Preface

The brief and frantically evolving history of computing and digital communications is entering another major paradigm shift.

It took computers barely half a century to evolve from grandiose isolated room-sized machines, affordable only by a handful of major organizations, to inexpensive multimedia-capable PCs, now commonplace in every home and office, connected to form a worldwide internet. The next major evolutionary step, in part already underway, brought about by a synergy of hardware miniaturization, wireless communications and distributed software systems, is going to be *ubiquitous computing* (*ubicomp* for short). No longer just one or two, but hundreds or thousands of computers per human being, now in the form of networked processors invisibly embedded in everyday objects rather than in conventional keyboard-and-monitor boxes.

Many of us have already lost track of the number of objects we own that contain a microprocessor (try listing them). In the future many more objects, from appliances to furniture to clothes, not to mention nanotechnology-based robots, will contain embedded processors, and will also be endowed with short-range wireless networking capabilities. Today, some manufacturers embed audio input hardware in their digital camera so that you can annotate your pictures by voice. This is an inelegant kitchen-sink-style design: why should a still picture camera be encumbered with audio hardware? Tomorrow, though, manufacturers will be able to embed ad hoc networking capabilities into everything, and you will be able to annotate the photographs in your camera by speaking into your cellphone, which already incorporates digital audio hardware as part of its primary function. Devices will be able to share hardware peripherals and offer their services to each other. Industry shares this vision: in 2001, membership in the Bluetooth SIG was almost unanimous among companies in consumer electronics, computing or communications.

However, when everything is capable of spontaneously and autonomously exchanging data with anything else in range, new concerns come about. You like to be able to "beam" your electronic business card from your PDA to that of a new acquaintance, but who exactly is in a position to consult the entries in your address list or diary? As these devices become more and more pervasively integrated in our daily routine, and as they get to know more and more about our preferences and habits, the privacy issues of the secrets held by our digital butlers acquire a new

relevance. Besides, if your wirelessly networkable PDA now even carries electronic money, how do you guard against invisible electronic pickpockets who don't even have to touch you to burgle you?

There are many fine books on computer security, and new ones are now coming out on ubiquitous computing, ad hoc networking and specific implementation technologies such as Bluetooth and 802.11. What's missing is a book focusing on the intersection of the two topics: sufficiently specialized on ubiquitous computing that it does not spend most of its page budget on unrelated issues, like most security books do, and at the same time much more detailed than the obligatory-but-not-particularly-insightful security chapter typically found in the current crop of books on wireless networking.

This is it. This is the book written for people interested in "the big picture" on the security issues of ubiquitous computing. It is aimed at a technical audience but does not require prior knowledge of either security or ubicomp. It will also be valuable to readers versed in only one of these two fields, who will find it a gentle introduction to the other.

The style is simple and equations-free. The book opens with a panoramic view of the many facets of the ubicomp phenomenon and continues with a readable jargon-busting primer on security and the important concepts of cryptology. After a survey of these fundamentals, the book focuses on the aspects that make ubiquitous computing security different from that of traditional distributed systems. It provides pointers to first-hand sources and to current research in an extensively annotated bibliography; where appropriate, it also presents new inventions to solve new problems in authentication, availability and anonymity. There is also an appendix reviewing, for comparison, the security solutions adopted in a number of well known distributed systems.

I know from direct personal experience that the engineers, researchers and managers who are interested in a sound technical introduction to ubicomp security are busy professionals whose reading time is limited. With this in mind, my aim has been to produce a readable, technically accurate, up to date and *short* book. This is not a cookbook full of implementation recipes, or an encyclopædia that tells the clueless practitioner what to do in every possible case. It is instead a technical overview of the field, including a broad framework to make sense of it all, a taxonomy of the major problems and a few in-depth discussions of specific problems.

Even though the first commercial implementations of some aspects of the ubicomp vision are now starting to appear, the grand scenario is still definitely a thing of the future; and ubicomp security, which would be a global property of the whole system, certainly hasn't happened yet. I wish it does before the deployment is complete.

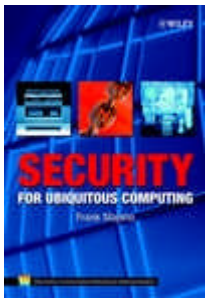
For this wish to be granted it is necessary for everyone involved to approach

ubicomp with the right mindset, and with a knowledge of what could go wrong. All too often, during the first iteration of building a new system and under pressure from time-to-market requirements, security (one of the least visible properties of a system, whether present or absent) is dismissed as inessential compared to the hard challenge of getting the system to work at all.

However, attempts at retrofitting security to existing designs tend to result in inadequate and vulnerable systems. My aim here is to provide awareness, primarily for system builders but also for the technically aware early adopters. Both the system architects planning entire ranges of ubicomp products and the programmers writing the actual firmware will do a much better job if they understand the security implications of what they do, even if the current focus is just on "getting it to work". The intelligent users, meanwhile, will want to be informed about the risks of the new technology so as to be able to make informed choices on what to accept, reject or demand when they vote with their wallets.

By reading this book you will gain a thorough understanding of the system-level security issues relevant to ubiquitous computing. You will acquire a sound background knowledge with which to assess and evaluate any practical implementation scenarios you might face. I will not try to teach you a series of unrelated cute tricks, but rather to give you a mental key with which to interpret and make sense of any new development in this field. Since the evolutionary speed of ubiquitous computing surprises even computer people, it is my firm belief that this "teaching how to fish" approach is the only one worth following.

Frank Stajano
Kawasaki, Japan



Frank Stajano (University of Cambridge)
Security for Ubiquitous Computing
John Wiley and Sons, Ltd
Wiley Series in Communications Networking & Distributed Systems
ISBN: 0-470-84493-0
Hardcover; pp. 267 (xx + 247)
Publication date: 2002-02-12
RRP: 34.95 GBP (UK); 59 EUR (rest of Europe); 60 USD (USA)

http://www-lce.eng.cam.ac.uk/~fms27/secubicomp/