IMS security challenges, the smartcard advantage

Gemalto (Gemplus, Axalto), 3

3GPP SA#33, 25 - 28 September, 2006

Security will play a key role in IMS success

- Past experience
  - Analog cellular networks plagued by fraud
  - Due to cloning, industry lost reached hundreds of millions per year
- Current deployments
  - Smartcards are used in Mobile Networks to secure authentication keys and algorithms
- IMS security challenges
  - IMS can be accessed from a wide range of access networks
  - Protection against attacks is absolutely needed

Authentication: the cornerstone of IMS security

- 3GPP authentication methods
  - AKA based solution (full long term solution)
  - Early IMS (an interim solution based on GSM security)
  - Both methods require the use of a smartcard
- TISPAN authentication methods
  - AKA based solution (using a smartcard: ISIM on a UICC)
    - Preferred TISPAN solution
    - IMS Residential Gateway to support legacy terminals
  - NASS Bundled Authentication
    - a wireline-based authentication
  - HTTP-Digest authentication
    - A weak authentication method, documented as informative

IMS convergence security issues

- Existing IMS authentication methods provide different levels of security
- The use of weak authentication methods will endanger the whole system security
  - Some of HTTP-Digest weaknesses are documented in 3GPP TR 33.978
  - All well-known weaknesses of password-based authentication apply to HTTP-Digest:
    - One-factor only authentication
    - Easy to guess, subject to dictionary attacks
    - Easy to snoop, visible in the clear when keyed
    - Easy to loose and forget
    - Easy to write down and share with others (cloning)
  - Vulnerabilities and weak authentication methods should not spread from one system to another
- 3GPP IMS security should be preserved
  - The use and documentation of weak authentication methods should be prohibited in 3GPP

The smartcard advantage

- Provides a secure authentication method
  - Tamper-resistant device designed to resist software and hardware attacks
  - Secure storage of user credentials
  - High level cryptographic capability
  - Strong two-factor user authentication (UICC and PIN)
  - An anchor in the user domain that is under operator's full control
- Improves IMS level roaming and service portability
  - The user data (subscription, credentials, …) are not bound to a device
  - Secure platform for operator's sensitive applications (e.g. DRM, eCommerce)
- A step towards fixed-mobile convergence and true access independence
  - ISIM on UICC based solution adopted by 3GPP, 3GPP2 and TISPAN
- Personalization tool
  - Branding, customization, provisioning, etc
  - Reduce cost and complexity of handset personalization and logistics

Conclusion

- Users need a highly secure and easy-to-use solution for accessing services
- 3GPP IMS security should be preserved
- The smartcard plays key role in 3GPP IMS security
- The smart card provides:
  - An operator controlled authentication token
  - A secured environment for operator applications
  - A portable environment for operator applications
  - A personalization and customization tool
  - A personal storage space