Universidad de los Andes

IoT: Utilidad (Comodidad)
vs.
Privacidad
Análisis de Seguridad de Dispositivos IoT

4to Foro en seguridad de la Información

Sandra Julieta Rueda Rodríguez, Ph.D.
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes
e-mail : sarueda @ uniandes.edu.co
http://sistemas.uniandes.edu.co/~sarueda

Agenda

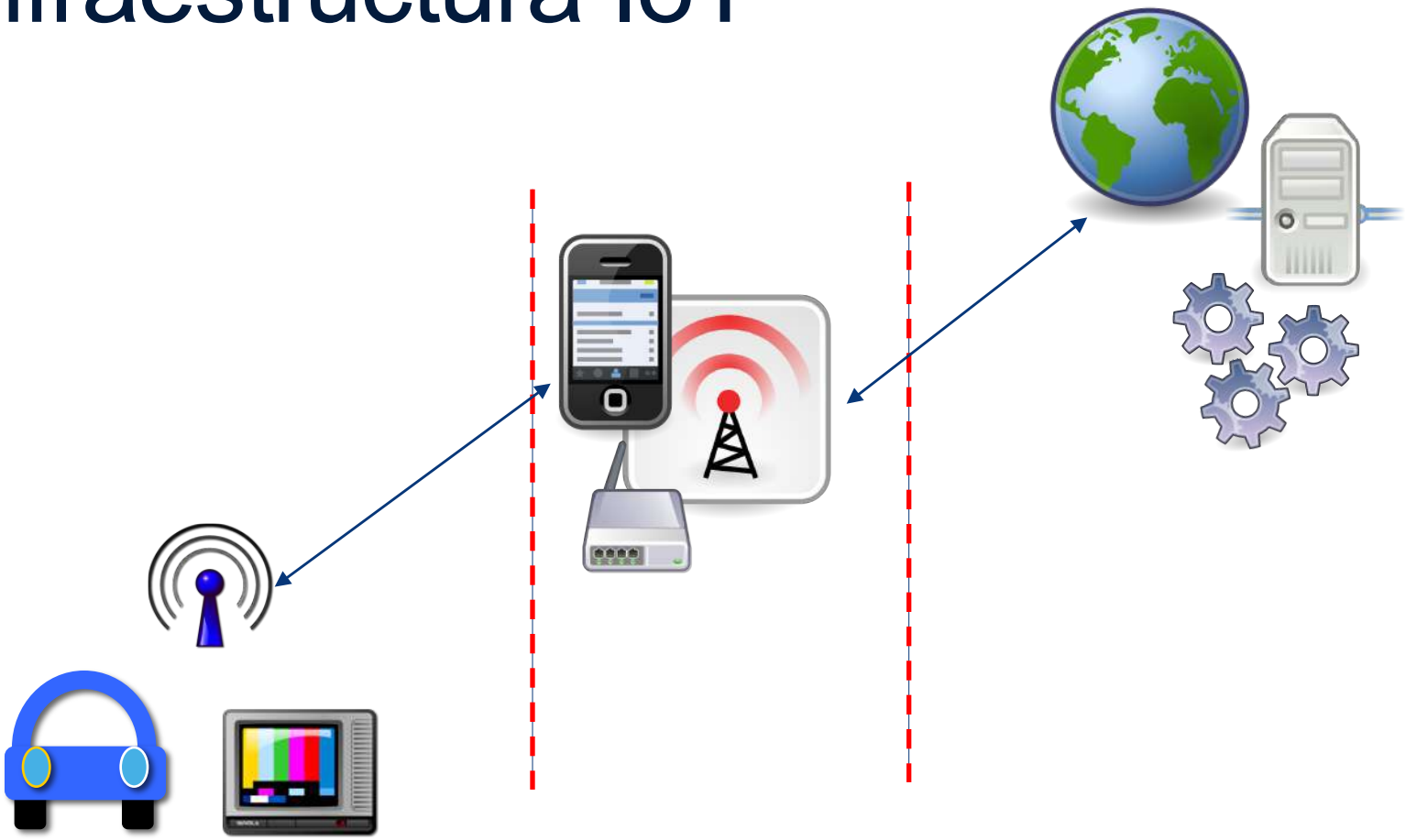
- Contexto
- Necesidades de Seguridad
- Casos de Estudio (wearables)
- Otros Casos
- Conclusiones

IoT

- Objetos variados están conectados
  - Electrodomésticos
  - Vehículos
  - Implantes médicos
- Creación de múltiples aplicaciones y entornos *inteligentes*
  - Smart Home
  - Smart City
  - Smart Grid

Universidad de los Andes

Infraestructura IoT



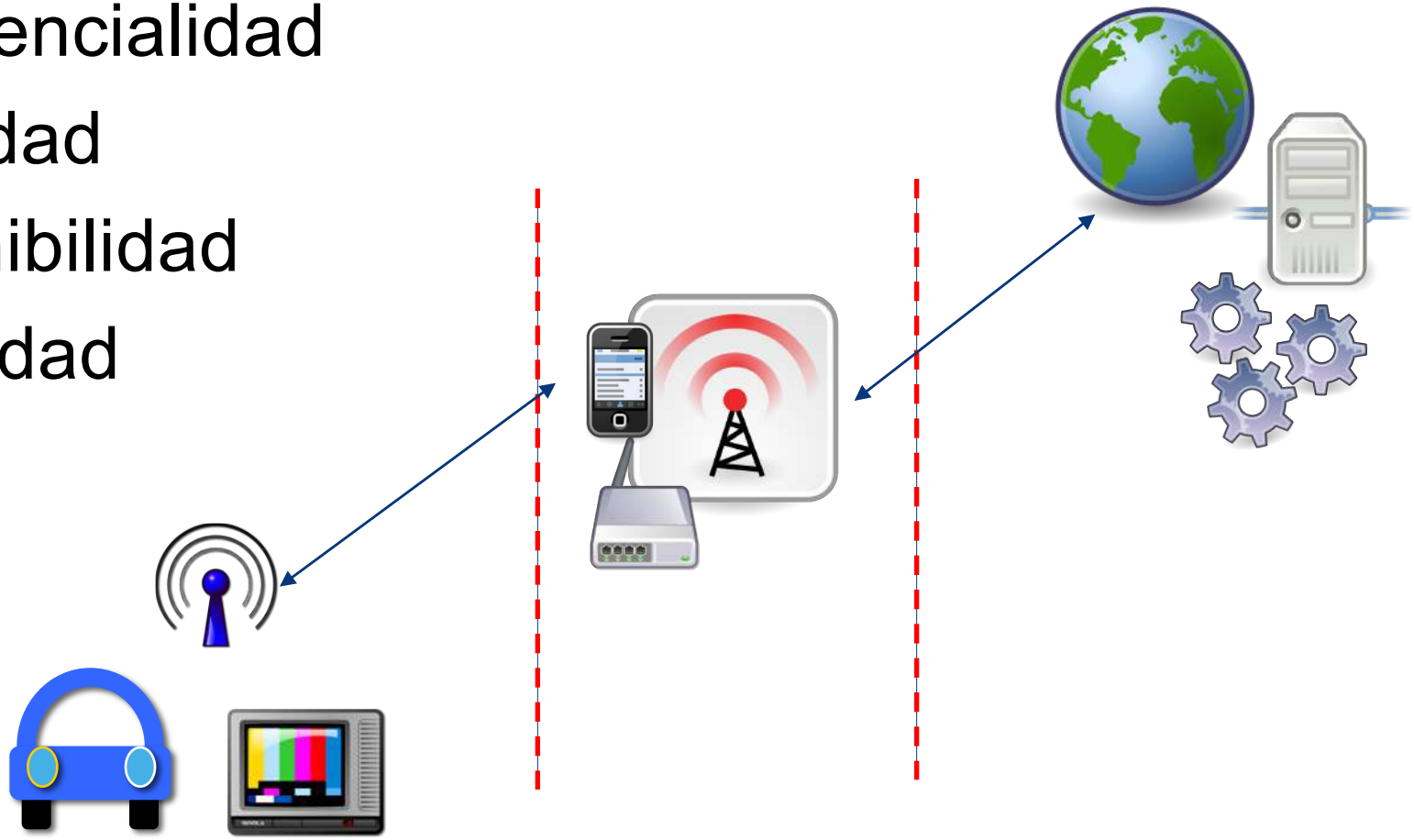
Dispositivos
Sensores

Servidor Personal
PC o celular inteligente
Aplicación o App

Decisiones
Usuarios y Aplicaciones

Necesidades de Seguridad

- Confidencialidad
- Integridad
- Disponibilidad
- Privacidad

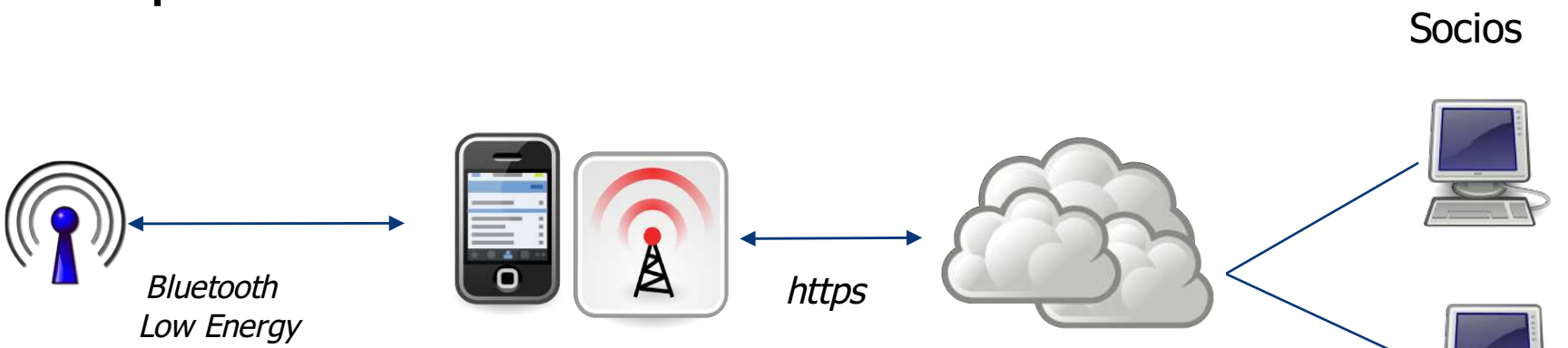


Seguridad y Privacidad en IoT

- Curso en verano 2017
  - Álvaro Cárdenas. University of Texas, Dallas
  - Sandra Rueda. UniAndes
- Proyecto:
  - Análisis de seguridad de dispositivos IoT
  - Esta presentación muestra los resultados de tres trabajos
    - Los demás trabajos también cuestionan el manejo apropiado de la privacidad por parte de los fabricantes de dispositivos IoT

Wearables

- Componentes



Dispositivo Wearable

Obtiene y almacena los datos

App

Recoge los datos (del dispositivo) para presentarlos al usuario y enviarlos al sitio web

Cloud
Servicios
Sitio web

Los usuarios pueden crear cuentas para ver sus datos (configuran edad, ubicación, email, perfil en redes sociales, etc.)

Terceros pueden tener acceso a los datos para mejorar el servicio.

[Alvaro Cárdenas – UT Dallas]

Wearables

Andrés González
Fernando Muñoz
Gustavo Salazar

- Garmin Forerunner 35
  - Dispositivo
    - Reloj Inteligente de gama media
    - GPS integrado para medir distancia y velocidad
    - Monitor de actividad y frecuencia cardiaca
    - Notificaciones inteligentes
  - App
    - Plataformas Android y iPhone
    - Permite hacer seguimiento de la actividad física
    - Fijar objetivos y evaluar cumplimiento
  - Comunidad en línea
    - Permite almacenar, analizar y compartir datos de la actividad física

Wearables

Andrés González
Fernando Muñoz
Gustavo Salazar

- Garmin Forerunner 35
  - Usa BlueTooth Low Energy (BLE) para comunicación inalámbrica con un celular o dispositivo similar
    - Anuncia su presencia en texto plano y legible
    - Establece sesión con el celular (emparejamiento)
    - Cambia su dirección MAC para evitar ser rastreado

Bluetooth Low Energy (BLE)

- Características:
  - Rango corto, huella baja de consumo

Periférico
. El dispositivo con menor capacidad
. Se anuncia
. Duerme y se despierta para anunciarse

Central
. PC o teléfono inteligente
. Escanea buscando anuncios
. Inicia la conexión ante un anuncio

- Seguridad:
  - Pairing (solo el central autorizado tendrá acceso a los servicios)
  - Uso de direcciones aleatorias (evita ser rastreado)

Wearables

Andrés González
Fernando Muñoz
Gustavo Salazar

- Garmin Forerunner 35
  - Permisos de la aplicación
    - Lectura del calendario, contactos, ubicación (fina y gruesa), estado del teléfono, cuentas de servicios
    - Lectura y escritura de log de llamadas y memoria externa
    - Uso de la cámara, recibir y enviar SMS
  - Livetrack
    - Permite generar URL para compartir la información (ubicación, velocidad, calorías gastadas)
    - La URL es enviada sobre http
    - El acceso no requiere autenticación

Wearables

Juan Carlos Arévalo
Jhon Fernando Avila
Julián Mauricio Jaramillo

- Spire Activity Tracker
  - Dispositivo
    - Monitorea la respiración
    - Envía los datos a la aplicación
    - La aplicación envía los datos a la nube
  - App
    - Deduce “estados anímicos” con base en la respiración
    - Muestra datos en tiempo real
    - Produce estadísticas de la última semana y el histórico
    - Envía notificaciones inteligentes
    - Permite fijar objetivos y evaluar cumplimiento

Wearables

Juan Carlos Arévalo
Jhon Fernando Avila
Julián Mauricio Jaramillo

- Spire Activity Tracker
  - Usa BLE para comunicación inalámbrica
    - Anuncia su presencia en texto plano y legible
    - Establece sesión con el celular (emparejamiento)
    - No cambia la dirección MAC

Wearables

Juan Carlos Arévalo
Jhon Fernando Avila
Julián Mauricio Jaramillo

- Spire Activity Tracker
  - Política de manejo de datos
    - Spire recopilara información que tiene que ver con datos de dispositivos, datos demográficos de clientes, patrones de tráfico, ventas, servicio, producto y uso del sitio, con propósitos comerciales incluyendo mejorar la usabilidad, el rendimiento y la eficacia del sitio web y puede ser divulgada a terceros como datos agregados sin ninguna de su información de identificación personal.

Wearables

Juan Carlos Arévalo
Jhon Fernando Avila
Julián Mauricio Jaramillo

- Spire Activity Tracker
  - Permisos de la aplicación
    - Cámara: permite tomar videos y fotos
    - Micrófono: permite grabar audio
    - Teléfono
    - Descargar archivos

Wearables

Alberto Barajas Ramon
Danilo José Erazo
John Edinson Lizarazo

- Fitbit
  - Dispositivo
    - Rastreo de actividad del usuario
    - Usa un acelerómetro para determinar los movimientos
    - Interfaz BLE para comunicación
  - Aplicación
    - Plataformas IOS, Android, Windows Phone, Windows y MAC

Wearables

Alberto Barajas Ramon
Danilo José Erazo
John Edinson Lizarazo

- Fitbit
  - Usa BLE para comunicación inalámbrica
    - Anuncia su presencia en texto plano y legible
    - Establece sesión con el celular (emparejamiento)
    - No cambia la dirección MAC
    - Negocia llaves y cifra la información
  - Permisos de la aplicación
    - Ubicación, cámara, almacenamiento, llamadas, contactos

Wearables

Alberto Barajas Ramon
Danilo José Erazo
John Edinson Lizarazo

- Fitbit
  - Uso de datos grabados por el dispositivo para aclarar casos criminales en los Estados Unidos
    - 2015. Richard Dabate.
      - La narración no correspondía con los datos registrados por el dispositivo de la esposa asesinada.
    - 2015. Jeannine Risley.
      - Su narración sobre un ataque sexual no correspondía con los datos registrados por el dispositivo.
    - 2017. Kelly Herron.
      - Su narración sobre su defensa contra un atacante fue comparada con los datos registrados por el dispositivo y si coincidían.

Casos Conocidos

- DEFCON 2016
  - Dos hackers evaluaron la seguridad de un vibrador conectado (IoT) y presentaron los resultados:
    - El dispositivo permite la conexión de un compañero, vía la aplicación móvil. Esta conexión podía ser hackeada.
    - El fabricante registraba y enviaba a un servidor central temperatura, intensidad de la vibración y frecuencia de uso, sin consentimiento del usuario.
  - Una usuaria presentó una demanda y la compañía decidió negociar (llegó a un acuerdo).
    - ¿Cómo proteger a los usuarios?
    - ¿Por qué recoger esta información?

Otros Casos

- Amazon Echo (Alexa)
  - Reconocimiento de voz “hands-free”
    - Manejo automático de llamadas y mensajes
    - Audio (360º audio omnidireccional)
    - Música wi-fi Amazon, Spotify, Pandora, TuneIn, iHeartRadio

Otros Casos

- Amazon Echo (Alexa)
  - *"J. Bates, Bentonville, Arkansas […] was arrested in February 2016 and charged with first-degree murder and tampering with evidence after a man was found dead in his hot tub."*
  - *"Police seized the Echo device and also requested Amazon release a history of voice recordings from the device during the time in which authorities believe the murder took place."*
  - *"Police also believe the device could have been inadvertently activated on the night of the murder, which could potentially provide recordings that offe insight into what happened that night."*

http://www.pbs.org/newshour/rundown/5-stories-last-week-deserve-second-look/

Otros Casos

- Amazon Echo (Alexa)
  - La Policía pidió una orden para obtener los datos registrados por Alexa
  - Amazon
    - Entregó el registro de las transacciones …
    - pero se negó a entregar las grabaciones de audio
    - Finalmente Amazon entregó las grabaciones, en marzo 7 de 2017, solamente después de ser autorizada por el propietario del dispositivo
  - *"Another smart device is also under authorities' radar — Bates' water heater, which flagged investigators to exorbitant amounts of water used during the early-morning hours that day."*

http://www.pbs.org/newshour/rundown/5-stories-last-week-deserve-second-look/

Conclusiones

Problemas Conocidos

- Lectura no autorizada
- Escritura o modificación no autorizada
- Disponibilidad del servicio
- Privacidad

Nuevos Dominios

- Electrodomésticos
- Implantes médicos
- Ciudades Inteligentes

Nuevas Consecuencias

- Hogar
- Vida
- Ciudad
- Servicios

Conclusiones

- Los dispositivos IoT ofrecen comodidad,
- Pero, pueden presentar vulnerabilidades:
  - Productos nuevos desarrollados por empresas que no tienen experiencia en seguridad
  - Fabricantes que recopilan datos de los usuarios sin su consentimiento
- Cada usuario debería ser consiente del compromiso entre comodidad y privacidad
  - Al menos buscar y leer la política de manejo de los datos privados

Preguntas

Gracias

Sandra Rueda
Ingeniería de Sistemas y Computación
Universidad de los Andes

Referencias

- J. Barajas, E. Hendry, I. Smith. 5 stories from last week that deserve a second look. An Amazon Echo device could be a witness in a murder trial. Feb. 27, 2017. http://www.pbs.org/newshour/rundown/5-stories-last-week-deserve-second-look
- Follower & Goldfisk. Breaking the Internet of Vibrating Things. DEFCON 2016.
- Alvaro Cárdenas. WearFit: Security Design Analysis of a Wearable Fitness Tracker. Curso Seguridad y Privacidad en IoT, UniAndes 2017.
- Andres González, Fernando Muñoz, Gustavo Salazar. Análisis del dispositivo Garmin Forerunner 35. Reporte Técnico, Curso Seguridad y Privacidad en IoT, UniAndes 2017.
- Juan Carlos Arévalo, Jhon Fernando Ávila, Julián Mauricio Jaramillo. Análisis de la seguridad y privacidad del dispositivo Spire Activity Tracker. Reporte Técnico, Curso Seguridad y Privacidad en IoT, UniAndes 2017.
- Danilo José Erazo, Alberto Barajas Ramón, John Edinson Lizarazo. Análisis de seguridad y rpovacidad del dispositivo Fitbit Flex. Reporte Técnico, Curso Seguridad y Privacidad en IoT, UniAndes 2017.