Factoring 512-bit RSA Moduli for Fun (and a Profit of $9,000)

Martin R. Albrecht, Davide Papini, Kenneth G. Paterson, and Ricardo Villanueva-Polanco

Information Security Group
Royal Holloway, University of London**

Abstract. The recent FREAK attack highlighted widespread support for export-grade RSA keys in TLS servers. We present the results of an IPv4-wide survey of TLS servers performed roughly one week after FREAK was announced. We found that only 9.7% of servers now support such export-grade RSA keys. However, we also found that some keys are repeated with high frequency, making each of them an attractive target for a direct factoring attack; one key in particular was repeated 28,394 times. We also computed the pairwise gcds of all the export-grade RSA moduli that we found, leading to 90 factorisations. These moduli correspond to 294 different hosts. The computation took less than 3 minutes on an 8-core system, saving the $9,000 that a cloud computation would have cost if each modulus had been attacked directly. We consider this to be a good return on investment for a Friday afternoon's work.

1 Introduction

The recent FREAK attack[1] showed that export-grade RSA public keys are commonly supported by TLS servers: 26% of servers support such keys according to the FREAK attack authors. These keys are typically 512 bits in size, rendering them individually vulnerable to (cloud-based) factoring using open-source software such as CADO-NFS[2]. However, this approach to factoring is not cost-free — a rough figure of $100 per factorisation has been reported (the exact figure depends on the spot price of cloud computing instances).

With export ciphersuites in TLS, the export-grade RSA keys are not directly certified, but instead are signed by an already certified, normal-strength key. So it is a plausible strategy to generate fresh export-grade keys regularly, in order to mitigate attacks exploiting their weakness. This generation would then typically be done on-device. As already shown in [1], low-end devices such as consumer or small business routers are prone to producing weak RSA keys. So we might expect repeated moduli and shared factors to appear amongst export-grade RSA keys, further reducing the cost of breaking such keys.

** {Martin.Albrecht,Davide.Papini,Kenny.Paterson}@rhul.ac.uk, Ricardo.VillanuevaPolanco.2013@live.rhul.ac.uk

[1] https://www.smacktls.com/.

[2] cado-nfs.gforge.inria.fr

We performed a crawl of the IPv4 address space searching for export-grade RSA public keys, filtered for repeated moduli and then subjected their moduli to a pairwise-gcd attack using the fastgcd software developed by Heninger *et al.*[3]. In doing so, we found large clusters of repeated moduli (up to 28,394 different IPs sharing the same modulus in one instance) and managed to factor 90 of the unique 1,551,168 512-bit RSA moduli that we gathered, corresponding to 294 different hosts (because of modulus repetition). Since we factored these 90 moduli in a matter of minutes using moderate computing infrastructure, we estimate that we saved $9,000 over the direct approach to breaking these particular keys one by one.

2 Scanning

We used the zmap tool[4] with some back-end modifications to scan the IPv4 address space for TLS servers supporting export-grade ciphersuites. Of 22,730,626 hosts supporting TLS that we discovered, 2,215,504 offered export-grade RSA keys (all at 512 bits) when probed. This figure of 9.7% is significantly lower than that observed by the authors of the FREAK attack. This could be attributable to administrators quickly removing export-grade ciphersuites from their server configurations. Note also that the scan reported by Heninger *et al.* in [1] discovered only 85,988 512-bit RSA keys. Presumably their scans did not involve offering any export ciphersuites to servers, or only offered them with low priority.

The scanning took 8 hours, with our code being limited to making at most 4,000 connections in parallel and consuming roughly 250KB/s of network bandwidth.

3 Factoring

We observed 664,336 duplicate moduli in the set of 2,215,504 512-bit moduli obtained from our scanning. One single modulus was found 28,394 times, two further moduli arose more than 1,000 times each and a total of 1,176 moduli were seen 100 times or more each. We did not investigate the high replication rate of these moduli, except for the modulus occurring 28,394 times which corresponds to a router with an SSL VPN module. These repeated moduli would be attractive targets for direct factoring. For example, spending $100 on factoring the most repeated modulus would enable a per-host breaking cost of only 0.3 cents for all the hosts using this modulus.

We removed the duplicates and then used the fastgcd software of Heninger *et al.* to compute the gcds between all the pairs of the 1,551,168 moduli remaining. The whole computation took 167s on eight 3.3Ghz Xeon cores. The computation required less than 2GB of RAM.

[3] `https://factorable.net/resources.html`
[4] `https://zmap.io`

We found 90 moduli for which we recovered a non-trivial prime factor. These correspond to 294 hosts due to modulus duplication. We computed the "graph structure" for these 90 moduli – we labelled the moduli as N_1 to N_{90}, created a graph with vertex set $\{1, \ldots, 90\}$ and added edges (i, j) whenever $\gcd(N_i, N_j) > 1$. The resulting graph consists of a 12-clique, two 6-cliques, a 5-clique, four 4-cliques, five 3-cliques, and 15 isolated edges. The largest of these cliques corresponds to 34 hosts (some of which share moduli) in the IP space belonging to a single organisation.

Acknowledgements

The research of Albrecht was supported by EPSRC Grant EP/L018543/1. The research of Papini was supported by EPSRC Grant EP/K006266/1. The research of Paterson was supported by an EPSRC Leadership Fellowship, EP/H005455/1 and by EPSRC Grant EP/L018543/1. The research of Villanueva-Polanco was supported by COLCIENCIAS.

References

1. N. Heninger, Z. Durumeric, E. Wustrow and J. Alex Halderman, Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. In *Proceedings of the 21th USENIX Security Symposium, Bellevue, WA, USA, August 8-10, 2012*, pp. 205–220.