Onderzoeksrapport

Groep 1 Tilburg

12-06-2025

Mohammed Salah – Lucas Lammers – Maher el Maziani – Obada Aljarrah – Mahmoud Ikhlaf – Rick Kanters

Contents

Versiebeheer

Versienummer	Datum	Auteur	Veranderingen
0.1	17-03-2025	Rick Kanters	Eerste opzet
0.2	15-04-2025	Maher el. Maziani	Deelvraag 1, 2, 5
0.3	21-5-2025	Groep 1 Tilburg	Feedback van groep verwerkt en document verbeterd. Huisstijl toegepast
0.4	23-5-2025	Groep 1 tilburg	Deelvragen aangepast en verbeterd.
0.5	28-5-2025	Groep 1 Tilburg	Deelvraag 3 en 5 toegevoegd
0.6	8-06-2025	Groep 1 Tilburg	Conclusie
1.0	12-06-2025	Groep 1 Tilburg	Inleveren

Inleiding

Dit document betreft het onderzoeksrapport van het onderzoek naar de digitale beveiliging van de Flient Smart Lock een modern elektronisch slot dat gebruik maakt van verschillende technologieën, waaronder Bluetooth, Wifi, NFC, een mobiele applicatie en biometrische toegangscontrole. Met de opkomst van smart home-devices groeit ook de behoefte aan diepgaand inzicht in de beveiligingsaspecten van dergelijke producten. In dit onderzoek is systematisch gekeken naar de potentiële kwetsbaarheden én sterke punten van de Flient Smart Lock.

Het rapport is opgebouwd rondom een centrale hoofdvraag, ondersteund door vijf zorgvuldig geformuleerde deelvragen die samen het onderzoeksraamwerk vormen. Elke deelvraag wordt afzonderlijk behandeld in een hoofdstuk, waarin de toegepaste onderzoeksmethoden worden beschreven, variërend van literatuuronderzoek en technische analyse tot praktijkgerichte penetratietesten en community-based threat assessments. Per deelvraag worden de bevindingen geanalyseerd en gekoppeld aan een onderbouwde conclusie met betrekking tot de veiligheid van het systeem.

Dit rapport is primair bedoeld voor docenten, medestudenten en overige belanghebbenden met een technische achtergrond of interesse in IoT- en smart home-beveiliging. Door het combineren van verschillende methoden en bronnen is gestreefd naar een zo betrouwbaar, reproduceerbaar en objectief mogelijk onderzoeksresultaat.

Door deze integrale aanpak biedt dit rapport een genuanceerd, diepgaand en toetsbaar beeld van de digitale weerbaarheid van de Flient Smart Lock binnen het huidige dreigingslandschap.

Onderzoeksdoel

Het doel van dit onderzoek is om diepgaand inzicht te verkrijgen in de digitale beveiliging van de Flient Smart Lock. De focus ligt hierbij op het identificeren van potentiële kwetsbaarheden binnen de technologieën die door het slot worden gebruikt, zoals Bluetooth, wifi en NFC. Door het systeem zowel theoretisch als praktisch te analyseren en te testen, willen we nagaan in hoeverre het slot bestand is tegen ongeautoriseerde toegang, zowel digitaal als fysiek.

Om een volledig beeld te krijgen van de beveiliging, wordt gekeken naar de robuustheid van de gebruikte protocollen en technieken op papier, maar vooral ook naar de praktische weerbaarheid in realistische scenario's. Het onderzoek combineert inzichten uit bestaande literatuur over industrienormen en bekende kwetsbaarheden met technische analyses van zowel het slot zelf als de bijbehorende mobiele applicatie. Daarnaast zijn er gestructureerde penetratietesten en gesimuleerde aanvalsscenario's uitgevoerd op de smart lock.

Door deze gecombineerde aanpak is het doel van het onderzoek een betrouwbaar en toepasbaar beeld te schetsen van de huidige beveiligingsstatus van de Flient Smart Lock. Op basis van de bevindingen worden er ook aanbevelingen geformuleerd die bijdragen aan het verbeteren van de digitale veiligheid van het product.

Onderzoeksvragen

In dit hoofdstuk worden de centrale onderzoeksvragen gepresenteerd die richtinggevend zijn voor het gehele onderzoek. Hieronder wordt allereerst de hoofdvraag geformuleerd, die de kern vormt van het onderzoek naar de digitale beveiliging van de Flient Smart Lock.

Om deze hoofdvraag op gestructureerde wijze te kunnen beantwoorden, is deze uitgewerkt in een vijftal deelvragen. Elke deelvraag behandelt een specifiek aspect van de gebruikte technologieën of het dreigingslandschap en draagt bij aan het verkrijgen van een volledig en onderbouwd antwoord op de hoofdvraag. Gedurende het onderzoek worden deze deelvragen afzonderlijk geanalyseerd, onderzocht en beantwoord.

Hoofdvraag

- Hoe kunnen we ongeautoriseerde toegang krijgen tot het Flient Smart Lock?

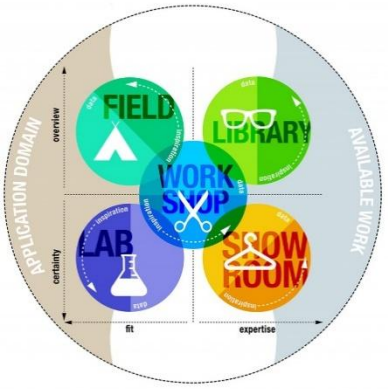
Deelvragen

- Welke technologieën worden in het Flient Smart Lock gebruikt en hoe werken ze?
- Hoe verhouden de encryptiemethoden en authenticatieprotocollen in Flient Smart Lock zich tot de industrienormen?
- Hoe communiceert de mobiele app met het Flient Smart Lock, welke beveiligingsprotocollen worden er gebruikt en is het mogelijk om de app te manipuleren en/of onderscheppen?
- Zijn er eerder gevonden kwetsbaarheden die nog steeds aanwezig zijn in Flient Smart Lock?
- Hoe vatbaar is het Flient Smart Lock voor fysieke aanvallen bijvoorbeeld pincode, slot en vingerafdruk?

DOT-framework

Dit onderzoek is verricht volgens de strategieën en methodes van het DOT-framework. Elke deelvraag binnen dit onderzoek is gekoppeld aan specifieke onderzoeksmethoden die helpen bij het verkrijgen van waardevolle inzichten en het waarborgen van de functionaliteit en veiligheid van het smart lock. Deze aanpak maakt het mogelijk om het smart lock in verschillende fasen te testen en de gevonden kwetsbaarheden uitgebreid te documenteren.

De methoden worden gekozen op basis van de beschikbare middelen voor het pentesten van het smartlock. Het doel is om ervoor te zorgen dat voldoende diverse methoden worden ingezet om de beveiliging van het smart lock te testen en te evalueren.



Figuur 1 DOT-Framework

Welke technologieën worden in het Flient Smart Lock gebruikt en hoe werken ze?

De Flient Smart Lock Advanced is een geavanceerd slim deurslot dat meerdere technologieën combineert om veilige en flexibele toegangscontrole te bieden. Hieronder volgt een overzicht van de gebruikte technologieën en hun werking:

Wi-Fi and Bluetooth Communication:
De Flient Smart Lock gebruikt Wi-Fi en Bluetooth voor draadloze communicatie. Hierdoor kunnen gebruikers het slot bedienen via een smartphone-app. De communicatieprotocollen zorgen voor een betrouwbare verbinding tussen het slot en de apparaten van de gebruiker, waardoor externe toegang en beheer mogelijk is (Jeffrey, 2025).

Een mobiel bediend deurslotsysteem dat gegevensuitwisseling tussen apparaten mogelijk maakt, heet Bluetooth. Het maakt verbinding met koptelefoons en andere accessoires, meestal in smartphones en andere mobiele apparaten. Het wordt recentelijk gebruikt in sloten om keyless entry mogelijk te maken en sloten te verbinden met mobiele apparaten. Maar hoe werkt een Bluetooth-slot en wat is het precies?

Volgens (Mmldigi, 2022) worden bluetooth slimme deursloten meestal gebruikt in combinatie met een smartphone en zijn ontworpen om u op afstand te beschermen. Zodra het slot is aangeschaft, moet het worden gekoppeld aan het primaire apparaat. Het slot kan alleen worden ontgrendeld door op een knop op uw smartphone te drukken. Instructies en tijdelijke sleutels kunnen ook aan andere familieleden en/of collega's worden gegeven. Deze mobiel bediende deursloten zijn eenvoudig te installeren en een fantastische vervanger voor traditionele deursloten. Ze moeten verbonden zijn met je Bluetooth om opdrachten van je smartphone te kunnen accepteren. Na het downloaden en installeren van de app moet je een speciale toegangscode invoeren op het apparaat dat je gebruikt. Voor de meeste slimme Bluetooth-sloten kunnen mensen tijdelijke virtuele sleutels aanmaken die alleen op specifieke tijden werken. Dus als je iemand binnen wilt laten, kun je een tijdelijke sleutel aanmaken waarmee die persoon op specifieke tijden toegang krijgt.

Fingerprint Scanner:
Een vingerafdrukscanner wordt gebruikt voor biometrische authenticatie. De gebruiker plaatst zijn vinger op de scanner, die de unieke vingerafdrukpatronen scant en vergelijkt met opgeslagen gegevens om toegang te verlenen. Dit biedt een veilige en gemakkelijke manier om de deur te ontgrendelen zonder dat er een fysieke sleutel of code nodig is (Jeffrey, 2025).

De Flient Smart Lock maakt gebruik van een geïntegreerde vingerafdrukscanner die tot 300 unieke vingerafdrukken kan opslaan. De scanner herkent een vingerafdruk binnen 0,1 seconde en geeft direct feedback bij een mislukte poging (Flient® Smart Lock Advanced - Slimme Deurslot - Deurklink met Vingerafdruk - Met APP & WiFi - BlueTooth - Kantoor Slot - Zwart - Anti inbraak - TT lockApp, sd).

Biometrische authenticatie wordt gebruikt door deursloten met vingerafdrukscanner om de unieke vingerafdruk van elke persoon te scannen en te identificeren. Het slimme slot koppelt uw vingerafdruk aan de opgeslagen informatie wanneer u uw vinger op de sensor plaatst. De deur wordt ontgrendeld als deze overeenkomt met een geautoriseerde afdruk, waardoor u veilig toegang krijgt tot uw huis zonder dat u kaarten of sleutels nodig hebt.

Vergeleken met conventionele deursloten zijn deursloten met vingerafdrukscanners handiger en veiliger dankzij hun verbeterde mogelijkheden. Door te garanderen dat alleen geautoriseerde personen toegang hebben, bieden deze sloten met vingerafdrukscanners een verhoogde beveiliging. (Strauss, 2025)

NFC Technology:
Tegenwoordig hebben veel slimme sloten naast Bluetooth ook NFC-chips – een gestandaardiseerde set regels die op RFID-chips worden toegepast. Radiofrequentie-identificatie, of RFID, is een technologie die in principe radiogolven gebruikt om identificatiegegevens tussen apparaten over te dragen (How to Use NFC Door Locks (and Unlock Them With a Phone), sd).

Near Field Communication (NFC)-technologie maakt het mogelijk om het slot te openen met een NFC-tag of -kaart. De gebruiker houdt de NFC-tag of -kaart dicht bij de NFC-lezer van het slot, waarna het slot via draadloze communicatie de tag uitleest en de toegangsrechten verifieert. Bij een geldige autorisatie wordt de deur automatisch ontgrendeld (Jeffrey, 2025).

Mobile App Integration:
Het Flient Smart Lock wordt beheerd via een speciaal ontwikkelde mobiele applicatie die beschikbaar is voor zowel iOS- als Android-platformen. Deze app vormt het centrale bedieningspunt voor gebruikers en stelt hen in staat om het slot te bedienen via een draadloze verbinding over Wi-Fi of Bluetooth Low Energy (BLE). De keuze tussen Wi-Fi en Bluetooth is contextafhankelijk: Bluetooth wordt voornamelijk gebruikt voor directe nabijheidsontgrendeling, terwijl Wi-Fi toegang op afstand mogelijk maakt via een beveiligde cloudverbinding.

De app biedt een breed scala aan functies die bijdragen aan zowel gemak als veiligheid. Zo kunnen gebruikers de deur op afstand vergrendelen of ontgrendelen, bijvoorbeeld om toegang te verlenen aan een bezoeker wanneer ze zelf niet thuis zijn. Daarnaast kunnen gebruikers digitale sleutels genereren en beheren, wat inhoudt dat tijdelijke of permanente toegang verleend kan worden aan andere personen, zoals familieleden, huishoudhulpen of huurders. Deze sleutels kunnen met specifieke rechten en tijdslimieten worden geconfigureerd, wat een fijnmazige toegangscontrole mogelijk maakt.

Een ander belangrijk kenmerk is het instellen van toegangsschema’s, waarbij toegang slechts mogelijk is binnen bepaalde tijdvakken. Deze functie is met name nuttig voor situaties zoals vakantieverhuur of kantoorbeheer. Verder kunnen gebruikers via de app pushmeldingen ontvangen bij iedere deuractiviteit, inclusief meldingen van mislukte toegangspogingen of pogingen tot sabotage, wat bijdraagt aan de algehele veiligheid en monitoring.

Keypad Entry:
Het slot heeft een toetsenbord voor het invoeren van een code om de deur te ontgrendelen. Gebruikers kunnen een vooraf gedefinieerde code invoeren om toegang te krijgen, wat handig is voor situaties waarin andere toegangsmethoden niet beschikbaar zijn of de voorkeur hebben.

Traditional Key:
Ondanks dat het een slim slot is, ondersteunt het ook traditionele sleuteltoegang. Dit biedt een back-upoptie in geval van technische problemen of voor gebruikers die de vertrouwdheid van een fysieke sleutel prefereren.

Gateway:
De Gateway-component verbetert de functionaliteit van het slot door externe toegang en controle via internet mogelijk te maken, waardoor gebruikers het slot overal ter wereld kunnen beheren.

Security Features
Het Flient Smart Lock is uitgerust met meerdere ingebouwde beveiligingsmaatregelen die ontworpen zijn om zowel digitale als fysieke aanvallen te detecteren en te voorkomen. Een van de kerncomponenten van deze beveiliging is de versleutelde communicatie tussen de mobiele applicatie en het slimme slot. Hiervoor wordt gebruikgemaakt van encryptieprotocollen zoals AES-128 of hoger, waardoor alle gegevens tijdens de overdracht versleuteld zijn en niet als platte tekst kunnen worden onderschept of gelezen. Daarnaast beschikt het systeem over automatische vergrendeling ("auto-lock"), waarbij het slot zichzelf na een vooraf ingestelde periode vergrendelt indien er geen activiteit wordt waargenomen. Dit voorkomt dat de deur per ongeluk open blijft staan. Een andere handige functie is de passage mode, waarbij het slot tijdelijk openblijft voor bijvoorbeeld een evenement of tijdens kantooruren, zonder dat herhaaldelijk ontgrendelen nodig is.

Op het gebied van toegangsbeheer biedt de Flient Smart Lock gedetailleerde configuratieopties. Gebruikers kunnen digitale sleutels aanmaken met specifieke rechten, tijdsbeperkingen en logische voorwaarden, zoals toegang op bepaalde dagen of tijdstippen. Dit stelt eigenaren in staat om per gebruiker verschillende machtigingen toe te kennen, wat met name nuttig is in gedeelde woonruimtes of verhuursituaties. Een belangrijke beveiligingsmaatregel tegen fysieke manipulatie is het actieve alarmsysteem. Wanneer een gebruiker vijfmaal een foutieve toegangscode invoert op het toetsenpaneel van het slot, treedt automatisch een beveiligingsprotocol in werking.

Dit protocol activeert een intern alarmgeluid en blokkeert tijdelijk verdere invoerpogingen om brute-force aanvallen te ontmoedigen. Tegelijkertijd ontvangt de eigenaar een melding via de mobiele app, zodat hij direct op de hoogte is van een mogelijke inbraakpoging. Deze functie draagt aanzienlijk bij aan de fysieke beveiliging van het systeem.

(Jeffrey, 2025)

Conclusie
De documentanalyses hebben bijgedragen aan een diepgaand inzicht in de werking en de beveiligingsstructuur van het Flient Smart Lock. Hoewel niet alle technische specificaties publiekelijk beschikbaar zijn, bieden praktijkobservaties en gebruikersdocumentatie voldoende aanknopingspunten om te concluderen dat het systeem over een veelzijdige en doordachte beveiligingsarchitectuur beschikt. In de daaropvolgende deelvragen wordt dit theoretische fundament verder verdiept door middel van concrete testcases. Hierbij worden de toegepaste technologieën van het slot getest in gecontroleerde scenario's, met als doel de betrouwbaarheid en veiligheid in de praktijk te evalueren. Daarnaast worden eventuele kwetsbaarheden geïdentificeerd en geanalyseerd.

Hoe verhouden de encryptiemethoden en authenticatieprotocollen in Flient Smart Lock zich tot de industrienormen?

Bluetooth Low Energy (BLE) Communication
Het TTLock smart lock-systeem maakt voornamelijk gebruik van Bluetooth Low Energy (BLE) voor communicatie op korte afstand tussen het slot en een mobiel apparaat. BLE is een populaire keuze in de smart lock-industrie vanwege het lage energieverbruik en de veilige gegevensoverdracht.

BLE in TTLock:
AES-128-versleuteling: TTLock gebruikt AES-128 om BLE-communicatie te versleutelen. AES (Advanced Encryption Standard) is een symmetrisch versleutelingsalgoritme dat breed wordt toegepast in verschillende sectoren. AES-128 biedt een goede balans tussen prestaties en beveiliging.

Challenge-Response-authenticatie: TTLock past een dynamische authenticatiemethode toe waarbij voor elke toegangspoging een unieke uitdaging (challenge) wordt verstuurd. Het gekoppelde mobiele apparaat moet reageren met de juiste cryptografische sleutel, waardoor hergebruik van onderschepte gegevens (replay-aanvallen) wordt voorkomen.

Veilige koppeling: TTLock maakt gebruik van BLE-koppelingsmethoden die ervoor zorgen dat versleutelingssleutels veilig worden uitgewisseld. Hoewel "Just Works"-koppeling vaak wordt gebruikt, worden veiligere methoden zoals Passkey Entry of Numeric Comparison steeds vaker als industriestandaard beschouwd voor extra bescherming.

Industrienorm voor BLE:
Binnen de industrie geldt AES-128 als de meest gangbare encryptiemethode voor Bluetooth Low Energy (BLE), vanwege de balans tussen veiligheid en energie-efficiëntie. Hoewel minder vaak toegepast, wordt AES-256 als een meer ideale optie beschouwd, zeker in toepassingen waar een hoger beveiligingsniveau vereist is.

Authenticatie binnen BLE vindt doorgaans plaats via een challenge-response mechanisme. Dit zorgt ervoor dat apparaten elkaar op een betrouwbare manier kunnen verifiëren zonder dat gevoelige gegevens direct worden uitgewisseld.

Voor het koppelen van apparaten wordt sinds de introductie van BLE 4.2 gebruikgemaakt van LE Secure Connection. Deze pairing-methode biedt aanzienlijk betere bescherming tegen afluisteren en manipulatie, waarmee het een belangrijke verbetering is ten opzichte van oudere BLE-versies. De combinatie van deze elementen vormt de kern van een veilige BLE-communicatie volgens de huidige industriestandaarden.

Advies verbeteringen BLE Security:
Om de beveiliging van Bluetooth Low Energy (BLE) te versterken, is het aan te raden over te stappen van AES-128 naar AES-256. Deze upgrade verhoogt de vertrouwelijkheid van de communicatie aanzienlijk en biedt betere bescherming tegen toekomstige cryptografische aanvallen. Daarnaast is het belangrijk om LE Secure Connections te implementeren, een functie die sinds BLE 4.2 beschikbaar is. Deze biedt een krachtigere bescherming tegen man-in-the-middle-aanvallen en voorkomt passief afluisteren door gebruik te maken van geavanceerdere sleuteluitwisseling en encryptietechnieken.

Verder draagt het periodiek roteren van BLE-sleutels bij aan een dynamischer beveiligingsmodel. Door sleutels regelmatig te vernieuwen, wordt de kans op langdurige blootstelling bij een eventuele compromittering van de sleutel aanzienlijk verminderd. Samen zorgen deze maatregelen voor een substantiële verbetering van de algehele BLE-beveiliging. (Hlapisi, 2023) (Ren, 2025)

WiFi Communicatie
Via een speciale WiFi-gateway maakt TTLock cloudintegratie mogelijk voor toegang, beheer en monitoring op afstand. Dit biedt extra functionaliteit, zoals het op afstand ontgrendelen van deuren en het ontvangen van activiteitsmeldingen.

WiFi in TTLock:

- TLS-versleuteling: TTLock gebruikt TLS (meestal TLS 1.2 of hoger) om de communicatie tussen de mobiele app, de cloud en het slot te beveiligen
    - TLS zorgt voor authenticatie en versleuteling van alle verzonden gegevens.
    - TLS-certificaten verifiëren de legitimiteit van verbonden servers, wat het risico op man-in-the-middle-aanvallen verkleint.
- JWT en OAuth 2.0: Het cloudplatform van TTLock maakt gebruik van JSON Web Tokens voor sessiebeheer en toegangscontrole. Tokens zijn tijdgebonden en hebben beperkte toegang, wat de veiligheid in omgevingen met meerdere gebruikers versterkt.

Industrienorm voor WiFi:
Binnen de industrie gelden duidelijke standaarden voor WiFi-beveiliging, waarbij encryptie en authenticatie centraal staan. TLS 1.2 wordt nog breed ondersteund, maar TLS 1.3 is de voorkeur vanwege zijn verbeterde snelheid en veiligheid. Het is dan ook wenselijk om waar mogelijk over te stappen op TLS 1.3 om te profiteren van de geavanceerdere cryptografische eigenschappen.

Op het gebied van draadloze beveiligingsprotocollen verschuift de standaard naar WPA3. Hoewel WPA2 nog steeds het meest gebruikt wordt in de praktijk, biedt WPA3 aanzienlijke voordelen, zoals betere bescherming tegen wachtwoordaanvallen en verbeterde beveiliging op openbare netwerken. Deze ontwikkeling maakt WPA3 tot de beoogde industriestandaard.

Voor authenticatie wordt doorgaans gebruikgemaakt van OAuth 2.0 in combinatie met JSON Web Tokens (JWT). Deze methode maakt het mogelijk om veilige en schaalbare toegang te realiseren, waarbij tokens op een efficiënte en gecontroleerde manier rechten toekennen aan gebruikers en apparaten. Deze combinatie van technieken vormt de ruggengraat van een moderne en robuuste WiFi-beveiligingsinfrastructuur.

Advies verbeteringen WiFi Security:
Om de WiFi-beveiliging te verbeteren, is het aan te raden om over te stappen op TLS 1.3. Deze versie biedt niet alleen betere prestaties door snellere sessiehandshakes, maar verhoogt ook de beveiliging dankzij verbeterde encryptieprotocollen. Voor extra bescherming van netwerkcommunicatie is het verstandig om Mutual TLS (mTLS) te implementeren. Dit zorgt voor wederzijdse authenticatie tussen client en server, waardoor alleen geverifieerde apparaten toegang krijgen.

Daarnaast blijft het cruciaal om WPA3 te hanteren als standaard voor draadloze communicatie tussen router en gateway. WPA3 biedt robuustere bescherming tegen brute-force aanvallen en verhoogt de veiligheid van openbare netwerken. Om de toegang tot netwerkbronnen verder te reguleren, kunnen kortlevende toegangstokens worden ingezet. Deze tokens verminderen het risico bij onderschepping, zeker wanneer ze worden gecombineerd met veilige vernieuwingstokens (refresh tokens) en een zorgvuldige verwerking daarvan. Deze maatregelen samen zorgen voor een solide, toekomstbestendige beveiligingsarchitectuur. (WPA3 | TP-Link, n.d.) (contributors, n.d.)

NFC
TTLock-sloten ondersteunen NFC-technologie (Near Field Communication), waarmee gebruikers deuren kunnen ontgrendelen met contactloze IC-kaarten of NFC-compatibele apparaten. Dit biedt een alternatief voor het gebruik van traditionele sleutels of ontgrendeling via Bluetooth op een mobiel apparaat.

NFC-implementatie in TTLock

- Supported Devices
  TTLock maakt gebruik van MIFARE-compatibele IC-kaarten die werken op 13,56 MHz.
- Access Management
  Beheerders kunnen NFC-kaarten toewijzen via de TTLock-app met de volgende toegangstypen:
  - Permanent – Kaarten blijven onbeperkt geldig.
  - Timed – Kaarten zijn alleen geldig binnen een opgegeven tijdsperiode.
  - Recurring – Kaarten zijn actief op specifieke tijdstippen op bepaalde dagen van de week.
- Kaart registratie
  NFC-kaarten kunnen rechtstreeks bij het slot worden toegevoegd via het mobiele apparaat van de beheerder met behulp van Bluetooth. Afstandsregistratie is ook mogelijk via een TTLock-kaartencoder wanneer het slot verbonden is via een WiFi-gateway.
- Toegangsintrekking
  Beheerders kunnen de toegang van kaarten intrekken via Bluetooth (in de buurt van het slot) of op afstand via de gateway.

Beveiligingsoverwegingen
TTLock maakt gebruik van NFC-kaarten die als "MIFARE-compatibel" worden aangeduid, maar geeft daarbij geen specifieke informatie over het exacte type kaart dat wordt ingezet. In de praktijk wordt vaak MIFARE Classic toegepast, een technologie die bekendstaat om zijn wijdverspreide gebruik, maar helaas ook om zijn verouderde en kwetsbare beveiligingsmechanismen. Voor toepassingen waarbij een hoger beveiligingsniveau vereist is, verdient MIFARE DESFire de voorkeur. Deze kaarten bieden geavanceerdere encryptiestandaarden, zoals AES, en zijn daarom aanzienlijk beter bestand tegen aanvallen.

Op het gebied van authenticatie laat TTLock eveneens ruimte voor verbetering. Er wordt geen duidelijkheid gegeven over het gebruik van veilige protocollen zoals een wederzijds challenge-response-mechanisme bij communicatie met NFC-kaarten. Het ontbreken van dergelijke methoden vergroot de kans op klonings- of replay-aanvallen, zeker wanneer er kaarten met een lager beveiligingsniveau worden gebruikt. Deze onzekerheid benadrukt de noodzaak voor transparantie en versterking van de authenticatietechnieken binnen het systeem.

Industrienormen voor NFC Security
Binnen de industrie worden voor NFC-beveiliging technologieën zoals MIFARE DESFire EV1 en EV2 als de standaard beschouwd. Deze bieden ondersteuning voor AES-versleuteling en wederzijdse authenticatie, wat essentieel is voor het realiseren van een veilige communicatie tussen kaart en lezer. Door deze eigenschappen zijn ze bij uitstek geschikt voor toepassingen waar een hoog beveiligingsniveau vereist is, zoals toegangscontrole in gevoelige omgevingen.

Een cruciaal aspect van NFC-beveiliging is de omgang met cryptografische sleutels. Het is van groot belang dat deze sleutels op een veilige manier worden opgeslagen en beheerd, en dat ze regelmatig worden vernieuwd. Dit voorkomt dat kwaadwillenden langdurig gebruik kunnen maken van een gecompromitteerde sleutel of dat kaarten eenvoudig kunnen worden gekopieerd.

Daarnaast speelt audit logging een belangrijke rol in het waarborgen van de integriteit van een NFC-systeem. Door het bijhouden van gedetailleerde toegangslogs kan men afwijkend gedrag tijdig signaleren en snel reageren op mogelijke beveiligingsincidenten. Deze combinatie van technologie, sleutelbeheer en monitoring vormt de kern van een robuust NFC-beveiligingsbeleid.

Aanbevelingen voor TTLock NFC Security
Voor een betere NFC-beveiliging binnen het TTLock-systeem is het belangrijk dat er duidelijkheid wordt geboden over welke kaarttypen daadwerkelijk worden ondersteund. Het onderscheid tussen MIFARE Classic en MIFARE DESFire is hierin essentieel, aangezien deze kaarten aanzienlijk verschillen in hun beveiligingsmogelijkheden. Transparante communicatie hierover stelt gebruikers in staat om weloverwogen keuzes te maken op basis van hun beveiligingsbehoeften.

In omgevingen waar beveiliging een hoge prioriteit heeft, verdient het aanbeveling om het gebruik van MIFARE DESFire EV1 of EV2 actief te stimuleren. Deze kaarten ondersteunen sterke versleuteling en wederzijdse authenticatie, wat ze aanzienlijk robuuster maakt tegen klonen en manipulatie dan oudere kaarttypen.

Daarnaast is het van belang dat TTLock inzicht geeft in de authenticatiemechanismen die worden toegepast bij het uitlezen van NFC-kaarten. Wanneer onduidelijk is of er sprake is van challenge-response of andere beveiligingslagen, ontstaat er onzekerheid over de weerbaarheid van het systeem tegen aanvallen zoals replay of card cloning.

Tot slot zou het waardevol zijn als TTLock optioneel ondersteuning biedt voor een rolling code-mechanisme of een dynamisch sleutelsysteem. Door sleutels bij elke interactie te vernieuwen of variëren, wordt het risico op succesvolle duplicatie van kaarten aanzienlijk verminderd en neemt de algehele veiligheid van het systeem toe.

Vergelijking smartlocks

Deze vergelijking belicht de belangrijkste beveiligings- en functionaliteitskenmerken van drie populaire smart locks ten opzichte van de huidige industriestandaarden. Zo is er inzicht in welke modellen voldoen aan basis- en geavanceerde eisen voor veiligheid en gebruiksgemak.

Feature/ Standaard	TTLock	Blugate 66	August Smart Lock	Industrienormen
BLE Communicatie	Ja	Ja	Ja	Ja
BLE Encryptie	AES-128	AES-128	AES-128	AES-128/ AES-256
BLE veilig pairing	Ja (LE)	N.V.T	Ja	LE Secure Connections
Challenge-Response Authentication (BLE)	Ja	Ja	Ja	Ja
WiFi Support via Gateway	Ja	Gedeeltelijk	Ja (Ingebouwd)	Ja (Via gateway of direct)
TLS Encryptie (WiFi)	TLS 1.2	N.V.T	TLS 1.2/ 1.3	TLS 1.2/ 1.3
OAuth 2.0 + JWT Authenticatie	Ja	N.V.T	Ja	Ja
WPA3 WiFi Security	Optioneel	N.V.T	N.V.T	WPA3
Cloud-Based Management	Ja	N.V.T	Ja	Ja
Mobiele App Integratie	Ja	Ja	Ja	Ja
AES-256 Support	Nee(default)	Nee	Optioneel	Optioneel
NFC Support	Ja (IC kaarten	N.V.T	Nee	Ja (DESFire EV1/EV2)

(How to use NFC door locks (and unlock them with a phone), n.d.) (Blugate 66 | Full Lock system, n.d.) (How August Smart Locks work | August Home, n.d.)

Alle drie de smart locks voldoen aan de basisveiligheid volgens de industriestandaarden, maar er zijn duidelijke verschillen in de mate van geavanceerde beveiliging en functionaliteit. August Smart Lock scoort het beste doordat het de nieuwste encryptiestandaarden (AES-256), moderne WiFi-beveiliging (TLS 1.3, WPA3) en robuuste authenticatiemechanismen volledig ondersteunt. TTLock volgt met een degelijke basis, maar mist op sommige punten de nieuwste beveiligingsprotocollen. Blugate 66 blijft achter door beperkte ondersteuning voor secure pairing en onvolledige WiFi-beveiliging.

Conclusie
De encryptiemethoden en authenticatieprotocollen die Flient Smart Lock toepast via het TTLock-platform vertonen sterke overeenkomsten met de geldende industrienormen, maar vertonen ook enkele aandachtspunten waar verbetering mogelijk is.

Op het gebied van Bluetooth Low Energy (BLE) communicatie maakt Flient gebruik van AES-128-encryptie en een challenge-responsemechanisme voor authenticatie. Dit sluit aan bij wat algemeen geaccepteerd is binnen de sector. Toch blijft er ruimte voor verbetering, zoals het toepassen van LE Secure Connections, dat sinds BLE 4.2 wordt beschouwd als de standaard voor veilige koppelingen. Hoewel AES-128 voldoende bescherming biedt, zou het upgraden naar AES-256 in omgevingen met hogere beveiligingseisen een logischere keuze zijn. Daarnaast ontbreekt informatie over de periodieke rotatie van sleutels, wat een belangrijk aspect is voor het reduceren van langdurige kwetsbaarheid in draadloze communicatie.

De WiFi-component van het systeem voldoet in grote lijnen aan de verwachtingen. De toepassing van TLS 1.2 voor gegevensoverdracht tussen slot, app en cloud biedt een goede basisveiligheid, en de inzet van OAuth 2.0 en JWT versterkt de controle over gebruikerssessies. In de context van hedendaagse beveiligingsstandaarden zou TLS 1.3 echter de voorkeur verdienen vanwege verbeterde prestaties en sterkere encryptie. Ook zou de implementatie van mutual TLS een waardevolle aanvulling zijn om wederzijdse authenticatie te realiseren tussen client en server.

Wat betreft NFC-toegang blijven er belangrijke vragen onbeantwoord. Flient geeft niet aan welk type MIFARE-kaarten wordt gebruikt. Indien het gaat om MIFARE Classic, zijn er significante beveiligingsrisico's, aangezien deze kaarten kwetsbaar zijn voor klonen en replay-aanvallen. Moderne toepassingen hanteren doorgaans MIFARE DESFire EV1 of EV2, die wel voldoen aan de eisen van veilige encryptie en wederzijdse authenticatie. Het ontbreken van transparantie over het type kaart en de gebruikte authenticatieprotocollen maakt het moeilijk om de effectiviteit van deze beveiligingslaag volledig te beoordelen.

Hoe communiceert de mobiele app met het Flient Smart Lock, welke beveiligingsprotocollen worden er gebruikt en is het mogelijk om de app te manipuleren en/of onderscheppen?

Mobiele applicaties die smart devices aansturen, zoals slimme sloten, vormen een essentieel onderdeel van het Internet of Things (IoT)-ecosysteem. In dit onderzoek is de communicatie tussen de Flient Smart Lock-app en de bijbehorende backend server geanalyseerd op basis van praktische pentests. Hiervoor zijn twee testcases uitgevoerd: Testcase 2 - Zwakke Encryptie en Testcase 4 - APK Reversen. Deze testcases dienden als empirische basis voor het vaststellen van gebruikte protocollen, beveiligingsmaatregelen en kwetsbaarheden.

Testcase 2 - Zwakke Encryptie
Uit Testcase 2 – Zwakke Encryptie blijkt dat de communicatie tussen de mobiele applicatie en de server verloopt via HTTPS, waarbij gebruik wordt gemaakt van Transport Layer Security (TLS) versie 1.2. TLS is een algemeen geaccepteerde standaard voor veilige gegevensoverdracht en beschermt tegen afluisteren, manipulatie en spoofing (Patil, 2025). Analyse met Wireshark en Burp Suite toonde aan dat de TLS-handshake correct wordt uitgevoerd en dat de gegevensstroom effectief versleuteld is.

Het wachtwoordverkeer tussen de app en server verloopt bovendien gehasht. Echter, hierbij wordt gebruikgemaakt van de verouderde MD5-hashfunctie, waarvan bekend is dat deze kwetsbaar is voor collision attacks en brute-force-aanvallen (The md5 hashing algorithm is insecure, sd). Hoewel MD5 voorkomt dat wachtwoorden in plaintext worden verzonden, is het algoritme niet geschikt voor moderne beveiligingseisen.

Testcase 4 - APK Reversen
In Testcase 4 – APK Reversen is de APK van de Flient-app gedecompileerd met tools zoals APKTool en JADX. De analyse van de broncode leverde meerdere ernstige beveiligingsproblemen op:

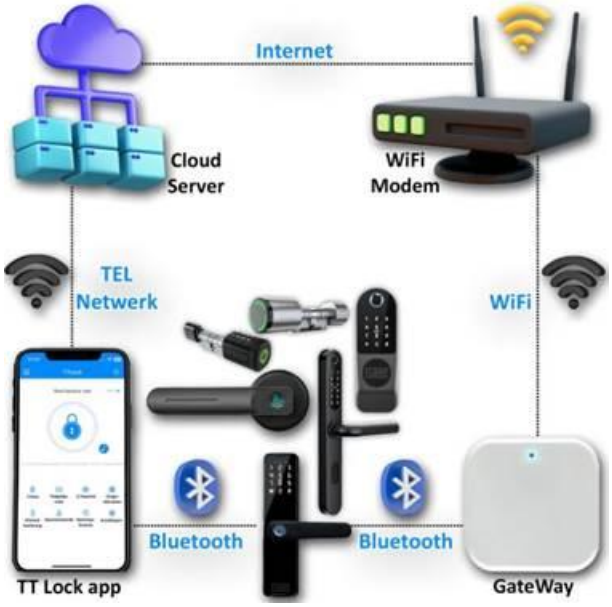
- Hardcoded secrets: De code bevat hardcoded waarden zoals API-sleutels, client secrets, UUIDs en wachtwoorden. Dit vormt een direct risico op ongeautoriseerde toegang tot de backend of tot smart lock-functionaliteiten.
- Ontbreken van code-obfuscatie: De applicatie is niet geobfusceerd, wat de leesbaarheid van de broncode en gevoelige logica aanzienlijk vergroot (Brook, 2024).
- Onveilige cryptografie: Naast het gebruik van MD5 voor hashing, is er een hardcoded AES-sleutel aanwezig die wordt gecombineerd met het MAC-adres van het apparaat om encryptiesleutels te genereren. Dit maakt de encryptie reproduceerbaar en dus kwetsbaar.
- Privacygevoelige permissies: De app vraagt toegang tot onder andere locatie, microfoon, contacten en opslag. Hoewel deze permissies technisch nodig kunnen zijn, vergroten ze het aanvalsoppervlak en verhogen ze het risico op misbruik (Hick, 2021).

De combinatie van een goed geïmplementeerde TLS-verbinding met een slecht beveiligde interne architectuur zorgt voor een vals gevoel van veiligheid. De aanwezigheid van hardcoded geheimen en het gebrek aan codebescherming maken het voor aanvallers relatief eenvoudig om toegang te krijgen tot gevoelige functionaliteiten of om onderdelen van het protocol na te bootsen. Hierdoor zijn aanvallen zoals spoofing, replay attacks en manipulatie van firmware-updates niet ondenkbaar.

G2 Gateway
Een van de manieren waarop de mobiele app communiceert met het Smart Lock is via de G2 Gateway. Deze Gateway maakt het mogelijk om het slot op afstand te ontgrendelen, zelfs als je niet thuis bent. De communicatie verloopt via wifi en Bluetooth Low Energy (BLE): de mobiele app stuurt gegevens via wifi naar de cloudserver van TTlock. Deze server stuurt de gegevens vervolgens door naar de Gateway, die het slot via BLE ontgrendelt.

De cloudserver weet naar welk slot de gegevens moeten worden gestuurd doordat het MAC-adres van het Smart Lock is gekoppeld aan het publieke IP-adres van het netwerk waarin het slot zich bevindt. Tijdens de communicatie wordt het dataverkeer versleuteld met behulp van een hardcoded AES-sleutel en een gegenereerde AES-sleutel. De hardcoded AES-sleutel is te achterhalen door reverse engineering van de app. De gegenereerde AES-sleutel wordt op basis van een vaste methode aangemaakt: een willekeurig gegenereerde 16-byte code wordt versleuteld met de hardcoded AES-sleutel. Daarnaast is de communicatie tussen de Gateway en de server beveiligd met TLS 1.2-encryptie.

Theoretisch is het mogelijk om de Gateway te emuleren (Aronsky, 2024), zodat het slot via deze nagemaakte Gateway kan worden ontgrendeld. Uit onze tests is echter gebleken dat dit tot op heden niet mogelijk is.



Figuur 2 Slot - Gateway communicatie

BLE (Bluetooth Low Energy)
Onafhankelijk van of het slot via de app of de gateway wordt geopend, vindt er altijd BLE-communicatie plaats. In testcase 3 – BLE Sniffing hebben we het BLE-verkeer tussen de app en het slot onderschept en geïnspecteerd. Hieruit is gebleken dat er gebruik gemaakt wordt van BLE-versie 4.x. Bij BLE versies hoger dan 4.0 wordt er gebruik gemaakt van AES-CCM (DigiKey Employee, 2021)

Dit is een vrij secuur protocol dat moeilijk te ontcijferen is. Door deze encryptie was het niet gelukt om het onderschepte verkeer in te zien. We hadden ook geprobeerd om het verkeer opnieuw te versturen om zo mogelijk het slot te ontgrendelen, alleen bleek er gebruik wordt gemaakt van een “rolling code” algoritme. Dit voorkomt dat BLE-verkeer opnieuw gebruikt kan worden.

De BLE-communicatie tussen de app en het slot is, zover wij hebben getest, veilig. Verdere tests zijn vereist om de volledige veiligheid van BLE vast te stellen.

Conclusie
Het antwoord op de deelvraag is dat de mobiele app communiceert met het Flient Smart Lock via een combinatie van TLS-versleuteld verkeer met de server, BLE voor lokale communicatie met het slot, en een G2 Gateway voor externe toegang. Ondanks het gebruik van erkende beveiligingsprotocollen zoals TLS 1.2 en AES-CCM, toont praktijkonderzoek aan dat de beveiliging in de applicatie-architectuur ernstig tekortschiet. De aanwezigheid van hardcoded sleutels, verouderde hashfuncties en het ontbreken van code-obfuscatie maken de app kwetsbaar voor reverse engineering en manipulatie.

Hierdoor is het mogelijk om onderdelen van het communicatieproces te onderscheppen of na te bootsen. De beveiliging lijkt dus in eerste instantie solide, maar bij nadere analyse blijkt dat deze onvoldoende bescherming biedt tegen goed voorbereide aanvallen. Echte veiligheid vereist meer dan alleen versleuteling van dataverkeer.

Zijn er eerder gevonden kwetsbaarheden die nog steeds aanwezig zijn in Flient Smart Lock?

Community-onderzoek
Voor dit onderzoek is gebruikgemaakt van community-based informatieverzameling, waarbij bestaande data uit gerenommeerde cybersecuritybronnen is geanalyseerd. De primaire informatiebronnen omvatten de National Vulnerability Database (NVD), Exploit Database (Exploit-DB), CVE Details, peer-reviewed academische literatuur, rapporten van cybersecuritybedrijven en relevante bijdragen op blogs en fora binnen de beveiligingsgemeenschap.

Een gestructureerde zoekmethodiek werd toegepast om kwetsbaarheden (CVE's) te identificeren die direct verband houden met de Flient Smart Lock, om terugkerende kwetsbaarheden bij vergelijkbare smart locks in kaart te brengen en om te evalueren of deze zwakke plekken ook van toepassing kunnen zijn op het Flient-systeem.

Bevindingen
Op basis van het onderzoek zijn twee CVE's gevonden die expliciet verband houden met de Flient Smart Lock: CVE-2023-50129 en CVE-2023-50124. Desondanks is de openbare informatie over de beveiliging van dit product schaars. De fabrikant hanteert een gesloten beleid voor kwetsbaarheidsbeheer, wat leidt tot een gebrek aan transparantie en publieke beoordelingen. Het ontbreken van openbaar gemelde kwetsbaarheden betekent echter niet automatisch dat het product veilig is. Bij veel IoT-apparaten is onderrapportage een bekend probleem, waardoor risico's mogelijk onopgemerkt blijven.

Uit de analyse van vergelijkbare smart lock-producten kwamen verschillende relevante kwetsbaarheden naar voren. Zo werd bij de Shenzhen Dragon Brother FB50 (CVE-2019-13143) een kwetsbaarheid in de cloud-API ontdekt die re-binding-aanvallen mogelijk maakte. In een ander geval, bekend als SweynTooth (CVE-2019-17517), leidde een buffer overflow in een Bluetooth Low Energy (BLE) chipset ertoe dat aanvallers op afstand het slot konden laten crashen. Daarnaast toonde onderzoek van F-Secure aan dat de KeyWe Smart Lock in 2019 een zwakke BLE-koppeling gebruikte, waardoor de cryptografische sleuteluitwisseling kon worden onderschept en het slot kon worden geopend zonder autorisatie.

Relevantie voor de Flient Smart Lock
Hoewel er voor de Flient Smart Lock slechts twee specifieke CVE's bekend zijn, wijzen de kwetsbaarheden in andere smart locks op bredere beveiligingsrisico's. Denk hierbij aan accountovername via onveilige API's, kwetsbaarheden in het BLE-protocol zoals bij SweynTooth, en onveilige implementaties van cryptografie tijdens het koppelen via Bluetooth.

Aanbevelingen voor teststrategieën
Om vast te stellen of deze kwetsbaarheden ook bij Flient aanwezig zijn, wordt aanbevolen om de BLE-communicatie te testen op gevoeligheid voor crashes, cloudservice-endpoints te analyseren op zwakke toegangscontrole, en de firmware te controleren op de correcte implementatie van beveiligingspatches. Deze aanpak sluit aan bij het labgedeelte van de Library & Lab-methode.

Conclusie
Dit community-onderzoek toont aan dat er wel degelijk publiek bekende CVE's voor de Flient Smart Lock bestaan; twee daarvan zijn gerapporteerd door Secura. Deze kwetsbaarheden, samen met bekende issues in vergelijkbare smart lock-producten, bieden waardevolle inzichten. Ze wijzen op terugkerende beveiligingspatronen binnen het smart lock-domein en moeten worden onderzocht binnen het Flient-systeem om de weerbaarheid ervan adequaat te kunnen beoordelen. Dit onderzoek ondersteunt de voorbereidingsfase van beveiligingstestactiviteiten binnen de *Library & Lab*-methode van het DOT-framework.

Security tests
Titel: NFC Copying via Flipper Zero
Verifiëren of de eerder ontdekte kwetsbaarheid van NFC-cloning nog steeds aanwezig is in de huidige versie van de Flient Smart Lock.

Bijbehorend CVE-nummer:
CVE-2023-50129

Testmethode:
Er werd gebruikgemaakt van een Flipper Zero-apparaat om het NFC-signaal van een geautoriseerde tag te lezen en vervolgens toegang te proberen verkrijgen met het gekopieerde signaal.

Procedure:
- Een geautoriseerde NFC-tag werd gescand met de Flipper Zero.
- De vastgelegde gegevens werden terug naar het slot geëmuleerd.
- Er werd geobserveerd of het slot de gekopieerde NFC-tag accepteerde.

Resultaat:
De kwetsbaarheid is nog steeds aanwezig: het slot accepteerde de gekopieerde NFC-tag. Een demovideo van de beveiligingstest is beschikbaar via de volgende link:
https://streamable.com/ncnp7u

Aanbeveling:
Gebruik nieuwere versies van de NFC-chips zoals de MIFARE DESFire EV2 en bijbehorende NFC-reader welke een hogere encryptie toepassen.

CVE-2023-50124 (Secura, 2023)
Tijdens het onderzoek is gebleken dat CVE-2023-50124, een kwetsbaarheid geïdentificeerd door Secura in de Flient Smart Lock, niet reproduceerbaar was binnen de scope van onze testopstelling. Het reproduceren van deze kwetsbaarheid vereist fysieke demontage van het apparaat en directe toegang tot interne hardwarecomponenten. Aangezien dit apparaat in bruikleen is verkregen, is ervoor gekozen het niet open te maken vanwege het risico op schade. Op basis van de beschikbare informatie verwachten wij echter dat deze kwetsbaarheid momenteel nog steeds aanwezig is, omdat er nog steeds gebruikt wordt gemaakt met dezelfde hardware sinds het rapport van Secura. De CVE is naar alle waarschijnlijkheid dus nog steeds uitvoerbaar, hoewel wij dit niet zelfstandig hebben kunnen bevestigen.

Hoe vatbaar is het Flient Smart Lock voor fysieke aanvallen bijvoorbeeld pincode, slot en vingerafdrukken?

Security test
Doel:
Onderzoeken hoe het Flient Smart Lock zich gedraagt bij fysieke aanvallen gericht op pincode, mechanisch slot en biometrische authenticatie.

Mechanisch slot (fysieke sleutel)
Bij onderzoek naar het mechanische slot is gekeken naar de opbouw van de sleutel en het gedrag van het slot tijdens lockpicking. De sleutel gebruikt een dimple-profiel met tweezijdige groeven en meerdere inkepingen. Pogingen tot lockpicking met standaard gereedschap lieten zien dat de pinnen telkens terugveerden naar hun oorspronkelijke positie, ondanks toegepaste torsiespanning. Dit wijst op een zekere mate van lockpicking-beveiliging.

Belangrijke bevindingen:

- Vermoedelijke aanwezigheid van anti-pick mechanismen zoals spool pins of false set bescherming.
- Standaard lockpicking-technieken zijn hierdoor niet effectief.

Pincode
Bij de pincode-invoer is specifiek gekeken naar mogelijke informatielekken via het fysieke gebruik van het toetsenpaneel. Vingerafdrukken en vetresten kunnen inzicht geven in welke toetsen frequent worden gebruikt, wat de kans op het achterhalen van de code vergroot.

Belangrijke bevindingen:

- Smudge attacks maken gebruik van vetvlekken om gebruikte toetsen te identificeren.
- Het aantal mogelijke codecombinaties kan hierdoor sterk worden verkleind.
- De kwetsbaarheid hangt af van:
- De lengte van de pincode.
- De aanwezigheid van lockout-mechanismen bij meerdere foute pogingen.
- Mogelijke randomisering van toetsen of andere aanvullende maatregelen.

In het geval van de Flient Smart Lock is vastgesteld dat na vijf foutieve pogingen het slot automatisch wordt gelocked. Ontgrendeling is daarna alleen mogelijk via het bijbehorende adminpaneel. Dit mechanisme bemoeilijkt brute-force aanvallen aanzienlijk. Hoewel smudge attacks theoretisch een zwakke schakel kunnen blootleggen, is het in de praktijk moeilijk om nauwkeurig de juiste pincode te achterhalen via vetvlekken alleen, zeker als het slot in een dynamische omgeving wordt gebruikt of regelmatig wordt gereinigd. Desondanks blijft het een aandachtspunt wanneer aanvullende beschermingen ontbreken.

Vingerafdrukscanner
De vingerafdrukscanner vormt een derde verificatiemethode. Hierbij is vooral gekeken naar de mogelijkheid om de scanner te misleiden via fysieke namaakvingers. Theoretisch kunnen achtergelaten vingerafdrukken worden gebruikt om mallen te maken.

Belangrijke bevindingen:

- Spoofing via siliconenafdrukken of 3D-printing is een bekend aanvalsscenario.
- De effectiviteit van deze aanval hangt sterk af van het gebruikte sensortype:
- Hoogwaardige sensoren met liveness detection bieden hiertegen weerstand.
- Goedkopere sensoren zonder anti-spoofingmaatregelen zijn gevoeliger.
- Zonder concrete informatie over de gebruikte scanner blijft dit een risicofactor.

In ons onderzoek is geprobeerd de scanner te misleiden met een eenvoudige namaakvinger, gebaseerd op een nagemaakte afdruk. Deze aanvalspoging is echter niet succesvol gebleken. Of dit te danken is aan ingebouwde anti-spoofingmaatregelen of aan andere technische eigenschappen van de scanner, konden we niet vaststellen vanwege gebrek aan inzicht in het exacte sensormodel. De kwetsbaarheid blijft daardoor theoretisch mogelijk, maar is in de praktijk door ons niet reproduceerbaar gebleken.

Conclusie
Het Flient Smart Lock toont in ons onderzoek een redelijke mate van fysieke beveiliging tegen veelvoorkomende aanvalstechnieken op drie belangrijke authenticatiemechanismen: het mechanische slot, de pincode-invoer en de vingerafdrukscanner.

Het mechanische slot, gebaseerd op een dimple-sleutelprofiel, vertoonde duidelijke weerstand tegen standaard lockpicking-technieken. De aanwezigheid van mogelijke anti-pickmechanismen zoals spool pins of false set-structuren maakte het ons niet mogelijk het slot succesvol te openen met conventioneel gereedschap. Dit duidt op een bovengemiddeld beveiligingsniveau binnen dit segment.

De pincode-invoer is in theorie kwetsbaar voor smudge attacks, waarbij vetresten op het toetsenpaneel aanwijzingen kunnen geven over de ingevoerde cijfers. In de praktijk bleek het echter lastig om daaruit betrouwbaar een volledige code te reconstrueren. Bovendien bevat het systeem een effectieve lockout-mechanisme: na vijf foutieve pogingen wordt het slot geblokkeerd, waarna alleen via het adminpaneel opnieuw toegang kan worden verkregen. Dit bemoeilijkt brute-force aanvallen aanzienlijk, al blijft het aan te bevelen om aanvullende beschermingen, zoals toetsrandomisatie, toe te passen.

De vingerafdrukscanner werd getest op gevoeligheid voor spoofing via een namaakvinger. Onze aanvalspoging mislukte, maar het blijft onduidelijk of dit te danken is aan liveness detection, sensorresolutie of andere ingebouwde beveiligingen. Door het ontbreken van documentatie over het gebruikte sensormodel blijft de kwetsbaarheid in theorie aanwezig, al konden wij deze niet bevestigen in de praktijk.

Samenvattend laat het Flient Smart Lock een gedegen fysieke beveiliging zien tegen standaard aanvalsmethoden. De combinatie van lockpicking-resistente mechanica, pincode-lockout en (mogelijk) anti-spoofing op biometrisch niveau draagt bij aan een solide algeheel beveiligingsniveau. Wel verdient het aanbeveling om transparantie te bieden over gebruikte technologieën en aanvullende maatregelen te overwegen tegen informatielekken via fysiek gebruik.

Community Research
Doel:
Peilen welke ervaringen, zorgen en kwetsbaarheden door gebruikers en experts in de community zijn gedeeld over soortgelijke smart locks.

Gevonden in literatuur en communities:
Volgens Secura zijn fysieke beveiligingsaspecten vaak onderbelicht bij smart locks. Fabrikanten richten zich meestal primair op de softwarematige kant.

Veel voorkomende community-zorgen:
- Slechte fysieke bouwkwaliteit maakt het slot kwetsbaar voor brute force (forceren van het slot).
- Gebruikers melden gevallen waarin goedkope sensors in de vingerafdrukscanner makkelijk te misleiden zijn.
- Pincode-lekken door smudge attacks zijn breed erkend als reëel risico.
- Sommige gebruikers melden dat mechanische back-up sleutels vaak slecht beveiligd zijn (matig complexe sleutels).

Aanbevelingen vanuit de community:
- Gebruik lange pincodes.
- Reinig regelmatig het keypad om vingerafdrukken te wissen.
- Gebruik covers of randomizer-opstellingen op het keypad.
- Combineer fysieke beveiliging altijd met softwarematige monitoring.

Aanvullende kwetsbaarheid geïdentificeerd door Secura
Secura heeft tijdens haar analyse een specifieke ernstige kwetsbaarheid vastgesteld (CVE-2023-50124), die directe gevolgen heeft voor de veiligheid van het biometrische systeem van het Flient Smart Lock.

De vingerafdrukscanner maakt gebruik van een AES1711-module, die zich fysiek in de deurklink bevindt. Twee schroeven aan de buitenzijde maken het relatief eenvoudig om de sensor los te halen. Door de sensor via UART aan te sluiten op een debug board, kan een aanvaller met behulp van het standaard ingestelde wachtwoord nieuwe vingerafdrukken toevoegen. Het slot controleert vervolgens alleen of de aangeboden vingerafdruk overeenkomt met een geregistreerde template, waarbij geen aanvullende authenticatie plaatsvindt.

Samengevat:
- De fysieke toegang tot de sensor is binnen enkele minuten te verkrijgen door het verwijderen van de externe schroeven.
- Via UART-toegang met standaard credentials kan een nieuwe vingerafdruk worden geprogrammeerd.
- Na herplaatsing van de sensor wordt enkel de nieuwe vingerafdruk geaccepteerd; de oorspronkelijke gebruiker wordt buitengesloten.
- Deze aanval is relatief eenvoudig uit te voeren en vereist slechts beperkte technische middelen.
- Het fundamentele probleem is dat het systeem vertrouwt op de integriteit van de opgeslagen vingerafdrukken zonder externe verificatie of versleuteling.

Conclusie Community Research
De community bevestigt dat fysieke aanvallen op smart locks een bekend probleem zijn, vooral bij goedkopere modellen zonder geavanceerde fysieke beveiliging. Zowel de pincode, sleutel als vingerafdrukscanner vormen potentiële aanvalsvectoren.

Conclusie

Het antwoord op de hoofdvraag is: ongeautoriseerde toegang tot het Flient Smart Lock is mogelijk. Hoewel het slot is uitgerust met moderne beveiligingstechnieken, blijken er in de praktijk zwakke plekken aanwezig te zijn die misbruik mogelijk maken.

Tijdens het onderzoek is duidelijk geworden dat het systeem gebruikmaakt van meerdere technologieën zoals Bluetooth, Wi-Fi, NFC en biometrie. Dit maakt het slot veelzijdig, maar vergroot ook de kans op kwetsbaarheden. De gebruikte encryptie voldoet deels aan de industrienormen, maar laat ruimte voor verbetering door het ontbreken van recente standaarden zoals AES-256 en TLS 1.3. Ook in de mobiele app werden beveiligingsproblemen gevonden, zoals hardcoded sleutels en verouderde cryptografie, waardoor manipulatie mogelijk is.

Verder is aangetoond dat bekende kwetsbaarheden nog steeds aanwezig zijn. Vooral de NFC-functionaliteit en fysieke toegang tot de vingerafdrukscanner bleken problematisch. Fysieke tests lieten zien dat het slot bestand is tegen standaardmethoden zoals lockpicking, maar niet volledig veilig is bij gerichte aanvallen.

Het onderzoek laat zien dat het Flient Smart Lock in theorie goed is beveiligd, maar dat in de praktijk verschillende zwakke plekken de deur openzetten voor ongeautoriseerde toegang. Dit benadrukt het belang van een betere implementatie van beveiligingsstandaarden en transparantie over de gebruikte technologieën.

Afbeeldingen

Bibliography

Aronsky, L. S. (2024, Februari 20). *Say Friend and Enter: Digitally lockpicking an advanced smart lock (Part 1: functional analysis).* Retrieved from alephsecurity: https://alephsecurity.com/2024/02/20/kontrol-lux-lock-1/

Blugate 66 | Full Lock system. (n.d.). Retrieved from https://www.fulllocksystem.com.ar/blugate-66/

Brook, C. (2024, March 24). *What Is Code Obfuscation & How Does It Work?* Retrieved from digitalguardian: https://www.digitalguardian.com/blog/what-code-obfuscation-how-does-it-work

contributors, W. (n.d.). *Transport layer security*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Transport_Layer_Security

DigiKey Employee. (2021, Maart 4). *A basic introduction to BLE 4.X Security - Wireless and IoT / RF and Wireless - DigiKey TechForum - an electronic component and Engineering solution Forum.* Retrieved from DigiKey TechForum - an Electronic Component and Engineering Solution Forum.: https://forum.digikey.com/t/a-basic-introduction-to-ble-4-x-security/12501

Hick, B. (2021, January 27). *Android's "Dangerous" Permissions*. Retrieved from thebinaryhick: https://thebinaryhick.blog/2021/01/26/androids-dangerous-permissions/

Hlapisi, N. (2023, September 22). *Bluetooth LE: security modes and procedures explained*. Retrieved from Technical Articles: https://www.allaboutcircuits.com/technical-articles/bluetooth-le-security-modes-and-procedures-explained/

How August Smart Locks work. (n.d.). Retrieved from August Home: https://august.com/pages/how-it-works

How August Smart Locks work | August Home. (n.d.). Retrieved from https://august.com/pages/how-it-works

How to use NFC door locks (and unlock them with a phone). (n.d.). Retrieved from https://www.getkisi.com/academy/lessons/how-to-use-nfc-door-locks

Patil, K. (2025, March 25). *Why Is TLS 1.3 Better And Safer Than TLS 1.2?* Retrieved from appviewx: https://www.appviewx.com/blogs/why-is-tls-1-3-better-and-safer-than-tls-1-2/

Ren, K. (2025, May 1). *Bluetooth LEsecure connections - numeric comparison*. Retrieved from Bluetooth® Technology Website: https://www.bluetooth.com/blog/bluetooth-pairing-part-4/

Secura. (2023, 1 1). *Safety risks in common smart home devices*. Retrieved from www.secura.com: https://www.secura.com/services/iot/consumer-products/security-concerns-in-popular-smart-home-devices

The md5 hashing algorithm is insecure. (n.d.). Retrieved from datadoghq: https://docs.datadoghq.com/security/code_security/static_analysis/static_analysis_rules/go-security/import-md5/

TTLock Locks | Seam API Docs. (n.d.). Retrieved from https://docs.seam.co/latest/device-and-system-integration-guides/ttlock-locks

WPA3 | TP-Link. (n.d.). Retrieved from TP-Link: https://www.tp-link.com/us/wpa3/