HOGYAN ÜLJÜK MEG A KRIPTOPÓNIT?

silent signal

Veres-Szentkirályi András 2019-04-05

WTF pwnie

silent signal

EFAIL: PGP és S/MIME

silent signal

- gyakorlatilag minden e-mail crypto
- már az alapok sem az igaziak: túl sok opció
- kliens implementációs bajokat használ ki, zseniálisan
- HTML, JS, CBC, CFB

Curl-P: IOTA

- eleve, cryptocurrency
- saját megoldások, ternáris számítás

“Curl could be broken using a cryptanalysis technique discovered in the 1970s and taught to college sophomores”

KRACK: Key Reinstallation Attacks // WPA2

silent signal

- nonce: number used once
- mégis többször sikerült

“The standard for WPA2 anticipates occasional WiFi disconnections, and allows reconnection using the same value for the third handshake (for quick reconnection and continuity). Because the standard does not require a different key to be used in this type of reconnection, which could be needed at any time, a replay attack is possible.”

ROCA: Return of Coppersmith's Attack // Infineon RSA crypto HW

silent signal

- Yubikey + Észtország
- sokáig kísérteni fog
- RNG bonyolult

"If you know some linear algebra, how to reduce a lattice basis, divisors in residue classes, extended linearization, and the implementation pitfalls of Joye–Paillier generators, you can factor an Infineon RSA key using EC2 instances."

ROBOT: Return Of Bleichenbacher's Oracle Threat // TLS

- RSA titkosítás fájdalmas
- TLS-ben is visszaköszön Bleichenbacher 1998-as oracle-je
- Facebook, Paypal, Cisco, F5, Citrix, BouncyCastle, Erlang, WolfSSL
- "Adaptive-chosen-ciphertext attacks were perhaps considered to be a theoretical concern but not to be manifested in practice until 1998, when Daniel Bleichenbacher of Bell Laboratories (at the time) demonstrated a practical attack against systems using RSA encryption"
- "The Bleichenbacher attacks, also known as the million message attack, took advantage of flaws within the PKCS #1 function to gradually reveal the content of an RSA encrypted message. Doing this requires sending several million test ciphertexts to the decryption device (e.g., SSL-equipped web server). In practical terms, this means that an SSL session key can be exposed in a reasonable amount of time, perhaps a day or less."

Konklúzió

- Kriptó bonyolult ☹
- Bízzuk jó és kevés gombos könyvtárra: libsodium!
- Legyünk szkeptikusak és gondolkodjunk!

KÖSZÖNÖM A FIGYELMET!

VERES-SZENTKIRÁLYI ANDRÁS

VSZA@SILENTSIGNAL.HU

FACEBOOK.COM/SILENTSIGNAL

@SilentSignalHU

@dn3t

silent signal