

# Аутентификация

Владимир Иванов  
[ivlad@malpaso.ru](mailto:ivlad@malpaso.ru)

# Парольная аутентификация

“Лица, которым известен пароль, обязаны хранить его в строжайшем секрете и при опросе сообщать его запиской, без оглашения, после чего записка немедленно уничтожается”

Устав гарнизонной и караульной службы

# Достоинства паролей

- Пароли дешевы
- Существуют везде
- Могут использоваться для выработки ключей (PBKDF2)

# Недостатки паролей

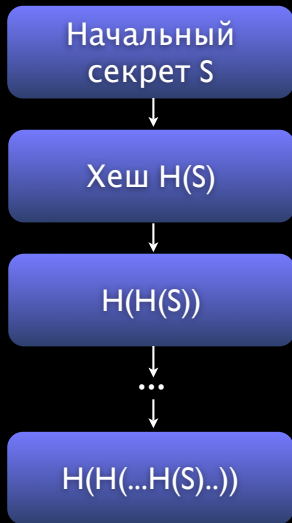
- Пароли дороги
- В зависимости от системы, централизованная аутентификация затруднена (не говоря уже об SSO)
- Пароли небезопасны

# Уязвимости

- Сложность пароля:  $(2*26+10+?)^N$ 
  - Реально ниже: John the Ripper
- Уязвимы при хранении (на бумаге)
- Уязвимы для replay attack

Одноразовые  
пароли

# S/Key



- Сложность  $2^{64}$  - меньше, чем для пароля
- Неуязвим для replay attack
- Уязвим для session hijacking
- Может бы уязвим для offline-перебора

# SecurID



- Функция хеширования, срабатывает один раз в минуту  $H(iv, time)$
- Инициализационный вектор известен серверу
- Синхронизация времени

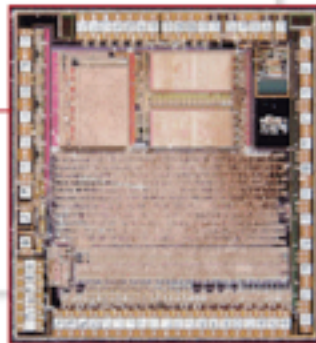


# Проблемы SecurID

Vendor unknown  
1C5737  
Real-time clock + LCD controller +  
number generator

Epoxy-encased  
electronics

Micro Crystal  
MS1V-T1K  
32.768-kHz crystal



# Криптографическая аутентификация

# Алиса и Боб

- Криптография с открытым ключом
- Хорошее масштабирование с учетом построения иерархической PKI
- Иерархическая топология X.509 хорошо работает в организации



# Алиса и Боб

- Простейший вариант
  - Алиса и Боб имеют пары ключей
  - Алиса шифрует случайное число своим приватным ключом
  - Боб может проверить, расшифровав открытым ключом
- Откуда Боб знает ключ Алисы?

# Центр доверия

- Пусть Боб доверяет Чарли
  - Чарли может подписать ключ Алисы (и любых других участников системы)
  - Тогда Бобу нужно знать всего один ключ - Чарли (certification authority)

# Иерархия

- Открытый ключ пользователя плюс служебная информация, подписанные ключем СА - сертификат
- Сертификат СА может быть подписан вышестоящим СА - вплоть до “корневого”

```
openssl x509 -in /etc/ssl/certs/dovecot_cacert.pem -noout -text
```

Data:

Version: 3 (0x2)

Serial Number:

95:89:81:84:3d:52:f8:3b

Signature Algorithm: md5WithRSAEncryption

Issuer: C=RU, ST=Moscow, L=Moscow, O=CA

**Validity**

Not Before: Nov 25 10:48:09 2005 GMT

Not After : Nov 24 10:48:09 2008 GMT

**Subject:** C=RU, ST=Moscow, L=Moscow, O=Company

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

**RSA Public Key:** (2048 bit)

Modulus (2048 bit):

00:a5:47:7a:8e:3a:81:f7:d9:da:81:96:20:58:e1:

[ ... ]

67:9d

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

50:EB:76:81:9E:54:65:B3:E3:D1:56:A3:AE:B3:80:6D:3C:3E:51:FA

X509v3 Authority Key Identifier:

keyid:50:EB:76:81:9E:54:65:B3:E3:D1:56:A3:AE:B3:80:6D:3C:3E:51:FA

DirName:/C=RU/ST=Moscow/L=Moscow/O=CA

serial:95:89:81:84:3D:52:F8:3B

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

9c:81:f6:4b:1b:49:db:cb:27:ab:83:2a:07:19:6b:13:d7:80:

[ ... ]

25:dd:82:2c

# PKI

- PKI хорошо работает в организации, где доверие определяется административно
- Делаются попытки корректно реализовать работу в Интернет
- Откуда я знаю, что сертификат ebay.com подлинный?



# CRL

- Валидность сертификата должна быть проверена
  - Проверка CRL
  - Использование OCSP

# Аутентификация

- Аутентификация по сертификатам работает для многих протоколов
  - HTTP
  - IMAP, SMTP
  - Telnet, SSH
- Электронная подпись

# Мораль

- Пароли плохи
- Одноразовые пароли лучше, но ненамного
- Сертификаты математически замечательны но в реальной жизни не добавляют достаточно безопасности