SICHERHEIT IST UNSERE PRIORITÄT

IN UNSEREN SMART SPACE LÖSUNGEN KOMMUNIZIEREN EINE REIHE VON BESTANDTEILEN KONTINUIERLICH MITEINANDER. UNSER HAUPTANLIEGEN IST ES DABEI DIESE KOMMUNIKATION SO ZUVERLÄSSLICH UND KRYPTOGRAPISCH SICHER WIE NUR MÖGLICH ZU MACHEN.

Bei der Sicherheit in der digitalen Welt ist es wichtig konstant darauf zu achten, dass man regelmäßig die möglichen Gefahren überwacht, bewertet und entsprechend antwortet. Mit diesem Grundprinzip im Hinterkopf haben wir unser Ökosystem so gestaltet und gebaut, dass wir kryptographisch-signierte Aktualisierungen -inklusive Sicherheitsbehebungen und Verbesserungen- schnell und transparent bereitstellen zu können: Ohne Auswirkungen auf unsere Kunden oder generell Personen, die mit unseren Smart Spaces interagieren.
Neben der Fähigkeit, schnell auf Sicherheitsprobleme antworten zu können, folgen wir aktuellsten open-source Sicherheitsstandards, die durch Fachleute begutachtet und verifiziert wurden. In Übereinstimmung mit eben diesen bewährten Sicherheitsstandards entwickeln wir deswegen nicht unsere eigenen Sicherheitskomponenten, sondern nutzen bereits etablierte.

Ziel dieses Dokumentes ist es, sie darüber aufzuklären, was der momentane Stand ist und wie die zukünftige Weiterentwicklung der Sicherheitskomponenten aussieht.

SMARTPHONE

Sowohl bei Android als auch bei iOS, verlassen wir uns, wo es sinnvoll und möglich ist, auf die bereits existierenden Sicherheitsstrukturen der Betriebssysteme. Das bedeutet, dass jegliche Sicherheitsaktualisierungen die von Google oder Apple ausgerollt werden, automatisch auch die Sicherheit unserer eigenen Applikation verbessern.

Neben dem Fokus auf kryptographische Sicherheit stellen wir auch sicher, dass die Benutzer der App sich mindestens einmal authentifizieren müssen, bevor sie die Möglichkeit haben mit der App zu interagieren; auch hier basierend auf etablierten und bewährten Standards der Betriebssysteme. Typischerweise sind das Fingerabdruck-, Gesichtserkennung- oder PIN-Authentifizierungsverfahren.

ZUGANGSDATEN SPEICHER

iOS bietet ein zentrales System zur Speicherung von Zugangsdaten an namens Keychain[1]. So wie alle Apple Anwendungen, verwenden auch wir Keychain, um die Zugangsdaten für die Back-end-Infrastruktur zu speichern.

Android bietet ein ähnliches zentrales System zum Speichern von kryptographischen Schlüsseln und Verschlüsselungsverfahren an namens AndroidKeyStore[2]. Ebenso wie Google dies für alle eigenen Anwendungen nutzt, greifen wir auf dieses System zurück, um Zugangsdaten zu ver- und entschlüsseln.

SMARTPHONE UND ACCESS HUB

Die Kommunikation zwischen dem Smartphone und unserer Hardware (z.B. dem Access Hub) erfolgt über den Bluetooth Low Energy[3] (BLE) Standard. Diese Technologie wird unter anderem in medizinischen Geräten, Smart-Tags, Fitnessarmbändern, und vielen weiteren Bereichen verwendet und ist eine Weiterentwicklung des Bluetooth Standards.

Neben der BLE eigenen Authentifizierungs-schicht, verschlüsseln wir zusätzlich alle vertraulichen Daten, welche vom Smartphone zu unserer Hardware und zurück gehen, mit RSA[4] Private-Public-Key-Verschlüsselung.

SMARTPHONE UND BACK-END

Für die Kommunikation zwischen dem Smartphone und unserer Back-end-Infrastruktur benutzen wir die aktuellste Version des TLS[5] Protokolls (1.2 und 1.3) . Um Man-in-the-Middle-Angriffen vorzubeugen, benutzt unser System HTTP-Public Key-Pinning[6].

[1] https://developer.apple.com/documentation/security/keychain_services
[2] https://developer.android.com/training/articles/keystore
[3] https://en.wikipedia.org/wiki/Bluetooth_Low_Energy
[4] https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[5] https://en.wikipedia.org/wiki/Transport_Layer_Security

So stellt das System sicher, dass die Kommunikation zwischen Smartphone und der Plattform API abgelehnt wird, wenn sie nicht mit dem Zertifikat von Sensorberg signiert wurde.

Sensorberg benutzt OAuth2[7], den Industriestandard für Authentifizierung von Benutzern. Dies ermöglicht uns, dass jedes Smartphone ein einzigartiges Token zur Kommunikation mit unserer API zugewiesen bekommt. Erst damit wird es möglich, Zugangskontrolle und Berechtigungen im Detail zu kontrollieren. In Notfällen können Tokens in unserer Plattform widerrufen bzw. gelöscht werden, um Geräten den Zugang zu verwehren, die keine Berechtigungen mehr haben.

Die Kommunikation innerhalb der Gebäudeinfrastruktur geschieht vollständig über RSA-Private-Public-Key-Verschlüsselung in Kombination mit der AES-Verschlüsselung (128-GCM, 192-GCM oder 256-GCM, abhängig vom Betriebssystem des Smartphones). Das bedeutet dass die Kommunikation von keinem anderen System innerhalb der selben Netzwerkstruktur entschlüsselt werden kann.

SMARTPHONE UND DRITTANBIETER-SYSTEME

Wir sind der Auffassung, dass die Verantwortung für ein sicheres System die Kommunikation mit Drittanbietern wie BlueID[8] und MyRenz miteinschließt. Deshalb arbeiten wir eng mit unseren Partnern zusammen, um sicherzustellen, dass Industriestandards wie z.B. TLS-Verschlüsselung und Public-Key-Pinning konsequent eingesetzt werden.

Wenn unsere Lösung mit Identitätsanbietern kommuniziert (wie z.B. OpenID, Cobot, oder Google's Identitätsplattform), stellen wir sicher, dass diese Dienste ebenfalls TLS 1.2 bzw. TLS 1.3 Verschlüsselung forcieren.

BACK-END

Unser Back-End ist die zentrale Verwaltungsstelle der Sensorberg Lösung. Sie ermöglicht es, den Benutzern Geräte, Sensoren und Berechtigungen aufzusetzen und zu managen.

Die Rechenzentren der Cloud-Dienstanbieter, auf denen unsere Anwendung läuft, sind alle in Deutschland angesiedelt. Deswegen ist der interne Datenverkehr geschützt vor Manipulation, weil Sensorberg die vollständige Kontrolle über diese Kommunikation hat.
Mehr Details und genauere Angaben über die hauseigenen Vorkehrungen finden sie direkt bei Hetzner und der Deutschen Telekom.

[6] https://en.wikipedia.org/wiki/HTTP_Public_Key_Pinning
[7] https://oauth.net/2/
[8] https://www.blueid.net/technology/security/

Verbindungen zu den Servern können nur ausgewählte Mitglieder des Sensorberg Infrastrukturteams über Virtual-Private-Networks[9] herstellen. Zugang zu diesen VPN benötigt ein kurzlebiges einmaliges Passwort-Token und die Secure Shell[10] mit Key-Exchange. Jeder Zugriffsversuch auf die Server wird aufgezeichnet in Audit-Logs, und jeder Befehl und Veränderung an den Servern wird in eine “Append-only” zentrale Logging-Instanz geleitet.

Unsere Infrastruktur wird über verschiedene Konfigurations-Management-Systeme verwaltet, von denen alle versionskontrolliert und automatisch getested sind. Zusätzlich wird jede Stunde ein Backup von allen Datenbanken erstellt.

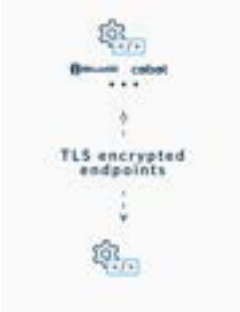
SMARTPHONE UND DRITTANBIETER-SYSTEME

Die Kommunikation zwischen dem Browser eines Smartphones und unserem Back-end ist nur möglich über TLS 1.2 bzw. TLS 1.3 Verschlüsselung. Zusätzlich verwenden wir bewährte Web-Design-Praktiken, um uns gegenüber allen üblichen Browserattacken, wie z.B. Cross-Site-Scripting und Man-In-The-Middle-Attacken zu schützen.

Alle Cookies die von unserem Back-End kommen, werden als Secure-Cookies[11] ausgestellt. Das heißt, dass der Inhalt der Cookies nur von einer validen Back-End-Domäne von Sensorberg und nur von Skripten geladen werden kann, die über eine sichere TLS-Verbindung hergestellt wurden.

BACK-END UND ACCESS HUB

Wenn Benutzer aus der Ferne mit unseren Geräten interagieren möchte, z.B. um Rollläden im Büro zu schließen von zu Hause aus, wird dem Access Hub ein spezieller Befehl geschickt, den er auf einem Aktuator ausführt. Für genau diese Kommunikation benutzen wir SaltStack[12], welches selbst ZeroMQ benutzt.
Jegliche Kommunikation über ZeroMQ ist vollständig verschlüsselt[13] mit Hilfe von elliptischen Kurven[14].



BACK-END UND DRITTANBIETER-BACK-ENDS

Für alle Drittanbieterintegrationen (wie z.B. einer “Resource-Management-Plattform wie Cobot), stellen wir sicher, dass die Kommunikation nur über sichere TLS-verschlüsselte Endpunkte stattfindet. Zu keinem Zeitpunkt werden Informationen unverschlüsselt über öffentliche Netzwerke geschickt.

[9] https://en.wikipedia.org/wiki/Virtual_private_network
[10] https://en.wikipedia.org/wiki/Secure_Shell
[11] https://en.wikipedia.org/wiki/Secure_cookie
[12] https://www.saltstack.com/
[13] http://zeromq.org/topics:encryption
[14] https://en.wikipedia.org/wiki/Curve25519

ACCESS HUB

Der Access Hub ist das einzige Element in unserer Infrastruktur, welches direkt verbunden ist mit den Aktuatoren und Sensoren.

Es wird daher empfohlen, dass diese Geräte Teil eines eigenen separaten Virtual-Local-Area-Network (VLAN) sind, um die Sicherheit zu verstärken. Ebenso empfehlen wir den Access Hub von anderen Geräten im lokalen Netzwerk zu separieren, weil man so die Anzahl der möglichen Attacken wie z.B. Brute-Forcing oder einem Überladen der Geräte mit zu vielen Anfragen verhindert.

ACCESS HUB UND SENSOREN BZW. AKTUATOREN

Die Sicherheit bei der Kommunikation zwischen dem Sensorberg Access Hub und Drittanbietersensoren/-aktuatoren hängt von den Standards und Protokollen dieser selbst ab. Sensorberg unterstützt und pflegt eine Liste von Standards und Protokollen, können diese aber nicht auf den Drittanbietergeräten selbst forcieren. Aufgrund dieser Tatsache senden wir nur simple Gerätebefehle und Informationen und keinerlei sensible und vertrauliche Informationen wie Benutzerdaten an die Drittanbietergeräte. Alle weiteren Details der Sicherheitsstandards und Protokolle (e.g. ZWave[15]) von Drittanbietergeräten können auf Wunsch im Detail besprochen werden.

BUILDING HUB

Das Building Hub hat die Aufgabe alle Access Hubs in einem Gebäude zu koordinieren und zu überwachen. Die Hauptaufgaben liegen also im Überwachen, Warten, Zwischenspeichern der Zugangsberechtigungen und der lokalen Gerätesteuerung.

[15] https://en.wikipedia.org/wiki/Z-Wave#Security

Es ist also eine Kernkomponente jedes Gebäudes, um sicherzustellen, dass das System zu jeder Zeit die Zugangskontrolle bieten kann, auch wenn das Internet einmal ausfällt.

BUILDING HUB UND BACK-END

Die gesamte Kommunikation zwischen dem Building Hub und dem Back-End findet mit Hilfe von TLS-Verschlüsselung und Zertifikaten statt.

BUILDING HUB UND ACCESS HUB

Die gesamte Kommunikation zwischen Building Hub und Access Hubs findet im Rahmen eines dedizierten VLAN statt und ist somit auf eine eigene Netzwerkschicht isoliert, welche sie unerreichbar für andere Geräte im Netzwerk macht. Zusätzlich wird die Verbindung selbst mit TLS verschlüsselt.

ZUSÄTZLICHE INFORMATIONEN

Fall sie weitere Informationen zum Thema Sicherheit und den Produkten benötigen, finden sie diese im Documentation Portal[16], Developer Portal[17], oder kontaktieren sie uns unter security@sensorberg.com

[16] https://documents.sensorberg.com
[17] http://developer.sensorberg.com