Identity and privacy in NGNs

The Authorisation challenge in NGNs

Scott CADZOW
C3L
© ETSI 2009. All rights reserved
Contents

- What is privacy?
  - In society
  - In legislation
  - Where exceptions are allowed
    - Lawful Interception
    - Data Retention

- What is identity?
  - In the general case
  - In the network case

- What is the role of ETSI and the other SDOs?
  - Standards
  - Guides and reports
  - Awareness
What is privacy?

Privacy definitions

- seclusion:
  - the state of being apart from other people and not seen, heard, or disturbed by them

- freedom from attention of others:
  - freedom from the observation, intrusion, or attention of others

- hidden condition:
  - the state of being kept secret

- From the Latin *privatus* 'separated from the rest, deprived of something, especially office, participation in the government', from *privo* 'to deprive'

- The ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.
Privacy in legislation

- Universal Declaration of Human Rights (article 12)
  
  "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

- EU Convention for the Protection of Human Rights and Fundamental Freedoms (article 8)
  
  "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."
Obligations of the NGN

- By analysis of the regulation the NGN is mandated to provide basic identity and privacy protection. This includes as a minimum:
  - The identity of an NGN user should not be compromised by any action of the NGN
  - No action of the NGN should make an NGN user liable to be the target of identity crime
  - The privacy of an NGN user should not be compromised by any action of the NGN
  - The correspondence of an NGN user should not be compromised by any action of the NGN
- Users in the NGN may be natural or legal persons or in some instances other legal entities (e.g. corporations).
The NGN as a collection of provider entities

CpoA: Covert point of Attachment
SpoA: Service point of Attachment
TpoA: Transport point of Attachment

The NGN

Service content (www)
IMS plane
IP network
Content privacy – user generated
Content privacy – provided
Content privacy – interactive sessions
One person – multiple persona
Privacy problems in the NGN

- The NGN is a platform for social and business communication
  - Social and business communication mores are different

- Private users are not terribly privacy aware
  - Slander
    - the act or offence of saying something false or malicious that damages somebody's reputation
  - Libel
    - a false and malicious published statement that damages somebody's reputation. Libel can include pictures and any other representations that have public or permanent form.
    - the making of false and damaging statements about somebody
  - Bullying
    - Slander and libel may lead to this, groups may be involved
    - the process of intimidating or mistreating somebody weaker or in a more vulnerable situation
Content separation

- Being a friend on Facebook™ should not imply friendship on BeBo™
- Being a user of service A should not imply also being a user of service B

- Aim is to provide unlinkability
  - But has to be reversible
  - Convergence of service platforms using RESTful approach
    - SIP, HTTP
  - But one network links all the services and content together
    - All pervasive IP
Who manages the user? (Subscription)

- There are a number of options for the NGN and they hold the key to the security of the NGN and the privacy of their users

  - IMS as root of subscription
    - Uses IMS-AKA to offer authentication and deliver keys for Confidentiality and Integrity services.
    - All authorisation is implicit

  - Access Network as root of subscription
    - For 3G uses UMTS-AKA (or CDMA2000-AKA) to offer authentication and deliver keys for Confidentiality and Integrity services.
    - All authorisation is implicit

  - Content or service provider as root of subscription
    - Top of the tree and almost forces a separate identity and authentication scheme for each service
    - Authorisation only for the content or service (no authorisation tree)
Privacy protection measures

- ISO 15408-2 (Common Criteria) identifies 4 key attributes that relate to privacy and which are undergoing assessment for application in the NGN
  - **Anonymity**
    - Does the NGN need to offer anonymous services?
  - **Pseudonymity**
    - How do we extend the GMS TMSI concept to the NGN stack?
  - **Un-Linkability**
    - Does one provider need to know if another provider is offering services to the same person?
  - **Un-Observability**
    - Does the NGN need to ensure that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used?
Anonymity

- Ensures that a user may use a resource or service without disclosing the user's identity.
  - Anonymity where the system requires that other users or subjects are unable to determine the identity of a user bound to a subject or operation.
  - Anonymity without soliciting information enhances the requirements of the above by ensuring that the NGN does not ask for the user identity.
Pseudonymity

- Ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.
  - Pseudonymity requires that a set of users and/or subjects are unable to determine the identity of a user bound to a subject or operation, but that this user is still accountable for its actions.
  - Reversible pseudonymity, requires the NGN to provide a capability to determine the original user identity based on a provided alias.
  - Alias pseudonymity, requires the NGN to follow certain construction rules for the alias to the user identity.
Unlinkability

- Ensures that a user may make multiple uses of resources or services without others being able to link these uses together.
  - Unlinkability, requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system.
Unobservability

- ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.
  - Unobservability requires that users and/or subjects cannot determine whether an operation is being performed.
  - Allocation of information impacting unobservability, requires that the NGN provide specific mechanisms to avoid the concentration of privacy related information. Such concentrations might impact unobservability if a security compromise occurs.
  - Unobservability without soliciting information requires that the NGN does not try to obtain privacy related information that might be used to compromise unobservability.
  - Authorised user observability, requires the NGN to provide one or more authorised users with a capability to observe the usage of resources and/or services.
Trust and identity in NGN

Untrusted domain

- Content provider

IMS domain

- IMS (trust established using IMS-AKA)

UMTS domain

- ECN (trust established using UMTS-AKA)

Untrusted CPE

Untrusted NT

SpooA (IMS)

TiaOA (UMTS?)

ETS1 Security Workshop 2010
Trust in the NGN

- How does the service trust the network?
- How does the content provider trust the service platform?

Proposal being considered in TISPAN for the NGN

- Keyed authorisation framework
  - Variant of X.509 based Privilege Management Infrastructure (PMI)
  - Elements of Kerberos ticket granting service too
- Will fully support the LI requirements in the “Dynamic Triggering” area
- May allow greater trust from users of the core network
- May act as a deterrent to SPAM, DDoS and other attacks
Explicit authorisation model

- **Assertions:**
  - Content providers require QoS, GoS guarantees
  - Network resource is finite
  - Detection and prevention of law breaking aids society

- **Considerations:**
  - Service providers want customer retention
  - Users want privacy
  - Users want freedom of expression

- Identification and authentication are not sufficient by themselves in the NGN and our e-world
  - Authorisation and privacy protection have to be added
SDOs and partners

ROLE OF STANDARDS
Who’s involved or needs to be involved?
Standardisation of authorisation frameworks

- **TISPAN and ETSI**
  - Expand the models developed in TS 187 016 (Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN; NGN Security; Identity protection (Protection Profile)) and apply them to generic and specific NGN models
  - Mandate them for the NGN core

- **ENISA?**
  - Promotion and encouragement of development

- **Others?**
  - For discussion – but everyone has a role they can play
Thanks and over to questions, debate, decisions?

THAT’S IT