Chapter 1

RESEARCH OVERVIEW

1.1 INTRODUCTION

The growth in popularity of ubiquitous computing requires the use of embedded network processors in everyday objects. Even though the idea of interaction between the digital devices around us could bring a great deal of convenience it also introduces great risks.

Field area networks are rapidly expanding to include a wide range of applications [1]. Embedded intelligent nodes on the network are generally connected to a centralized gateway used by a service provider to monitor and control various applications. Field area networks have previously been implemented as autonomous systems as shown in figure 1.1, therefore security has never been a great concern.

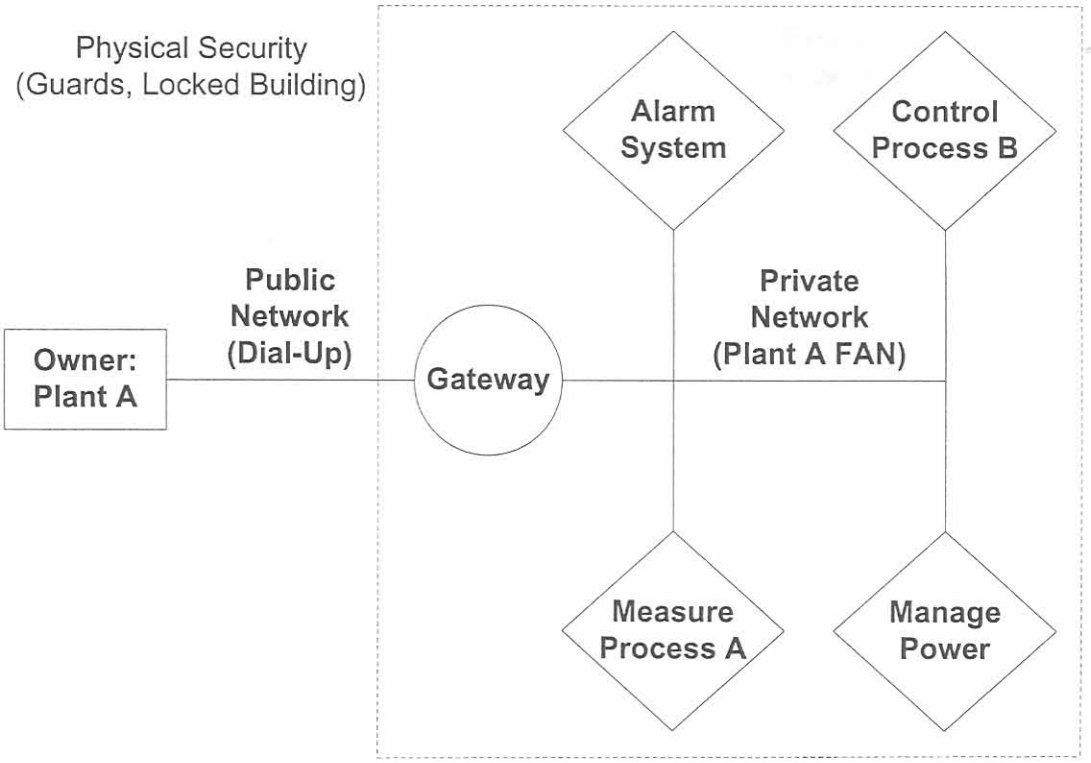

Figure 1.1:
Autonomous field area network

These days entities from different vendors, or with different owners, may be connected to the same network and therefore networks are no longer guaranteed to be autonomous. Embedded intelligent nodes on the network can be installed in a small to medium geographical area (e.g. an office, a group of flats or a factory) as is shown in figure 1.2. Each entity needs a secure way to relate to its owner, vendor and peers in the network without being compromised [2].

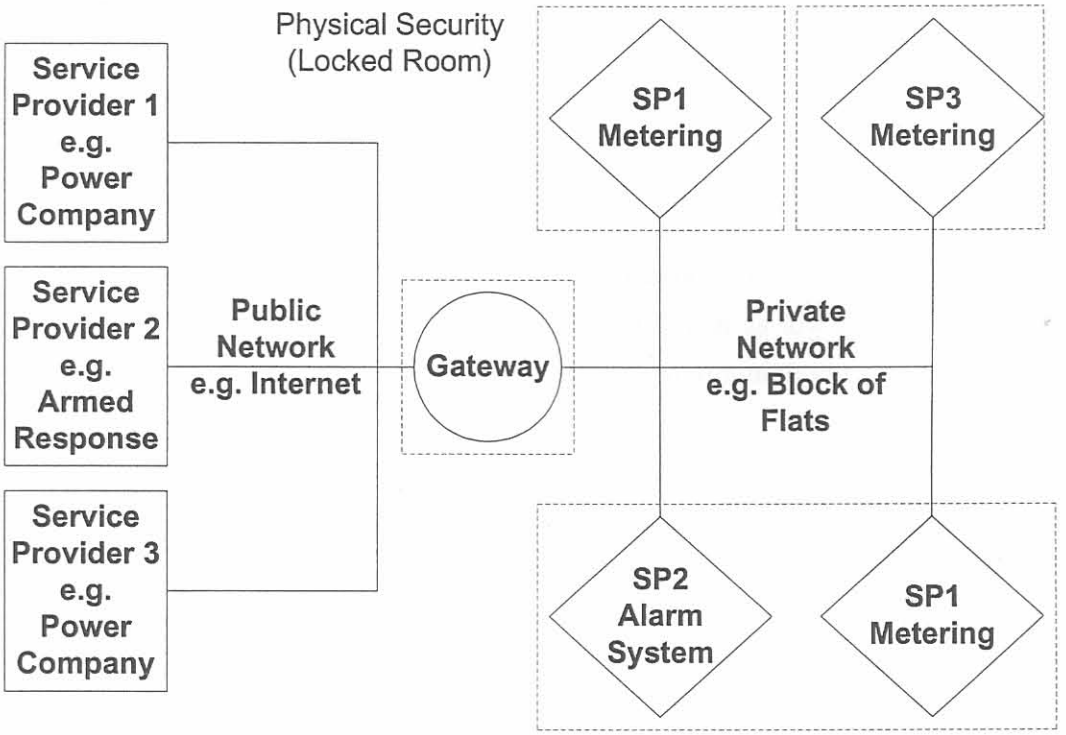

Figure 1.2:
Non-autonomous field area network

Some new applications such as power metering or prepaid systems require that the data on the network be secured. In these cases the users, or unauthorized third parties, cannot be allowed to have the means to possibly manipulate such data. For such applications the client would not only require measurement, control and communication functionality but also a high level of security. The node must therefore be able to capture, manipulate and secure data and send it to the gateway, from where it is presented to the service provider. To physically secure the entire system like the previous autonomous model would be im-

possible. The gateway and the nodes can be housed in secure containers or locked rooms, but the networking infrastructure would be vulnerable to intrusion. The gateway is also more vulnerable to attacks from the public network as it can now be accessed by multiple users.

Smart cards offer a simple, inexpensive method of incorporating a cryptographic processor into an embedded system that will allow for the implementation of security services. This dissertation discusses the implementation of a security policy for embedded networks, using smart card technology. This chapter defines the problem statement, research objectives, research approach, context and scope of the work undertaken.

1.2 PROBLEM STATEMENT

The real problem to be addressed is the implementation of security services, using smart cards, in a field area network with resource limitations such as low bandwidth, limited processing power, limited storage capacity and limited communication protocols.

The challenge would be in identifying the inherent risk and threats for embedded networks in context of possible applications for these systems. A novel security policy must then be formulated to address information security within field area networks. The proposed security policy must ensure that the confidentiality, integrity, availability and authentication services are upheld. All security services must be implemented using only mechanisms provided by smart card technology.

1.3 SCOPE

The scope of the research is to propose a security policy, using smart card technology, that will provide security services to an embedded field area network used in distributed real-time applications. Performance issues related to the implementation of security mechanisms using smart cards are also addressed. It does not focus on distributed real-time programming, network architecture or communication protocol issues beyond those required to implement a sound security policy. The security policy incorporates accepted security mechanisms and does not introduce new cryptography techniques.

1.4 RESEARCH CONTEXT

A field area network offers a reliable solution for critical real-time systems functioning in a harsh environment. Separate systems have been developed to incorporate the functionality of FAN's [3],[4] and to take advantage of the security features offered by smart card technology [5],[6],[7]. The two technologies have never been combined to provide secure networking services. FANs have previously been implemented as autonomous systems, and therefore security has never been a great concern. These systems can be applied in home automation, prepaid systems, real-time distributed systems and e-commerce (the user could request a service online and an enabling token passed through the system connected to his/her TV, Hi-Fi, etc.). For these networks to be a commercially viable proposition a range of security services must be provided in order to protect the system from malicious activity [8]. Smartcards might provide a viable way of providing the security functions needed to implement a sound security policy, which will allow field area network applications to expand significantly. A few applications that will be made possible are:

- prepaid network systems for commercial services,
- secure data logging applications (power consumption metering),
- remote control & measurement of critical processes,
- secure home or office automation and
- security application such as access control to a building.

1.5 RESEARCH OBJECTIVES

The main objective would be to formulate a policy which could be implemented successfully into a field area network, using the security mechanisms provided by a smart card, while maintaining reasonable system performance. The secondary objective will be to determine how the security mechanisms provided by smart card technology can be applied to secure an embedded network. To achieve this, a number of sub-objectives need to be accomplished. These sub-objectives are:

- Field area network implementations must be analysed and the way in which various entities interact studied. The main assets of the network system must be identified in order to determine which entities are critical to the overall operation of the system.

Once the important entities have been identified and the operation of the system studied a list of functional requirement must be drawn up. These are the operations that must be performed by the network entities in order for the system to function correctly. Vulnerabilities and possible threats to the system assets and functional requirements should then be determined.

- Security policy implementations in other types of networks must be analysed. Possible security service and mechanisms used in implementing these security policies must be investigated. It should also be noted which services address which threats and vulnerabilities.

- Develop a security policy which will mitigate threats and enforce the functional requirements. Determine the security services which are required to enforce the security policy. It must be determined which mechanisms must be combined to implement the security services required by the policy. In order for this policy to be successful a set of specifications for each network component needs to be formulated. These specifications give guidelines of which mechanism needs to be implemented where and what information needs to be communicated and stored.

- Smart card technology must be studied and the different security mechanisms provided investigated. Different means to implement the required services using these mechanisms must be proposed. These mechanisms must be successfully implemented in order to test performance and ensure functionality.

- Criteria must be defined in order to evaluate the overall security policy. Assurance must be provided that the policy is effective and that system vulnerabilities and threats are addressed. A benchmark needs to be defined to measure the performance and security level of individual mechanisms used to provide security services. This should then be used to compare different service implementations in order to determine which are best suitable to secure an embedded network.

1.6 RESEARCH APPROACH

A number of questions were identified to assist in better defining and solving the problem at hand:

The operation of current networks and how functionality is provided need to be researhed, including hardware and resource considerations, the requirements for such a network to ensure functionality, how these functional requirements can be disrupted and how these functional requirements and assets can be protected. This will include an investigation into the critical components of such networks, whether these components are vulnerable and how these components are threatened, the services generally provided to mitigate these threats and what role each component plays in the success of the policy.

Security mechanisms to provide the necessary security services needed to be defined, including issues such as the mechanisms provided by smart cards, how these mechanisms can be used to implement the security services required, whether these mechanisms can successfully be implemented into a working system, how the performance of different mechanisms can be measured and compared, the performance of the implemented mechanisms, and whether the security mechanisms provided by the smart cards can secure the network while ensuring reasonable network performance.

How can it be assured that the formulated security policy is feasible for embedded field area networks, as well as secure and effective in addressing all vulnerabilities?

1.6.1 Research Method

1. Literature Study

   - The scope of the work is further defined.
   - Relevant work from other sources are identified.
   - General information security principles are discussed.
   - Available security services and mechanisms are documented.
   - Common threats and vulnerabilities are documented.
   - The design considerations and architecture of distributed field area network are discussed.
   - Different smart card technologies are identified.
   - Mechanisms provided by smart cards are studied.
   - The advantages and disadvantages of smart card technologies are discussed.
   - Industry standards addressing security assurance for security policies are discussed.

2. Problem Analysis

   - Field area network implementations are analysed.
   - A network system is defined to model a field area network.
   - Assets and functional requirements are determined.
   - Possible vulnerabilities and threats to the system are identified.
   - Risk analysis is performed to determine the significance of the vulnerabilities and threats.
   - Guidelines are given for the functions required by each component in the network.
   - Special hardware requirements of embedded networks are determined.
   - The security services needed to secure the system are identified.

3. Design

   - A security policy that addresses the vulnerabilities and threats is defined.
   - Mechanism needed to provide the necessary services are determined.

- A communication protocol implementing the 3rd and 4th layer of the OSI layer is suggested.
- Methods of implementing the required mechanisms using smart cards are proposed.
- Determine evaluation criteria for the security policy
- Determine benchmarks for evaluating system performance and performance of implemented mechanisms.

4. Implementation
   - Detail is given of how the services will be implemented using smart cards.
   - The security mechanisms are implemented on smart cards.
   - A test system is build and documented.
   - Security services are implemented in the system using smart card mechanisms.
5. Review and Assessment
   - Using the test system collect data on the performance of the individual services and mechanisms.
   - Evaluate these mechanisms and system performance by comparing results to the benchmarking criteria.
   - Assurance is provided that the proposed security policy is secure and addresses all identified threats and vulnerabilities.

1.7 DOCUMENT OVERVIEW

This dissertation consists of the following sections:

Chapter 1 (Research Overview):
Describes the problem and the research approach to finding a viable solution.

Chapter 2 (Literature Study):
Provides background information on relevant technology and possible solutions.

Chapter 3 (System Overview):
Defines the system's boundaries and functional requirements.

Chapter 4 (System Specifications):
Identifies aspects that the solution must address.

Chapter 5 (Implementation):
Outlines possible solutions and describes how they can be implemented.

Chapter 6 (System Testing):
Shows the experimental procedures used to verify and quantify the performance of the proposed implementations.

Chapter 7 (Results):
Documents and explains the results achieved during testing.

Chapter 8 (Conclusion):
Places the proposed solution and the findings from the results in context. Also suggests some further topics of research in this field.