특집

보안프로세서 기술의 현황과 전망

김기영, 오진태, 장종수 (한국전자통신연구원 네트워크보안그룹)

I. 서 론

최근 인터넷 사용의 급증으로 인터넷 가입자 수가 폭발적으로 증가하고 있으며, 온라인 거래와 다양한 인터넷 서비스 제공 등으로 인하여 고속 네트워크 트래픽 양의 증가가 현저해지고 있다. 이러한 변화로 인하여 네트워크 사용자들은 예전보다 훨씬 많은 양의 정보를 고속 네트워크 인프라를 통하여 쉽게 주고 받을 수 있다. 이러한 편리함의 역기능으로 바이러스, 웜 및 해킹과 같은 사이버 테러를 말할 수 있으며, 이로 인하여 개인의 사생활 정보 유출은 물론 국가 안보까지 위협받는 상황에 이르렀다.

2000년도 초기까지 사이버테러는 특정 서버를 목표로 한 해킹 중심이었으나, 최근 웜, 바이러스 등에 의한 불특정다수를 겨냥한 네트워크 공격이 중심을 이루고 있다. 이러한 웜, 바이러스 등에 의한 공격으로 패킷 양이 증가하여 네트워크 인프라 자체가 공격받는 상황이 되었다. 또한 새로운 취약점 공격에 의해 네트워크 전반적인 위협은 꾸준히 증가하고있다.

한편, 해킹 기법의 발달과 소스코드 공개에 의한 해킹의 대중화가 이루어지고 있으며, 자동화된 해킹 툴 사용한 해킹이 급격히 증가하고 있다.

지금까지 해킹에 대응하기 위하여 대부분 소프트웨어 기반의 보안 기능을 제공하였으나, 이미 네트워크의 고성능화로 인하여 성능의 한계에 봉착하고 있다. 보안 시스템에서 탐지 기술의 다양화와 고속화로 인하여 정확성, 고속성, 비정상행위 탐지 능력 등의 특성들을 해결하기 위하여 실시간 보안 핵심기술들을 하드웨어화 할 필요가 있다.

본 고에서는 이러한 보안기능을 제공하는 고속 보안 핵심 칩들의 기술의 현황과 전망에 대하여 알아보고자 한다. 본 고의 구성은 II절에서 고성능 침입탐지 칩 기술, VPN 칩 기술, RFID 칩 기술 및 요즘 한창 관심을 끄는 생체인식 칩 기술 등에 대하여 알아보고, III 절에서는 이러한 고속 보안 핵심 칩들의 개발현황에 대하여 알아본 다음 IV절에서 앞으로 이러한 고속 보안 핵심 칩들의 전망에 대하여 기술한다.

II. 보안 프로세서 기술의 개요

최근에 개발된 보안 프로세서들은 보안 관련 암호 및 침입탐지 알고리즘을 하드웨어로 구현

하여 성능이 매우 향상되어 출고되고 있다. 이런 고속 보안 프로세서는 매우 큰 대역폭을 요구하는 현 네트워크 보안 솔루션 장비 개발에는 필수 요소가 되고 있다.

현재 고속 보안 프로세서로는 고성능 침입탐지 칩 기술, VPN 칩 기술, RFID 칩 기술, 다중 생체인식 칩 기술 등이 있으며 이들은 각각 다음과 같다.

1. 고성능 침입탐지 칩 기술

네트워크 공격의 다양화와 네트워크 인프라의 고속화로 네트워크 인입점에서 다량의 트래픽을 분석하고, 유해트래픽을 실시간 감지, 분석 및 대응할 수 있어야 한다. 고성능 침입탐지 칩 기술은 이러한 분석 및 대응 기법이 적용된 보안 알고리즘을 칩으로 구현하는 기술이다.

지금까지 개발된 보안 시스템들은 대부분이 소프트웨어기반의 알고리즘들을 적용한 것으로 네트워크에서 요구하는 성능을 지원하는데 한계를 보이게 된다.

이미 네트워크 프로세서에 소프트웨어기반의 보안 알고리즘을 적용하는 예가 있으나, 근본적인 하드웨어 기반의 보안 알고리즘이 개발되지 않는 한 성능의 한계를 극복할 수 없다. 기 개발된 네트워크 프로세서 중에서 최고성능의 네트워크 프로세서에 1Gbps급 패킷 포워딩 정도를 구현하면 남는 리소스가 거의 없어 추가적인 보안 알고리즘을 구현하기 어려운 실정이다. 그리고, 1Gbps급의 Misuse 기반의 패턴 매칭 정도의 기술도 현재의 네트워크 프로세서에 적용하기 쉽지 않다. 일반적으로 네트워크 프로세서에서 탐지 룰의 구현은 각각의 룰들을 모두 하드코딩하여야 하며, 새로운 룰 추가의 경우 이를 다시 코딩하여야 하므로 룰 추가가 매우 힘든다. 따라서 룰의 필드가 비교적 한정된 헤더룩업 정도만 구현하는 수준이다. 대부분의 탐지룰들은 헤더정보와 페이로드의 특정한 시그니처를 동시에 탐지하여야 하며, 한정된 헤더비교만으로 판단할 수 있는 공격은 몇 개에 불과하다. 따라서, 기본적인 Misuse기반의 탐지엔진을 네트워크 프로세서로 구현하는 것도 현재 네트워크 프로세서 기술로는 어려워 보인다.

또한 대부분의 보안 시스템은 L7까지 모든 계층에 걸쳐 보안 검사를 요구하고 있어 네트워크 프로세서에 의한 완벽한 해결책은 기대하기 어렵다. 이미 국내 여러 곳에서 네트워크 프로세서를 적용하여 보안제품을 개발하고자 노력하였으나 탐지엔진 구현의 어려움과 성능 한계로 인한 어려움을 겪고 있다.

이러한 고속 탐지엔진은 많은 수의 룰들을 동시에 비교할 수 있는 하드웨어 알고리즘을 필요로 하며, 이러한 검색 알고리즘 없이 단순한 소프트웨어의 하드웨어화로는 해결되지 않는다.

이미 IPS 기술의 우위를 선점하고 있는 외국의 티핑포인트 유니트원, NA의 맥아피 인터루쉴드 등의 회사에서도 보안전용 ASIC을 개발하여 적용한 시스템을 출시하였으며, 네트워크 프로세서에 기반한 고성능 제품은 찾아볼 수 없다. 따라서 고성능 알고리즘 개발을 통한 FPGA 및 ASIC 솔루션이 유일한 해결책으로 보인다.

현재 한국전자통신연구원의 액세스급 보안게이트웨이 시스템개발사업에서 하드웨어기반의 고성능 침입탐지 알고리즘이 개발되었으며, 이를 적용한 시스템이 2003년에 개발 완료 되었다. 본 시스템에는 Misuse기반의 탐지 알고리즘과 휴리스틱기반의 탐지 알고리즘, 그리고 Anomaly 기반의 트래픽 분석 알고리즘이 적용되어 있다.

이러한 기능들은 2Gbps Wire - speed 성능 요구사항을 만족하는 것으로 시험 완료되었다.

2004년도에 목표시스템에서는 세션관리, IP Reassembly, Protocol Anomaly 등의 추가기능을 제공하며 모두 5G급의 성능 요구사항을 가지고 있다.

현재 개발된 침입탐지 기법은 알려진 공격에 대하여 Misuse 기반의 탐지기법과 알려지지 않은 공격을 탐지하기 위한 비정상행위 기반의 탐지기법을 제공한다. 이들이 기본적으로 제공하여야 하는 기능은 다음과 같다.

- 침입 유형별 탐지 및 차단 기능
- 웜, 바이러스 탐지 및 차단 기능
- 인라인 모드 지원을 통한 정책기반 자체 차단기능
- 침입탐지 내역 및 차단 현황에 대한 로그 및 보고 기능
- 유연하고 실시간성이 보장되는 정책 Update 기능
- 실시간 네트워크 트래픽 분석 기능
- 알려지지 않은 공격 탐지를 위한 Anomaly 분석 기능

위와 같은 기능들은 오탐으로 인한 서비스 제한 방지를 위한 탐지기능의 정확성과 수기가급의 네트워크에서 wire - speed를 보장하는 고성능화를 보장하면서 제공되어야 한다.

2. VPN 칩 기술

VPN 기술은 개방된 공중망에서 보안이 유지된 가상 사설망을 구현하기 위한 기술로 네트워크 자원을 보다 효율적으로 사용하게 하는 정보보호기술이다. VPN의 보안 기능은 터널링과 암호화로 구성된다. 터널링 프로토콜로는 PPTP, L2TP, IPsec 등이 있다. 이중 IPsec이 가장 강력하고 융통성을 제공하는 터널링 프로토콜이며, VPN은 이를 기본적으로 지원해야 한다.

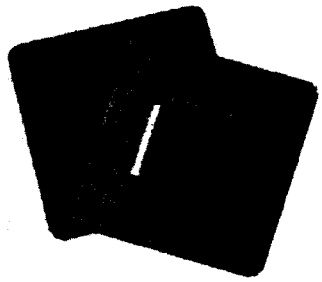
지금까지 기술한 VPN 기능들은 고속 보안 프로세서를 사용하여 구현하여야 한다. 고속 보안 프로세서는 다양한 암호 알고리즘을 하드웨어로 구현한 것으로 많은 블록 암호 알고리즘과 공개키 알고리즘이 구현되어 있다.

하드웨어로 블록 암호 알고리즘을 구현한 고속 보안 프로세서를 이용하는 것은 3DES, RC4와 같은 간략한 알고리즘의 구현뿐만 아니라 AES 등과 같은 복잡한 블록 암호 알고리즘의 속도를 높일 수 있기 때문이다.

이러한 고속 보안 프로세서들 중 Hifn 8154 및 Cavium Nitrox - II와 같은 상용 VPN 칩과 Netscreen에서 자체 개발한 GigaScreen - II ASIC 칩에 대하여 간단히 살펴본다.

* Hifn 8154

Hifn사의 8154는 IPsec이나 SSL 등 다양한 알고리즘 및 프로토콜을 지원하고, 최대 초당 1,500개의 메인 모드 IKE의 성능을 가지며, 32/64bit의 33/66MHz PCI 등의 다양한 인터페이스를 지원한다. 본 제품의 안전성은 FIPS

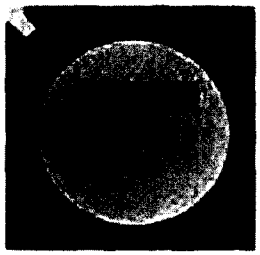


〈그림 1〉 Hifn 8154

140 - 1의 수준 3을 만족하고 있으며, Linux나 BSD 등 다양한 운영 체제를 지원한다.

* Cavium Nitrox-II

Cavium사의 Nitrox - II 역시 다양한 알고리즘 및 프로토콜을 지원하고, 최고 10Gbps의 IPsec 성능과 최대 초당 15,000개의 메인 모드 IKE 성능을 갖는다. PCI나 SPI - 3 등 다양한 인터페이스를 지원하며, FIPS 140 - 1의 수준 3 안전성과 Linux, BSD, Windows 등 다양한 운영 체제를 지원한다.



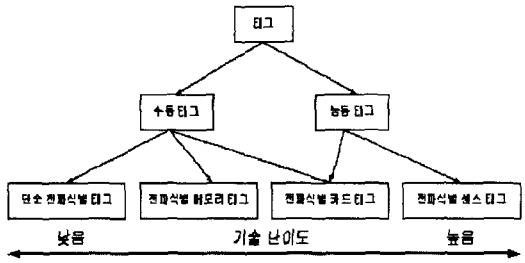
〈그림 2〉 Cavium Nitrox-II

* NetScreen GigaScreen-II

GigaScreen - II ASIC 칩은 2Gbps firewall, 1Gbps 3DES 처리 성능을 가진다. 또한 여러 보안 알고리즘이 최적의 형태로 구현되어 있어 패킷의 크기에 따른 성능 저하의 폭이 적으며, 2Gbps firewall, 1Gbps 3DES 처리 성능을 가진다. 또한 여러 보안 알고리즘이 최적의 형태로 구현되어 있어 패킷의 크기에 따른 성능 저하의 폭이 적으며, Programmability 기능이 우수하여 프로그램으로 패킷 분류 기능과 내용 검색 기능을 제공한다.

3. RFID 칩 기술

태그의 기술은 전파식별 시스템의 응용분야에



〈그림 3〉 RFID 칩 기술의 분류

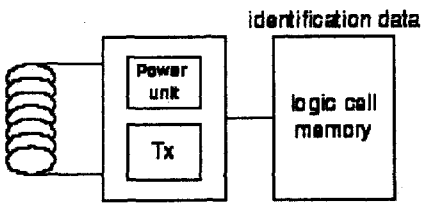
따라 다양하게 기술된다. 우선, 전력 공급에 의하여 태그 자체에 밧테리(battery)를 사용하여 구동하는 능동 RF 태그와 RF 리더기(reader)에서 송신하는 전파를 태그가 수신하여 전력 에너지로 이용하는 수동 태그로 구분한다.

능동 태그는 밧테리로 인해, 태그의 크기와 소모전력, 수명에 대해서는 수동 태그와 비교해서 단점으로 작용하지만, 무선 인식 거리, 다양한 센서 네트워크, 유연한 정보보호 기술 적용에서 유리한 점을 가지고 있다. 현재 주종을 이루는 태그는 가격과 수명에 유리한 수동 태그를 많이 사용하고 있다.

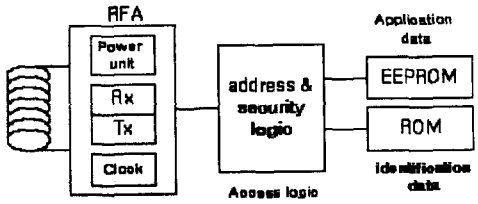
전파식별 태그는 무선 인식영역 안에서 직접 접촉하거나 스캐닝할 필요 없이 자동 인식하므로 기존의 바코드 등과 같은 인식 시스템을 대체할 수 있는 훌륭한 시스템이다.

현재는, 바코드를 대신하는 개념, 바코드에 비해 많은 데이터 용량 처리, 무인 자동 출입(gate) 인식시스템을 중심으로 대부분의 전파식별 시스템이 구성된다. 앞으로는 유비쿼터스 센스 네트워크(ubiquitous sensor network), 정보보호, 상품의 운송/유통 관리 및 처리 등을 중심으로 전파식별 시스템이 빠르게 발전할 것이다.

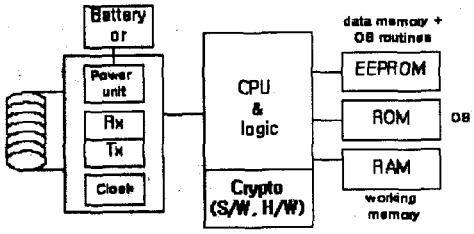
태그의 핵심 기술은 저전력, 초소형 기술이며 안테나 기술을 포함한 태그 제작 기술이라고 할



〈그림 4〉 단순 전파식별 태그



〈그림 5〉 전파식별 메모리 태그



〈그림 6〉 전파식별 카드 태그

수 있다. 이를 핵심으로 보는 이유는 태그의 저가격 정책 때문이다. 이에 따라 태그는 센스 온 칩(sensor on chip) 기술과 안테나 온 칩(antenna on chip) 기술이 성패의 관건이 될 것이다. 그림 4는 전파식별 태그를 하드웨어의 구조 측면에서 구분한 것이다. 여기서, 하드웨어 기술 난이도 중심으로 4가지로 구분하면 다음과 같다.

가) 단순 전파식별 태그

그림 4는 단순 전파식별 시스템 기능으로서, 대부분 수동 태그로 제작된다. 바코드의 대체 개념으로 보안 논리 모듈이 없이 읽기 기능의 로직 셀 메모리만 존재하는 단순 태그라고 말할 수 있다. 이 태그는 저가격 및 단순 인식처리에 유리하다.

나)전파식별 메모리 태그

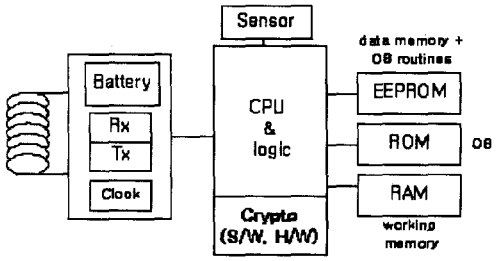
그림 4의 단순 전파식별 태그에 비해, 간략한 보안 기능과 읽고 쓰기 기능이 추가된 형태의 태그를 그림 5에 기술하였고, 이를 전파식별 메모리 태그라고 명명할 것이다. 이 전파식별 태그는 간략한 데이터 관리 및 처리를 수행할 수 있다. 이는 실질적인 전파식별 시스템의 개념 모델로서, 많은 응용 분야에서 사용되고 있으며, 수동 태그 중심으로 발전하고 있다.

다) 전파식별 카드 태그

암호 모듈 및 프로세서 기능까지 첨가된 그림 6의 태그를 전파식별 카드(card) 태그라고 부른다. 전파식별 카드 태그는 암호 모듈을 하드웨어 또는 소프트웨어 형태로 태그에 내장함으로써 강화된 보안 상품에 사용할 수 있는 태그이다. 다양한 응용 분야 즉, 전자화폐, 교통카드, 건강카드 등에 사용할 수 있을 것이다. 이 전파식별 카드 태그는 사용 분야에 따라 능동 태그 또는 수동 태그로 구별하여 사용할 수도 있다. 이 전파식별 카드 태그에서 수동 태그의 대표적인 예로 국제 표준 ISO 14443 비접촉 스마트 카드(contactless smart card)가 있다.

라) 전파식별 센스 태그

위에서 논의한 3가지가 전파식별 태그를 말하는 일반적인 하드웨어 구조이다. 그림 7은 그림 6의 전파식별 카드 태그에 센스 모듈 또는 칩을



〈그림 7〉 전파식별 센스 태그

부착하여 구성한 전파식별 센스 태그이다. 여기의 센스는 주로 온도, 습도, 압력, 광 등의 주변 환경 센스를 말한다. 이 센스 태그는 능동 태그로 사용에 따라서는 센스 노드(node)로 유비쿼터스 센스 네트워크의 정보 수집을 위한 물리적인 인프라로 사용된다.

위에서 기술하였던, 태그들의 구조들은 태그를 어떤 용도로 사용할 것인가에 따라 시스템에 적합하고 다양한 구조로 개발할 수 있다. 전반적인 태그 칩의 구성은 무선 주파수 아날로그(RFA:radio frequency analog) 모듈, 논리 암호 모듈, 프로세서, 메모리로 구성된다고 볼 수 있다.

지금까지 소개된 내용을 바탕으로 전파식별 태그들을 개발하기 위해서는 다음과 같은 요소들을 고려해야 한다.

첫째, 전파식별 시스템은 무선 주파수를 이용하여 전자 데이터 통신을 실시하는 것이므로, 전파 즉, 무선 주파수의 인체 또는 동물 등의 생물체에 대한 유해성을 반드시 고려해야 한다. 다시 말하자면, 우리의 실생활 및 의료 등에서 적용할 경우 전파 충돌에 의한 이상동작 등을 고려해야 할 것이다. 일반적으로, 가축에는 저주파 대역인 135kHz 이하에서 큰 문제가 없는 듯하다.

둘째는 태그의 인식거리를 반영한 전력 공급을 고려해야 한다. 즉, 능동 태그를 사용할 것인가 아니면, 수동 태그를 사용할 것인가를 결정해야 한다. 이것의 결정에 따라 태그와 리더기의 하드웨어의 구조는 상당한 차이를 가지고 개발된다.

셋째는, 응용 시스템에 적합한 전파식별 태그를 개발하는 것이다. 여기에는 태그의 가격, 크기, 전력 등을 고려하여 사용자가 요구하는 전파식별 태그를 개발하는 것이 바람직하다.

4. 다중 생체인식 칩 기술

고인식 다중 생체인식 전용 칩 기술은 유비쿼터스 환경에서 타인수락 에러율(FAR) 0.0001% 이하의 개인인증이 가능한 실시간 다중 생체인식(multi - modal biometrics) 알고리즘을 고속 보안 프로세서에 구현하는 기술이다.

즉, FAR 0.0001% 이하의 다중 생체인식(얼굴/지문/홍채) 알고리즘과 비접촉식 IC카드 탑재용 저전력(50mW 이하) 다중 생체인식 핵심 칩을 말한다. 현재 다중 생체인식 칩 기술은 ISO/IEC JTC1 SC37의 생체인식기술 국제 표준규격을 준수하도록 하고 있다. 현재 고속 다중 생체인식 칩 기술은 연구 개발단계 수준이다.

III. 보안 프로세서 기술의 발전방향

지금까지 연구 및 개발된 고성능 침입탐지 칩 기술, VPN 칩 기술, RFID 칩 기술, 다중 생체인식 칩 기술 등의 보안 프로세서에 대하여 살펴보았다.

먼저 고성능 침입탐지 칩 기술의 발전방향에 대하여 알아본다.

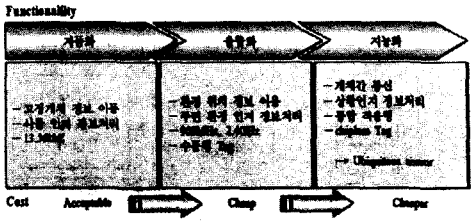
현재까지는 개별적인 침입탐지 알고리즘 들을 단순히 하드웨어로 구현하는 수준이었다. 이러

한 형태의 단순통합은 개별 탐지엔진의 결과를 연동하여 효과적인 결과를 제공하는데 한계를 가지고 있다. 따라서 향후, 고성능 침입탐지 프로세서의 탐지결과를 능동적으로 융합하여 효율적인 종합 대응 능력을 제공할 수 있는 형태로 발전되어야 할 것이다.

이와 더불어 알려지지 않은 네트워크 공격들에 대한 탐지방법으로 사용되던 비정상 행위 탐지 능력 향상을 통하여 탐지 영역 또한 확장될 것으로 예상된다. 하지만 현재의 비정상 행위 탐지 방법은 높은 오탐율과 탐지속도의 문제를 여전히 가지고 있다. 따라서 이를 해결하기위한 노력이 지속적으로 이루어져야 할 것이다.

다음으로, RFID의 기술의 발전방향에 대하여 알아본다.

RFID의 발전방향으로 현재 관심을 기울여야 할 부분은 기능적 측면에서의 발전 가능성과 비용적 측면에서의 발전 가능성이다. 우선 기능적 측면에 있어 현재 가장 널리 검토되고 있는 방식은 Passive형태의 RFID칩으로서 고정된 개체 인식 코드 획득 수준에 머무르고 있으나 2010년 이후에는 주변 환경 인지 기능, 개체 간 통신 기능, 상황 인지 정보처리 능력 등이 부가될 것으로 보여 유비쿼터스 센서로서의 역할이 보다 확대될 전망이다. 비용적 측면에 있어, 전자태그가 소형화, 지능화하는데 비해, 가격은 수 센트대로 저가화가 실행될 조짐을 보이고 있어 물류, 유통분야뿐만 아니라 동물관리, 환경, 재해예방, 의료관리, 식품관리 등 실생활에서 활용이 확대될 전망이다. 산업자원부, 대한상공회의소 등의 예측에 따르면, 2004년 RFID 주파수 대역에 관한 국제 표준이 결정되고 RFID chip가격이 5센트대



〈그림 8〉 RFID-Chip의 발전단계

로 하락하면 주요 산업분야로 급속히 확산될 것으로 예측하고 있으며, 이미 일부 업체에서는 RFID - chip의 가격을 7센트대로 떨어뜨리는데 성공했다. 따라서, RFID의 시장 발전 가능성은 크다고 판단된다.

다음으로, VPN 칩 기술의 발전방향에 대하여 알아본다.

고성능 VPN 칩 기술은 다양한 암호 알고리즘을 하드웨어로 구현한 것으로 많은 블록 암호 알고리즘과 공개키 알고리즘이 구현되어 있다. 하지만 현재 구현된 고성능 VPN 칩 기술은 지속적으로 발전하는 고속 보안 프로세서의 성능 및 기능, 안전성 등에서 향상의 여지를 가지고 있다. 블록 암호 알고리즘을 하드웨어로 구현한 고속 보안 프로세서를 이용하는 것은 Federal Information Processing Standard(FIPS) 140 - 1 또는 140 - 2의 보안 레벨을 높일 수 있고, 3DES, RC4와 같은 간략한 알고리즘의 구현뿐만 아니라 AES 등과 같은 복잡한 블록 암호 알고리즘의 속도를 높일 수 있기 때문이다.

마지막으로 고인식 다중 생체인식 전용 칩 기술의 경우, 아직 연구개발 단계로 유비쿼터스 환경에서 타인수락 에러율(FAR) 0.0001% 이하의 개

인인증이 가능한 실시간 다중 생체인식(multi - modal biometrics) 알고리즘, 칩 셋 및 응용 기술 개발이 ISO/IEC JTC1 SC37의 생체인식기술 국제 표준 규격을 준수하도록 발전되어야 할 것이다.

Ⅳ. 결 론

본 문서에서는 고속 보안 프로세서의 현재 기술과 향후 발전방향에 대하여 살펴보았다.

최근 급증하고 있는 온라인 거래와 다양한 인터넷 서비스의 확대로 인하여 많은 사람들이 쉽게 정보를 주고 받거나, 얻을 수 있다. 그러나 바이러스 또는 해킹과 같은 사이버 테러로 인하여 개인의 사생활 정보 유출은 물론 국가적 안보까지 위협하고 있다. 이러한 네트워크 환경에서 정보를 보호하기 위한, 가상사설망(Virtual Private Network: VPN), 방화벽(Firewall), 침입탐지(Intrusion Detection System: IDS), 고속 다중 생체인식 칩, RFID 칩 등과 같은 정보보호 기술의 개발이 필수적이며, 이를 활용한 다양한 보안제품들의 개발을 통하여 앞으로 도래한 BcN 및 유비쿼터스 환경의 보안을 철저히 대비하여야 할 것이다.

참고문헌

[1] 이근호, "무선식별(RFID 기술)", TTA 저널 89호
[2] 이은곤, "RFID 확산 추진현황 및 전망", 정보통산정책 제16권 6호 통권 344호
[3] 2004 RFID 국제심포지엄, 2004.2.5
[4] 주학수, 주홍돈, 김승주, "고속 암호연산 프로세서 개발현황," 정보보호학회지, 제12권 3호, 2002.
[5] 김기현, 한종욱, "Giga급 보안 프로세서 및 VPN 장비 기술 동향", 주간기술동향 1131, 2004.2.3.

저자소개

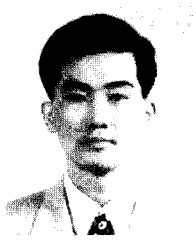
김 기 영

1988년 전남대학교 전산통계학과 이학사
1993년 전남대학교 전산통계학과 이학석사
1999년 충북대학교 컴퓨터공학과 공학박사
1988년-현 재 한국전자통신연구원 책임연구원, 보안게이트웨이연구팀 팀장
주관심분야 네트워크보안, 비정상행위탐지기술

오 진 태

1990년 경북대학교 전자공학과 공학사
1992년 경북대학교 전자공학과 석사
1992년-1998년 한국전자통신연구원 선임연구원
1998년-1999년 MinMax Tech. 연구원
1999년-2001년 10월 Engedi Networks Inc. Director
2001년-2003년 Winnow Networks Inc. CTO 부사장
2003년-현 재 한국전자통신연구원 선임연구원, 보안게이트웨이연구팀 과책
주관심분야 네트워크보안, 비정상행위탐지기술, 고성능침입탐지엔진기술

저자소개



장 종 수

1984년 경북대학교 전자공학과 공학사
1986년 경북대학교 전자공학과 공학석사
2000년 충북대학교 컴퓨터공학과 공학박사
1989년-현 재 한국전자통신연구원 책임연구원, 네트워크보안그룹장
주관심분야 네트워크보안, 정책기반보안관리기술, 유해정보차단기술 등