Update for TF-Storage

TF-Storage meeting @Uppsala, September 22nd, 2014
National Data Storage 2

Short reminder what is this about:
The cloud is secure enough to use, said panelists at the annual RSA Conference in San Francisco on Wednesday. From left to right: Bruce Schneier, independent security analyst; Eran Feigenbaum of Google; Wade Baker of Verizon; and Bret Arsenault of Microsoft.
Is AuthZ+AuthN enough?
We need cryptography!

- AES-256
- SHA-512
- RSA-4096
- AES-256
- SHA-512
Cryptography is NDS2

RSA-4096 MASTER KEY PAIR

AES-256 PER-FILE

AES-256 PER-FILE

AES-256 PER-FILE

AES-256 PER-FILE
Cryptography is NDS2

- Decrypt (open the secret case)
- Encrypt (lock the secret case)

User's public
User's private
Directory's public
Directory's private
File's symmetric
ABC
Unencrypted file

- Decrypt (open the secret case)
- Encrypt (lock the secret case)

User's public
User's private
Group's public
Group's private
Directory's public
Directory's private
File's symmetric
ABC
Unencrypted file
Cryptography?
SECURE DATA SYNCHRONISATION & STORAGE & ACCESS TOOLS ECOSYSTEM

- Security
- Ease of Use
- Availability

- Data Sync!
- Drive
- GUI
- Web interface

- Notebook
- PC
- Mobile

EFFICIENCY  LOW OVERHEADS  OPENNESS
Virtual disk for Windows – bulk transfers
Data sync & virtual disk together

User’s home
- Archives
- HPC input data

Sync
- Docs
- Spreadsheets
- Pictures

HPC outputs

User's home

HPC input data

Sync

HPC outputs
National Data Storage 2

Status:
- In the beta phase
- **Clients available for download:**
  + nds.psnc.pl/download
- Code to be open soon (being moved to github)
- Continuous integration etc. on the way
- Presented and demo-ed at TNC2014
- Users:
  + Internal users mainly
  + Some external users:
    - clinical hospital, some universities
  + Rollout planned, but still sth to do

- **Why won’t you use it?** - Testers welcome!!!
Latest developments (1):

- LCFS – Loopback/Local Crypto File System:
  + stores encrypted data in the local filesystem
  + enables usage of encryption on top of ANY local or networked storage
  + Windows version available
  + Linux version on the way

+ works with:
  - FAT/NTFS
  - samba / CIFS
  - NFS
  - Dropbox! and other clouds (e.g. Google Drive)
National Data Storage 2

Latest developments (2):

- LCFS – WHY?
  + we wanted to facilitate integration of NDS2 functionality with existing stuff
  + some storage providers does not support SFTP
  + SFTP introduces relatively high latency:
    => while OK in WAN (main application)
    => some other protocols perform better in LAN
Latest developments (3):

- Windows Phone client
  
  + re-uses some part of regular NDS2 Windows client
    
    => encryption / integrity control
    => SFTP client

  + status – on the way, should be available 1Q2015

  + WHY:
    
    > a lot of „managers” uses Windows Phone
    at least in Poland iOS not that popular
    (real-life observations, confirmed by telcos)

  + challenges:
    
    > dealing with certificates, encryption
    > interface to be developed „from scratch”
    to match platform specifics
Latest developments (5):

- LDAP and Active Directory integration
  + running in some deployments
    > e.g integrated with PSNC’s LDAP
  + proof of concept:
    > prepared AD PoC for large user
National Data Storage 2

Roadmap:

- Go on with stabilizing the code
- Further internal tests and beta-tests with users

- Improving documentation + website
  + e.g. movies with how-tos
  + whitepapers explaining the details and security aspects

- Possibly tests with TF-Storage partners
  + don’t you care security?
  + tell us what’s wrong with our solution?
    (we would be happy to argue)
National Data Storage 2

Roadmap (2):

- NDS2 version 2

  + more symmetric, less asymmetric cryptography for simple cases:
    > better performance with many files (less latency)
    > bulk transfer/encryption already acceptable

  + paranoid-mode options (less trust on servers)
    > stronger data vs meta-data integrity protection
    > client-side cryptography-based access control
    > write non-repudiability
    > write signing / verification
National Data Storage 2

Roadmap (3):

- Storage and AAI

  + need to attack the problem
    > not a trivial task
    > several approaches exist but
      not obvious where to go

  + take up existing solutions?
National Data Storage 2

Roadmap (4):

- Web interface?
  
    + we’re examining some solutions:
      > testing / trying pydio
      > evaluating in-browser encryption options
National Data Storage 2

Lessons learnt:

- Way from prototype to product:
  + 2x the way from idea to prototype

- Real life verifies the solutions the best:
  + some ideas / mechanisms to be dropped
  + the more complexity/components the worse ;]