IT-Sicherheit

Axel Pemmann

03. September 2007

1. Grundlagen Kryptografie
   - Authentifizierungsmöglichkeiten
   - Zwei Verschlüsselungsverfahren
   - Authentifizierung von Nachrichten
   - Handshake-Protokolle
   - Verwaltung von Schlüsseln

Was ist echt, was ist schlecht?

Welche Möglichkeiten gibt es, Zugriffsschutz zu realisieren? Reicht einfacher Passwortschutz oder sollte die stärkere Zwei-Faktor-Authentifizierung angwendet werden?

Arten der Authentifizierung:

- mittels Wissen (PIN)
- Besitz (Smardcard, Token)
- Körperliche Merkmale (Biometrie, Fingerabdruck)

Siehe dazu
`http://de.wikipedia.org/wiki/Authentifizierung`

Von alters her: Symmetrie, neuerdings: Asymmetrie

Zwei grundlegende Verfahren

Symmetrische Verschlüsselung

- Einfachere Handhabung
- Bei vielen Schlüsseln hoher Verwaltungsaufwand
- KRITISCH: Schlüsseltransport!!

Asymmetrische Verschlüsselung

- Schwierigere Handhabung
- Einfachere Verwaltung in PKI
- Sicherer Schlüsseltransport

Ein Leben in Symmetrie...

Symmetrische Verfahren, Kennzeichen: Jede Seite ist in Besitz des selben Schlüssels.

- DES (Data Encrytion Standard)
- 3DES Der Nachfolger: Bereits geknackt!!
- Blowfish
- AES (Advanced Encrytion Standard)

Aber Asymmetrie bringt erst Leben in die Bude!

Asymmetrische Verfahren: Jede Seite besitzt ein eigenes Schlüsselpaar, einen öffentlichen sowie einen privaten Schlüssel.

- RSA (Erfinder: Rivest, Shamir und Adleman) Einsatz: SSH (Secure Remotelogin und Remotecopy), TLS (Transport Layer Security, z.B. httpS://url)
- DiffieHellmann (z.B. VPN mit IPsec)
- El Gamal (Erweiterung des Verfahrens zum Schlüsselaustausch von Diffie und Hellman)

Eindeutigkeit durch Fingerabdruck

Digitale Signaturen: Fingerabdrücke von Nachrichten oder Dateien

- DSA (Digital Signatur Alghorithm, kritisches Verfahren)
- HashFunktionen: MD5, SHA1, ...

Siehe dazu auch:
`http://www.henniger-online.de/lehre/...`

Digitaler Fingerabdruck

Informieren Sie sich in diesem Zusammenhang über Einweg-Hashfunktionen.

Nach welchem Protokoll die Hände schütteln?

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Protocol)
- Microsoft NTLM
- Kerberos

ACHTUNG

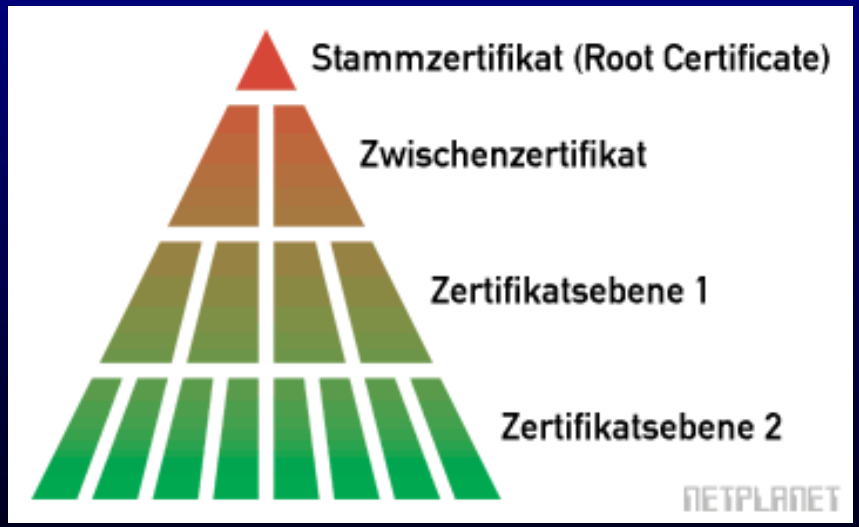
PAP versendet Passwörter im Klartext!

Schwer zu tragen: der große Schlüsselbund (1)

PKI – Public Key Infrastrukture: Verwaltung von Schlüsseln und Zertifikaten

Es gibt zwei große Verwaltungsprinzipien, erstens:

Hierarchiemodell Ein klassisches PKI Vertrauensmodell ist streng hierarchisch und pyramidenförmig aufgebaut.



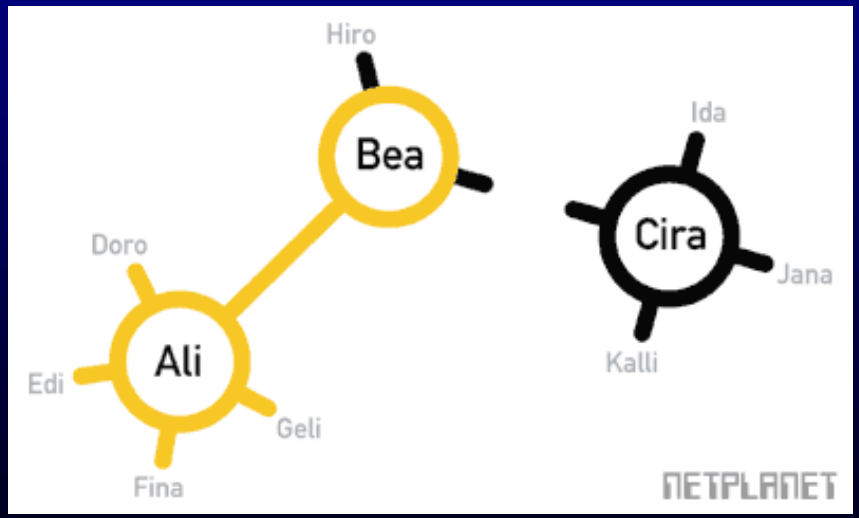
http://www.netplanet.org/kryptografie/vertrauen.shtml

Schwer zu tragen: der große Schlüsselbund (2)

PKI – Public Key Infrastrukture: Verwaltung von Schlüsseln und Zertifikaten

Das zweite Verwaltungsprinzip:

Vertrauensmodell «Ich kann jedem vertrauen, dem ich vertrauen möchte.»



http://www.netplanet.org/kryptografie/vertrauen.shtml

Hilfsmittel zur Verwaltung vieler Schlüssel

PKI – Public Key Infrastrukture: Verwaltung von Schlüsseln und Zertifikaten

Open Source Software für Trustcenter:

- XCA (auf MS-Windows portiert)
- TinyCA (GUI in Perl/Tk)
- OpenCA (umfangreiche Client-Server-Lösung)

Weiterführende Seiten:
`http://www.pki-page.org`
`http://www.staff.uni-marburg.de/~mennehar/speyer/SS01/s203-Dateien/digsigtechtext.htm`

Vielen Dank für Ihre Aufmerksamkeit!

IT-Sicherheit

Axel Pemmann

03. September 2007

Ende