Social Contract of Communication Service Providers

Problem

- Many users cannot or should not trust their hosting and communication providers
- Many providers often make claims they cannot keep about user privacy and infrastructure security
- Anonymous access is rarely available

http://and.nothingtohide.is/

What do we want?

- Increased user awareness of privacy issues
- Enabling users to make more conscious decisions about which providers to use
- Increased solidarity between groups and individuals who use and maintain services
- Better compatibility between different organisations (e.g. for networking services together)
- Increased security provision

http://and.nothingtohide.is/

How do we get it?

- To define a set of standards that are easily understandable by sysadmins *and* users
- To provide examples of best practice
- To provide a 'modular' system that can be adapted to the needs of different organisations
- Projects can announce and advertise their adherence to the policy (modularly)

http://and.nothingtohide.is/

Providers Commitment for Privacy

A policy for system administrators

http://and.nothingtohide.is/

Providers commitment for Privacy

- Problem
- Demands
- Solution
- Methods
- Results
- Modules
- Availability
- Discussion

http://and.nothingtohide.is/

Methods

- International group of participants
- English-language based
- Discussion over 3+ years
- Practising privacy-aware sysadmins
- Technology agnostic

http://and.nothingtohide.is/

Results

- Up to 45+ participants
- Policy document version 1.0 completed
  - 8 modules (NOT exhaustive)
  - 3 security levels for each module
- Started 'best practices' document
  - Parallel design to the policy
  - Needs more work!

http://and.nothingtohide.is/

Modules

- What to do in case of fire?
- Mail
- Webmail
- Certificates and keys for encrypted-stream based services
- Filesystems and Storage
- Logs
- Users
- Evaluation of policy compliance

http://and.nothingtohide.is/

Security levels

- **Level 1:** encryption
- **Level 2:** encryption + anonymisation
- **Level 3:** available as Tor hidden service
  (Note: this is not technology agnostic enough, maybe “anonymising relay network”.)

http://and.nothingtohide.is/

Webmail

- **Level 1:**
  - User – Provider connection encrypted
  - Inform users if IP included in mail headers
- **Level 2:**
  - Session info as cookies, not included in URLs
  - IPs stripped from mail headers
- **Level 3:**
  - No javascript
  - No IPs in session management
  - Available via Tor [NOTE: wording is currently confusing!]

http://and.nothingtohide.is/

Logs

- **Level 1:**
  - Logs stored encrypted or only in memory
- **Level 2:**
  - Anonymised logs
- **Level 3:**
  - No logs stored

http://and.nothingtohide.is/

Certificates and Keys

- **Level 1:**
  - Strong cryptographic algorithms
- **Level 2:**
  - Private keys encrypted
- **Level 3:**
  - Private keys encrypted and off-site

Best Practices

- Technology specific
- Similar structure to modules
- Links to already available resources
- Incomplete! Needs love.

http://and.nothingtohide.is/

Availability

- **Web:** http://and.nothingtohide.is/policy

  Current version of policy is cryptographically signed:

  ```
  CE8B A231 83EC 5CB6 9760
  E02F 8BC0 E739 D064 5843
  ```

- **Git:** [see website for details]

http://and.nothingtohide.is/

How to get involved

- Use policy for your servers and services!
  - Declare your compliance levels publicly
  - Link to http://and.nothingtohide.is/policy
- Contribute to the 'Best Practices' document
- Help improve the future versions of policy
  - Clone the git repository and make your changes
  - Send details of your local repository to the policy team for review

http://and.nothingtohide.is/

Discussion

- Debates over name, proposal to change it to Provider Social Contract or something else
- Want a public discussion or announcement list? Write to us!

http://and.nothingtohide.is/

Contact

Email:

- pcp@and.nothingtohide.is

OpenPGP:

`93A3 28B9 CF38 200F AF0A 67F2 77D9 5A90 12B3 EEDA`

http://and.nothingtohide.is/