REAL OPTIC

Seguridad Digital Integrada

sera4

Control de Acceso con Criptografía Asimétrica

Sera4 ha diseñado una solución de control de acceso sin llaves que utiliza criptografía asimétrica para implementar de forma segura llaves digitales en dispositivos móviles.

- El servidor de Teleporte utiliza una llave privada criptográfica como raíz de confianza para firmar certificados digitales con información de acceso, que representa la versión digital de la *llave de la cerradura*.
- El servidor también utiliza una llave pública criptográfica que se distribuye a los dispositivos móviles inalámbricos para que puedan validar la autenticidad de las cerraduras cuando se detectan.
- La llave pública criptográfica también se distribuye a las cerraduras de fábrica para validar la identidad de los dispositivos móviles inalámbricos.

La criptografía asimétrica proporciona un mecanismo de autenticación bidireccional confiable, a través de certificados digitales, para validar la identidad de los dispositivos móviles y las cerraduras.

Bluetooth con Criptografía Asimétrica

Sera4 también utiliza principios de criptografía asimétrica para cifrar la comunicación entre dispositivos móviles y cerraduras.

- Bluetooth solo se utiliza como canal de transporte para comunicar los controladores Sera4 con dispositivos móviles. Esto significa que los mecanismos y protocolos de seguridad Bluetooth, incluyendo emparejamiento, no se utilizan.
- Cada controlador utiliza un generador de números aleatorios basado en hardware para derivar su propio conjunto de llaves criptográficas privadas y públicas.
- Las llaves públicas criptográficas se comparten con dispositivos móviles para que puedan encriptar la información de acceso enviada a los controladores a través de Bluetooth.
- Los controladores utilizan la llave privada criptográfica para descifrar la información. Esta llave privada nunca es compartida ni vista por nadie. Incluso si fuera posible, hackear una llave privada solo daría acceso a una sola cerradura.
- Para obtener más información, consulte las patentes de seguridad digital de Sera4: (***US Patents 10,008,061, 10,403,070***)

Algoritmo de Encriptación

Sera4 utiliza el estándar ECDSA (Algoritmo de firma digital de curva elíptica) de 192 bits, recomendado por NIST, para firmar digitalmente certificados, proporcionar autenticación y encriptar comunicaciones.

- ECDSA proporciona la misma seguridad criptográfica con tamaños de llave más pequeños en comparación con otros algoritmos. Esto nos permite proporcionar las mismas protecciones que los más grandes (como 256 bits) algoritmos de forma mas eficiente.
- La implementación de curvas elípticas en criptografía es ideal para aplicaciones IoT (internet de las cosas), ya que permite la escalabilidad de soluciones para admitir un número ilimitado de usuarios y cerraduras.
- La criptografía de curva elíptica también se utiliza ampliamente en aplicaciones de computación en la nube, que es el caso de las monedas criptográficas como Bitcoin y Ethereum.

Otras Características de Seguridad

Autenticación con Límite de Velocidad

Los controladores utilizan la limitación de velocidad basada en el tiempo de las autenticaciones para garantizar que el sistema no pueda ser manipulado con códigos de bloqueo en ataques de fuerza bruta.

Reloj en Tiempo Real

Cada controlador tiene un reloj en tiempo real para un seguimiento de tiempo independiente. Esto evita ataques "basados en el tiempo" en los que los hackers intentan modificar la validez de las llaves y el registro de acceso cambiando la fecha y la hora de sus dispositivos móviles.

Almacenamiento Integrado sin Información de Identificación Personal (PII)

Los registros de acceso se almacenan en el controlador; cuando los registros no son transferidos de nuevo a los servidores de Teleporte por el usuario iniciador, los registros se guardan y se envían cuando otros usuarios realizan transacciones con el controlador en el futuro. Además, los registros almacenados en el controlador no contienen ningún PII, de esta forma cualquier acción malintencionada no podrá exponer información personal.

REAL OPTIC

Diferenciadores Inalámbricos

sera4

sera4

Recopilación automática de registros de accesos almacenados en cerraduras por medio de dispositivos móviles cercanos .

Detección pasiva. Los controladores Sera4 siempre son detectables.

No se utiliza emparejamiento

La arquitectura Sera4 está patentada para usar certificados digitales, al igual que la banca por Internet.

Solo se usa la capa de transporte de los estándares Bluetooth

ECDSA permite la máxima seguridad para el menor número de bits - transmisiones de menor potencia

Cifrado asimétrico patentado NIST utilizando ECDSA de 192 bits

La asignación de usuario y llave se maneja independientemente

Si la llave privada del servidor de una empresa se ve comprometida, no afectará a otros clientes de Sera4

Las llaves Sera4 se firman como certificados digitales mediante llaves privadas específicas de la empresa, con el servidor Teleporte del cliente como raíz de confianza

Triple sincronización de registros de acceso entre controlador, móvil y servidor, utilizando relojes independientes

Descubri-miento → Empareja -miento → Conexión → Encripta-ción → Validación de Usuario → Validación de Llave → Validación de Actividad

Código PIN y lista de emparejamiento

El emparejamiento no permite que dispositivos móviles infinitos se conecten a la cerradura, ya que necesita almacenar información para cada cerradura.

Estándares de Bluetooth con vulnerabilidades conocidas, generalmente AES de 128 bits.

Se envía un token a la cerradura para verificar la coincidencia

Otras Soluciones

Se necesita presionar el botón para activar

Dependencia de Botones con fallas que pueden causar problemas de conexión

Se utilizan los estándares de encriptación y encapsulación de Bluetooth.

La seguridad de Bluetooth continúa comprometida, su modelo de seguridad es fundamentalmente complejo y vulnerable debido a la amplia gama de uso y la necesidad de admitir muchos dispositivos y aplicaciones.

Cualquier persona con un código abierto puede abrir una cerradura

Suposición de éxito o retorno de estado único