II. One-time passwords (OTP: S/Key и OPIE)

1. Що е то - обща идея

- Преодоляване на sniffers и keyloggers.

2. Начин на работа

- От сигурна конзола: въвеждаш passphrase за инициализация на последователността;
- През несигурна среда: auth request за определен потребител;
- OTP libs намират последователността и текущата позиция;
- OTP libs изчисляват и изпращат въпросването (challenge);
- От сигурна конзола: въвеждаш passphrase и изчисляваш отговора;
- През несигурна среда: предаваш отговора в cleartext;
- OTP libs изчисляват отговора и сравняват.

3. Реализации
- logdaemon: кофти, rebuild на всички системни програми, които искат автентикация... какво правят другите OS's?
- S/Key: добра последователност от идеи, криптографски силни hash алгоритми;
- OPIE: развитие на S/Key с MD5 вместо MD4, много portable, много лесно за използване.
  <URL:http://www.inner.net/pub/opie>

4. Реализации в програми - local support, PAM

5. Предимства и недостатъци от гледна точка на използваемост

- con: досадно е всеки път да си въвеждаш паролата :) но може да си напишеш keychain;
- con: не може да се разпредели между повече машини;

6. Предимства и недостатъци от гледна точка на security

- con: не може да се разпредели между повече машини, изобщо не се връзва с идеологията за single sign-on;
- pro: никаква възможност за replay attacks;
- pro: в новите реализации (OPIE) е достатъчно криптографски силно, така че няма никаква опасност и от brute-force атаки.

7. OTP calculators

- Unix-like OS's: в самото OPIE идват opiepasswd(1) и opiekey(1);
- Windows: WinKey, <URL:http://www.inner.net/pub/opie/contrib/WinKey.exe>
- Java: много са, <URL:http://google.com/search?q=Java+OTP+calculator>