



## SECURITY FOR UBIQUITOUS COMPUTING

**Autor:** Frank Stajano

**Editorial:** John Wiley & Sons

**Año:** 2002 – 247 páginas – ISBN: 0-470-84493-0

**www.wiley.com - www.diazdesantos.es**

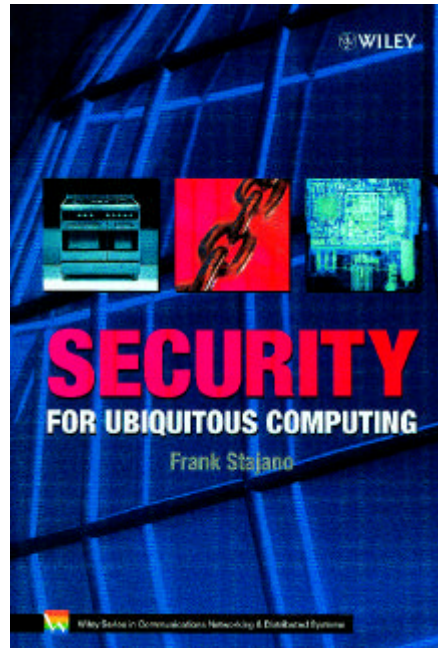
Sólo con grandes dosis de osadía –y no menos de desparpajo– se puede ejercer de augur de las T.I., pues su progreso y despliegue es tan acelerado (y en ocasiones esquizofrénico) que las previsiones –incluso a medio o corto plazo– sobre tendencias tecnológicas o impacto social yerran reiteradamente. Sin embargo, siempre hay algunos desarrollos que por estar lo suficientemente maduros –y satisfechas las condiciones para su difusión– tienen el éxito garantizado, aun cuando sean escasamente conocidos incluso por los especialistas en las tecnologías antedichas. Ese es el caso de la computación ubicua o, como prefieren algunos, virtualidad incorporada o aun computación invisible.

La computación ubicua, como tantas otras tecnologías de gran aceptación en el campo de la informática (recuérdese el ratón, las ventanas, las redes locales –o más concretamente Ethernet–, etc.), surgió del Centro de Investigación de Xerox en Palo Alto (más conocido por sus siglas en inglés: PARC), apareciendo sus primeros prototipos a fines de la década de los 80.

En su acepción más común, y de manera sintética, el término tiene que ver con la integración de los ordenadores (o más atinadamente –desempolvando una vieja taxonomía– ordenadores de propósito específico, pues éstos, más que los denominados de propósito general, constituyen los componentes de la citada computación ubicua) en nuestro entorno espacial (vestuario, calzado, paredes, equipos de electrónica de consumo, terminales eléctricos, etc.) de manera imperceptible para nosotros y, por tanto, sin que su aprovechamiento nos distraiga en lo más mínimo de nuestro quehacer cotidiano. Es decir, justamente lo contrario de lo que acontece hoy en día con los ordenadores, cuyo uso requiere, tiránicamente, de nuestra atención permanente. Dicho en palabras de su principal desarrollador e ideólogo, Mark Weiser: “(la computación ubicua) ... *es concebir un nuevo modo de pensar sobre los ordenadores que tenga en cuenta el mundo humano y permita que las máquinas se difuminen en su transfondo*”.

Pues bien, de estos sistemas ubicuos, su interconexión y, principalmente, de sus insoslayables requisitos de seguridad versa –a lo largo de sus más de 200 páginas, articuladas en 9 capítulos y 2 anexos– el libro cuya reseña nos ocupa. Éste, de título *Security for ubiquitous computing*, tiene como autor a **Frank Stajano** y está editado dentro de la serie *Communications Networking Distributed Systems* por la editorial Wiley en el presente año.

Tras un irrelevante capítulo primero, de título *Introduction*, en el que se establece el escenario, los términos, las notaciones, etc., el segundo, *Ubiquitous computing*, pretende alcanzar el primero de los objetivos citados, es decir el estudio de estos sistemas ubicuos y su interconexión. Para ello comienza por conceptualizar el término y exponer las investigaciones y desarrollos que acerca de la materia están llevando a cabo distintos centros de



investigación (HP, MIT, PARC, AT&T Cambridge, etc.). Tras ello, se detiene en presentar las redes diseñadas y desarrolladas para conectar estos equipos, redes denominadas por el autor como “ad hoc”. En todos sus apartados y subapartados presenta los prototipos que van apareciendo, lo que debería bastar a los más escépticos para convenirse de la tangibilidad de estos dispositivos. Sin embargo, por su cariz casi omnicomprensivo el capítulo puede resultar de tediosa lectura.

El tercero, *Computer Security*, constituye un repaso –no por ello menos relevante, debido a su acusado cariz didáctico– de las características de la información que la seguridad trata de preservar y los mecanismos que las implantan: confidencialidad –mediante el cifrado–, integridad –hash, MAC, firma digital–, disponibilidad, autenticación –contraseñas, reto–respuesta–. Igualmente, para finalizar, se repasan los aspectos de política de seguridad y los correspondientes modelos que centrarán la atención, casi exclusiva, del resto de los capítulos.

En sus restantes capítulos el manual se centra en exclusiva en los aspectos de seguridad de esta computación, incluida sus redes. Éstos son en gran medida específicos a los sistemas (“ubicuos”) que nos ocupan, pues aunque sus fundamentos teóricos y bases técnicas (mostradas en el ya comentado capítulo tercero) sean comunes con las mismas de la seguridad que podríamos denominar convencional, las políticas y modelos de seguridad a aplicar en estos sistemas son a menudo muy diferentes. En todo caso, estos capítulos son altamente especulativos, y a menudo basados en modelos y protocolos del autor, cuyo éxito conoceremos se-

gún vaya difundiendo esta tecnología.

De este modo, el capítulo cuarto, *Authentication*, versa sobre los requisitos que la computación ubicua le impone, para exponer después nuevas políticas y consiguientes modelos (alguno del autor, como el *Resurrecting duckling*), en parte basados en los conocidos modelos multinivel. Por su parte, el siguiente capítulo, *Confidentiality*, trata de las limitaciones que al cifrado impone el reducido tamaño de los procesadores (*peanut processors*) y por ello los algoritmos adecuados. Y aquí cabe hacerse la pregunta, que no se plantea en el texto, de hasta qué punto el incremento de potencia de los microprocesadores no variará drásticamente estas previsiones. El siguiente, *Integrity*, estudia los problemas que presenta, y sus posibles soluciones, la integridad de los mensajes que circulan por las redes de estos dispositivos, y la integridad de estos mismos dispositivos. En el de título, *Availability*, se detiene en amenazas inusuales a la disponibilidad en la computación convencional, como las que presentan las baterías, así como las dudas que suscita el código móvil. Por último, *Anonymity*, se centra en los riesgos acentuados que para la anonimidad exhiben estos sistemas (pues los servidores deben estar en lugares públicos y, a menudo, de fácil acceso) y los protocolos con que defender la «anomicidad» (principalmente el *Cocaine Auction Protocol*, nuevamente del autor).

Llegados a los apéndices, no es posible sino alabar su claridad y concisión. Así, en el referido como anexo A, *A short primer on functions*, encontrará el lector una brevísimas, a la par que completa, exposición de los conjuntos, relaciones y funciones, cuya única objeción podría ser su poca utilidad en el contexto de la obra, que hace gala de la parquedad del formalismo matemático. Mientras, en el Anexo B, *Existing network security solutions*, se estudian los protocolos usuales de seguridad en redes (Needham Schoeder, IPsec, Kerberos, SSL/TLS) y los sistemas más populares que incorporan mecanismos de seguridad (GSM, Bluetooth, 80.11), todos los cuales conciernen a las redes “ad hoc”. Más, si cabe, que antes, es obligado reseñar las capacidades didácticas del autor que en pocas y amenas palabras presentan, es cierto que microscópicamente, los temas citados. Muy bueno.

Por otra parte, no es posible concluir esta presentación general de la obra, pasando por alto las abundantes (un total de 271) y notables referencias que jalonan todo el texto y que en su correspondiente apartado, *Annotated bibliography*, aparecen glosadas e incluso, algunas, marcadas como especialmente relevantes. En resumen, un buen puñado de citas (muchas con su dirección URL) que constituyen uno de los principales atractivos de la obra.

En fin, aunque algunos tachen el libro de futurista (y no sin alguna razón, pues los sistemas no han hecho sino aparecer), su lectura ayudará a los más inquietos y prevenidos a prepararse para un próximo mañana, en el que sin duda la computación ubicua nos envolverá, bien que por fortuna inadvertidamente. n

**ARTURO RIBAGORDA GARNACHO**

Catedrático y Director del Dpto. de Informática

**UNIVERSIDAD CARLOS III**

arturo@inf.uc3m.es