The evolution of the "Lucky Thirteen" attack from its inception to its cross-VM applicability and further to the exposure of pseudo constant time countermeasures' inadequacies underscores a critical narrative in cryptographic research. It highlights the continuous arms race between attack methodologies and cryptographic defenses, emphasizing the need for constant vigilance, rigorous security analysis, and the adoption of robust countermeasures to protect against evolving threats. The collective contributions of these studies not only advance our understanding of specific vulnerabilities in TLS and DTLS protocols but also contribute broadly to the field of cryptographic security, offering invaluable insights into the design and implementation of secure cryptographic systems in an increasingly interconnected and virtualized world.

**Original Lucky 13 attack**

A major cryptographic flaw in the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols is discovered and thoroughly examined in the "Lucky Thirteen Attack" by Nadhem J. AlFardan and Kenneth G. Paterson the vulnerability pertains to the handling of padding and Message Authentication Code (MAC) verification in CBC-mode encryption within these protocols. This attack exploits minute, yet exploitable, timing discrepancies in the padding and MAC (Message Authentication Code) verification processes. The essence of the "Lucky Thirteen" lies in its ability to discern between correct and incorrect padding through careful timing analysis, thus creating a channel for leakage of plaintext information. This vulnerability stems from the protocol's structural design, where decryption, padding validation, and MAC verification occur in a sequence that inadvertently reveals critical information through timing variances. AlFardan and Paterson's work was not only seminal in identifying this vulnerability but also in demonstrating the practical feasibility of such timing attacks against real-world implementations, notably OpenSSL.[1]

A diagram of data processing

Description automatically generatedFigure 1: Encryption and authentication in the TLS record protocol when using HMAC and a block cipher in CBC mode.

**The Cross-VM Setting Enhancement**

Building upon the "Lucky Thirteen" framework, Irazoqui et al. expanded the attack vector to a cross-VM (Virtual Machine) setting, demonstrating the viability of executing the "Lucky Thirteen" attack in cloud environments. This modification leveraged the FLUSH+RELOAD cache timing technique, showcasing that the attack could be potentiated in a shared hardware context, particularly on deduplication-enabled platforms. The significance of this work lies in its exploration of side-channel attacks in a virtualized environment, a common setup for cloud services, thereby amplifying the real-world implications of the "Lucky Thirteen" attack. Irazoqui et al.'s contribution was crucial in illustrating the broader applicability and potential risks of the attack, especially in the increasingly prevalent cloud computing landscapes.[2]

**"Pseudo Constant Time Implementations Are Only Pseudo Secure"**

Ronen, Paterson, and Shamir's contribution further advances the understanding of the "Lucky Thirteen" attack by revealing vulnerabilities in the pseudo constant time countermeasures adopted by various TLS implementations (Amazon’s s2n, GnuTLS, mbed TLS, and wolfSSL) against CBC-mode attacks. This study introduces three new attack types that exploit these vulnerabilities, demonstrating that these countermeasures are inadequate for ensuring real security. The attacks employ variations of the PRIME+PROBE cache timing technique, coupled with an innovative extension of the original "Lucky Thirteen" attack, to achieve plaintext recovery under a cross-VM attack setting. This work is particularly illuminating in its systematic uncovering of implementation bugs across several major TLS libraries, emphasizing the inherent challenges in crafting secure pseudo constant time countermeasures. The conclusion drawn is unequivocal in advocating for truly constant-time processing as an essential defense against timing and cache-based attacks, underscoring the necessity of rigorous, security-first approaches in cryptographic protocol implementations.[3]

# References

**There are no sources in the current document.**

|  |
| --- |
|  |
| 1. Al Fardan, Nadhem J., and Kenneth G. Paterson. "Lucky thirteen: Breaking the TLS and DTLS record protocols." *2013 IEEE symposium on security and privacy*. IEEE, 2013. 2. Irazoqui, Gorka, et al. "Lucky 13 strikes back." Proceedings of the 10th acm symposium on information, computer and communications security. 2015. 3. Ronen, Eyal, Kenneth G. Paterson, and Adi Shamir. "Pseudo constant time implementations of TLS are only pseudo secure." Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018. |
| APA |  |