Nomination Statement for Video-based Cryptanalysis (S&P'24)

Over the past three decades since the first cryptanalytic timing side-channel attack was discovered (Kocher et al., 1996), the scientific community has explored numerous channels attackers could exploit for cryptanalytic side-channel attacks. These include the power channel (Kocher et al., 1999), the EMR channel (Agrawal et al., 2002), the optical channel (Ferrigno et al., 2008), and the acoustic channel (Genkin et al., 2013).

However, exploiting these channels has traditionally required **specialized hardware** (e.g., oscilloscopes, ultrasonic microphones, software-defined radios, photodiodes) and **advanced expertise** in digital signal processing. Consequently, cryptanalysis was largely confined to **state actors** or highly skilled academic researchers. This led to the prevailing belief that cryptanalytic side-channel attacks posed a low risk to average organizations or individuals, as they were deemed **impractical for non-state actors**.

The advent of Video-based cryptanalysis (Nassi et al., 2024) has fundamentally challenged this notion. It demonstrated that cryptanalytic side-channel attacks could have been performed for years using **ubiquitous devices** such as smartphone cameras or hijacked IP cameras, with **far lower technical expertise** required (e.g., basic video processing skills). Specifically, video-based cryptanalysis leveraged the rolling shutter effect of standard video cameras and exploited a device's power LED as a visual indicator of power consumption. By recording a device's power LED and ensuring the LED filled the camera frame, attackers achieved a sampling rate of 60,000 measurements per second. This capability threatens IoT devices with constrained CPU rates, such as smartcards and smartphones.

This observation allowed the researchers to replicate two recent attacks using this method:

1. Minerva Attack (Jancar et al., 2020)**:** Extracted a 256-bit ECDSA key from a smartcard by recording the power LED of the smartcard reader via an IP camera—without requiring malware, unlike the original attack. This scenario was demonstrated on six different smartcard readers that researchers purchased from Amazon.
2. HerzBleed Attack (Wang et al., 2022)**:** Recovered a 378-bit SIKE key from a Samsung Galaxy device by recording the power LED of USB speakers connected to a USB hub used to charge the Samsung, using an iPhone 13 Pro Max's video camera.

By presenting a **practical**, **low-cost** threat model that could be applied **remotely** (using an IP camera), video-based cryptanalysis demonstrated that the risk of cryptanalytic side-channel attacks is significantly higher than previously believed. Moreover, the expected improvements in video camera capabilities (e.g., higher color depth, faster shutter speeds) and the increased proliferation of IoT devices with limited CPU capacities will likely exacerbate this risk over time.

This work calls for a reassessment of the threat landscape by the scientific community and industry, emphasizing the need to protect information confidentiality. In light of its profound implications and practical impact, I wholeheartedly nominate this paper for the 2024 NSA's Best Scientific Cybersecurity Paper Competition.

Ron Bitton Principal AI/GenAI Security Researcher at Intuit