Vulnerabilidades en dispositivos de monitorización continua de glucosa

Análisis técnico del sistema Abbott FreeStyle Libre 14-Day

RF Village HackGDL 2025:

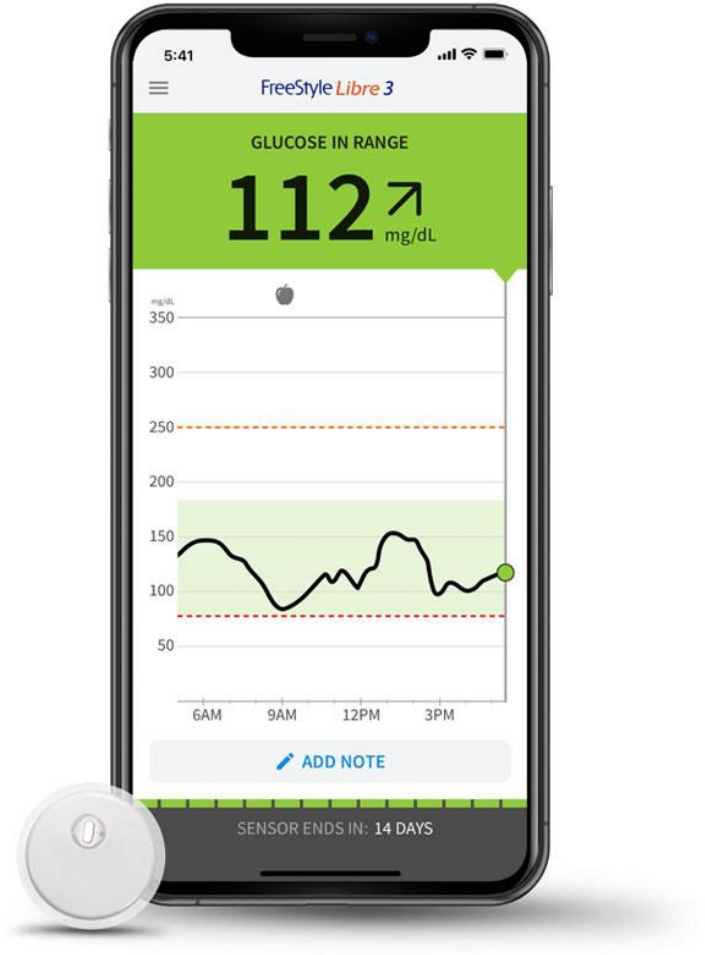
Wulfrano Moreno / wulfrano@mexbalia.mx

Acerca de mí

- CTO, empresario, arquitecto empresarial e instructor
- Entusiasta de la ciberseguridad
- 30 años en TI
- 25 años Web/Nube (1,2,3)
- Amplia experiencia en diversos escenarios de integración
- Certificaciones TI
- Creador digital
- OpenEnchilada OG

Agenda

1. Introducción al sistema FreeStyle Libre
2. Aplicaciones médicas y validación clínica
3. Diseño biomédico y características técnicas
4. Aspectos químicos del sensor
5. Hardware y firmware
6. Vulnerabilidades identificadas
7. Prueba de concepto
8. Demo
9. Implicaciones éticas y médicas
10. Estrategias de mitigación
11. Conclusión



Introducción al FreeStyle Libre

- Propósito: Monitorización continua de glucosa (CGM) para diabetes.
- Tecnologías clave:
  - Sensor subcutáneo con NFC pasivo (13.56 MHz).
  - Mide glucosa en líquido intersticial (sin punción en dedo).
- Beneficios:
  - Menos invasivo
  - Datos en “tiempo real”
  - Integración de sensores y plataformas digitales

Aplicaciones médicas y validación clínica

Uso en diabetes

- Tipo 1 y 2
- Gestacional

Monitorización remota y telemedicina

Alta precisión (

- MARD ~9,4%
- Zona A de error

Aprobaciones

Diseño biomédico y características técnicas

Biocompatibilidad y Portabilidad

- Adhesivo hipoalergénico
- Resistente al agua y al sudor

Mecánica del sensor

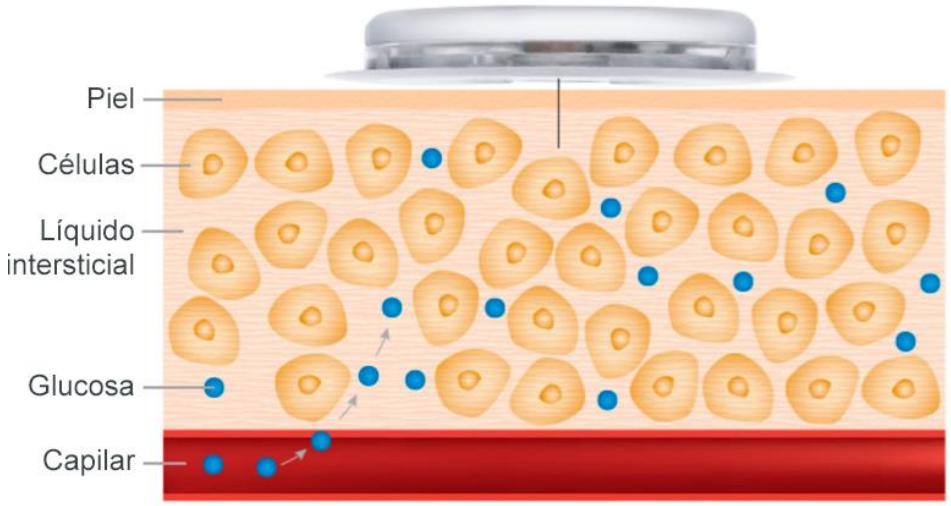
- Microfilamento biocompatible (5 mm bajo la piel).
- Reacción enzimática (glucosa oxidasa → peróxido de hidrógeno → señal eléctrica).

Transmisión de datos

- NFC 13.56 MHz ISO/IEC 14443 (almacena datos cada 60 segundos, 8 horas de historial).
- Sin batería: alimentado por el lector durante el escaneo.

Aspectos químicos del sensor

- Cableado enzimático:
  - Uso de glucosa oxidasa (GOx) modificada con polímeros redox (osmio).
  - Transformación de la enzima en un conductor de carga
  - Generación de corriente proporcional a la concentración de glucosa
  - Evolución desde el cableado con ferroceno hasta hidrogeles redox
- Ventajas: No lixiviables, permeables a la glucosa.
- Comparación de mediciones: Retraso de 5-10 minutos vs. glucosa en sangre.



Hardware y Firmware

- Componentes clave:
  - Chip RF430 TAL TI (procesamiento NFC, memoria FRAM).
  - Sensor de temperatura (termistor para calibración).
  - Antena NFC y batería de respaldo.
- Diseño:
  - Ensamblaje compacto y sellado
  - Protección de memoria mediante CRC16 para integridad de memoria y contraseñas
- Limitaciones: Chip Texas Instruments personalizado sin documentación pública.

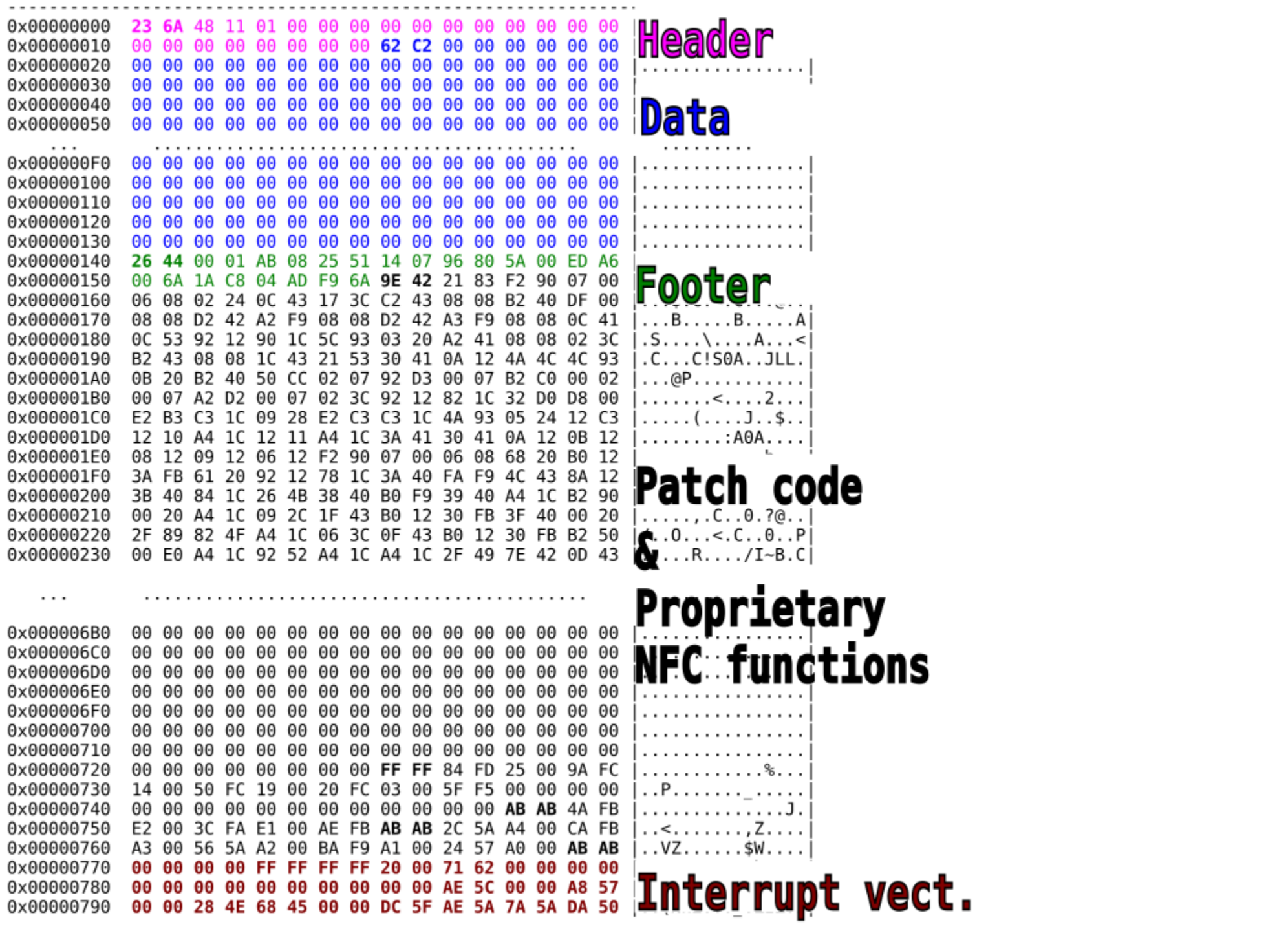
Vulnerabilidades identificadas

- Riesgos en NFC:
  - Ataques de repetición.
  - Inyección de datos.
  - Manipulación de memoria.
- Ejemplos:
  - Alteración del tiempo de uso del sensor.
  - Anulación de bloqueo geográfico.
  - Falta de autenticación mutua.

Prueba de Concepto (NFC)

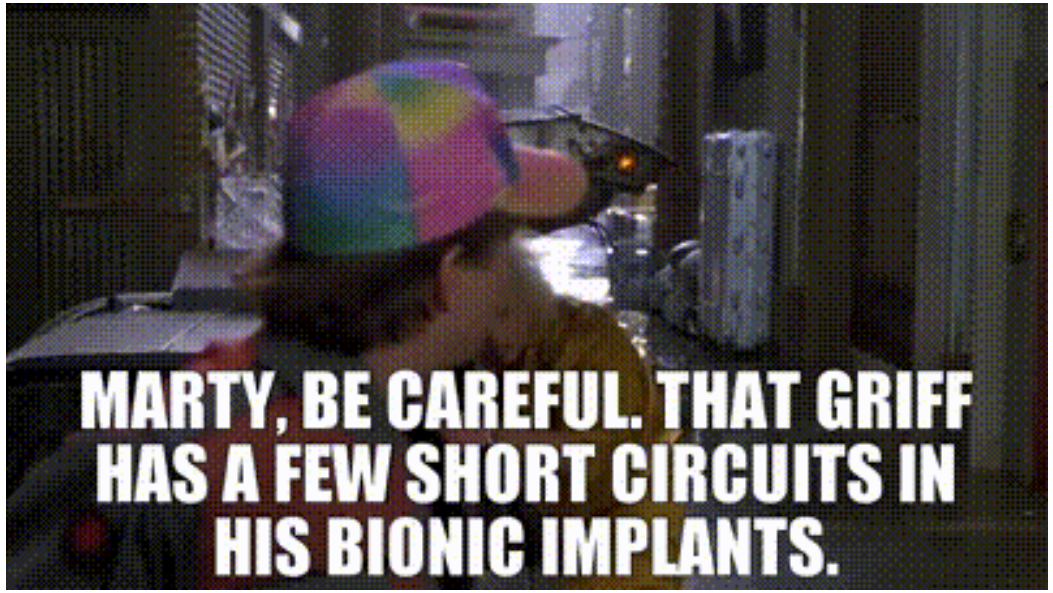
- Hardware usado: HunterCat NFC (Electronic Cats)
- Implicaciones en la manipulación de datos y en el estado del sensor
- Pasos:
  - Configuración y conexión hardware
  - Captura y análisis de datos NFC
  - Reproducción de datos para demostrar vulnerabilidades

Demo


Header
Data
Footer
Patch code
&
Proprietary
NFC functions
Interrupt vect.

Implicaciones éticas y médicas

- Riesgos para pacientes:
  - Sobredosis de insulina por datos falsos.
  - Privacidad: Exposición de historiales médicos.
- Regulatorios: Sensores manipulados infringen certificaciones (FDA/CE).
- Éticos: Mercado negro de sensores pirateados.



Estrategias de mitigación

Mejoras técnicas

- Cifrado NFC (ej. AES) y códigos rodantes.
- Autenticación mutua sensor-lector.
- Actualizaciones periódicas de firmware.

Ciberseguridad en dispositivos biomédicos

- Reforzamiento de normativas y estándares

Concientización

- Educación de usuarios sobre riesgos.
- Aplicaciones móviles con anti manipulación.

Conclusión

- Fortalezas:
  - Innovación en CGM.
  - Precisión clínica.
  - Portabilidad.
- Retos:
  - Las vulnerabilidades identificadas plantean riesgos significativos, especialmente en la manipulación de datos.
  - Se requieren medidas integrales de seguridad para salvaguardar la salud del paciente.
  - Retraso en mediciones.
  - Vulnerabilidades NFC.
- Futuro:
  - Equilibrar avances tecnológicos con robustos mecanismos de seguridad.
  - Integración de Bluetooth para alertas en tiempo real.
  - Sensores más seguros con IA y biosensores avanzados (parches de microagujas).