2025 Best Scientific Cybersecurity Paper Competition
Nomination Statement for:

ProvCam: A Camera Module with Self-Contained TCB for Producing Verifiable Videos
ACM Mobicom'24

In recent years, the Internet (especially social networks) is inundated with growing numbers of bogus or doctored visual content -- deep-fake photos and videos. While some are exposed, the majority go unnoticed and are unfortunately considered real, resulting in either blind trust or blanket mistrust by users of potentially dubious content. The situation is so dire in part because of rapid advances in photo/video manipulation techniques, including generative AI. Curiously, the very same advances also help deep-fake detection techniques. This results in the familiar and seemingly never-ending "arms race" between state-of-the-art technologies that create and detect deep-fakes. This race is unlikely to be won by the latter, for at least two reasons: (1) if we look at the history of malware detection for an apt analogy, malware authors are always at least a tiny bit ahead of malware detectors, and (2) however effective, deep-fake detection techniques lack the fundamental means of providing solid/credible evidence of detecting a fake, i.e., detection is often probabilistic.

The nominated paper takes a very different preventative approach: it envisions a world where, to be considered genuine, a visual content must be strongly authenticated and integrity-protected from its genesis, i.e., from the moment when analog input is initially digitized. Specifically, this paper constructs an elegant and novel secure camera architecture, called ProvCam, which generates a cryptographic proof of video authenticity. At the core of ProvCam is a small Trusted Computing Base (TCB) that prevents any tampering during all processing steps between initial (analog) photo/video capture by the camera sensor and the generation of digital video output. The viability and practicality of ProvCam is illustrated via a fully functional prototype using a commodity Xilinx FPGA evaluation board. Based on extensive measurements, the nominated paper shows that ProvCam incurs fairly low computational, energy, and hardware overheads, and has no impact on throughput. Although some small hardware changes are required, they are limited to only one ProvCam hardware component: the secure camera sensor. On the other hand, ProvCam uses a unique approach for its software stack and does not impact the software of current cameras. Its hybrid (hardware/software) design makes ProvCam easy to adopt by camera-equipped devices, such as smartphones.

While the ProvCam architecture is not a panacea (e.g., it only works with compliant cameras), it represents a significant technical and scientific advance by showcasing a practical and secure means of producing and recognizing trustworthy (authentic) visual content.