Bypassing disk encryption

Bypassing Local Windows Authentication To Defeat Full Disk Encryption

In 2007, starting with Windows Vista, Microsoft began shipping a full disk encryption feature named BitLocker with professional and enterprise versions of Windows. Full disk encryption helps protect users from threats that include physical access. This can, for example, prevent the exposure of proprietary information and account credentials if a company laptop is lost, stolen, or even left temporarily accessible to an attacker.

Under the hood, BitLocker uses a system's Trusted Platform Module (TPM) to store the secret key used for full disk encryption, and is able to use the features of the TPM to safely provide transparent, password-less decryption of the disk on boot. Because BitLocker can work transparently without any extra passwords or prompts on boot, many enterprises have opted to enable this form of full disk encryption as a part of their data loss prevention strategy.

This session by Ian Haken, presented at Black Hat 2016 demonstrates how one can abuse physical access in order to bypass Windows authentication thus accessing all of a user's data even when the disk is fully encrypted by BitLocker. This platform-independent attack effectively bypasses all of the protection offered by BitLocker, reliably and quickly allowing an attacker to retrieve all of the sensitive data on the machine, all without having to perform any cryptographic brute-forcing or hardware manipulation.

---

bypassing-local-windows-authentication-to-defeat-full-disk-encryption.mp4

Bypassing of Self-Encrypting Drives

Full-Disk Encryption (FDE) solutions are used by both legitimate enterprises and “unlawful individuals” to protect the disclosure of sensitive data at rest. Hardware-based FDE, known as Self-Encrypting Drives (SED), have taken the market by storm and are advertised as being more secure and as having zero overhead. This session by Daniel Boteanu presented at B Sides Calgary 2016 explores SED solutions and fundamental security issues with the current state of the standards that can be used to bypass the encryption and access the data on protected drives.

---

bypassing-of-self-encrypting-drives.mp4

---

forensics, disk, filesystem, windows, encryption, bypass, bypassing, sessions, conferences