Cyber Security Services at TÜV Süd

(or why I left CERN&Physics to do something completely different)

Mehr Wert.
Mehr Vertrauen.

Add value.
Inspire trust.

Andreas Alexander Maier

At least 60 G€ damage in 2017

How many passwords do you have?

Service	Password of 99% of population	Effort with regular PC and GPU
[Service you signed up for as a child]	DadIsAnnoying1999	1ms – 1 day
Yahoo	DadIsAnnoying2004	%
Google Single Sign on	!D4d1s4nnoying13!	%
CERN	!D4d1s4nnoying13!CERN	%
Facebook	AnnoyingDadFB	%
Dropbox	!D4d1s4nnoying16!Drop	%

Attacks: Dictionary Attack (ms), Brute Force (days)

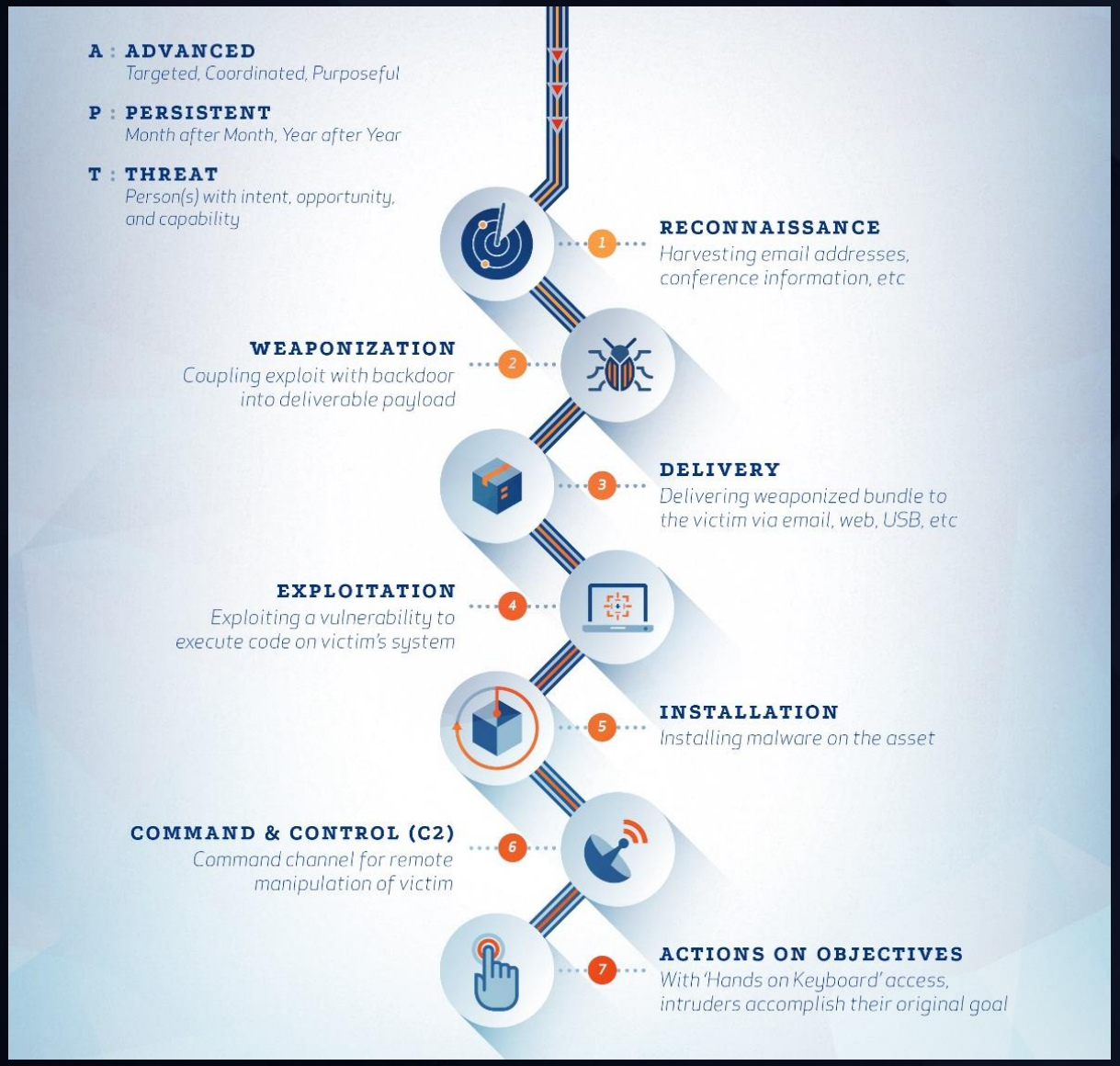
Have you been pwned? https://haveibeenpwned.com/

Hope you have many!

Service	Password of 99% of population	Effort with regular PC and GPU
[Service you signed up for as a child]	DadIsAnnoying1999	0 ms (pwned, but irrelevant)
Yahoo	DadIsAnnoying2004	< 1 ms (changing numbers doesn't help)
Google Single Sign on	!D4d1s4nnoying13!	< 1 ms (l33t speak doesn't help)
CERN	!D4d1s4nnoying13!CERN	< 1 ms (adding stuff doesn't help)
Facebook	AnnoyingDadFB	< 1 ms (removing stuff surely doesn't help)
Dropbox	!D4d1s4nnoying16!Drop	< 1 ms (see above)

- Protection:
  - One long random password per service, never reuse or alter! (e.g. I^j9AN_-#njaH6%AhD.<)
  - Single sign on (let somebody else take care of the problem)
  - Two (or three!) factor authentication (fingerprint, face, SMS, compagnon app)
  - Pass phrase with unrelated words (e.g. CorrectHorseBatteryStaple)

Cyber Kill Chain



- 7 Steps to describe a cyber attack
- Break it once and you are save
- Defender vs. Analyst vs. Attacker
  - Defender wants to break the chain
  - Defensive analyst wants to understand the chain and targets and prefered tactics of an attacking group
  - Attacker wants to stay secret

My time at MPP and CERN

"There's so much interesting to learn!"

"There's so much to do and understand and so little time!"

"I want to do A, B, C but I first have to finish other stuff"

2011-2012: ATLAS
Diploma student at MPI in Richard Nisius' group

- **Data analysis**
  - Top quark mass measurement

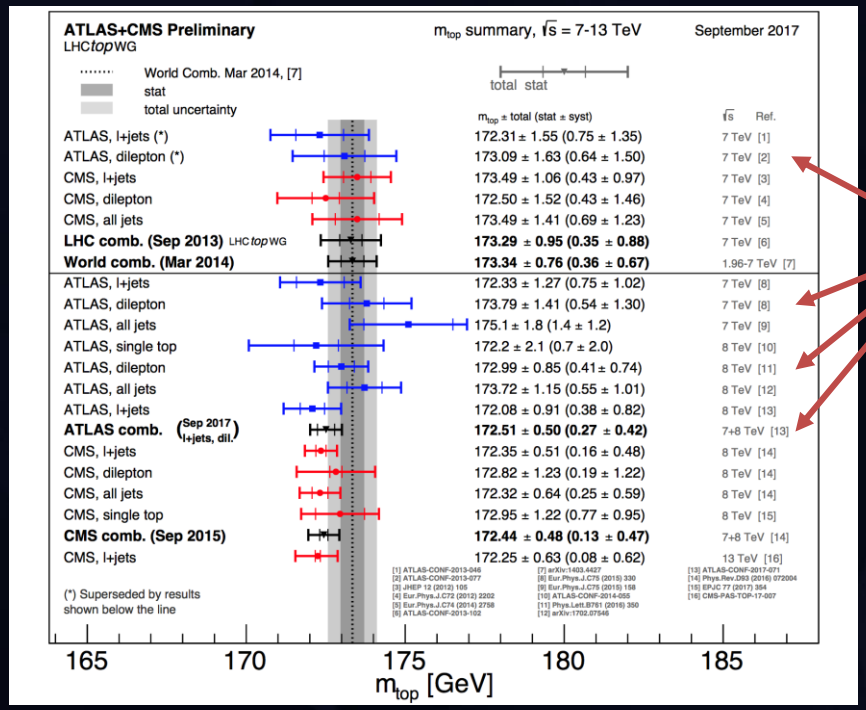
2012-2016: ATLAS
PhD at MPI and CERN in same group, quali task at CERN

- **Data analysis**
  - Top quark mass measurements
- **Phenomenology study**
  - Effects of full NLO calculation on ttbar observables
- **Detector construction**
  - IBL construction and pixel detector refurbishment

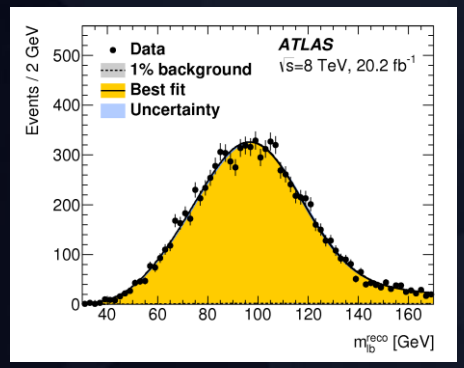
2016 – 2018: CLIC / CMS
Postdoctoral fellow at CERN

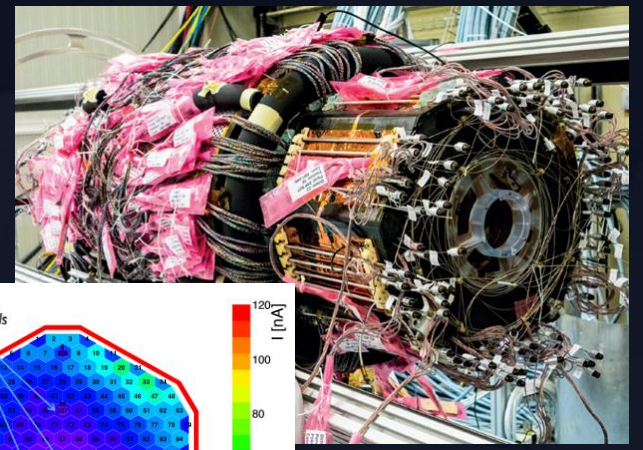
- **Data analysis**
  - Triple gauge boson coupling, particle flow validation
- **Phenomenology study**
  - Parton shower effects on ttbar observables
- **Detector construction**
  - Sensor testing for the CMS HGCAL project

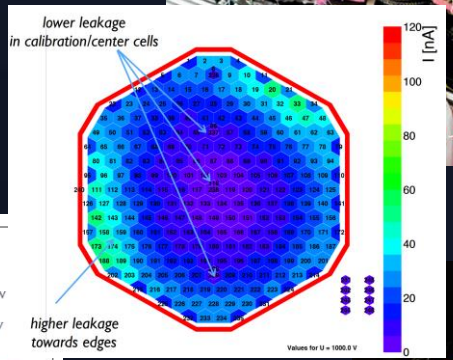
A collection of memories

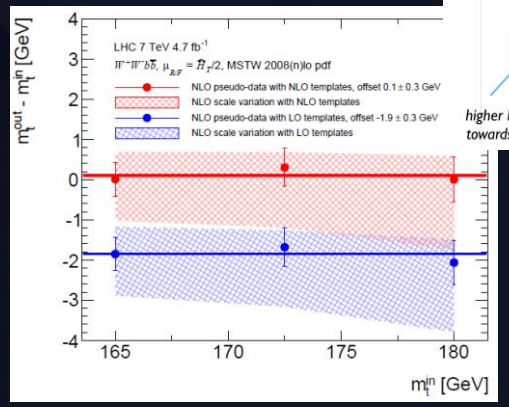


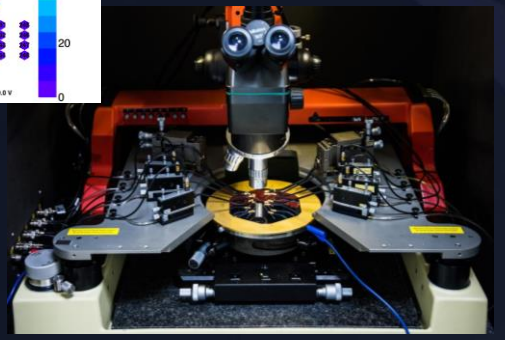
my contributions









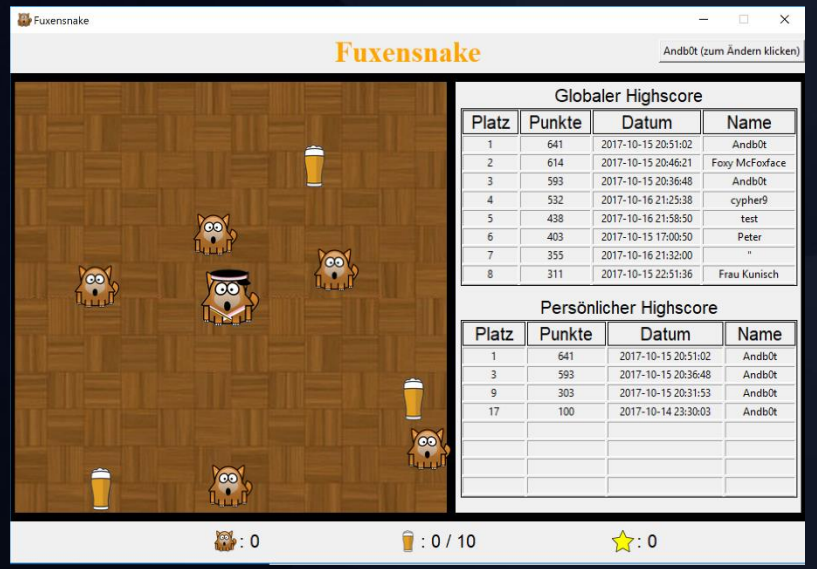


What's out there?

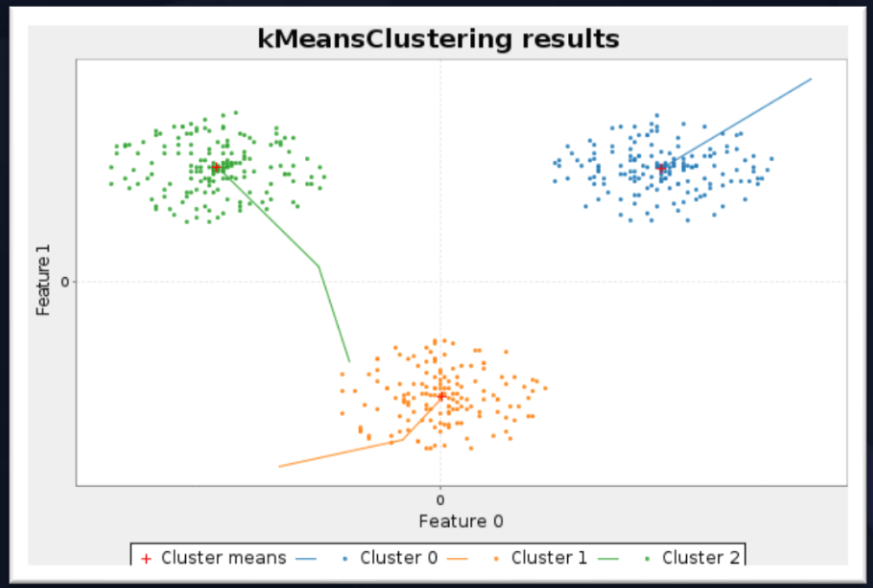
- What I love(d)
  - Trust
  - Responsibility
  - Impact
  - Learning
  - Solving puzzles
  - Physics
    i. Phenomenology
    ii. Statistics
    iii. Machine learning

- What I was good at
  - ATLAS data science in C++

So I started to write code…



A game (python)…fun but quite plain



A machine learning library (scala)…fun and challenging!

Possible jobs for me

- Data science
  - Various fields, e.g. automotive, energy
  - Machine learning
  - PhD position in Informatics
- Analytics
  - High frequency trading
  - Portfolio optimization for banks
- Software development
  - Join a startup, e.g. crypto currency
  - Study computer science
- Consulting
  - Tech consulting, e.g. Accenture
  - Management consulting, e.g. the big two and a hole lot of others

Cyber ~~Kill~~ Defense Chain

- Example scenario:
  Customer “MPP Kantine” wants to ensure they’re safe

- Steps for Reconnaissance
  - Find out about their infrastructure (how many servers, webservices, etc)
  - Test infrastructure (remotely)
  - Correlate with other sources ((dark) web for info, known exploits)

Cyber ~~Kill~~ Defense Chain

System design!
Software Dev.!
Data Science!

- Example scenario:
  Customer “MPP Kantine” wants to ensure they’re safe

- Steps for Reconnaissance
  - Find out about their infrastructure (how many servers, webservices, etc)
  - Test infrastructure (remotely)
  - Correlate with other sources ((dark) web for info, known exploits)

Cyber ~~Kill~~ Defense Chain

- Steps for action:
  - Give intermediate report to penetration testers (“hackers”) for attack
    i. Remotely
    ii. Social engineering
    iii. Red teaming
  - Automatize attacks as far as possible to let “pentesters” concentrate on the hard problems

Cyber ~~Kill~~ Defense Chain

Software Dev.!
Machine learning!

- Steps for action:
  - Give intermediate report to penetration testers (“hackers”) for attack
    i. Remotely
    ii. Social engineering
    iii. Red teaming
  - Automatize attacks as far as possible to let “pentesters” concentrate on the hard problems

Cyber ~~Kill~~ Defense Chain

- Steps for delivery to customer
  - Compile all information for a report, including e.g.
    i. Customer industry (consumer goods, maybe there's other hacks in the past?)
    ii. Countries of exposure (maybe steaks from business partner in Austria?)
  - Compose vulnerability report and strategy for mitigation

Cyber ~~Kill~~ Defense Chain

Machine learning!

Analysis!

Web development!

- Steps for delivery to customer
  - Compile all information for a report, including e.g.
    i. Customer industry (consumer goods, maybe there's other hacks in the past?)
    ii. Countries of exposure (maybe steaks from business partner in Austria?)
  - Compose vulnerability report and strategy for mitigation

Cyber Security Lifecycle

Information Gathering
- Collect and understand requirements
- Assessment Framework Design
- Customer specific Profiles

Analytics & Correlation
- Automated analysis of gathered information
- Correlation and synch up check with other data (e.g. CVSS)
- Enrichment with relevant Add-On Information

Enhanced Info-based Assessment (ACV)
- Execution of defined Assessment based on valuable and relevant information
- Assessments under realistic conditions

Advisory
- Definition of actionable insights
- Support for implementation of countermeasures
- 3rd party solution evaluation

Contact info

- If you want to know more about data science, software development, or cyber security:
  - Good: andreas.maier@tuev-sued.de
  - Better: talk to me! Now!
  - Best: come visit us!

- More about TÜV Süd Cyber Security Services:
  - https://www.tuev-sued.de/fokus-themen/it-security/cyber-security-check

- More about me:
  - Stalk me: https://www.linkedin.com/in/andreas-alexander-maier-769a78b9/
  - Write code with me: https://github.com/andb0t

Thank you for your attention!