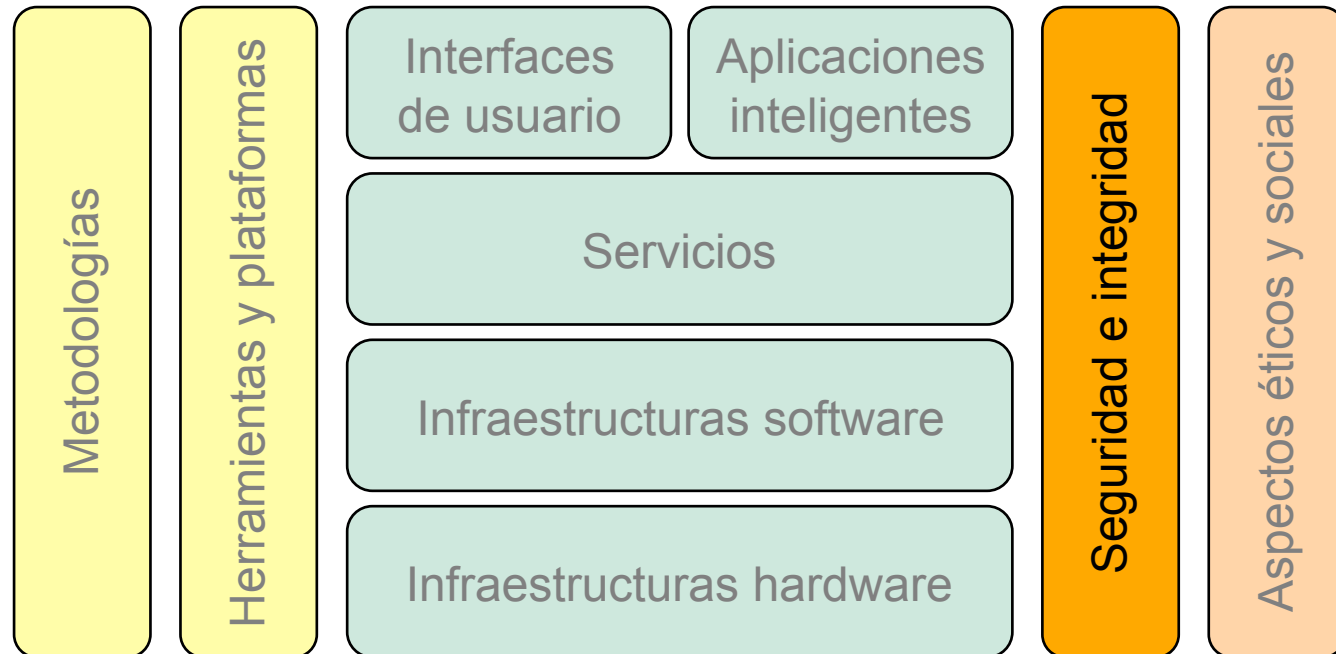


UPV / EHU

Sistemas Ubicuos

6. Seguridad y privacidad

Plataformas y arquitectura middleware



UPV / EHU

Seguridad y privacidad

The logo of the University of the Basque Country (UPV/EHU) is located on the left side of the slide. It consists of a stylized white graphic of a tree or a similar structure on a green background, with the text 'UPV / EHU' below it.

UPV / EHU

1. Definiciones
2. Aspectos de la seguridad en sistemas ubicuos
3. Computación distribuida segura

Seguridad y privacidad



UPV / EHU

1. Definiciones
2. Aspectos de la seguridad en sistemas ubicuos
3. Computación distribuida segura

Definiciones

UPV / EHU

- **Políticas de seguridad:** establecen límites definidos en la compartición de recursos. Independientes de la tecnología.
- **Mecanismos de seguridad:** cómo se implementan las políticas. Conjunto de técnicas dependientes de la tecnología.

Definiciones

Amenazas (Pfleeger, 1997)

- **Intercepción.** Escucha de mensajes, ...
- **Interrupción.** Retardo de mensajes, denegación del servicio, ...
- **Modificación.** Alteración o corrupción de mensajes, ...
- **Fabricación.** Suplantación de identidad, ...

Definiciones

Políticas

- **Confidencialidad**
 - La información estará disponible sólo para los sujetos autorizados.
- **Integridad**
 - Las modificaciones de la información sólo se realizarán por los sujetos autorizados.

UPV / EHU

Definiciones

Mecanismos

- Cifrado
 - Simétrico (clave secreta)
 - Asimétrico (par de claves pública y privada)
- Autenticación
 - Passwords
 - Protocolos de reto-respuesta.
- Autorización
 - Listas de control de accesos, Credenciales
 - Firewalls
- Auditoría
 - Mantenimiento y análisis de trazas (*logs*)

Seguridad y privacidad

UPV / EHU

1. Definiciones
2. Aspectos de la seguridad en sistemas ubicuos
3. Computación distribuida segura

Aspectos de la seguridad en sistemas ubicuos

UPV / EHU

- Los sistemas ubicuos incluyen los mecanismos generales de la seguridad en redes (p. ej, cifrado)
- Aspectos específicos que afectan a:
 - La autenticación
 - La autorización

Aspectos de la seguridad en sistemas ubicuos

- Autenticación:
 - Hay que evitar que sea explícita (el usuario está fuera del bucle).
 - En general, no puede contarse con una autoridad autenticadora (exigiría infraestructura):
 - ¿Podemos confiar en el funcionamiento general del sistema aunque alguno de sus elementos se comporte maliciosamente?
 - Es un problema de evaluación segura de funciones (SMC), más fuerte que Consenso.

Aspectos de la seguridad en sistemas ubicuos

- Autorización:
 - Seguridad dependiente del contexto:
 - El derecho de acceso se evalúa en función de la inferencia a partir de un conjunto de parámetros.
 - P. ej: el acceso a un recinto en automóvil en función de la congestión de tráfico, el nivel de contaminación, las características del vehículo, el número de viandantes...

Seguridad y privacidad



UPV / EHU

1. Definiciones
2. Aspectos de la seguridad en sistemas ubicuos
3. Computación distribuida segura

Computación distribuida segura

UPV / EHU

- Un problema ejemplo:
 - Calculemos cuánto pesamos entre todos...
 - ...pero sin que nadie conozca el peso de los demás
- Enfoques:
 - a. Contratemos a una autoridad externa y fiable
 - b. Ejecutemos un algoritmo distribuido (*Secure Multiparty Computation, SMC*)

Computación distribuida segura

UPV / EHU

Modelo

- n participantes: P_1, \dots, P_n
- Objetivo:
 - Computar una función $f(x_1, \dots, x_n) = (y_1, \dots, y_n)$, tal que P_i obtiene y_i pero ninguna otra información.

Ejemplo

- Tres participantes, P1, P2, P3. Cada uno aporta un valor A_i
- Función a calcular:
 - $f(A_1, A_2, A_3) = A_1 + A_2 + A_3$
- Estrategia ejemplo:
 - Cada P_i elige 3 números entre 0 y 1000: dos al azar, el tercero es tal que la suma de los 3 números sea igual a $A_i \bmod 1000$
 - P. ej., para $A_i = 54 \rightarrow 300, 550, 204$

Ejemplo (cont)

1. Elección de los números

UPV / EHU

P1	P2	P3
300	700	320
550	180	500
204	197	239
1054	1077	1059

Ejemplo (cont)

2. Cada uno entrega dos de sus números a los otros por separado

P1	P2	P3
300	700	320
180	500	550
239	204	197

UPV / EHU

Ejemplo (cont)

3. Cada uno suma módulo 1000

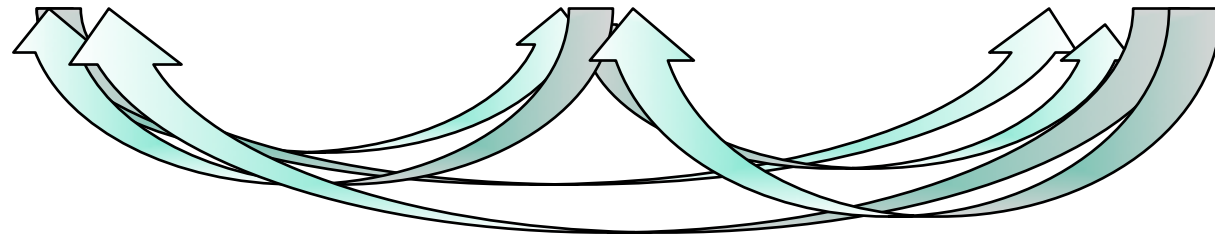
UPV / EHU

P1	P2	P3
300	700	320
180	500	550
239	204	197
719	404	67

Ejemplo (cont)

4. Cada uno difunde su resultado

P1	P2	P3
300	700	320
180	500	550
239	204	197
719	404	67



Ejemplo (cont)

5. Y suma módulo 1000

UPV / EHU

P1	P2	P3
719	719	719
404	404	404
67	67	67
190	190	190

Computación distribuida segura

- ¿Qué pasa si alguno de los participantes se comporta maliciosamente?
 - En principio, modelo de fallos *bizantino*.
 - Con un módulo Hw de seguridad (p. ej., *tarjeta inteligente*) en cada nodo → modelo de *omisión*.
 - Suponemos que el adversario conoce los algoritmos y puede interceptar, interrumpir y fabricar mensajes, pero no conoce el código del módulo Hw.
 - Modelo de *Trustedpals*
 - ¿Es el modelo de TustedPals adecuado para sistemas ubicuos?

UPV / EHU