1530 - Exploiting 0ld Mag-stripe information with New technology

Thursday at 15:30 in 101 Track 2
20 minutes | Demo, Tool, Exploit
Salvador Mendoza*Hacker*

A massive attack against old magnetic stripe information could be executed with precision implementing new technology. In the past, a malicious individual could spoof magstripe data but in a slow and difficult way. Also brute force attacks were tedious and time-consuming. Technology like Bluetooth could be used today to make a persistent attack in multiple magnetic card readers at the same time with audio spoof.

Private companies, banks, trains, subways, hotels, schools and many others services are still using magstripe information to even make monetary transactions, authorize access or to generate "new" protocols like MST(Magnetic Secure Transmission) During decades the exploitation of magstripe information was an acceptable risk for many companies because the difficulty to achieve massive attacks simultaneously was not factible. But today is different.

Transmitting magstripe information in audio files is the faster and easier way to make a cross-platform magstripe spoofer. But how an attacker could transmit the audio spoof information to many magnetic card readers at the same time? In this talk, we will discuss how an attacker could send specific data or achieve a magstripe jammer for credit card terminals, PoS or any card reader. Also, how it could be implemented to generate brute force attacks against hotel door locks or tokenization processes as examples.
Salvador Mendoza
Salvador Mendoza is a security researcher focusing in tokenization processes, mag-stripe information and embedded prototypes. He has presented on tokenization flaws and payment methods at Black Hat USA, DEF CON, DerbyCon, Ekoparty, BugCON and Troopers. Salvador designed different tools to pentest mag-stripe and tokenization processes. In his designed toolset includes MagSpoofPI, JamSpay, TokenGet and lately SamyKam.

@Netxing
Blog: salmg.net

#defcon25/by_track/101-Track2/Thursday #defcon25/By_Day/_thursday