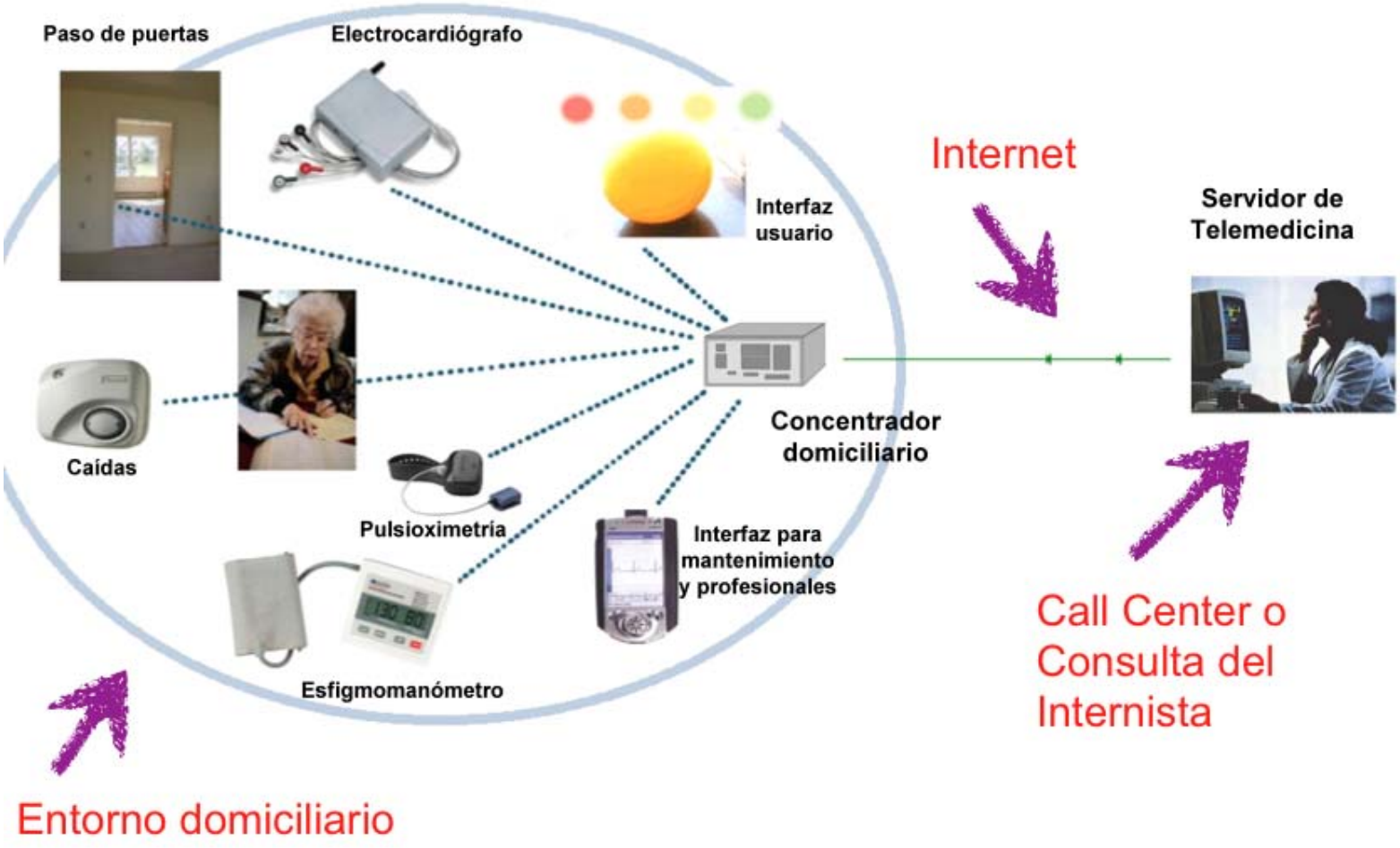
La Telemedicina como Herramienta Asistencial del Internista

La Seguridad en los Sistemas para la Atención Domiciliaria

Sistema de Atención Domiciliaria



Las grandes preguntas

- ¿Es mi sistema seguro?
  - **NO**
- ¿Puedo **considerar** mi sistema seguro?
  - **SI**
  - Definición de una métrica de seguridad

Riesgos:
- Pérdida de información y equipos
- Pérdida de prestigio
- Problemas legales
- ¿Chantajes?

Coste:
- Económico
- Pérdida de prestaciones y flexibilidad de utilización
- Formación de los usuarios

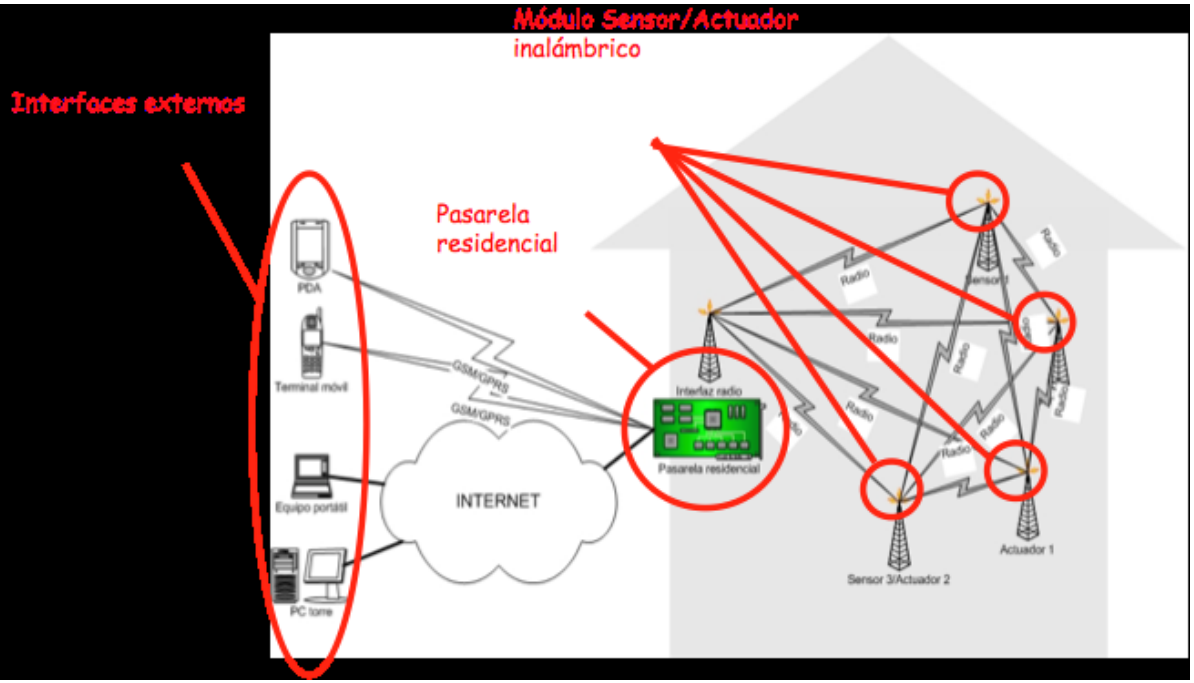
Taxonomía del atacante

- Recreacional (Hackers)
  - Acceso a Internet gratuito
  - Reto de “saltar” un sistema
- Obtención de beneficio
  - Robo e inserción de información fraudulenta
  - Destrucción de información e infraestructura
  - Obtención de información sensible

- Fuerzas de Seguridad
  - Bajo mandato judicial
  - Medios tecnológicos muy sofisticados

MINISTERIO DEL INTERIOR

ESPAÑA CNI CENTRO NACIONAL DE INTELIGENCIA



Modelo de Sistema

Domicilio

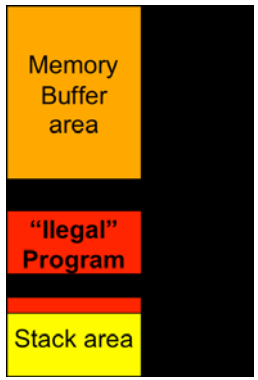
Internet

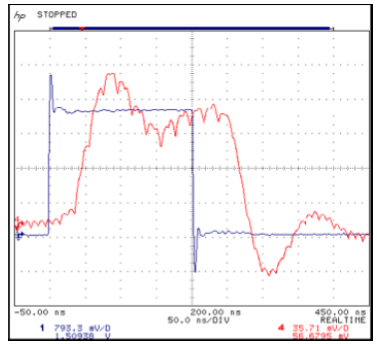
Consulta Médica

Sistema bajo un punto de vista de seguridad:

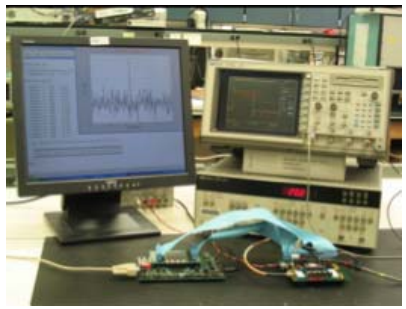
- Equipos
  - Terminales cerrados
  - Terminales abiertos
- Comunicaciones
  - Internet (no controlable por el usuario)
  - Cableadas
  - Radio

Ataques a Equipos - Terminales





- Ataques lógicos
  - Ejecutar un programa en el terminal
  - Ejemplo: Buffer overflow de la PSP
- Ataques de temporización
  - Obtención de claves de cifrado analizando tiempos de ejecución
  - Ejemplo: Tarjetas inteligentes de tipo bancario



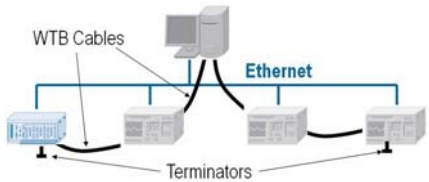
- Ataques de consumo
  - Obtención de claves analizando el consumo
  - Ejemplo: Tarjetas inteligentes
- Ataques variados
  - Ataques físicos, eléctricos, ingeniería inversa, emisión electromagnética, modos anómalos de inicialización, etc.
- Campo en auge para los diseñadores de equipos

Defensa de Equipos - Terminales Abiertos

- Ordenadores personales
  - Seguridad del equipo: Antivirus, buenas prácticas de software, firewalls, etc.
  - Usuarios del equipo: Política de utilización de HW/SW y buenas prácticas

- PDA´s
  - Buenas prácticas del usuario del equipo
- Teléfonos móviles
  - Seguridad del equipo
  - Buenas prácticas del usuarios

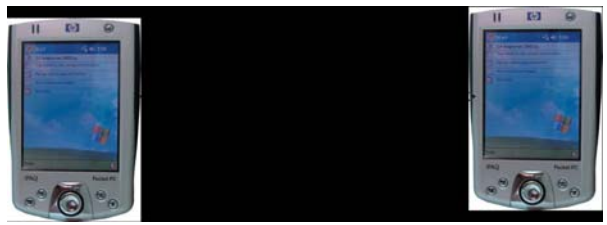
Protección - Comunicaciones Cableadas



- Intranet:
  - Razonablemente seguras con un mínimo cuidado en el tendido de la red
  - Su vulneración requiere habitualmente contacto físico con el medio (cable o fibra) o acceso a los equipos de rutado
  - Mantenimiento de la seguridad asociada al sistema de seguridad física
- Internet:
  - Incontrolable por el usuario y responsabilidad del proveedor de servicio

Comunicaciones Inalámbricas

- Ventaja: Ubicuidad, movilidad y no instalación
- Reto: La información es accesible en la vecindad física de los equipos y sistemas, lo que implica anonimato y mínimo riesgo del atacante
- Soluciones:
  - Cifrado



  - Autenticación

Resumen

- Necesidad de definir una métrica de seguridad **razonable** para la aplicación específica
- Definición e implantación de una **política de seguridad** de equipos y terminales
- Definición e implantación de una **política de seguridad** en las comunicaciones
- Definición de una política de **buenas prácticas** “best practices” para los usuarios del sistema
- Definición de una política de **actualización** de la seguridad ya que es un tópico que evoluciona