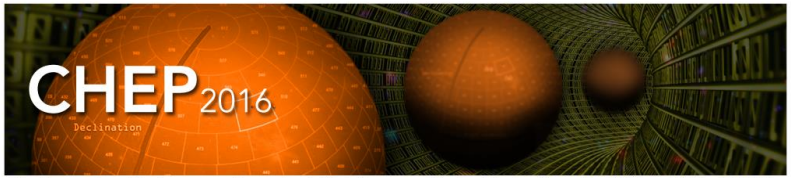
CERN | Computer Security
Sécurité informatique



22nd International Conference on Computing in High Energy and Nuclear Physics, Hosted by SLAC and LBNL, Fall 2016

Internal security consulting, reviews and penetration testing at CERN

Sebastian Lopienski

CERN Deputy Computer Security Officer

CHEP 2016, San Francisco

What do security teams usually do?

Incident Response	Intrusion Detection	Vulnerability Management
Education, Training, Awareness Raising	Firewall, Network Security	Etc. etc.

Obviously, we do all that at CERN, too

But we need to do more

Too often it's too late:

- *"My site runs on WordPress, because I didn't know CERN uses Drupal"*
- *"The system is in production now, so we cannot change its architecture or technology choices"*

Too often people have good(?) excuses:

- *"I inherited this code, but have no idea how it works"*
- *"This was deployed back in 2003 and no one looked into it since"*
- *"I followed a software security course, but it was many years ago"*
- *"I didn't think that such an attacks was possible"*

“We are there to help you”

Security consulting

We provide input and expertise for CERN software and services

- Thread modeling and risk assessment
- Secure system architecture and design
- Security measures

E.g.

- software projects and systems (from all CERN departments and experiments)
- computing infrastructure (e.g. COMPASS experiment, GIS services)
- services provided by the IT department (e.g. Drupal, git)
- procedures and tools (e.g. user pre-registration, payment workflows, transmitting root passwords to sysadmins, radio-protection data privacy)

Security consulting

- Technical expertise for procurement of external software/services
  - often SaaS
  - technical specifications for tender calls
  - requirements for contracts

E.g.

- service management ticket handling system (for IT)
- applicant tracking system (for HR)
- payment systems (for finance dept.)

Security evaluations

(for systems already implemented)

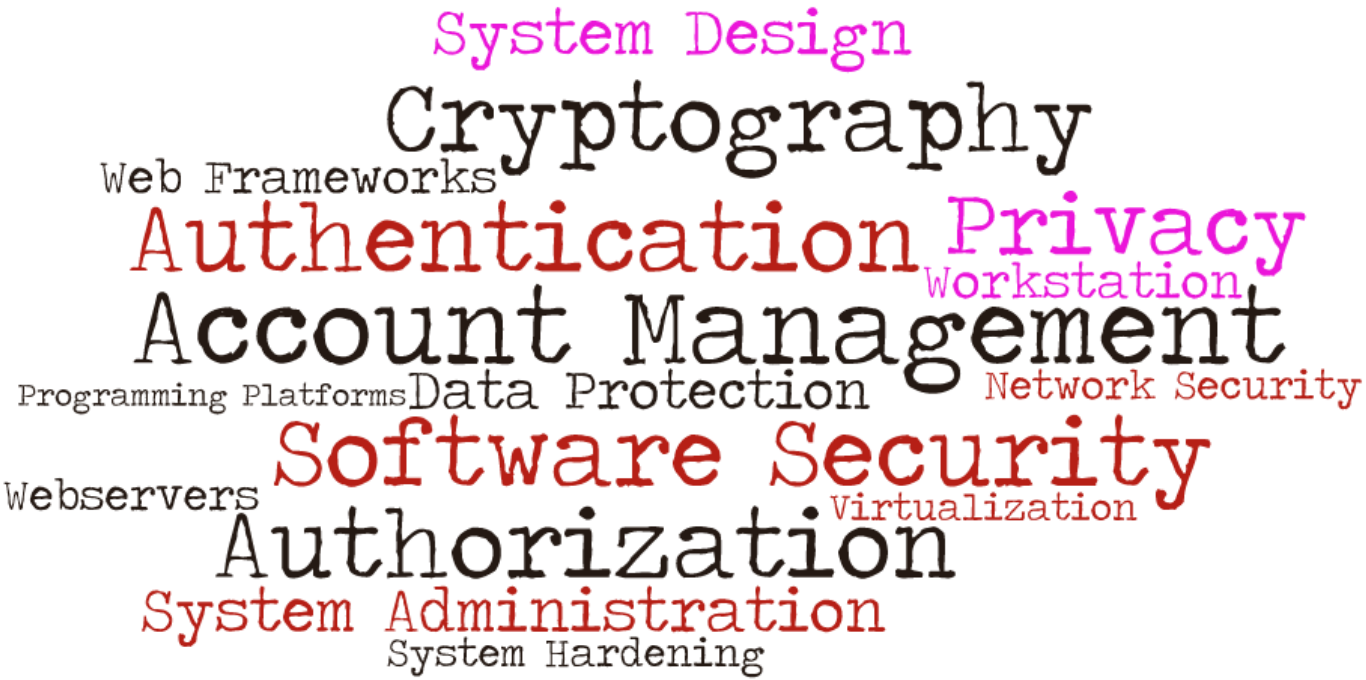
- Penetration testing
  - mostly web apps - but also other systems, sometimes unexpected (e.g. point of sale, dosimeter reader station etc.)
  - both in-house developed
    - (too many examples to list here)
  - … and external developed (for CERN or not), e.g.
    - CERN alumni web app
    - CERNjobs mobile app
    - Questions2answers *(stackoverflow alike)*
    - PyBossa *(crowd-sourcing/microtasking)*

Security evaluations

(for systems already implemented)

- Code reviews
  - for particularly sensitive systems or modules (e.g. authentication, credentials handling, privileged access)
  - E.g.
    - Volunteer Computing Credential Service
    - Kerberos unification
    - secrets handling in puppet infrastructure
    - handling (financial) donations

Often touching many technical domains



Considerations, lessons learned

- Push or pull model?
  - Who makes the first contact? How much should we reach out?
- Suggest or require?
  - i.e. how actively should we push for security
- How to explain and convince?
  - sometimes, we have to exploit in order to demonstrate a vulnerability
- Slow start, but a busy activity after a couple of years
  - ~10 bigger + dozens of minor requests per year
  - CERN people more security aware? More willing to contact us?
  - Still, we learn about many projects too late

Offspring and related initiatives

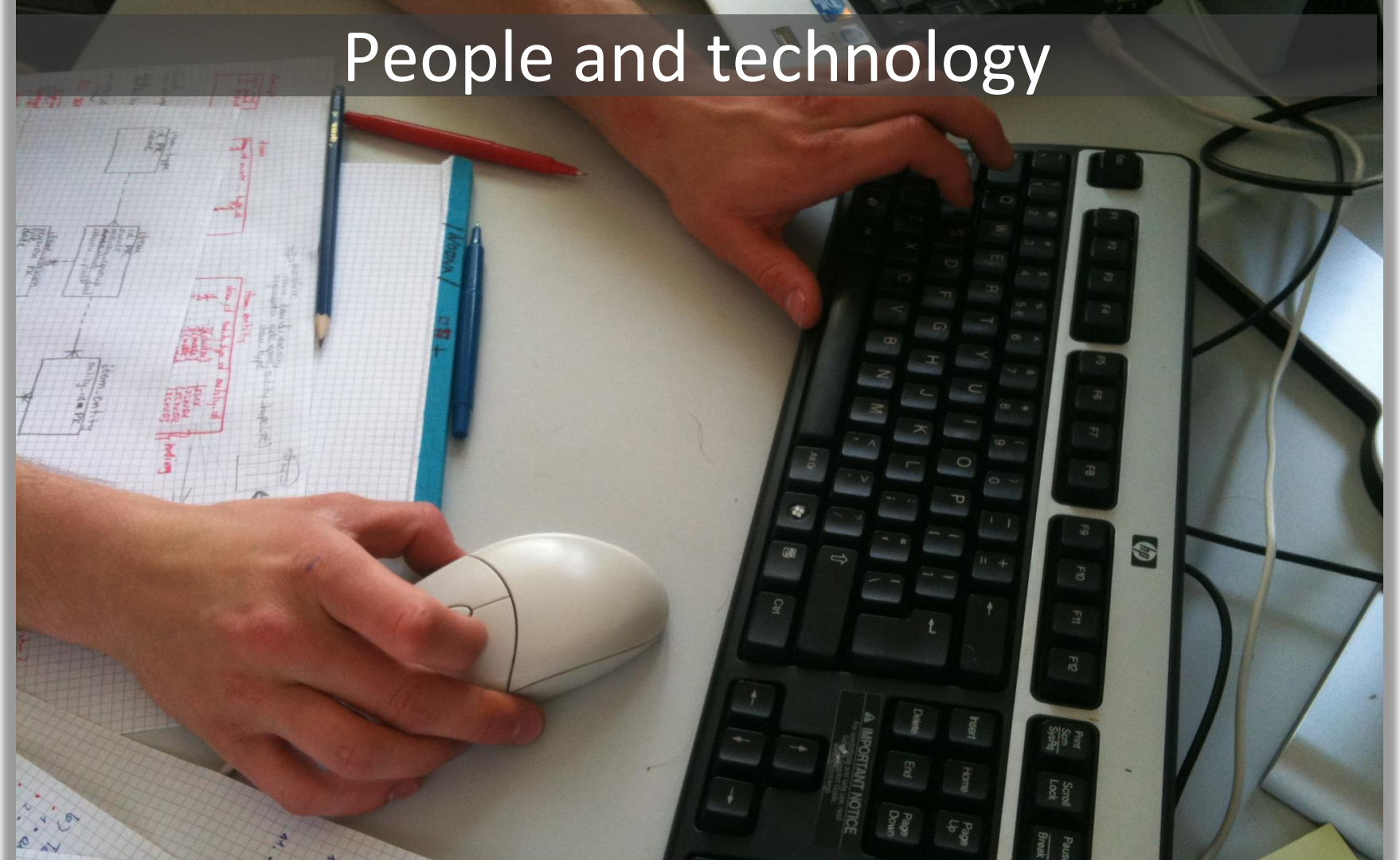
(IT department, last 2 years)

- WhiteHat challenge (for CERN people and external universities)
  - providing training on web security and penetration testing
  - inviting non-security people to learn and do pentesting
  - https://cds.cern.ch/journal/CERNBulletin/2014/45/News%20Articles/1958281
- CERN Software Developers Forum
  - building a community, providing starting information for newcomers
  - https://cds.cern.ch/journal/CERNBulletin/2015/32/News%20Articles/2038500
- IT Consulting Service
  - advising CERN community, directing to existing services & solutions
  - https://cds.cern.ch/journal/CERNBulletin/2016/24/News%20Articles/2159641

Conclusions *(perhaps obvious?)*

- Working *together* is very beneficial, and appreciated
  - security people + service managers/developers/physicists
- Cases often touch more than security
  - e.g. *"Auto-commit to git from a website on the technical network"*
- Back covering exercises? Sometimes.
  - *"Security team accepted it, so now they are responsible"*
  - …but that's OK with us!
- Advertising our activity is not easy
  - especially in a heterogeneous environment as CERN
  - how to reach everyone? especially the newcomers?

People and technology



Thank you

PS: Do other labs have such activities existing? formalized?


CERN