III. Single Sign-on: Kerberos

1. Що е то и защо е нужно - обща идея

- single sign-on - ами.. удобство си е :)
- mutual authentication - понякога наистина е важно да знаеш с кого говориш :)

2. Кратък преразказ на A Dialogue in Four Scenes -
<URL:http://web.mit.edu/kerberos/www/dialogue.html>

3. По-подробно описание: domain controller, tickets, expiration, TGT, etc
<URL:ftp://athena-dist.mit.edu/pub/kerberos/doc/krb_evol.PS>

4. Реализации - krb4, krb5, MIT Kerberos

5. Разлики между Kerberos 4 и Kerberos 5 – много!

- Случайни стойности на всяка крачка за дори по-малко predictability;
- forwardable, proxiable, renewable tickets;
- ASN.1 за message encoding;
- authorization data;

5. Предимства и недостатъци от гледна точка на usability

- con: изисква специална поддръжка от всяко приложение; не може да се "мине тънко" примерно с PAM;
- pro: single sign-on, baby!
- pro: industry standard, interoperable implementations
- pro: може да бъде използвано и remotely
- pro: има и cross-realm auth! (но виж по-долу за krb4)

6. Предимства и недостатъци от гледна точка на security

- con: krb4: кажи-речи никъде не се използват случайно-генерирани данни
- con: krb4: проблем с използването на 3DES в CBC-mode: cross-realm auth gone to hell.
- krb5 няма лоши страни, поне не и засега известни :)

7. Разни
- Поддръжка на Kerberos се прави най-лесно с GSSAPI (RFC 2078)
- Напоследък се появяват все повече гласове и идеи за Kerberos auth дори и на web applications, както Windows поддържа NTLM auth между IIS и MSIE, а напоследък и между IIS и Mozilla.

Още информация:
- <URL:http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#v5vsv4>
- <URL:http://web.mit.edu/kerberos/>
- <URL:http://www.faqs.org/rfc/rfc2078.txt>