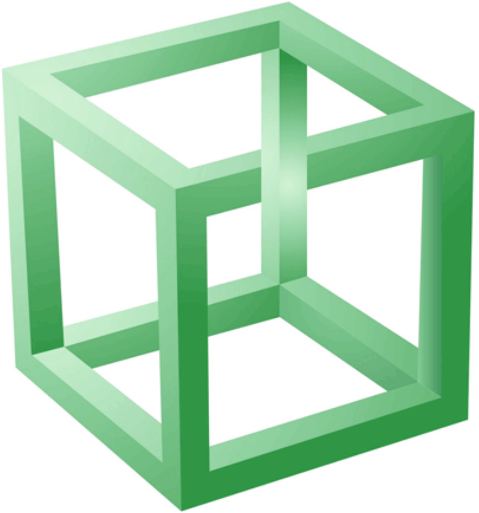
smartphones, tablets, etc.



3rd party datacenter

Here’s what I think

Main pillars of your current security architectures are vanishing



- Concept of locality
  - Physical location of data processing entities no more known.
  - And associated controls (e.g. physical access to datacenter) no more relevant.
- Concept of control of management
  - It’s not your systems anymore ;-)

Before it's getting boring…

Internet of Things

Control networks

smartphones, tablets, etc.

3rd party datacenter

RSA , X.509 Certificates etc.

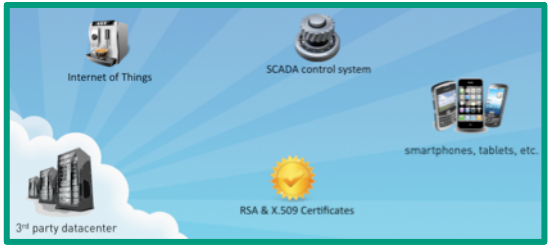
What does this mean?

- You will need another set to tools.
- *Trust management* instead of system management.
  - Yes, I'm talking about *Trust* here.
  - Not about *Control*.
    - When did you audit RSA for the last time? ;-)
  - [and not about *Faith* either]

- See also:
  - http://www.ernw.de/content/e7/e181/e1612/download1614/ERNW_LANline_VirtCloudSec_Keynote_ger.pdf

What does this mean? (2)

- Some parts of the above diagram might be “in an infant state”, security-wise.



- Remembering “good old basics” might be helpful.
  - Those exist for a reason.
  - It’s the base of everything you do.

To illustrate my point

Smartphones!

- „Another major problem is the fact that there are growing pressures to interlink separate but related computer systems into increasingly complex networks [...]
- Underlying most current users' problems is the fact that contemporary commercially available hardware and operating systems do not provide adequate support for computer security [...]
- Attempts to "patch" an off-the-shelf system for security tend to obscure penetration routes, but have little impact on underlying security problems. Existing systems have so many central privileged functions that the operating system becomes quite large and capable of concealing numerous flaws."

I still owe you the reference

Year of Starship Enterprise!

- James P. Anderson: *Computer Security Technology Planning Study*

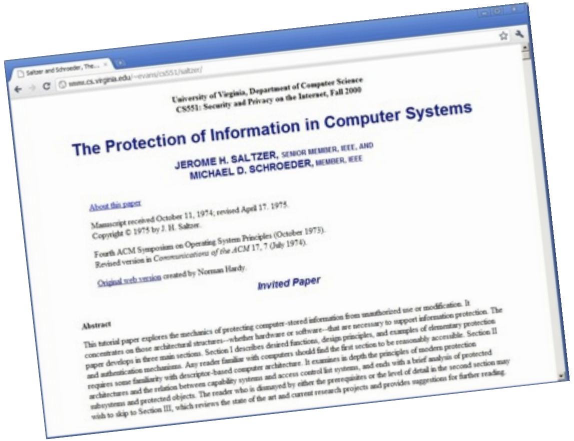
- 1972!

1972!

We're talking about the year of "PONG"

What do you mean with “good ole basics”?

Visibility



Saltzer and Schroeder, The...
www.cs.virginia.edu/~evans/cs551/saltzer/

University of Virginia, Department of Computer Science
CS551: Security and Privacy on the Internet, Fall 2000

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND
MICHAEL D. SCHROEDER, MEMBER, IEEE

About this paper

Manuscript received October 11, 1974; revised April 17, 1975.
Copyright © 1975 by J. H. Saltzer.

Fourth ACM Symposium on Operating System Principles (October 1973).
Revised version in *Communications of the ACM* 17, 7 (July 1974).

Original web version created by Norman Hardy.

Invited Paper

Abstract

This tutorial paper explores the mechanics of protecting computer-stored information from unauthorized use or modification. It concentrates on those architectural structures--whether hardware or software--that are necessary to support information protection. The paper develops in three main sections. Section I describes desired functions, design principles, and examples of elementary protection and authentication mechanisms. Any reader familiar with computers should find the first section to be reasonably accessible. Section II requires some familiarity with descriptor-based computer architecture. It examines in depth the principles of modern protection architectures and the relation between capability systems and access control list systems, and ends with a brief analysis of protected subsystems and protected objects. The reader who is dismayed by either the prerequisites or the level of detail in the second section may wish to skip to Section III, which reviews the state of the art and current research projects and provides suggestions for further reading.

Saltzer Schroeder

What do you mean with "good ole basics"?

Access Control

Isolation

Encryption

Secure Management

Visibility

ERNW Seven sisters

Hardening

Restriction

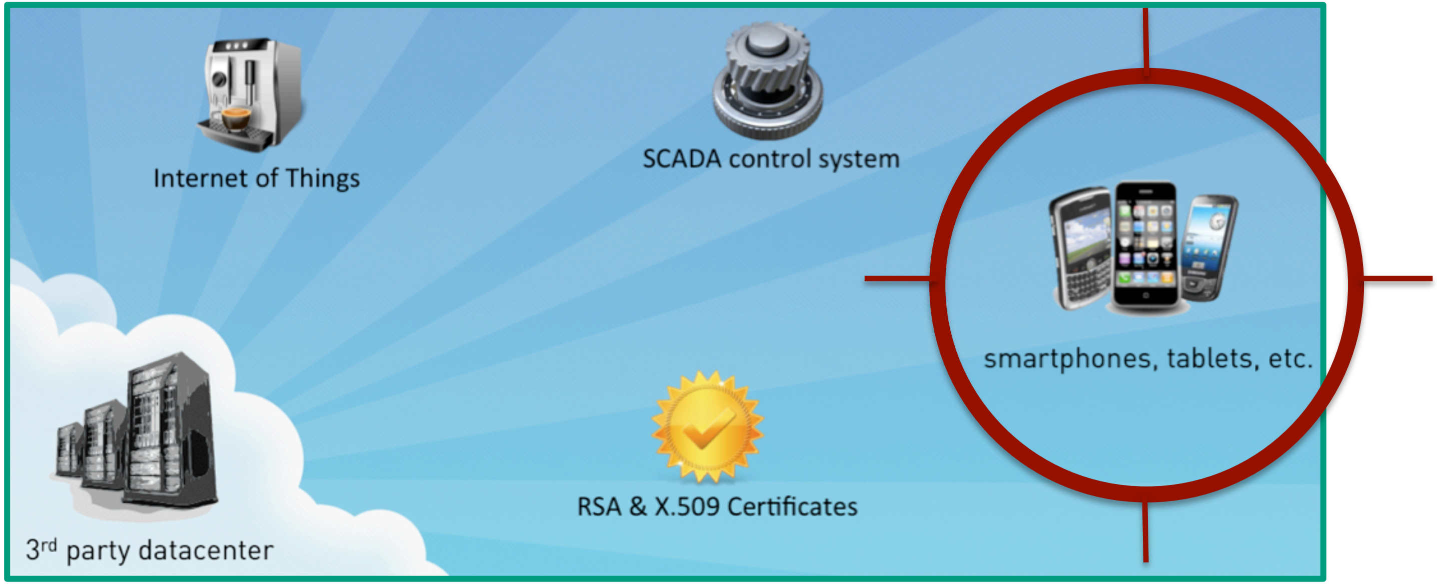
What do you mean with “good ole basics”?

This stuff has been written/
formulated for a reason.
Keep this in mind!

Ok, let's get back on track

The crucial question is

- Can this be secured?



Here‘s what I think

Just one simple rule:

- Pls pls pls do not process sensitive data on smartphones!

Well, not only the IT world changes

And with it the infosec part

- Tempora mutantur, nos et mutamur in illis.

Nature of threats changes as well

RSA SECURITY™

COMODO
Creating Trust Online®

- If there's a main information security lesson to learn from 2010 (and early 2011, for that matter) it's this one.
- Still let's have a closer look at some of the attacks that happened.

Getting into 2010

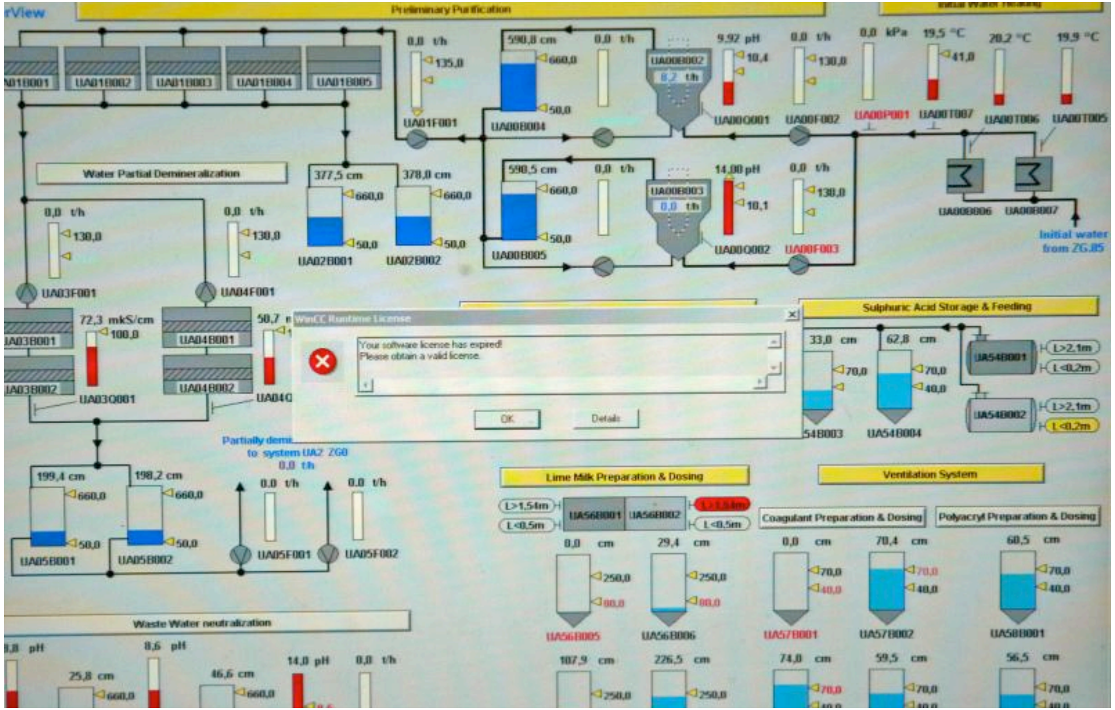
Operation Aurora

- Targeted attacks against a number of US high tech, security and defense contractor companies.
  - Presumably going after source code repositories.
- In the interim it is assumed that a very large number of organizations was affected.
  - See Mudge's keynote at ShmooCon 2011
- If this wasn't a game changer...

... certainly this one was

No keynote @SOME_2011_SEC_CON without a mention of...

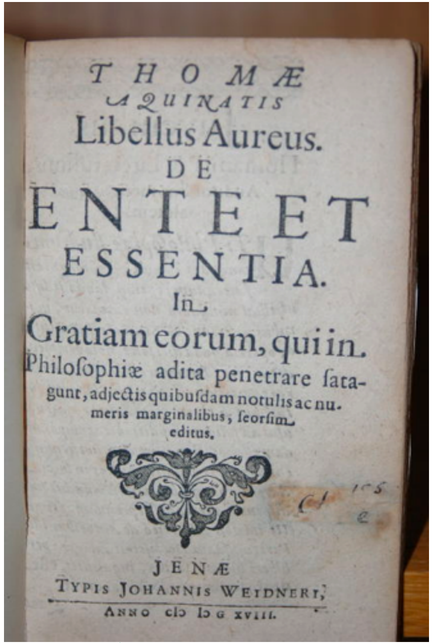
Stuxnet


rView
Preliminary Purification
Initial Water Heating
Water Partial Demineralization
Sulphuric Acid Storage & Feeding
WinCC Runtime License
OK
Details
Partially demi...
to system UA2 ZG0
Lime Milk Preparation & Dosing
Ventilation System
Coagulant Preparation & Dosing
Polyacryl Preparation & Dosing
Waste Water neutralization
Initial water from ZG.85

Your software license has expired!
Please obtain a valid license.

Stuxnet

What was so special about it?



THOMÆ
AQUINATIS
Libellus Aureus.
DE
ENTE ET
ESSENTIA.
In
Gratiam eorum, qui in
Philoſophiæ adita penetrare ſatagunt, adjectis quibuſdam notulis ac numeris marginalibus, ſeorſim
editus.

JENÆ
Typis JOHANNIS WEIDNERI,
ANNO cIↃ IↃ c XVIII.

- Stuxnet was a targeted attack
  - Well, occasionally I hear rumors that such things happen.
- Stuxnet included four 0-days
  - Ok, seemingly some party was willing to invest those, for some reason. What's the point?
- Probably, Stuxnet was not developed by some bunch of hackers.
  - Yes, there might be powerful organizations out there.
  - Maybe they are even going after you.
  - → If you think you could be a target for them, you might reconsider your controls…
- It's mere existence!
  - From theory to reality!

Some additional reflections on Stuxnet

I just can't refrain from this one ;-)

- Initial infection vector assumed to have been USB device.
  - Why would you allow ("unmanaged") USB devices in a control system network anyway?
  - Or, for that matter, in your organization's "office network"?

- Main network propagation methods include network shares on target machines or exploitation of MS08-067 ("Conficker").
  - Sorry guys, if you think some control systems should be protected, those pesky *Security Best Practices* from "the office world" might be worth a look.
- Stuxnet includes some rootkit functionality by installing a driver manipulating filesystem queries.
  - How many drivers do you install on your average control system after putting it into production?
- My theory is that quite some Stuxnet infections could have been prevented by $FOLLOWING_SOME_SIMPLE_OLD_SECURITY_RULES.

Following the line of history into 2011

It wasn‘t only attacks...

- But humanity‘s dreams and mother nature took their toll, too.
- Egypt uprise
  - Paradigm of ever rerouted Internet shattered?
- JP Earthquake

We think of the victims.

Japan Earthquake

- From the infosec perspective, there's two things we might learn here:
- In a globalized world events like this not only affect availability.
  - Cisco deferred patch day.
- There might be limits for the reasonable use of risk assessment...

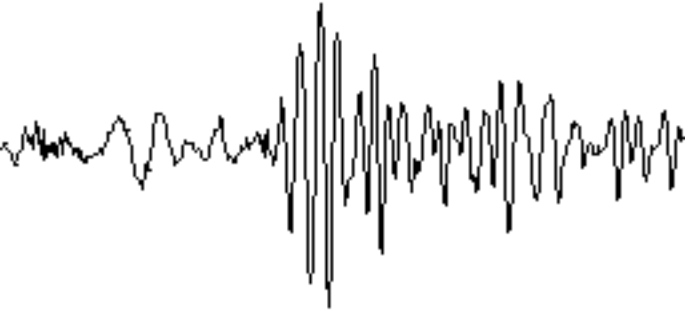
There‘s limits for the reasonable use of risk assessment

My political statement of the day

- Even though we at ERNW strongly believe in risk assessment tools as a daily practice of infosec professionals.
- They only work within some limits, of “normal values”.
- There’re events outside these limits
  - Draw your own conclusions…
  - in the interest of our kids…

Back to the infosec world

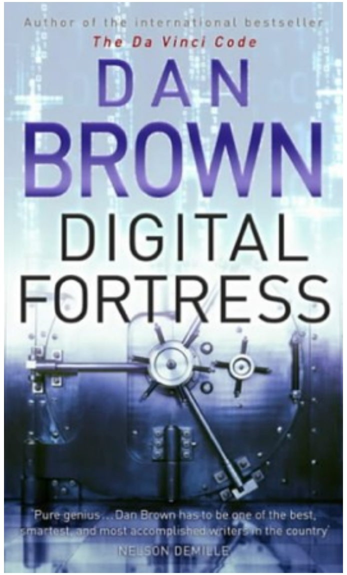
Just recently, it had it's own eruptions



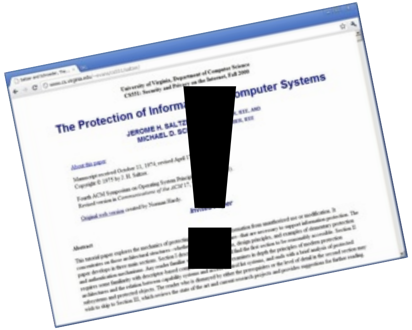
- RSA Breakin
- Comodo Compromise

RSA breakin

Many people in this room have heard of this... and are potentially affected...


Author of the international bestseller
The Da Vinci Code
DAN BROWN
DIGITAL FORTRESS
'Pure genius... Dan Brown has to be one of the best, smartest, and most accomplished writers in the country'
NELSON DEMILLE

- Some speculation comes to mind:
  - Why did they keep customers' seed files?
  - There's an official version...
    - and an inofficial one
  - Wasn't there an air gap protecting the seed files?


University of Virginia, Department of Computer Science
CS551: Security and Privacy on the Internet, Fall 2000

The Protection of Inform omputer Systems

JEROME H. SALTZ
MICHAEL D. SC

About this paper

Abstract

Comodo

“Privately held group of companies offering computer software and SSL certificate products.”

- Presumably registration agent "somewhere in South Europe” compromised.
- Fraudulent issuing of SSL certificates for main websites (mail.yahoo.com).
- Comodo spreads rumors that Iran is behind attacks (uhuh APT™ is around…).

O RLY?

Now, ask yourselves

If you were an attacker capable of compromising RSA or Comodo, what would you go after next?

- Yes, correct: "The cloud"

It's certainly not my intent to spread FUD.

But I'd like you to take away some messages from this talk.

- The "theoretical" might happen.
  - Sooner than you think.
  - → Be prepared!
    - Have the right tools (Risk Assessment ;-)
- Figure out who to trust.
  - And why.
  - Again, you may need some methodology.
- Basic security rules are there for a reason.
  - It's *your* duty to wave their flag!

We understand this might leave you feeling like Alice in Wonderland

When she meets the Red Queen.

'A slow sort of country!' said the Queen. 'Now, HERE, you see, it takes all the running YOU can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!'

Still, there's hope.

We might face the challenge together.

We are TROOPERS

TROOPERS: Maximize your personal development.