Seguridad en IoT (Internet de las Cosas)

Club de Investigación Tecnológica

San José, Costa Rica
18-feb-2016

Theodore Hope <theodorehope@gmail.com>

IoT - Intro

- Conjunto de dispositivos inteligentes que se comunican a través del Internet, y los datos que transmiten.
- Aprox 25,000,000,000+ dispositivos hoy.
- Ejemplos (todos "inteligentes"):
  - Medidores de servicios públicos y medio ambiente
  - Automatización del hogar ("domótica")
  - Sensores médicos & agrícolas
  - Vigilancia y atención a emergencias

IoT – Mi historia reciente

- 2008-2015 (tecnología 2006-2013)
  - Dispositivos AVL – Rastreo y monitoreo vehicular
    - OS propietario, h/w limitado
    - GPS, GPRS/3G, SIM
    - Ninguna autenticación, ninguna cripto
    - Fácil de enviar datos falsos a servidores (id=IMEI)
    - Bajo interés económico en hackear equipo o datos

IoT – Mi historia reciente

- 2012-2015 (tecnología 2011-2013)
  - AFC – Validadores de pasaje de transporte
    - CPU 32 bits con Linux (embedded)
    - Tarjetas RFID inteligentes
    - Comunicación via GPRS/3G, encriptada por SSH
    - SAM (Secure Access Module) para cripto entre validador y tarjetas, y para firma digital
    - Retos:
      - ¿Cómo corroborar identidad de equipo, remotamente?
      - ¿Cómo proteger llaves privadas en cada equipo?

Ataques a IoT

- Ataques a los dispositivos en sí:
  - Robados, modificados, intercambiados, clonados
- Ataques al software de los dispositivos
  - Modificación (firmware, OS, app)
  - Extracción de credenciales
  - DoS (Denial-of-Service)

Ataques a IoT (Cont…)

- Hackeo para convertir en spambots a:
  - Enrutadores, TVs, termostatos, media players, refrigeradoras
- Inhabilitar sistemas de seguridad / alarmas
- IoT está convirtiendo el hogar en un centro de datos, pero sin administrador de sistemas
- Preocupación:
  - "Botnets" de miles/millones de dispositivos IoT

Ataques a IoT (Cont…)

- Medidores eléctricos en España
- Vehículos Jeep Cherokee
- Marcapasos con WiFi
- Bombas de morfina
- Monitores de bebé (cámaras de video)

- Buscador de dispositivos IoT visibles:
  - shodan.io

Seguridad: IoT vs. IT

- Dispositivo IoT mucho más limitado que PC
  - Cripto, en particular, a veces ausente
- Existe un dispositivo físico
  - Puede ser hackeado por terceros
  - Actualización de s/w es más difícil
- Mindset de Embedded Systems
  - Fabricados con otra mentalidad
  - Security as an after-thought
  - La maldición del "minimum viable product"

OWASP IoT

- OWASP.org - recomienda enfoque holístico y revisar todas las "superficies de ataque"
  - Muy parecido a seguridad general en IT
    - v.g. Contraseñas débiles, puertos abiertos, falta de cripto, s/w o f/w inseguro, etc.
  - *Dèja vu* de problemas de seguridad en el web hace 20 años :-p
  - Ojo: Un par sí son *muy* relevantes:
    - Problemas de seguridad física
    - f/w o s/w no protegido

Llaves y Credenciales

- Toda comunicación entre dispositivo y servidor debe estar encriptada (TLS o SSH), y debe autenticarse con credenciales.
- Credenciales (llaves), root certs están guardadas en el f/w o s/w del dispositivo, y pueden ser copiadas o modificadas :-(
- PKI al rescate …

PKI en Dispositivos IoT

- PKI: Infraestructura para manejo de llaves públicas en certificados digitales (CD).
- A cada dispositivo se le genera e instala CD.
- Al iniciar, el dispositivo se autentica ante servidor con su CD. El servidor le otorga credenciales *temporales* que se utilizan para envío de datos.
- Mitiga el problema de dispositivo robado o hackeado.

PKI (Cont…)

- Pero persiste un problema:
  El certificado digital del dispositivo puede ser leído por hackeo físico, y clonado :-(
- Necesitamos:
  - Un mecanismo que impida la lectura, o por lo menos la modificación, de ciertos datos en el dispositivo.
  - Extender el concepto de "chain of trust" del PKI para que abarque incluso el sistema de arranque.
  - Que toda instrucción iniciada en el dispositivo (f/w, OS, app) sea verificada a través de un "chain of trust".

TPM (Trusted Platform Module)

- Hardware que establece un "root of trust" para el resto del "chain of trust", a partir de "secure boot".
- Almacenaje de llaves "tamper-resistant" usado para arranque seguro. Revisa integridad de F/W, y de allí sigue el "chain of trust".
- TPM frustra ataques "below-software":
  - Impide corrupción de f/w, boot s/w, CD, etc.

Recomendaciones Generales

- Aplicaciones no críticas, y productos OTF:
  - OWASP mejores prácticas
  - Sopesar riesgos de IoT posiblemente inseguro
- Aplicaciones críticas (o productos propios):
  - Hardware TPM
  - Hardware “tamper-proof”
  - PKI
  - Diseño de seguridad desde el inicio, no un parche


航班不正常服务台
Service Counter For Abnormal Flights
www.engrish.com