Inteligentné zámky

Za inteligentne zámky považujeme zámky a uzamykacie systémy, ktoré obsahujú elektronický komponent, umožňujúci odomknutie zámku. Za inteligentný zámok teda nepovažujeme napr. mechanický zámok s elektronickým alarmom, ktorý sa aktivuje keď deteguje manipuláciu.

Rozdelenie inteligentných zámkov

Inteligentné zámky sa dajú zaradiť do viacerých kategórií podľa základných vlastností. Na prvý pohľad najvýraznejším je spôsob, akým bránia otvoreniu dverí.

Prvou kategóriou sú zámky, ktoré sa nainštalujú na existujúci mechanický zámok, a zamykanie je riešené štandardnými mechanickými elementami. Takáto konfigurácia často umožňuje ponechanie fyzického kľúča, ako metódy na otvorenie dverí, alebo ako zálohy v prípade zlyhania elektroniky.

Do druhej kategórie patria zámky, ktoré využívajú elektromechanické elementy. Jedným typickým riešením tohoto druhu je elektromechanická západka. Západka mechanicky bráni pohybu elementu pripevneného ku dverám, a keď dostane pokyn otvoriť, odblokuje sa typicky pomocou elektromagnetických solenoidov.

Finálnym typom je plne elektrický zámok, ktorý na blokovanie dverí používa elektromagnety. K dverám je pevne pripevnený kus feromagnetického kovu, ktorý pri zavretí príde do kontaktu s elektromagnetom, keď ten je aktívny silne bráni pohybu dverí.

Zámky sa tiež dajú deliť podľa podporovaných metód otvárania a komunikácie, v mnohých prípadoch je podporovaných metód viac ako jedna.

Otváranie je často dostupné numerickým alebo iným kódom, prípadne čítačkou odtlačkov prstov. Pre odomykanie pomocou iného hardwaru sú potom

podporované rôzne metódy komunikácie, typicky Bluetooth, jeho low energy varianta, NFC, Wi-Fi a mnohé iné. Komunikácia typicky prebieha medzi zámkom a hardwarovým tokenom, ako napr. RFID čipom, alebo zámkom a nejakou aplikáciou pre mobilné zariadenia.

Prieskumy o inteligentných zámkoch a zariadeniach

V posledných rokoch bolo vykonaných viacero prieskumov verejnej mienky o inteligentných zámkoch. Ako zákazník vníma schopnosti systému je kritické pre posúdenie kvality, keďže precenenie zámku môže viesť k značným škodám.

Jedným z týchto prieskumov je Smart home security report 2016, vykonaný spoločnosťou IFSEC Global a sponzorovaný ASSA Abloy. Prieskum bol vykonaný na potenciálnych zákazníkoch z Európy, Blízkeho východu a Afriky, zameriavajúc sa na otázky požadovanej funkcionality. Vyše polovica opýtaných bola vo veku 30 až 50 rokov, väčšina ostatných nad 50 rokov. Nadpolovičná väčšina tiež žije v domácnosti s aspoň 3 ďalšími ľuďmi, pričom 90% opýtaných má partnera.

Až 99% sa vyjadrilo, že bezpečnosť je aspoň trochu dôležitá, pričom 90% ju označilo za veľmi dôležitú. Takmer tri štvrtiny opýtaných sa následne vyjadrilo, že je tiež veľmi dôležité mať možnosť otvoriť dvere mechanicky pri zlyhaní elektroniky. Len 4% toto nepovažovali za dôležité vôbec. Tretia najžiadanejšia vlastnosť bola kvalita kontroly práv a prístupu, ktorá bola veľmi dôležitá pre 65% opýtaných.

Aj najmenej žiadaná vlastnosť, možnosť ovládať a nastavovať zámok na diaľku pomocou notebooku a podobných zariadení, mala 50% hodnotenie ako veľmi dôležitá. Len 13% ju považovalo za nepodstatnú, pre ostatné vlastnosti to spravidla nebolo viac ako 10%.

Užívatelia mohli tiež navrhnúť vlastnosti, ktoré neboli spomenuté, pričom viacerí mali rozumné pripomienky. Napríklad kvalita batéria ako zálohy pri výpadku

elektrickej siete, odolnosť voči vandalizmu, varovanie pri použití záložného mechanického kľúča a podobne.

Ďalšia séria otázok sa sústredila na porovnanie s tradičnými mechanickými zámkami. Porovnávané elementy boli smart karta, PIN kód, smartphone aplikácia a diaľkové ovládanie vo forme prívesku na kľúče. Vo všetkých kategóriách boli ako bezpečnejšie vyhodnotené elektronické systémy. Smart karta mala najväčší rozdiel medzi opýtanými, ktorí ju považovali za bezpečnejšiu, a opýtanými, ktorí ju považovali za menej bezpečnú. Diaľkové ovládanie malo najväčší podiel opýtaných, ktorí ho ohodnotili ako rovnako bezpečné ako tradičný kľúč, až 40%. Mnohí opýtaní sa vyjadrili, že sú neistý, a že odpoveď závisí na mnohých premenných. Viacerí sa taktiež zamýšľali nad bezpečnosťou kombinácie technológií, buď ako paralelné možnosti, alebo ako viacfaktorová autentizácia.

Ďalšia otázka sa zamerala na funkcionalitu mobilnej aplikácie pre zámok, kde mali opýtaní vyhodnotiť relatívnu dôležitosť funkcionalít. Výsledky boli veľmi tesné pre všetky funkcie, tesným víťazom bola notifikácia pri otvorení dverí. S malým rozdielom nasledovalo zistenie stavu dverí na diaľku, pridávanie a odoberanie prístupových práv na diaľku, a tesne posledné bolo odomykanie dverí.

Nasledujúca otázka sa sústredila na riadenie prístupových práv. Najpopulárnejšia možnosť, vyše 60%, bola kombinácia ovládania cez aplikáciu a cez samotné zariadenie. Z možností, kde funguje len jeden z týchto prístupov, bola preferovaná aplikácia, aj keď niektorí opýtaní sa vyjadrili, že ju považujú za potenciálny bezpečnostný risk.

Čo sa týka inštalácie, väčšina opýtaných sa vyjadrila, že preferujú jednoduchú inštaláciu, ktorú potenciálne vedia vykonať svojpomocne. Niečo vyše polovica by tiež ocenila inštaláciu bez nutnosti úprav dverí ako vŕtanie dier a podobne. Pre nainštalovaný zámok si až 40% myslí, že batérie vydržia aspoň 1 rok, a 20% že

aspoň 2 roky. Len 16% odhaduje výdrž na 6 mesiacov a menej. Typovo je mierne preferované použitie dobíjateľných batérií, takto sa vyjadrilo 57% opýtaných.

Takmer tretine opýtaných nezáleží na type predajní, kde by takýto zámok kúpili, asi štvrtina by preferovala konkrétne predajcu smart home prvkov. Len 14% by si inteligentný zámok chcelo kúpiť u profesionálneho zámočníka. Zvyšný opýtaný by podobným dielom nakupovali buď cez internet, v železiarstve, alebo u predajcov domácej elektroniky. Za základný inteligentný zámok by asi dve tretiny boli ochotné zaplatiť do 100 dolárov, pri možnosti nastavovania cez aplikáciu je takmer polovica ochotná zaplatiť 100 až 200 dolárov.

Druhá štúdia, ktorá sa zaoberá bezpečnosťou domácej elektroniky pripojenej k internetu, je Avast Smart home security report 2019. Táto štúdia sa prevažne zaoberá zariadeniami pripojenými k internetu, medzi ktoré patria aj mnohé inteligentné zámky. Avast získal dáta pomocou automatického skenovania zariadení, hľadajúc zariadenia s prednastavenými heslami od výrobcu a chýbajúcimi bezpečnostnými záplatami. Skenovanie bolo vykonané koncom roka 2018, preskenovaných bolo 16 miliónov domácich sietí, ktoré tvorilo spolu 56 miliónov zariadení.

Podľa výsledkov štúdie vyše tretina domácností s inteligentnými zariadeniami má aspoň jedno zraniteľné. Výsledky sú tiež rozdelené podľa krajiny, kde najhoršie dopadla India s vyše 50% zraniteľnosťou, Slovensko skončilo ôsme so 42%.

Takmer 70% zariadení, ktoré boli zraniteľné, mali slabé heslá zvyšným 30% chýbali bezpečnostné záplaty. V mnohých prípadoch bol jedným zo zraniteľných zariadení router. Toto je veľmi podstatná informácia aj pre inteligentné zámky, ktoré na diaľku komunikujú cez internet. Ako vieme zo štúdie z 2016, toto je tiež relatívne želaná vlastnosť, systém teda skutočne musí byť navrhnutý pre bezpečnosť aj pri kompromitácii siete, do ktorej je pripojený.

Ďalšia relevantná štúdia je Consumer Attitudes Towards IoT Security, vykonaná Ipsos MORI na žiadosť britskej vlády.

Podľa tejto štúdie len 20% majiteľov nových smart zariadení skontroluje, či zariadenie nemá prednastavené heslo rovnaké pre všetky kusy. 90% z nich následne takéto heslo zmenia.

Takmer 85% opýtaných súhlasí, že reťaz dodávateľov by mala byť zodpovedná za bezpečnosť produktov, ktoré ponúkajú. Ešte o trochu viacero si myslí, že smart zariadenia by mali mať zabudovanú ochranu súkromia a bezpečnosti.

Vyše tretina opýtaných tiež priznala, že smart zariadenia naďalej používajú aj po skončení podpory výrobcu. To znamená, že potenciálne používajú zariadenia s chýbajúcimi bezpečnostnými záplatami a podobnými problémami.

Tretina si tiež inteligentné zariadenia kupuje s minimom výskumu, asi polovica si len prečíta hodnotenia iných používateľov.

Podobne ako štúdia od Avastu, výsledky zabezpečenia domácich routerov, ku ktorým sú ostatné smart zariadenia pripojené, sú slabé. Menej ako štvrtina užívateľov niekedy zmenila heslo svojej Wi-Fi siete alebo routera. Len osmina aplikuje bezpečnostné záplaty pre router.

Bezpečnosť pre zámky

Bezpečnosť je všeobecne netriviálne definovateľný pojem. Pre účely zámkov a iných fyzických systémov je treba definovať niekoľko kategórií, kde celková bezpečnosť systému je spravidla najnižšie čiastkové hodnotenie.

Zámky musia byť odolné voči dvom základným typom útokov, prvým typom sú útoky hrubou silou a druhým útoky manipuláciou zámku. Pre každú z týchto

kategórií následne môžeme definovať rôzne úrovne bezpečnosti, podľa náradia, schopností a času potrebného na prekonanie zámku.

Pre oba typy útokov je takmer nemožné úplne zabrániť prekonaniu zámku. Tvrdiť, že zámok je neprekonateľný, či už hrubou silou alebo manipuláciou, je ako nazývať Titanic nepotopiteľným.

Pre útoky hrubou silou sa dá pomerne priamo definovať odolnosť zámku. Keďže útok typicky nevyžaduje veľké schopnosti, stačí zistiť, ako dlho trvá prekonať zámok zvoleným deštruktívnym nástrojom. Toto môže byť pílka, uhlová brúska, vŕtačka alebo iné náradie.

Pre útoky manipuláciou je potrebné do úvahy brať aj schopnosti útočníka a náradie, ktoré ma k dispozícii. Deviant Ollam, audítor a tréner v oblasti fyzického zabezpečenia, navrhuje podľa úrovne potrebného náradia a schopností definovať nasledujúce skupiny zámkov.

Základné zámky nemajú žiadne ochranné elementy, a sú takmer triviálne otvoriteľné pomocou manipulácie. Na ich otvorenie stačí len malá úroveň schopností a základné nástroje. Často sú tiež bezbranné proti takzvaným 'zero-skill' útokom, ktoré nevyžadujú prakticky žiadne schopnosti, len vlastníctvo príslušného nástroja. Tieto zámky sú typicky dostupné u bežných predajcov, ako vstavane základne zámky do kancelárskeho nábytku a podobne.

Odolné zámky su tie, ktoré majú aspoň nejaké špeciálne elementy, a mali by odolávať jednoduchým útokom. To znamená, že blokujú útoky typu zero-skill, a pre útoky založené na schopnostiach vyžadujú aspoň niekoľko minút od priemerného útočníka. Samozrejme, skúsený útočník so správnymi nástrojmi ich stále môže otvoriť podstatne rýchlejšie. Žiaľ, neexistuje jednotný štandard

značenia, podľa ktorého by sa dalo jednoznačne rozlíšiť tento typ od základného zámku.

Zámky s vysokou bezpečnosťou by na rozdiel od odolných zámkov mali brániť manipulácii. Teda kým odolný zámok sa snaží útočníka frustrovať, mierne skúsený útočník s normálnym náradím ho nakoniec otvorí. Vysoko bezpečný zámok by mal byť proti takémuto útoku úplne odolný, a vyžadovať značnú mieru schopností a špecializované náradie.

Finálnou kategóriou sú "unpickable" zámky. Tu Ollam okamžite pripomína, že úvodzovky sú to skutočne dôležité, inak sa nájde niekto, kto to urobí. Sem zaraďuje zámky, ktoré vyžadujú vysoko špeciálne náradie, techniky a výskum, a ich otvorenie by aj skúsenému útočníkovi malo trvať aspoň 30 minút. Tento čas by podľa neho mal byť dostatočný na to, aby útočníka zachytil zvyšok bezpečnostného systému. Ďalšou dôležitou pripomienkou k tomuto typu je, že Ollam nevyžaduje fyzickú nezničiteľnosť tohoto typu zámku, dôležité je, aby útočník bol prinútený použiť hrubú silu. Vďaka tomu je zaistené, že v prípade kompromitácie bude na prvý pohľad zjavné, že k nej došlo. Včasná reakcia na kompromitáciu je kritická pre riešenie vzniknutej situácie. Nutnosť použitia hrubej sily zároveň znamená, že ak neexistujú zjavné známky jej použitia, nedošlo ku kompromitácii zámku.

Napriek tomu, že tieto definície sú prevažne postavené na mechanických zámkoch, Ollam ich aplikuje aj na elektronické. Najmä v poslednej kategórii explicitne spomína niektoré typy elektronických zámkov používaných vládami a korporáciami pre maximálne zabezpečenie.

Útoky na mechanické zámky a systémy

Mnoho elektronických zámkov má ako záložný systém obyčajný mechanický zámok. Žiaľ, mnohokrát je tento záložný zámok z bezpečnostného hľadiska slabý, a je jednoduchšie prekonať ho ako snažiť sa prekonať hlavný elektronický zámok.

Pre mechanické zámky existuje niekoľko typov zraniteľností, ktoré sú spôsobené chybným alebo slabým dizajnom, prípadne implementáciou. Typicky sú relatívne lacno riešiteľné úpravou návrhu a opravením implementácie. Napriek tomu sa stále vyskytujú v nových zámkoch, ktoré sú dostupné na trhu pre obyčajného zákazníka.

Jednou z najhorších zraniteľností tohoto typu je možnosť odomknutia pomocou hrebeňového pakľúča. Tento prakticky funguje ako univerzálny kľúč na ľubovoľný zraniteľný zámok, stačí, aby počet a vzdialenosť zárezov na kľúči súhlasila s nástrojom. Chyba je pritom triviálne napraviteľná opravou dizajnu, kde stačí zabezpečiť, aby diery vnútri mechanizmu neboli nadbytočne hlboké. Napriek tejto trivialite sa vyskytuje aj v zámkoch, ktoré výrobca označí vysokým stupňom bezpečnosti.

Druhou zraniteľnosťou je možnosť útokov typu bypass alebo shimming. Pri týchto útokoch útočník použije tenký kúsok plechu, ktorý vstrčí do vhodnej štrbiny zámku a priamo manipuluje s vnútrom mechanizmu. Vďaka tomu dokáže otvoriť zámok úplne ignorujúc jadro a teda mechanizmus na použitie kľúča. V najhorších prípadoch toto znamená, že útočník otvorí zámok rýchlejšie ako použitím originálneho kľúča alebo kombinácie. Toto je typicky spôsobené chybou dizajnu, prípadne implementácie, ktorá neblokuje prístup k internému mechanizmu, alebo mechanizmus, ktorý nebráni posúvaniu dôležitých súčastí v zamknutej polohe. Variantou tohoto typu útoku je útok gumeným kladivom, kde sa pri vhodne mierenom údere posunú časti interného mechanizmu a zámok sa otvorí. Gumené kladivo je tu použité preto, aby nezanechalo stopy, keďže útočník typicky môže zámok bez problémov uzavrieť.

Komplexnejšie útoky už typicky vyžadujú nejakú úroveň zručnosti a vhodné nástroje, a fungujú na princípe opatrnej a premyslenej manipulácie s jednotlivými súčasťami jadra zámku. V závislosti od kvality návrhu a prevedenia zámku môže byť náročnosť týchto útokov prudko rozdielna. Je takmer nemožné zabrániť tomu, aby dostatočne skúsený útočník s vhodným náradím a dostatkom času prekonal

zámok. Zvolením vhodného dizajnu a kvalitným prevedením sa však dá podstatne zvýšiť náročnosť až natoľko, že menej skúsený útočník nebude úspešný v rozumnom čase.

Útoky na elektronické zámky

Jednoduché útoky na elektronické zámky sú často analogické útokom na mechanické zámky. Základným problémom je existencia výrobcom prednastavených kódov, rovnakých pre všetky kusy. Toto je prakticky analogické univerzálnemu kľúču, stačí, keď útočník pozná typ zámku a vie si vyhľadať, či a aký je kód výrobcu. Pri elektronických zámkoch toto môže byť riešiteľný problém, ak je užívateľ schopný kód zmeniť a aj tak urobí.

Analógiou bypass útokov sú pre elektronické zámky útoky pomocou magnetov. Zdrojom zraniteľnosti je tu dizajn, kde na ovládanie otvárania je použité elektromagnetické relé, ktoré je dostatočne prístupné z nechránenej strany dverí a nie je chránene pred vplyvom dostatočne veľkých externých magnetov. Typicky stačí, že útočník priblíži magnet na vhodné miesto takéhoto zámku, a dvere sa otvoria. Zámok je teda otvorené rýchlejšie, ako použitím takmer ľubovoľnej normálnej metódy. V extrémnych prípadoch sa táto zraniteľnosť môže vyskytnúť aj na mechanickom systéme, napr. Kaba Simplex.

Trochu pokročilejším typom útoku je útok pomocou skrutkovača. Pri tomto type útoku útočník použije skrutkovač alebo podobné náradie na odstránenie zámku, alebo na otvorenie tela zámku a sprístupnenie elektroniky. V prípade sprístupnenia elektroniky, ktorá riadi otváranie dverí, môže následne, podobne ako pri útoku magnetom, aktivovať otvorenie dverí obídením mechanizmu. Stačí, keď spinkou alebo iným vodivým materiálom prepojí správne miesta na plošnom spoji, ktoré sú typicky pre účely inštalácie jasne označené ako ovládanie dverí. Tento problém je opäť spôsobený chybou dizajnu, kde otváranie dverí je ovládané na nezabezpečenej strane dverí, a systém nie je dostatočne chránený pred otvorením tela systému. Problém sa dá zmierniť napr. pridaním kontaktného prepínača pripojeného k zvukovému alarmu, ktorý sa aktivuje, keď deteguje otvorenie krabičky s elektronikou. Toto opatrenie však nie je vždy postačujúce,

keďže útočník v závislosti od dizajnu môže kontaktný prepínač podržať v správnej polohe.

Približnou analógiou jednoduchých manipulačných útokov na mechanické zámky sú útoky hádaním hesla hrubou silou. Útok je založený na postupnom preberaní možných hesiel, pričom sa z odpovede snaží zistiť čo najviac informácií o skutočnom hesle, a tak minimalizovať časovú náročnosť. Typickým predpokladom praktickosti týchto útokov sú relatívne krátke heslá, a možnosť neobmedzene ich skúšať bez priveľkých zdržaní. V najhoršom prípade zámok akceptuje pokusy tak rýchlo, ako sa dajú posielať, čo pre malé rozsahy umožňuje v akceptovateľnom čase heslo uhádnuť. Toto sa stalo napr. zámku August Smart lock pri obnovovaní hesla, alebo niektorým ovládačom garážových brán, kde Samy Kamkar za využitia ďalších vlastností kódu znížil časovú náročnosť na menej ako 10 sekúnd. Podobne sa na niektorých zámkoch dá obísť klávesnica a pripojiť automatické zariadenie nie nepodobné filmovým, ktoré tiež za pár minút zámok otvorí.

Ďalším typom útoku je jamming, ktorý funguje na základe zahltenia komunikačného pásma medzi inteligentným zámkom a diaľkovým ovládačom. Týmto bráni komunikácii medzi zámkom a ovládačom, len použitím relatívne jednoduchej rušičky. V základnej verzii tento útok neumožňuje otvorenie dverí, len bráni legitímnemu užívateľovi v otvorení dverí. Ak však zámok potrebuje pokyn aj na uzamknutie, v prípade nepozorného užívateľa sa dá zneužiť aj na získanie prístupu. Stačí, keď útočník aktivuje rušenie skôr, ako užívateľ vydá pokyn na zamknutie. Podobne sa dá využiť na zneškodnenie alarmu, ak senzor komunikuje s centrálnou jednotkou bezdrôtovo. Napr. senzor otvorenia dverí potom nedokáže nahlásiť, že dvere boli otvorené, a alarm sa nerozozniе.

Nasledujúce útoky už sú komplexnejšieho charakteru, typicky vyžadujú vhodné náradie a príležitosť. Prvým z nich je útok typu replay. Tento útok sa spolieha na zraniteľnosť v komunikačnom protokole medzi zámkom a ovládačom, kde prehranie komunikácie od ovládača, ktorú útočník predtým nahral, je vyhodnotené ako legitímne. Typicky to znamená, že ovládač posiela signál, ktorý

je pre daný kus konštantný, aj keď môže byť odlišný pre rôzne kusy. Túto zraniteľnosť majú napr. zámky Ceomate Bluetooth Smartlock, Elecycle Smart Padlock, Vians Bluetooth Smart Doorlock a Lagute Scienter Smart Doorlock.

Trochu komplexnejšou variantou je útok typu relay, ktorý sa dá najlepšie využiť ak ovládač komunikuje s ovládaným zámkom aj bez interakcie užívateľa. Príklad zámkov tohto typu sú automobily s funkciu bezkľúčového otvárania, takéto auto sa odomkne len na základe fyzickej blízkosti k ovládaču, detegovanej na základe dosahu signálu. Táto vlastnosť sa dá zneužiť tak, že útočník zabezpečí prenos signálu medzi zámkom a ovládačom, simulujúc tak fyzickú blízkosť. Podobne ako v predchádzajúcom prípade útočník nevyžaduje znalosť komunikačného protokolu, stačí, keď dokáže správy preposielať medzi komunikujúcimi stranami.

Ešte pokročilejším typom útoku je útok na plávajúce kódy, ktoré sa snažia brániť proti replay útokom. Princíp plávajúceho kódu je založený na počítadle, ktoré si udržujú obe strany. Pri pokuse o otvorenie si ovládač od aktuálneho stavu počítadla odvodí jednorazový kľúč, ktorý použije, a následne inkrementuje svoje počítadlo. Pri prijatí jednorazového kľúča si zámok overí, či je odvodený z aktuálneho stavu počítadla, prípadne o nie viac ako konštantne väčšieho stavu počítadla. Ak áno, otvorenie je považované za úspešné a zámok si aktualizuje počítadlo na hodnotu nasledujúcu po použitej. Vďaka tomuto zámok neakceptuje predtým použité jednorazové kľúče, za predpokladu, že funkcia ktorá ich odvádza z počítadla je kvalitná. Je tiež nežiaduce prezradiť stav počítadla a iné tajné spoločné parametre, funkcia na odvádzanie kľúča by teda mala byť ťažko invertovateľná.

Útok na tento typ kódu pracuje ako kombinácia replay a jamming, kde útočník nahrá prvý vyslaný kód ale zablokuje jeho použitie. Keď následne užívateľ skúsi použiť ovládač znovu, útočník nahrá aj druhý kód, tiež ho zablokuje, a namiesto neho pošle prvý nahraný kód. Po takejto sekvencii dôjde k otvoreniu zámku, a útočníkovi zostane najbližší valídny kód, platný kým ho jednorazovo použije alebo kým užívateľ znova nepoužije ovládanie, čím spôsobí opätovnú synchronizáciu

počítadiel. V roku 2015 tento princíp demonštroval Samy Kamkar, so zariadením nazvaným RollJam.

Ďalšie typ útokov sa zameriavajú na využitie čítačky odtlačkov prstov. Na rozdiel od iných metód sú odtlačky pomerne nemenné, a tým pádom extrémne cenné. Keďže ľudia zanechávajú odtlačky na prakticky všetkom, čoho sa dotknú, stačí odtlačok získať a následne použiť. V extrémnych prípadoch dokonca stačia kvalitné fotky na získanie odtlačku, ako sa stalo napr. v prípade nemeckej političky, ktorej odtlačok bol extrahovaný z fotky, získanej počas tlačovej konferencie. Získaný obraz odtlačku sa následne premení na fyzický použitím vhodného materiálu, ako napr. latex alebo lepidlo aplikované na vytlačený odtlačok (s hrubou vrstvou toneru). Na ochranu proti tomuto typu útoku sa pokročilejšie čítačky odtlačkov snažia overiť, či je k nim skutočne priložený ľudský prst, na základe fyziologických vlastností.

Útok na stavovú konzistentnosť je založený na zneužití spôsobu, akým zámok komunikuje s pripojenými zariadeniami a spôsob ukladania prístupových práv. V tomto prípade je útok založený na tom, že mobilná aplikácia komunikuje so serverom výrobcu zámku, ale so zámkom komunikuje priamo. Ďalej je nutné, aby informácia o práve na ovládanie zámku bola uložená v klientskej aplikácii, a aktualizovala sa komunikáciou so serverom.

Nech Alica je správcom takéhoto zámku, a udelí právo na jeho otváranie Bobovi. Neskôr sa rozhodne Bobovi prístupové práva zrušiť, napríklad preto, že dokončil prácu, ktorú v chránenej oblasti vykonával. Pomocou svojej aplikácie k tomu vydá pokyn, na čo jej server odpovie, že práva boli odobrané. Ak ale Bobove mobilné zariadenie nie je pripojené k sieti, a server ho nevie kontaktovať, jeho aplikácia si stále pamätá, že práva má, a zámok sa na jeho pokyn odomkne. Náchylnosť na tento typ útoku bola odhalená u štyroch typoch zámkov.

Útoky na spôsob ukladania údajov a kľúčov v aplikáciách sú založené na predpoklade, že aplikácia ukladá niektoré citlivé údaje bez dostatočnej ochrany. Toto môžu byť napríklad symetrické šifrovacie kľúče, napevno definovane v zdrojovom kóde alebo vypísane v logoch. Podobne to môžu byť konfiguračné dáta uložené v zariadení v nešifrovanej podobe, ktoré sa dajú útočníkom skopírovať (potenciálne vyžaduje root) a následne použiť na ovládanie zámku. Tieto typy zraniteľností boli prítomné napríklad v aplikácii k zámkom August Smart lock a Danaloc. Podobne môže byť zraniteľnosť prítomná v iných pripojených zariadeniach, ako sa stalo v prípade Zipato smart hub.

Útok typu fuzzing sa spolieha na vlastnosť niektorých zámkov, ktoré pri prechode do chybového stavu automaticky odomknú. Toto nie je pre zámok nutne nerozumné správanie, keďže tak nehrozí, že bude nemožné zámok otvoriť v prípade núdze. Problém nastáva, keď je možné takýto stav jednoducho vyvolať napríklad poslaním nekorektne štruktúrovanej správy. Toto sa prejavilo napríklad na zámku Okidokey, ktorého správa štandardne začína dvoj-bajtovým kódom operácie, a na vynútenie chybového stavu stačí tretí bajt zmeniť na hodnotu 0.

Man-in-the-middle je útok, ktorý sa zameriava na zneužitie dôvery zámku v server výrobcu bez dostatočného overenia identity tohto servera. Táto zraniteľnosť sa prejavila napríklad na zámku August Smart lock, v ktorého aplikácii sa da zmeniť adresa servera, na ktorý sa pokúša pripojiť, a následne komunikáciu preposielať reálnemu serveru. Vďaka tomu je možné čítať komunikáciu so serverom, a dokonca aplikácii podsúvať falošné odpovede od servera. Toto napríklad umožňuje odstrániť logovanie, kde zámok dostane falošnú odpoveď o zapísaní záznamu, ale záznam nie je preposlaný na server. Podobne sa v danom prípade dali eskalovať privilégia zmenou parametru userType na superuser v odpovedi určenej aplikácii. Ak je toto spojenie tiež použité na aktualizáciu firmwaru, dá sa takto získať a prípadne poupraviť, ak nie je chránená proti úprave použitím digitálneho podpisu. Tak tomu bolo aj v prípade spomínaného zámku, ktorého aktualizácie neboli vôbec podpísané.