Proceedings of the 33rd USENIX Security Symposium

Errata Slip #2

For the paper "With Great Power Come Great Side Channels: Statistical Timing Side-Channel Analyses with Bounded Type-1 Errors" by Martin Dunsche, Marcel Maehren, and Nurullah Erinola, *Ruhr University Bochum*; Robert Merget, *Technology Innovation Institute*; Nicolai Bissantz, *Ruhr University Bochum*; Juraj Somorovsky, *Paderborn University*; Jörg Schwenk, *Ruhr University Bochum* (Friday session, "Crypto VIII: Side Channel", pp. 6686–6704 of the Proceedings), the authors provide the following correction on pages 6689 and 6699. In the original paper, we reported a timing vulnerability in NSS as exploitable. While this was initially confirmed by the NSS developers, a subsequent discussion led to the conclusion that the timing leaks do not enable an attacker to mount a Bleichenbacher attack.

Original Contribution Claim #4 (Section 1, p. 6689)

- We verify our results in the newest version of the analyzed libraries through manual code review. Our tool could detect eight potential attacks, of which we could pinpoint seven to specific locations in the code, resulting in three Vaudenay Padding Oracle vulnerabilities, three Bleichenbacher vulnerabilities, and two Lucky13 vulnerabilities (cf. Section 7).

Corrected Contribution Claim #4 (Section 1, p. 6689)

- We verify our results in the newest version of the analyzed libraries through manual code review. Our tool could detect eight potential attacks, of which we could pinpoint seven to specific locations in the code, resulting in three Vaudenay Padding Oracle vulnerabilities, two Bleichenbacher vulnerabilities, and two Lucky13 vulnerabilities (cf. Section 7).

Original Paragraph (Section 7.2, p. 6699)

Vulnerabilities in NSS For NSS, RTLF indicated grave timing differences between Bleichenbacher vectors. Our analysis found that the code for RSA key exchanges is not written to run in constant time. NSS is mostly used in client implementations (e.g., in Mozilla's Firefox or Thunderbird), limiting the impact of this vulnerability. Mozilla has confirmed the vulnerability and is preparing a patch to address the issue.

Corrected Paragraph (Section 7.2, p. 6699)

Timing Differences in NSS For NSS, RTLF indicated grave timing differences between Bleichenbacher vectors. Our analysis found that the code for RSA key exchanges is not written to run in constant time. In our report for this issue, Mozilla initially confirmed the vulnerability. However, in a later discussion of our report, Robert Relyea pointed out that the identified timing differences do not enable an attacker to successfully mount a Bleichenbacher attack. While the timing differences exist, an attacker is unable to identify specific padding error cases.