Foreword

Twenty or even ten years ago, computer security was a marginal speciality for geeks who liked to obsess about things like enciphering email. Nowadays, it is centre stage. Cyberterrorism and electronic fraud are the subject of hand-wringing press articles; but that's only the beginning.

Financial and political power are now largely exercised through networked systems. Cash machine and credit card networks decide whether you can get money; burglar alarm networks decide whether the police will come to your house; identify-friend-or-foe systems tell the military which aircraft might be worth intercepting. Most of the investment in cryptography and computer security goes to ensure that these sinews of civilisation will continue to perform dependably in the way that their builders envisaged.

Within another ten years, all sorts of devices that are stand-alone or not even computerized will be connected to the net; your fridge, your heart monitor, your bathroom scales and your shoes might all work together to monitor (and nag you about) your cardiovascular health. There will be more sinister aspects: the military is already funding research on "smart dust" to provide universal surveillance, and tiny robot insects to sting enemies to death.

How will power and control be exercised in this brave new world?

Already, powerful interests are staking out huge territories. Hollywood has bullied the consumer electronics industry into building copyright control mechanisms into a wide range of gadgets; now DVD players, games consoles and even some PCs enforce security rules that are often against their owners' interests and wishes. You may record your lectures on a minidisc recorder, and then find that you can't back up the recordings anywhere. And it's not just "information" goods that end up being controlled in annoying ways by others. Insurance firms in Norway insist that the owners of expensive cars fit an alarm that monitors the car's location using GPS and reports it using a GSM mobile phone. But what's the point of buying a Jaguar if you have to fit an alarm whose log will invalidate your insurance if the car is ever driven at half its rated top speed? For whom is the system providing "security"?

Security in ubiquitous computing is going to be a huge issue, for both engineers and policy people alike. That's why this book is important.

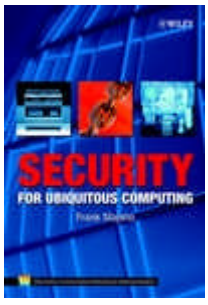
As Frank Stajano worked for years at AT&T Labs, which spawned much of the technology, he can give many good examples—active badges, smart floors,

intelligent coffee machines, even CD covers that cause your home music system to play the album when you open them. Many of these have raised surprising new security issues, involving complex trade-offs between usability, privacy, reliability and control.

Protecting large networks of simple devices also raises a lot of difficult technical problems. Conventional solutions, such as public key infrastructures, tend to be unworkable or just simply irrelevant; conventional security policies, such as protecting those transactions deemed "confidential", don't block the attacks we are most concerned about. Here we come to Frank's original work—protection mechanisms with such delightful names as the "Resurrecting Duckling Security Policy", the "Grenade Timer" and the "Cocaine Auction Protocol".

Security in the twenty-first century is going to be a much more complex business. It will include a lot more technical issues and will touch the everyday world at many more points. Developers and policy people are going to have to learn to think in new ways. Frank's book can help make that fun.

Ross Anderson
Cambridge, UK



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/