Master-Projekt
Wintersemester 2017/18

Hack
Grid

Komplexe
Softwaresysteme

HSB
Hochschule Bremen
City University
of Applied Sciences

WEBCAM HACKING

Nichts ist angenehmer, als ein bewegtes Bild zu einer Stimme zu erhalten. Doch eine Webcam bringt auch einige Risiken mit sich. Etwa wenn der eigene PC gehackt wurde und die Webcam zum Spionage-Tool wird. In diesem Szenario wird eine Webcam Attacke auf eine fiktive Person inszeniert, um diese auszuspionieren. Ziel ist es, sich unbemerkt Zugriff auf ein fremdes Gerät zu beschaffen. Dies wird durch die Verwendung einer manipulierten Datei ermöglicht.

FireTV REMOTE

Viele Haushalte dürften einen Amazon FireTV bei sich zuhause haben. Dazu gehört außerdem eine Sprachfernbedienung, die ein Mikrofon enthält. Die Verbindung mit dem FireTV wird per WiFi-Direct aufgebaut. Nun stellt sich natürlich die Frage, wie sicher diese Fernbedienung gegen Manipulations-versuche von außen ist. Es werden die einzelnen Soft- und Hardwarekomponenten auf mögliche Angriffsvektoren untersucht. Besondere Aufmerksamkeit wird dabei dem NAND-Flashspeicher gewidmet, aus dem die Firmware extrahiert werden soll. Im nächsten Schritt wird der Versuch unternommen, eine manipulierte Firmware aufzuspielen.

TPM

Eingebettete Systeme stellen eine besondere Herausforderung an die Softwaresicherheit für deren Entwickler dar. Die Systeme können vertrauliche Daten enthalten, die zur Verwendung benötigt werden, aber vom Nutzer nicht einsehbar sein sollten. Bei diesen Daten kann es sich z.B. um private Schlüssel zur Authentifizierung gegenüber eines Updateservers oder Lizenzschlüssel handeln. Ein Ansatz zum Schutz dieser Daten ist die Verwendung eines Trusted Platform Modules (TPM). In diesem Szenario wird die Kommunikation zwischen TPM und CPU angegriffen um an die geschützten Informationen zu gelangen.

VoIP

In vielen Unternehmen, aber zunehmend auch in Privathaushalten werden klassische Telefonanlagen durch IP-basierte Systeme ersetzt. Neben Vorteilen wie geringeren Kosten im Vergleich zur Analogtechnik birgt die IP-Telefonie jedoch auch Gefahren, da sie durch gängige Cyberattacken angreifbar ist.
In diesem Projekt soll ein Man-In-The-Middle-Angriff auf ein VoIP-System ausgeführt werden, bei dem ein Telefonat nicht nur durch einen Angreifer abgehört, sondern auch über das Injizieren von zusätzlichen Audiodaten manipuliert wird. Mithilfe von Verschlüsselungsmethoden soll daraufhin das System gegen derartige Attacken abgesichert werden.

SPS

Das Szenario baut auf ein S7-Passwort Bruteforce-Tool auf. Dieses benötigt einen Wireshark Mitschnitt der Kommunikation zwischen TIA-Portal und SPS. Beinhaltet der Mitschnitt eine Passwortauthentifikation, extrahiert das Tool den Hash-Wert des Passwortes und gibt diesen aus. Es lässt per Bruteforce oder Rainbowtable das ursprüngliche Passwort ermittel. Das S7-Passwort Bruteforce-Tool stammt aus dem Jahr 2013. Es wird eine aktuelle SPS betrachtet und untersucht, wie das Passwort übertragen wird und ob es noch möglich ist dieses zu knacken.

TEILNEHMER

André Weiner, Arndt Balfanz, Steffen Christiansen,
Tolga Özer, Torben Woltjen

Betreuer: Prof.Dr.Sethmann