Verifiability and Authenticity of Data and Beyond

H. C. Pöhls, University of Passau - PRISMACLOUD

Networking Session:

"Key challenges in end-to-end privacy/security in untrusted environments".

Cluster: Security and Trust. *ICT 2015* - Innovate, Connect, Transform

October 22nd 2015. Lisbon, Portugal

With the support of:

Wide-Impact cyber SEcurity Risk framework

Challenge

Many useful (novel) cryptographic techniques exist !

Why are they currently not used at all to protect users ?

Challenge

prisma cloud

little enforceable security for cloud users

- how to keep confidentiality of data ?
- verify integrity of data at rest & after computations ?
- how to verify properties of the cloud‘s structure ?

missing enforceable privacy protection for users

- can we protect the privacy of users when interacting with cloud services ?

existing cryptographic approaches not used

- why is there no library, no tools, no crypto-as-a-service ?

“Key challenges in end-to-end privacy/security in untrusted environments”
ICT 2015 - Innovate, Connect, Transform. October 22nd 2015.

Expected Results

cryptographic techniques

understand

innovate

implement

optimize

‘servicify’

guide

cryptographically secured cloud services

Expected Results

cryptographic confidentiality for data at rest

verifiability of data (at rest & after computation)

verifiable structure & properties of cloud topologies

cryptographically strong privacy protection

provide '*enablers*' for fast adoption:

implementations & methods, guidelines

Ideas for the future

prisma cloud

- **extend PRISMACLOUD use cases**
  - e-health, SmartCity, e-Government
- **continue working at an interdisciplinary level**
  - Security & Cryptography Researchers
  - Developers & Software Architects
  - Users
  - Lawyers
  - Policy Makers
  - Privacy Advocates
- **standardizing and certification of secure and privacy friendly cloud service**
- **cryptographic software engineering**
- **raising more awareness on EU level**

Thank you for you attention!

Further information:

- Henrich C. Pöhls, UNIVERSITY OF PASSAU
- hp@sec.uni-passau.de
- https://prismacloud.eu