Workshop Report "Applications (II): TNC"

Josef von Helden
josef.vonhelden@inform.fh-hannover.de

First European Summer School on Trusted Infrastructure Technologies
September 2006

TNC: workshop report (1) overview

- discussion of applicability / extensibility of several scenarios
  - P2P
  - various wireless scenarios
  - mobile scenarios
  - VPN scenario
- TNC policy management

TNC: workshop report (2)

- P2P
  - TNC is mainly designed for client-server architectures
  - important difference in P2P: roles change dynamically
  - impact on TNC:
    every entity has to act as AR, PEP and PDP
- generalisation: „contract scenario“
  - (dynamical) contract negotiation between partners
  - local „contract enforcement point“
  - possible evolution of TNC to this kind of scenario

TNC: workshop report (3)

- Wireless
  - Checking policy conformance (not limited to security issues) on clients by provider,
    - examples: conformance to RFCs, limited transmission data rate, ...
    - TNC seems to be well suited
      - mainly: implementing IMC / IMV pairs
  - Checking provider properties by clients
    - mapping on generalised contract scenario (s.a.)

TNC: workshop report (4)

- Mobile
  - scenario: mobile devices connect to network of service provider(s)
    - TNC seems to be well suited
    - some design and implementation aspects:
      - what are PEPs in this scenario?
      - development restrictions of mobile devices
      - (re)use of special protocols
  - question: will TNC be the enabler to put classified information on mobiles
    - answer: possibly, if mobile devices will be equiped with TPMs

TNC: workshop report (5)

- VPN scenario
  - e.g. remote access to corporate network via Internet
    - TNC seems to be well suited
    - some aspects:
      - PEP: VPN gateway
      - use different technologies at NAL, e.g. VPN instead of 802.1x

TNC: workshop report (6)

- TNC policy management
  - main question: how to make decisions?
    - comparisions to completly other areas (immigration, clinical diagnostics)
  - differentiation between
    - decisions based on semantical specialities -> IMVs
    - decisions based on parameterisable algorithms with a set of well known input values -> TNC Server
  - IMV policies
    - vendor specific and not completly generalisable
  - TNC Server policy
    - state machine interpreting a certain policy language
    - important precondition: IMVs must be identifiable (unsure if conformable with spec)

TNC: workshop report (7) conclusion

- more implementation oriented tasks
  - scenarios
    - TPM integration
    - Wireless (partly)
    - VPN
  - others, e.g.
    - implementing more IMCs
    - porting client to Linux
- more design oriented task
  - TNC policy management (?)
  - mobile (?)
  - evolution of TNC to generalised „contract scenarios“