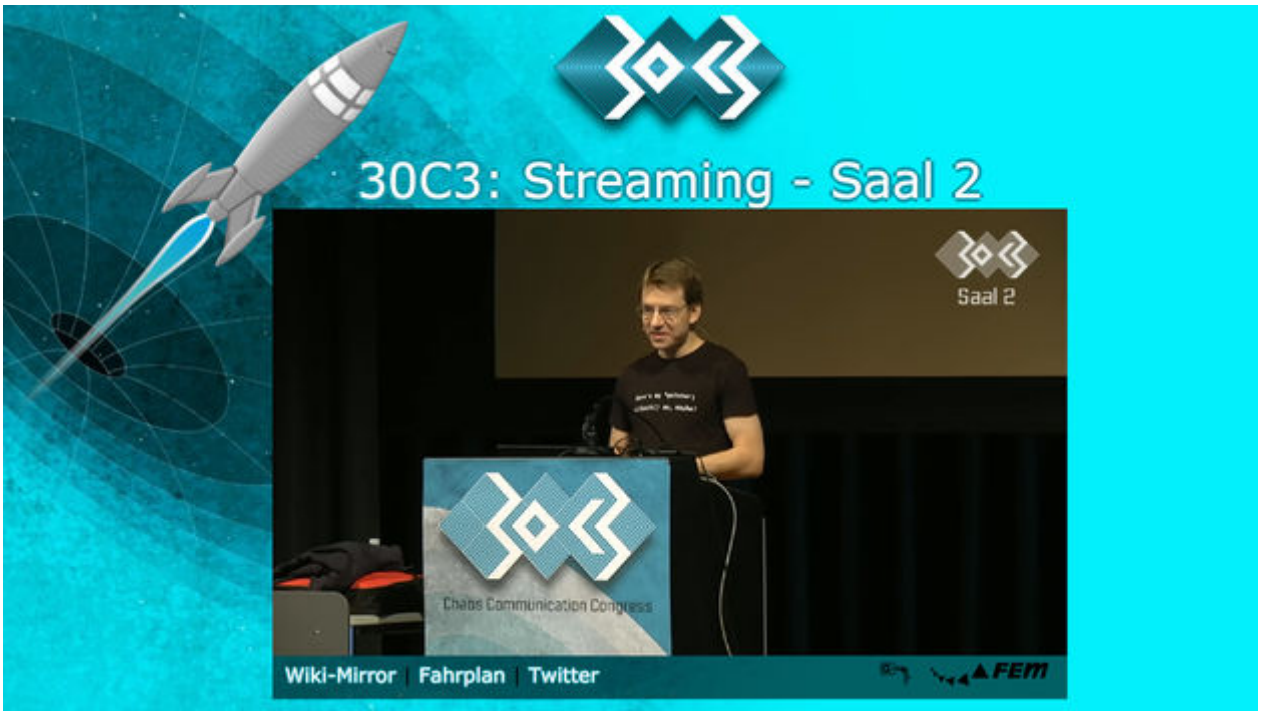
Quelle: futurezone.at
Adresse: http://futurezone.at/science/forscher-knackt-rfid-zutrittssystem-via-skipass/43.174.691
Datum: 29.12.2013, 19:42

30C3

Forscher knackt RFID-Zutrittssystem via Skipass

Der Wiener Sicherheitsforscher Adrian Dabrowski hat beim Hackerkongress 30C3 in Hamburg eine gravierende Sicherheitslücke beim RFID-Zutrittssystem der Firma Begeh aufgezeigt.

Autor: Mag. Barbara Wimmer



Adrian Dabrowski bei seinem Talk am 30C3-Kongress. - Foto: Screenshot CCC-Livestream

Die österreichische Firma Begeh wirbt bei ihrem Zutrittssystemen damit, dass sie sicherer als herkömmliche mechanische Zutrittssysteme zu Wohnhäusern oder Bürogebäuden sind. Überfälle in Stiegenhäusern, unerwünschte Werbung, nächtliche nicht sesshafte Gäste sollen das Haus nicht betreten können, weil das Zutrittssystem von Begeh nicht mit einem herkömmlichen Postschlüssel, der sich relativ einfach besorgen lässt, geöffnet werden kann, heißt es.

Stattdessen wird zum Öffnen der Haustür eine Begeh-Card erforderlich, die vor die Begeh-Antenne auf der Sprechanalage gehalten werden muss. Dahinter steckt laut eigenen Angaben eine RFID-Technologie, die mit einer Transponderfrequenz von 13,56 MHz arbeitet und die dem internationalen Standard ISO 15693 entspricht. Ist die Begeh-Card des Hausbewohners oder Büromitarbeiters autorisiert, öffnet sich beim kontaktlosen Hinhalten der Karte automatisch die Tür.

Geknackt mit Skipass

Der Wiener Sicherheitsforscher Dabrowski, der für SBA Research arbeitet, hat nun am

Hackerkongress 30C3 erklärt, dass er das System mit einfachen, kostengünstigen Mitteln - natürlich ausschließlich zu Demonstrationszwecken - knacken konnte. Dazu baute er einen Midrange-Reader, den er sich in einem Post-Paket an sich selbst geschickt hat und der ihm das Auslesen des Begeh-Systems ermöglicht hat.

Dabrowski probierte in seiner Heimatstadt Wien, in der das System bereits bei rund 16 Prozent der Wohnhäuser zum Einsatz kommt, im Anschluss mit zwei unterschiedlichen Methoden die Türen zu öffnen. 43 Prozent der Installationen ließen sich mit einem alten, umprogrammierten Skipass knacken, der die herkömmliche Nutzerkarte eines Hausbewohners simulierte.

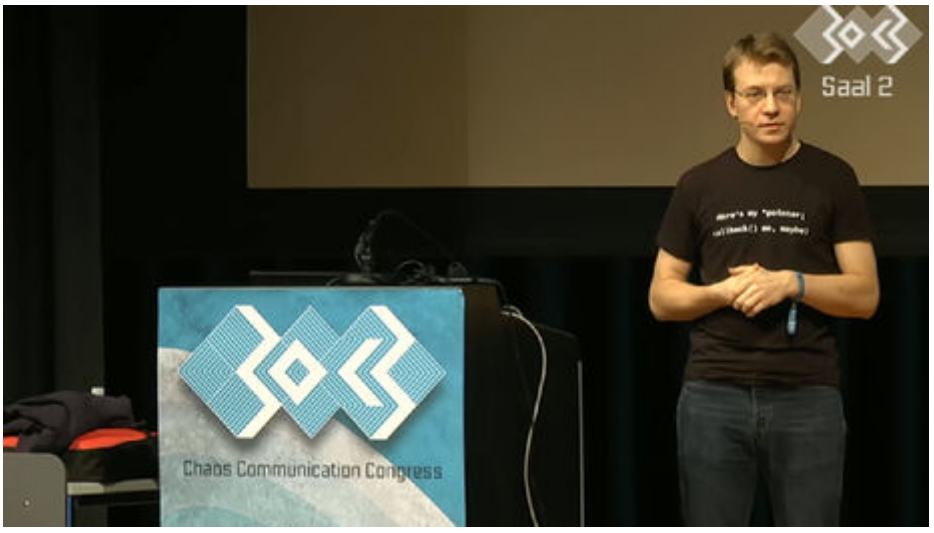


Foto: Screenshot CCC-Livestream

"Die Kosten für diese Aktion: Zwei Euro Deposit vom Skiresort deiner Wahl", so Dabrowski. Natürlich musste der Skipass entsprechend umprogrammiert werden, damit er auch die Begeh-Türen öffnen konnte. Dazu entwickelte Dabrowski eine Android-App für NFC-Smartphones. Die Erfolgsrate, das Zutrittsystem mit einem selbst gebauten Kartensimulator zu öffnen, lag noch wesentlich höher: bei 93 Prozent. Um einen solchen zu bauen, braucht man laut Dabrowski ebenfalls weniger als 20 Euro.

Nicht sicherer als Schlüssel

Der Sicherheitsforscher will mit dieser Aktion beweisen, dass digitale Systeme wie das Begeh-Zutrittsystem in der Regel nicht sicherer sind als mechanische Systeme. "Es gibt keine zusätzliche Sicherheit, die uns der Hersteller verkaufen möchte", so Dabrowksi bei seinem Vortrag. Um bei seinem Versuch, die Türen zu öffnen, möglichst unauffällig zu wirken, legte er sich eine Techniker-Jacke zu. "Doch niemanden hat meine Anwesenheit interessiert", so Dabrowski.

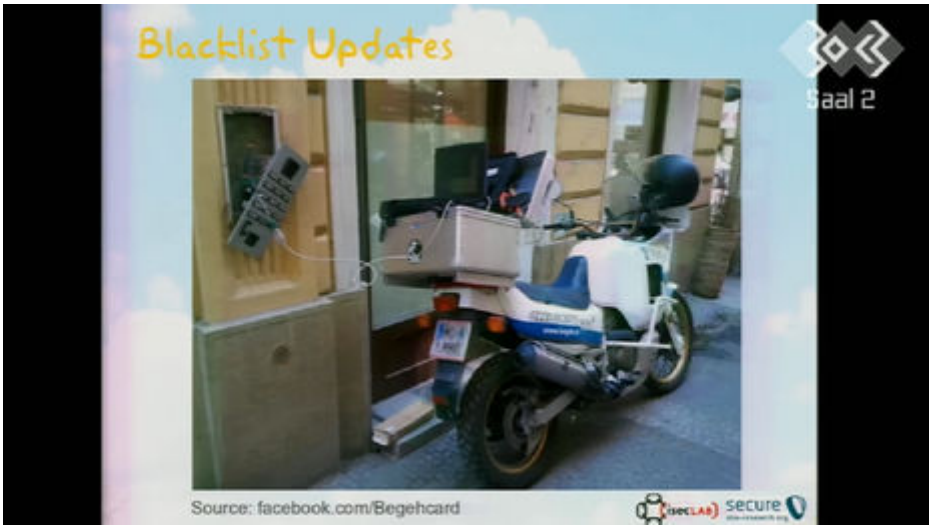


Foto: Screenshot CCC-Livestream

Er meldete die gravierende Sicherheitslücke, die er entdeckt hatte, via Cert.at dem Hersteller der Zutrittssysteme. Als einzige Reaktion seitens Begeh sei zurückgekommen, dass man sich nicht vorstellen könne, dass ein unabhängiger Sicherheitsexperte hinter der Aufdeckung dieser Lücke stecke. Begeh-Kunden sei daher geraten, nicht zu erwarten, dass das Sicherheitssystem wirklich besser sei als das bei einem herkömmlichen, mechanischen Schlüssel. Auch das Begeh-System lässt sich austricksen.

Dem Hersteller des Zutrittssystem empfiehlt Dabrowski neben dem Fix der Sicherheitslücke auch den Einbau eines GSM-Moduls, um Updates künftig zügig und regelmäßig durchführen zu können. Derzeit verspricht der Hersteller nämlich nur Kunden eines Premium-Produkts ein jährliches Update von Blacklists. Dadurch bleiben die Systeme für einen relativ langen Zeitraum mit einer einzigen Methode angreifbar. Auf der Facebook-Website des Herstellers fand Dabrowski zum Blacklist-Updating zudem ein Bild eines Laptops, der während des Update-Vorgangs sehr dubios vewahrt wurde (siehe Bild). Premium-Security schaut in der Tat anders aus.

(FUTUREZONE) ERSTELLT AM 29.12.2013, 16:00

Stichworte: Sicherheit, Sicherheitsexperten, RFID, chas computer club,