What are State-sized adversaries doing to spy on us? Or how to backdoor Diffie-Hellman

Jun 27, 2016 • David Wong

In the history of American cryptography, companies wanting to export their products abroad would have needed to comply to a few official laws called the *U.S. Export rules*. These stated that no strong cryptographic algorithms could be shipped outside of the country, unless weakened down to brute-forceable sizes (for the government). Some exceptions were made, notably in the Lotus Notes software, where an asymmetric backdoor had to be implemented in exchange for the right to use stronger cryptography.

Many years have passed, and the US has now lost its computational advantage: China is ranked first on the top 500 super computers in the world with the Tianhe-2 machine. The U.S. Export rules have now overcome their stay and have been gently relaxed, although they still are the source of many troubles including the recent critical attacks on TLS: FREAK and LOGJAM. Backdoors seem to be the new hot area of research for the NSA, GCHQ and probably other governmental secret agencies.

In this work we'll talk a bit more about the recent history of these backdoors: from the *Dual EC* PRNG standardized by the NIST organization to the recent Juniper Networks and socat cryptographic vulnerabilities. We'll also explain how we figured out a way to subtly backdoor one of the oldest-in-use and still-considered-secured asymmetric cryptographic construction: **Diffie-Hellman**.

The paper is available on ePrint as well as on NCC Group.