Инфраструктура открытых ключей – унаследованные проблемы и попытки их решения

Алексей Смирнов, Parallels
arkenoi@parallels.com

X.509: это ITU

- Стандарт разработан до того, как интернет стал таким, как мы его знаем (80-е)
- +: он универсален
- +: он расширяем
- -: все плюсы ничего не значат, если ими пользоваться неправильно и не думать вперед

Реализация

- В 90-х все еще было иначе
- Можно было подумать заранее о многом, но зачем?

Когда жареный петух, наконец, клюнул

- 2001: фальшивые сертификаты Microsoft от Verisign
- 2002: отсутствие проверки basic constraints
- 2003: фишинг, downgrade-атаки
- 2008: фальшивый сертификат mozilla.com через Comodo RA
- 2009: Etisalat
- 2011: icksunx2 и снова Comodo (google, mozilla, live.com)
- 2011: Diginotar и снова icksunx2
- 2011: Malware, 512-битные ключи (Малазия)
- 2012: Trustwave и сертификаты для DLP

Давайте-ка посмотрим (SSL Observatory)

- 4.3M из 11.3M сертификатов валидны
- 1,482 CA пользуются доверием MS и Mozilla
- 30,000 проблемных ключей
- 37,000 localhost, mail, IP-адреса и чорт знает что
- 33,916 EV сертификатов

Что делать?

- Защити себя сам? (Certificate Patrol)
- Доверенная (необязательно) четвертая сторона и репутационные системы? (Google, DANE, MonkeySphere, Convergence, Perspectives, MECAI, EFF Sovereign Keys)
- OCSP stapling
- Закрутим гайки немного и будем жить, как раньше

Кто?

- CA/B forum
- mozilla-dev-security-policy
- SSL Obvservatory
- pkix@ietf.prg

Обсуждение

Вопросы?