유비쿼터스 컴퓨팅을 위한 보안 하드웨어 구조 분석

김정태

목원대학교

Analyses of Security Structure for Ubiquitous Computin

Jung-Tae Kim,

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

요 약

Processsive ubiquitous networks have impressed us with alternative features, divesity or security. When the diversity from small devices to large machines is in normal states, ubiquitous networks are fundamental and useful. We have developed a mobile processor dedicated to multimedia cryptography. We have focus on the multimedia cryptography by the dedicated processor.

I . Introduction

We will present the multi-lateral security for ubiquitous audiovisual services. Today, large scale audio visual service on the network is about becoming reality. Such services allows us to access any audiovisual contents at anywhere in the world, freely combine them and use other contents to create new contents. After those services become widely available, we think that we need new security consideration for large scale open loop system on the global network, which is different to the small closed loop system. Facing with progressive ubiquitous environment, we have felt alternative impressions, diversity or security. While the ubiquitous network is really functional and useful when the diversity is in normal states, it is hard to control if abnormal states once happen among widely spread devices. Actually, the diversity is the cause of illegal attack, intrusion, pretension, etc. Sice ubiquitous devices treat large quantity of multimedia data, it is expedient to build in power conscious high-performed hardware cryptography. However, safety aware chips to protect multimedia date itself have never appeared to the best of our knowledge. Thus, we have exploited hardware cryptography embedded multimedia mobile processors. We have developed multimedia mobile processors, hardware cryptography embedded processors, and safty aware multimedia mobile processors embedded on the application of a hardware cryptography embedded multimedia mobile processor.
In the era of ubiquitous computing, we are faced with the disturbance of privacy and the spread of multimedia information. The protection of privacy and provision for security are crucial for further promoting everlasting ubiquitous trend. A key technology in ubiquitous community will be a simpler yet stronger cryptographic procedure for multimedia data. Although the actual public key scheme, RSA, guarantees extremely high reliability, it is rather time-consuming. RSA suffers a trade-off between high reliability and long processing time.

We have to consider the aspect of the architecture.

- Hardware SMT to swiftly deal with large quantity of multimedia data.
- Wave-pipeline for execution units that brings about PC like high speed and low power dissipation proper to mobile devices
- Interpreter type java CPU to enhance sophisticated multimedia processing
- Microprogamming techniques for a hardware thread branch that covers picojava technique.

Ⅱ. Requirement for security

It is a popular misconception that "security" is synonymous with "encryption:, In many cases, confidentiality via encryption is that least important element of a security solution. Network security involves a number of different elements.

1. data origin authentication
2. command authorization
3. message integrity protection
4. message replay prevention
5. data confidentiality
6. key distribution
7. trust versus trustworthiness

III. Hardware cryptography embedded architecture

A hardware cryptography embedded multimedia mobile processor we have developed for ubiquitous computing. This is completely different from trusted platform module and is able to implement an extremely huge length common key scheme. In view of efficiency, usability, and cryptographic strength. According to the discussion described above, a reasonable choice for such applications will be multimedia cryptography in bidirectional communication. This is impossible for TDM, a cutting edge technique commonly known as security chip. TPM implements RSA, and its major role is implicitly digital signing. TPM works for a short, password size text data, but the encryption of long length multimedia data like an image is definitely outside of the security chip in view of running time. In view of efficiency, usability,, and cryptographic strength, Embedded processor is suitable for the cryptography of multimedia data.

IV. Computational Requirements of Security Processing

The computational power available in a mobile appliance is significantly limited compared to the processing capabilities of a desktop computer. To understand the difference, compare the MIPS ratings of a 2.6GHz pentium desktop and a state-of-the-art PDA featuring the Intel StrongARM 1100 processor. While the former is capable of delivering roughly 2890 MIPS, the latter can supply only 235 MIPS at its fastest. The above scenario actually represents the higher end of the embedded processor spectrum. At the other end of this spectrum, we have the Motolrola 68EC000 processor core used in Palm OS products used in cell phones typically deliver 15 to 20 MIPS processing power running at speeds of 30 to 40 MHz. While power dissipation and size requirements of mobile appliance restrict the processor architectures and, hence, their MIPS ratings, the level of security desired in data communicated by the mobile appliance remains unchanged or even increases. As a consequence, the computational requirements of standard security protocols tend to be significantly higher than the embedded processor capabilities. Some example reveals that the total processing requirements for a security protocol that uses 3DES for encryption/decryption and and message authentication at 10 Mbps is around 651.3MIPS. A similar trend has also been

observed for RSA based connection set-ups performed in client/server handshake phase of the SSL protocol. A 235 MIPS embedded processor can be used to establish connection latencies at 0.5sec, but not at 0.1 sec. Thus, there exists a clear mismatch between the security processing requirements and the available processor capabilities, even if the workload of the appliance is assumed to be completely dominated by security processing. In other words, this mismatch is likely to be worse in reality since the processor is typically burdened by a workload that also includes other application software, network protocol and operating system execution. The effective computational requirements of a typical security protocol that performs RSA based connection set-up, 3DES-based data encryption and SHA-based integrity are shown for various combinations of connection latencies and data rates. The processing capabilities of an embedded processor can be represented as a plane in the 3 dimensional space. Clearly, the processing requirements above the plane can not be supplied by the embedded processor, leading to a wireless security processing gap. While embedded processor performance can be expected to increase and improvements in fabrication technologies and innovations in processor architecture, the increase in data rates, and the use of stronger cryptographic algorithm threaten to further widen the wireless security processing gap.

V. Secure Hardware Flatform Architecture

Security challenges are usually complex even when viewed in a limited perspective. Thus from a system perspective, it is imperative to take a hieeraaaachical approach where each layer of security provides a foundation for the one above it.

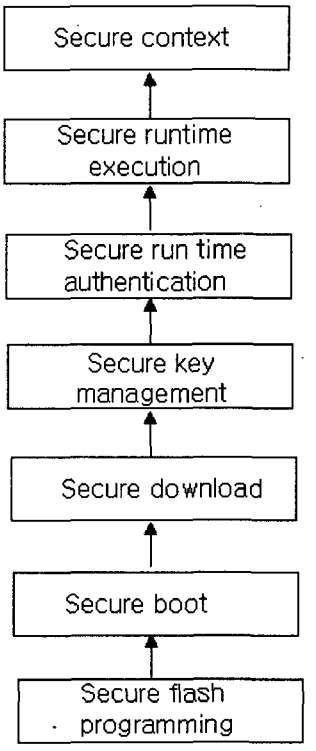

Figure 1. Hierarchical approach to security

A base platform architecture must be flexible and scalable to meet the needs of each stratum in the marketplace. Flexible and scalable base platform architectural simplify the development and deployment of new applications and services and the associated security requirements.

VI. Security Processing Architectures

Security processing refers to computation that need to be performed specially for the purpose of security. For example, in a secure wireless data transaction, security processing includes the execution of any security protocols transactions, security processing includes the execution of any security protocols that are utilized at all layers of the protocol stack.

A. Embedded processor enhancement for

securing processing

There have been several attempts to improvement the security processing capabilities of general purpose processors. Since most microprocessors today are word oriented, researchers have targeted accelerating bit level arithmetic operations such as the permutations performed in DES/3DES. Multimedia in struction set architecture

B. Cryptographic hardware accelerators

Highest levels of efficiency in processing are often obtained through custom hardware implementations. Since cryptographic algorithm form a significant portion of security processing workloads, various companies offer custom hardware implementations of these cryptographic algorithms suitable for mobile appliances including smart cards and wireless handsets.

C. Programmable security protocol engines

While cryptographic accelerators alleviate the performance and energy bottlenecks of security processing to some extent, achieving very high data rates or extreme energy efficiency requires a view of the entire security processings workload. In additional to cryptographic algorithms, security protocols often contains a significant protocol processing components, including packet header/trailer allocation parsing

VI. Conclusions

Security is critical to enabling a wide range of applications involving mobile appliances. While security has been addressed in the context of traditional computing systems and the wired internet, mobile appliances usher in many new challenges.

References

[1] Y.Frankel, A, Herzberg, etcs, "Security issues in a CDPD wireless network," IEEE Personal Communictions, v..2, pp.16-27, August 1995

[2] C. Brookson, "GSM security: A description of the reasons for security and the techniques," in Proc, IEE Colloqium on Security and Cryptography Applications to Radio Systems, pp.1-4, June, 1994

[3] S. K. Miller, "Facing the Challenges of Wireless Security," IEE Computer, v.34, pp.46-48, July 2001

[4] D. S몸 and A. Mukherjee, "Pervasive Computing: A Paradigm for the 21st Century," Computer Magazine, v.36, n.3, pp.25-31, Mar. 2003

[5] P. H. W, Leong, etc, "A microcoded elliptic curver processor using FPGA technology," IEEE TRANS. on VLSI Syst., v.10, n.5, pp.550-559, Oct, 2002

[6] M, Fukase, etc, "An experiment in the design and development of a multimedia processor for mobile computing," Technical report of IEICE, v.102, n.400, pp.13-18, Oct. 2002