

# "Theoretical Technique to Abuse EMV Cards Detected Used in the Real World"

Submitted by [grigby1](#) on Fri, 07/31/2020 - 12:40pm

Researchers from Cyber R&D Lab conducted an experiment in which they examined how 11 banks from the US, the UK, and the EU implement EMV (Europay, Mastercard, and Visa) chip cards on their networks. The researchers used tools similar to those used by cybercriminal groups to copy information from EMV cards and their magnetic stripes. The data copied from the EMV card was then used to create a magnetic stripe version of the same card but without the chip. This technique, known as EMV-Bypass Cloning, was first described in 2008. However, fears surrounding this technique's abuse had been dismissed due to the expectation of banks to move all users to EMV cards and remove magstripe cards. Banks have not met these expectations or performed a set of security checks before approving inter-technology payments. Therefore, the loop first described in 2018 remains. A report recently published by the security firm Gemini Advisory reveals that the EMV-Bypass Cloning technique has been abused in the wild this year. This article continues to discuss new research on the EMV-Bypass Cloning method and evidence showing the abuse of this technique by criminals.

[ZDNet reports "Theoretical Technique to Abuse EMV Cards Detected Used in the Real World"](#)

---