Proceedings of the
30th USENIX Security Symposium

Errata Slip #1

For the paper "Raccoon Attack: Finding and Exploiting Most-Significant-Bit-Oracles in TLS-DH(E)" by Robert Merget and Marcus Brinkmann, *Ruhr University Bochum*; Nimrod Aviram, *School of Computer Science, Tel Aviv University*; Juraj Somorovsky, *Paderborn University*; Johannes Mittmann, *Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany*; Jörg Schwenk, *Ruhr University Bochum* (Wednesday session, "Cryptography: Attacks," pp. 213–230 of the Proceedings), the authors provide the following correction on page 224. In the original paper, we reported calculation times for repeated measurements of the *same* secret exponent due to a software bug (reported by Sebastian Bach). The corrected calculation times are in the table below.

Original table:

DH group	n	ε	k				
			24	20	16	12	8
RFC 5114	1024	0.532	$\beta = 40, d = 50$ $T = 6s \pm 0s$	$\beta = 40, d = 60$ $T = 10s \pm 1s$	$\beta = 40, d = 80$ $T = 26s \pm 4s$	$\beta = 40, d = 100$ $T = 111s \pm 4s$	$\beta = 60, d = 200$ $T = 9295s \pm 467s$
LibTomCrypt	1036	0.000	$\beta = 40, d = 50$ $T = 6s \pm 0s$	$\beta = 40, d = 60$ $T = 10s \pm 1s$	$\beta = 40, d = 80$ $T = 28s \pm 1s$	$\beta = 40, d = 100$ $T = 52s \pm 5s$	$\beta = 60, d = 180$ $T = 5613s \pm 205s$
SKIP	2048	0.056	$\beta = 40, d = 100$ $T = 112s \pm 5s$	$\beta = 40, d = 120$ $T = 207s \pm 18s$	$\beta = 60, d = 160$ $T = 977s \pm 46s$	$\beta = 60, d = 250$ $T = 13792s \pm 47s$	
RFC 3526	3072	0.000	$\beta = 40, d = 150$ $T = 1243s \pm 59s$	$\beta = 40, d = 190$ $T = 2390s \pm 65s$	$\beta = 60, d = 250$ $T = 27192s \pm 312s$		
RFC 7919	4096	0.000	$\beta = 40, d = 200$ $T = 3601s \pm 6s$	$\beta = 60, d = 250$ $T = 30023s \pm 85s$			

Table 3: Our parameter choices and calculation costs to recover g^{ab} in a Raccoon attack for five well-known DH groups, using BKZ 2.0 with block size β, number of equations d and average calculation time T. We aborted the BKZ reductions as soon as the hidden number was found (up to BKZ loop completion). Each simulation was repeated 8 times with random secrets on a vCPU with 2 GHz clock speed. The bit-size n of the modulus and its bias $\varepsilon = n - \log_2(p)$ are also given. Note that for $k = 8$, we had to use more equations for the RFC 5114 group than for the LibTomCrypt group, mainly due to the larger bias ($\ell = 7.468 \ll 8$).

Corrected table:

DH group	n	ε	k				
			24	20	16	12	8
RFC 5114	1024	0.532	$\beta = 40, d = 50$ $T = 6s \pm 1s$	$\beta = 40, d = 60$ $T = 9s \pm 2s$	$\beta = 40, d = 80$ $T = 26s \pm 5s$	$\beta = 40, d = 100$ $T = 111s \pm 33s$	$\beta = 60, d = 200$ $T = 29881s \pm 26085s$
LibTomCrypt	1036	0.000	$\beta = 40, d = 50$ $T = 5s \pm 1s$	$\beta = 40, d = 60$ $T = 10s \pm 1s$	$\beta = 40, d = 80$ $T = 24s \pm 6s$	$\beta = 40, d = 100$ $T = 63s \pm 11s$	$\beta = 60, d = 180$ $T = 6045s \pm 2101s$
SKIP	2048	0.056	$\beta = 40, d = 100$ $T = 119s \pm 26s$	$\beta = 40, d = 120$ $T = 282s \pm 57s$	$\beta = 60, d = 160$ $T = 1417s \pm 136s$	$\beta = 60, d = 250$ $T = 17369s \pm 1686s$	
RFC 3526	3072	0.000	$\beta = 40, d = 150$ $T = 1120s \pm 96s$	$\beta = 40, d = 190$ $T = 2669s \pm 232s$	$\beta = 60, d = 250$ $T = 32852s \pm 4356s$		
RFC 7919	4096	0.000	$\beta = 40, d = 200$ $T = 5373s \pm 355s$	$\beta = 60, d = 250$ $T = 22551s \pm 2385s$			

Table 3: Our parameter choices and calculation costs to recover g^{ab} in a Raccoon attack for five well-known DH groups, using BKZ 2.0 with block size β, number of equations d and average calculation time T. We aborted the BKZ reductions as soon as the hidden number was found (up to BKZ loop completion). Each simulation was repeated 16 times with random secret† on a vCPU with 2 GHz clock speed. The bit-size n of the modulus and its bias $\varepsilon = n - \log_2(p)$ are also given. Note that for $k = 8$, we had to use more equations for the RFC 5114 group than for the LibTomCrypt group, mainly due to the larger bias ($\ell = 7.468 \ll 8$).