CWI Quarterly Volume 7 (1) 1994, pp. 67 – 72

HUYGENS — Carrying the World in Your Back Pocket

Sape J. Mullender
Department of Computer Science, University of Twente
Enschede, The Netherlands

1. INTRODUCTION

In the fifty years that electronic computers exist, they have shrunk from the size of a room to the size of a wallet, a reduction in volume of a factor one million. At the same time, the storage capacities of these computers have grown from a few bytes to several megabytes, computer memories have become a million times larger. And they have also become almost a million times faster.

We can now hold a powerful computer in the palm of our hand — powerful enough to combine the functions of diary, wallet, telephone and briefcase. With our *"Personal Digital Assistant"* we will be able to make telephone calls and make payments and we can use them to store all the information we now carry in our briefcases.

Pocket-sized, very powerful, computers form an enabling technology for two important new possibilities: Computers are small and light enough to be mobile, so we do not have to be at our desk to be able to make use of them, and they are powerful enough to be usable for multimedia applications, so we can use them to communicate effectively with other people and with the machine itself.

The HUYGENS Project[1] at the University of Twente addresses research questions this new technology raises. The focus of this research is more on the architectural framework in which portable and stationary computers will be used than on the technology that builds the devices themselves. Much of this research is carried out jointly with other research groups.

The PEGASUS Project[2] is a project of the Universities of Twente and Cambridge whose goal is to define an architecture for operating systems that sup-

[1] The HUYGENS Project is partially supported by the ESPRIT BRA projects Pegasus (BRA 6586) and BROADCAST (BRA 6360); Digital Equipment Corporation; Xerox EuroPARC Cambridge; Olivetti Research Laboratory Cambridge; and Hewlett-Packard Laboratories, Palo Alto.

[2] The PEGASUS Project is supported by the European Union's' ESPRIT Programme through BRA project 6586. It is additionally supported by the Olivetti Research Laboratory Cambridge and a grant from Digital Equipment Corporation.

port distributed multimedia applications. This architecture will be evaluated through the design and implementation of a prototype system.

In the BROADCAST Project[3] of the Universities of Bologna, Newcastle, and Twente, the Ecole Polytechnique Fidirale de Lausanne, INRIA Rocqencourt and Rennes, IMAG, and INESC, research is carried out on issues of scale in the design of distributed systems that span a continent.

In the TRUST project[4] the University of Twente collaborates with Xerox EuroPARC Cambridge and the IBM Zürich Research Laboratory on the design of secure mobile computing. This work addresses protection of location information, secure communication and authentication, signature and auditing services for financial operations.

2. MOBILE COMPUTERS

Portable computer technology is guided to a large extent by the need to limit the device's power consumption to a bare minimum. Batteries form the bulk of the weight of portable computing devices and foreseeable improvements in the capacity-to-weight ratio for batteries will probably only be modest.

The biggest drain on a portable device's capacity will be communications. Wireless communication over short distances can be done via infrared light, but, to bridge longer distances, radio communication will be necessary. Communication to satellites would tax the batteries extremely heavily, so that is not an option for hand-held devices. Wireless networks will, therefore, be cellular ones. A cell is an area covered by a radio transceiver. Cells overlap such that a device is always inside at least one cell. As devices move, communication is relayed from one cell transceiver to another.

For most purposes, a modest bandwidth between a portable device and the rest of the world suffices. Video is probably the most demanding in terms of bandwidth. Given the size of the screen of small portable devices and assuming video signals will be transmitted in compressed form, a bandwidth of between one and ten megabits per second is enough. The construction of infrared or radio networks that run at these speeds has already been demonstrated.

We expect that there will be many types of portable devices, some very small so that they can be carried in one's pocket, or even worn like a wrist watch, some with a screen the size of a page of paper for use while sitting down in the office, in meeting rooms or at home. Some will have a keyboard, others will have a writable screen.

In addition to screen input and output, some devices may be equipped with audio input and output as well, so that they can be used to replace the telephone. If, in addition, a video camera is present, one can have multimedia interaction from anywhere.

It may be very useful to equip some portable devices with a global-positioning

[3] The BROADCAST Project is supported by the European Communities' ESPRIT Programme through BRA project 6360.

[4] The TRUST Project is supported by Xerox EuroPARC Cambridge, and grants from Olivetti Research Laboratory Cambridge, and Digital Equipment Corporation.

system, so that the device knows its orientation and where it is. This can make portable devices very useful for giving directions, but it can also be used for devices to learn where they are with respect to other devices.

Portable devices will be used for financial interactions, so, buried inside them, there will be an encryption system that allows them to be used as a *smart card*. A *secret key* will have to be embedded in the system in such a way that it can be used by the owner for making financial transactions, but also in a way that only privileged software can reach it. We will have more to say about security in Section 4.

3. Systems architecture

Pocket computers will derive most of their usefulness from integration into a global system. Such integration can only come about through wide-spread agreement on the functions of various components and their interactions.

Users of the system will not only use their pocket computer, of course, but a combination of the devices around. When near a large screen, for instance, the user will prefer to read documents on that screen to reading them on the tiny screen of the pocket computer. For audio output, the user may prefer a nearby hi-fi stereo system over the tiny speaker of the pocket computer. And for CPU-intensive jobs, the user will always prefer a powerful work station over the not-so-fast pocket computer.

We may expect the user interface to become distributed over the network. Naturally, a user interface will be made up of devices in physically close proximity to the user, but that does not imply that they will be logically close to each other. Portable devices may have connections to the stationary ones via a wireless-network gateway that is quite far away; maintenance of security may require that part of the processing of a job must be done at the user's home site which may be far removed from the user's current location.

The Universities of Cambridge and Twente have been studying the architecture of systems where the devices that make up the user interface are distributed. In the architecture developed in the Pegasus project, devices, such as displays, cameras, microphones, keyboards and so on, are connected directly to the network and can be addressed directly from anywhere in the system.

Every device does have an owner, however: a system near the device that controls the connections through the network switch to which it is attached. The idea is illustrated in Figure 1; the shaded areas indicate the autonomous subsystems.

4. System support for mobility

Infrared networks are mainly useful indoors, where distances are small and there is not too much ambient infrared radiation corrupting transmissions. Infrared light does not penetrate walls, so infrared networks will also have to be organized as cellular ones with cells no larger than a single room.

Buildings will provide relay services to public networks, while planes, trains and automobiles could provide a relay service that couples a device's infrared

FIGURE 1. Networked devices in the Huygens architecture

network to a satellite network or a radio-based cellular network.

The communication infrastructure will be provided by the public networks, building owners, airlines, railways and others. This suggests interesting research problems. One is finding simple and effective ways in which bandwidth allocation and charging for bandwidth can be done in internetworks of communication-service providers. Another is the problem of *locating* a mobile device in order to send a message to it. Cellular telephone networks solve this problem today, but the number of cellular telephones is relatively small and the infrastructure is wholly managed by a single organization. Keeping track of billions of mobile devices in an internet of thousands of organizations requires completely new solutions – the present ones do not scale nearly enough.

When one carries a pocket computer into an railway station, we may expect two kinds of services offered through the building network. One, as discussed above, is that of providing a connection to the internetwork, allowing the pocket computer to communicate to the outside world. The other is a service specific to railway stations: offering information about the railway timetable, platform information, directions through the building and the possibility to buy a ticket.

These services, offered by organizations receiving visitors and customers, work by virtue of a mechanism that detects newly arrived pocket computers and establishes a connection to them over which services provided by the organization are announced. Detecting new arrivals is needed for locating devices and data-relay services in any case.

An interesting area of study is how information services should be offered

on a pocket computer. Allowing the organization offering the service to run arbitrary programs on one's highly personal pocket computer constitutes a serious security risk — programs could, for instance, masquerade as regular applications and steal information from the unwitting user, or they could try to take over the pocket computer and steal its secrets (such as encryption keys).

The security architecture of the pocket computer and the infrastructure in which it is used will have to be very carefully designed, especially since pocket computers will also be used in financial transactions.

A financial transaction can only be conducted if there is a trustworthy mechanism for authentication, protection of the information exchanged and record keeping. Such a mechanism exists. It is based on public-key cryptography, and requires users making a payment to authenticate themselves by signing statements using a secret key. This key can be verified by another party without revealing the secret key itself.

Revelation of a secret key can be just as serious as having one's ATM card or wallet stolen. Since the key is kept hidden inside a pocket computer, it is clear that one should not lightly set about running programs 'found in the street' in one's pocket computer.

It is not clear whether pocket computers can be equipped with an operating system that is secure enough to allow secret keys and untrusted programs to cohabitate it. It is also not clear whether it is necessary at all to guest software in it. All that is really required is a communication channel between a service provider's software running elsewhere and the pocket computer's user interface and financial software. Thus, interaction between the untrusted service providers' systems and the trusted pocket computer is confined to the communication interface, which can be small enough to make it feasible to verify its security.

5. Acknowledgement

This article describes current research at the Universities of Twente and Cambridge. The ideas described here are only partially those of the author himself. The reader is referred to the bibliography to learn more about Huygens, Pegasus and the ideas described here.

Richard Earnshaw's help in preparing this article is gratefully acknowledged.

6. References

We recommend reading

1. Mark Hayter and Derek McAuley (1991). The Desk-Area Network, *ACM Operating System Review* **25**(4), 14–21.

for a description of using a network to connect computers, memories and devices, and

2. Ian M. Leslie, Derek McAuley and Sape J. Mullender (1993). Pegasus — Operating System Support for Distributed Multimedia Systems, *ACM Operating System Review* **27**(1), 69–78.

3. Sape J. Mullender, Ian M. Leslie and Derek McAuley (1994). Operating-System Support for Distributed Multimedia, *Proceedings of the Summer Usenix Conference* in Boston, MA.

for a description of the Pegasus project on operating system support for multimedia systems.