Network and Information Security Report ICTSB/NISSG

Stefan Goeman

Background

- Existing NIS-Report from 2003
- The new EU Report
  - Communication form the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions:
    A strategy for a Secure Information Society – “Dialog, partnership and empowerment”
- A lot of new developments in Network and Information Security

My Expertise

- Each member of the team has some specific expertise. In my case, this is:
  - Telecom (IP-based), ICT Industry, ISP
    - Authentication protocols
    - Web Service Security
  - Identity & Privacy Management
  - Digital Rights Management

Contributions to the Report

- In section 5, a section on Next Generation Networks (NGN)
- In Section 9:
  - Section 9.3 on Electronic mail encryption
  - Section 9.4 on Network Encryption
- Numerous other smaller improvements to the document
  - Mostly a link with protocols and standards coming from standardization bodies like IETF, W3C, OASIS

Contributions to Section 5

- Next Generation Networks
  - About convergence between voice communication networks and data communication networks
  - Convergence between fixed and mobile networks
  - All IP-based network → more open network
    - Threats from IP data communication world will now also impact the voice communication world (VoIP spamming, SIP spamming → SPIT)
  - Standardization in ETSI TISPAN, also based on activities in 3GPP (on IMS) and IETF
  - NGN will provide security measure that will counter the threats: Authentication, Authorization, Policy Enforcement, Key Management, Confidentiality and Integrity protection

Optional contribution to Section 5

- On Web Services and Web Services Security
  - Provide description of Web Services and Web Services based SOAs (Service Oriented Architectures). Currently, the report only provides a description of WS Security in Annex 1.
  - Problems with Web Services Security:
    - Lots of security standards in this area. But, the standards are only building blocks. You have to apply the correct standard in the correct way.
    - Reference: J. Viega, J. Epstein, “Why applying standards to Web Services is not enough”, IEEE Security & Privacy, July/August 2006.

Optional contribution to Section 5

- On Trusted Computing ()
  - It will have an impact in our daily life. Trusted Platform Modules (TPM) will eventually be integrated in every electronic device (PC, mobile phone, set-top box, …)
  - What security will it bring:
    - All in all, more secure computing environments
    - Stop spreading of illegal software copies
    - Hardware support for DRM implementations
  - What security problem will it not solve!!
    - It will not solve the problem of viruses and worms exploiting bugs in trusted software (like the OS)

Section 9.3 on E-mail Encryption

- E-mail is still one of the most used communication applications today (although Instant Messaging application are very popular as well)
- Updated section 9.3 to reflect the continuing work on S/MIME
  - Inclusion of AES as encryption protocol
  - References to the latest versions of RFCs
- Also included the work of the OpenPGP IETF working group → create an interoperable solution with PGP of Phil Zimmermann

Section 9.3 on E-mail Encryption

- RFC3850: S/MIME Version 3.1 Certificate Handling
- RFC3851: S/MIME Version 3.1 Message Specification
- RFC3852: Cryptographic Message Syntax
- RFC3853: S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)
- RFC3565: Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Format
- RFC2440: OpenPGP Message Format
- RFC3156: MIME Security with OpenPGP

Section 9.4 on Network Encryption

- Describes network encryption at different layers in the protocol stack
  - IP layer → IPsec
  - TCP/UDP → TLS and DTLS (DTLS provides security on top of UDP)
  - Web Services Security
- Updated this section to reflect the latest work in these areas
- → See also Annex 1 for more detailed descriptions

Section 9.4 on Network Encryption

- IPsec Protocol Suite:
  - RFC4301: Security architecture for the Internet Protocol
  - RFC4302: Authentication Header security protocol.
  - RFC4303: Encapsulating Security Payload protocol.
  - RFC4306: The Internet Key Exchange (IKEv2) protocol.
  - RFC4308: Cryptographic Suites for IPsec

- TLS / DTLS:
  - RFC4346: The Transport Layer Security (TLS) Protocol Version 1.1
  - RFC4492: ECC Cipher Suites for Transport Layer Security (TLS)
  - RFC4279: pre-Shared Key Ciphersuites for TLS
  - RFC4347: Datagram Transport Layer Security
  - …

Section 9.4 on Network Encryption

- Web Services Security Standards:
  - OASIS WS-Security Standard:
    - WS-Security Core Specification
    - Username Token Profile
    - X.509 Token Profile
    - SAML Token Profile
    - Kerberos Token Profile
    - Rights Expression Language (REL) Token Profile
    - SOAP with Attachments (SWA) Profile
  - XML Signature
  - XML Encryption
  - WS-Policy specification by W3C
  - OASIS Security Assertion Markup Language (SAML) specification
  - OASIS XACML (eXtensible Access Control Markup Language) specification
  - OASIS XKMS (XML Key Management Specification) specification

Other Contributions

- Section 3.3.4 on Longevity of Archiving
  - Provide a description of the work of the IETF LTRANS working group (Long-Term Archive and Notary Services). IETF LTRANS will use work of other IETF working groups, like PKIX, S/MIME and XMLDSIG as the basis to define the necessary data structures and protocols
  - Included is also a small section on of ARMA on records management
- Reworked Section 6.2 on requirements for Small and Medium Enterprises (SMEs)

Other Contributions

- Section 7: General Threats to NIS
  - We all worked on defining the treats
  - In particular on
    - (Threat T6 on illegal content decryption (DRM related))
    - Threat T8 on disruptive attacks on the Internet infrastructure (DoS, DDoS, VoIP spamming)
    - Threat T9: on the vulnerability of VoIP networks
- Reworked Section 8.1.4 on Effective User Authorization and Access Control:
  - Included the section on Role Based Access Mechanisms (RBAC)
  - Included the section on SAML and XACML and how they can be used to implement an RBAC system.

Other Contributions

- Reworked section 8.1.5 on Effective User Management

- In section 8.2.1 on Passwords, included a paragraph on the use of zero-knowledge protocols as improvement to the current username/password approach
  - SRP and the use of SRP in TLS → RFC2945: Using SRP for TLS authentication