Stone Knives and Bear Skins: Why Does the Internet Run on Pre-historic Cryptography?

Eric Rescorla

RTFM, Inc.
ekr@rtfm.com

Abstract. While cryptography has advanced greatly since since 2001, Internet security protocols have not. Here is a list of the algorithms that are used in common SSL/TLS stacks:

- RSA in PKCS#1 1.5 mode (1993)
- MD5 (1982)
- SHA-1 (1993)
- DES (1976) and AES (2001) in CBC mode (with chained IVs)
- RC4 (1987, leaked 1994)

The situation is similar for other protocols such as IPsec and S/MIME. Without exception, all of these algorithms have known deficiencies, and in many cases these deficiencies have led to practical or semi-practical attacks. Despite this, implementors and users have responded either by ignoring these issues or by adding layers of countermeasures to the attacks which are presently known. Even when new protocols are designed – for instance the IETF's new JSON-based secure messaging effort – designers often select older algorithms over newer, more secure ones. In this talk, we explore how we got into this situation, if we can get out, and if we even want to.

D.J. Bernstein and S. Chatterjee (Eds.): INDOCRYPT 2011, LNCS 7107, p. 343, 2011.