신뢰성 있는 인터넷 서비스 제공을 위한 교정 보안 프레임워크

이 승 민[†]·남 택 용[††]·손 승 원[†††]·한 치 문[††††]

요 약

본 논문에서는 신뢰성 있는 인터넷 서비스를 안전하게 제공하기 위한 차세대 보안기술로서 교정 보안 프레임워크를 제안한다. 교정 보안 프레임워크는 외부의 공격이나, 침입, 취약성 등의 장애요인에도 불구하고 일정수준의 지속적인 서비스를 제공할 수 있게 한다. 교정 보안의 핵심 개념은 복구와 개선 기술이다. 복구 기술은 네트워크의 생존성 기술과 빠른 서비스 복원을 가능하게 하는 네트워크 제어기술을 포함한다. 개선 기술은 장애요인이 지속되거나 반복될 경우에 이를 방지하여 서비스의 완료성을 보장하는 기술로서 시스템 자체의 개선 방안과 취약성분석시스템, 망관리시스템, 통합보안관리시스템 등과 같은 타 시스템과 연동하여 동적으로 기능을 개선시킬 수 있는 방안을 포함한다. 본 논문에서 제안하는 프레임워크는 단독 시스템 뿐만 아니라 대규모 네트워크에도 적용되어 네트워크의 생존성을 보장하고 신뢰성 있는 사용자 서비스를 제공할 수 있을 것이다.

A Correction Security Framework for Reliable Internet Services

Seung Min Lee[†]·Taek Yong Nam[††]·Sung Won Sohn[†††]·Chi Moon Han[††††]

ABSTRACT

We propose a correction security framework as next generation security technology to provide secure and reliable Internet services. The framework guarantees durability of the services in spite of external attack, intrusion, vulnerability of Internet. The main concepts of correction security consist of the recovery and improvement technology. The recovery technology includes network survivability for fault tolerance, and network management technology that covers the set of techniques aimed at providing rapid service recovery. The improvement technology includes system itself improvement and dynamic improvement preventing faults from being re-activated, in cooperation with other systems such as vulnerability analysis system, NMS, ESM. It is expected that our framework will be applied to global networks as well as system alone, and be able to guarantee the network survivability and reliable Internet services.

키워드 : 교정 보안(Correction Security), 복구(Recovery), 개선(Improvement), 네트워크 보안(Network Security), 신뢰성 있는 인터넷 서비스(Reliable Internet Service)

1. 서 론

최근 인터넷을 이용한 사이버 공격이 단순 시스템 위주에서 특정 서비스를 마비시키는 네트워크 공격으로 변화하고 있다. 인터넷 웜을 이용하여 인터넷 서비스를 마비시킨 지난 1.25 인터넷 대란이 대표적인 사례로 볼 수 있다. 이는 사이버 공격이 개인의 사생활 침해를 떠나서 국가적인 경제적 손실은 물론이고, 국가 안보와 사회질서를 위협하기까지 이르렀음을 보여주고 있다.

† 정 회 원 : 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀 연구원
†† 정 회 원 : 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀 팀장
††† 정 회 원 : 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 부장
†††† 정 회 원 : 한국외국어대학교 전자정보공학부 교수

논문접수 : 2003년 7월 22일, 심사완료 : 2003년 10월 10일

공격 유형의 변화에 따른 최근의 보안 이슈를 크게 백본망과 액세스망, 그리고 서비스영역을 포함한 가입자망 등의 네트워크 영역관점에서 분류하면 다음과 같다.

백본망의 경우, 네트워크의 생존성 보장이 가장 핵심적인 보안 이슈로서, 이를 위하여 DDoS(Distrubuted Denial of Service) 등으로부터 트래픽 폭주 방지, 트래픽 조절 및 차단, 그리고 네트워크의 대역폭 및 보안성능 보장 등을 들 수 있다. 그리고 외부 침입에 대하여 네트워크 서비스의 연속성을 제공하기 위한 교정 보안이 중요한 보안 이슈로 등장하고 있다.

액세스망의 경우, 가입자의 서비스를 백본망에 안전하게 전달하여 서비스의 안정성을 확보하는 것이 가장 중요한 이슈로 들 수 있으며, 이를 위하여 해킹과 바이러스 등으로부터 네트워크 침해를 방지하고, 국지적으로 침해를 제한하기 위한 대응책이 요구된다.

서비스영역이 존재하는 가입자망의 경우, ISP와 협력하여 신속하고 동적인 대응 방안이 시급한 보안 이슈로 등장하였으며, 향후 사용자 서비스에 대한 신뢰성 보장이 핵심적인 보안 이슈로 대두 될 것으로 보인다. 이는 유무선 통합과 음성과 데이터의 통합으로 서비스 융합이 본격화 되는 시점에서 가장 핵심적인 요구 사항이 될 것이다[4].

(그림 1)은 네트워크 영역관점의 보안 이슈를 요약한 것이다.

이상과 같은 보안 이슈에 대한 해결책으로서, 최근의 보안 기술은 네트워크 기반의 고성능 보안장비[3], 통합보안 서비스, 그리고 글로벌 네트워크에서 외부의 침입을 능동적으로 탐지하고 대응할 수 있는 네트워크 생존성 기술[4-7]로 발전하고 있다. 나아가서 인터넷을 이용하는 사용자 서비스의 품질을 보장하면서 신뢰성을 강화하고 네트워크의 생존성을 만족시키며, 새로운 공격 유형에 대해서도 유연하게 대처할 수 있는 차세대 보안 기술의 등장이 예상된다[1-2].

본 논문에서는 이와 관련하여, 2장에서 관련 연구동향을 살펴보고, 3장에서 본 논문에서 제안하는 신뢰성 있는 인터넷 서비스를 제공하기 위한 차세대 보안기술로서 교정 보안 프레임워크를 소개한다. 마지막으로 결론을 맺는다.

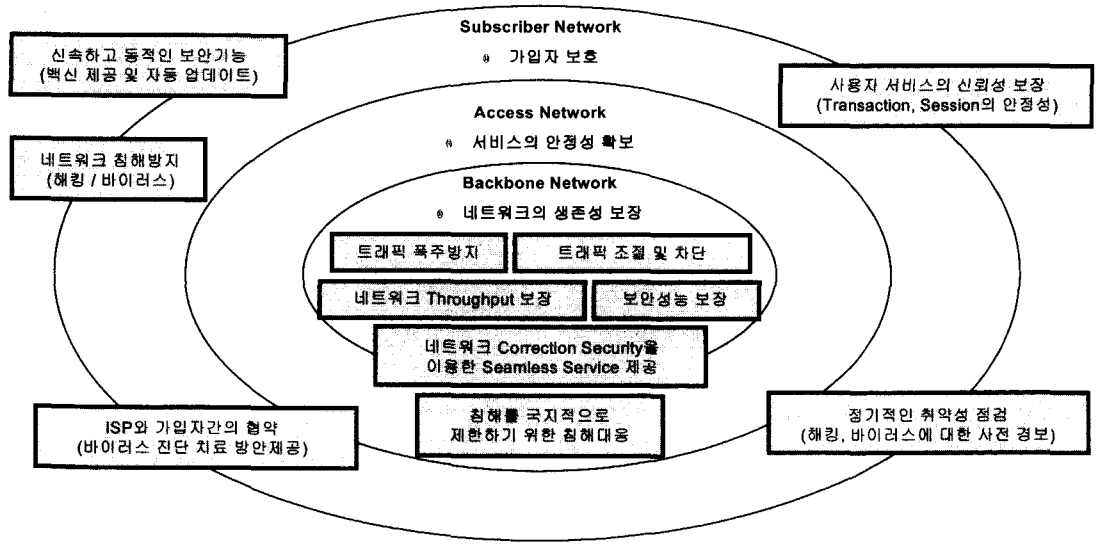
2. 연구 동향

신뢰성 있는 인터넷 서비스를 제공하기 위하여 진행되고 있는 대표적인 연구로 DARPA 의 FTN(fault tolerant network) 프로그램[5]을 들 수 있다. FTN 프로그램은 1999년부터 시작된 프로젝트로서, 성공적인 공격의 후에도 지속적인 네트워크의 동작을 지원하기 위한 기술을 개발하는 것을 목표로 하여, ISP 등에서 제공하는 네트워크 기반 서비스의 생존성과 안정성을 보장하기 위해 글로벌 환경에서 DDoS 공격을 방어 및 대응하기 위한 연구를 진행한다. 해당 프로그램에서는 공격자 침입경로 고립기술, 보안 네트워크, 네트워크 인프라에서의 공격방어 및 생존성 기술, 능동 네트워크 기반 침입대응기술 등에 대한 과제를 진행중이다.

시스템의 생존성에 관한 연구로는 우선 DARPA에서 추진중인 ITS(intrusion tolerance systems) 프로그램[6]을 들수 있다. 이 프로그램의 목적은 침입에 대한 저항성(resilience)과 허용성(tolerance)을 가지는 시스템의 개념, 설계, 개발, 검증 구조와 방법론에 대한 기술을 개발하기 위함이다. 연구 개발 범위는 악의적인 침입에 대한 데이터와 프로그램의 무결성 유지와 서비스 거부 공격에 대한 대응 및 시스템의 가용성 보장에 초점을 두고 있다.

DARPA의 OASIS 프로그램[7]은 국가정보 방어에 생존성 있는 시스템을 유기적으로 활용할 수 있는 기술과 구조의 개념정립, 설계, 개발, 구현 및 검증을 목적으로 한다. 이를 위한 기술적 이슈는 생존성 있는 시스템을 구축하기 위하여 다중 허용 계층형태로 3세대 보안 기술을 제공하는 것이다. 3세대 보안 기술은 1세대의 신뢰할 수 있는 컴퓨팅 환경(Trusted Computing Bases), 암호화(Encryption), 인증(Authentication) 기술과 접근제어(Access Control) 기술 및 2세대의 경계 제어기(Boundary Controllers), 침입탐지시스템(Intrusion Detection Systems), 공개 키 하부구조(Public Key Infrastructure) 기술과 바이오메트릭스(Biometrics) 보안기술을 보완한 것을 의미한다.

EC(European Commission)에서는 IST(Information Society Technologies)의 MAFTIA(Malicious and Accidental Fault Tolerance for Internet Applications) 프로그램[8]을 통하여, 시스템의 우연히 발생한 고장이나 악의적인 공격을 포함한 부주의한 행동으로부터 분산된 인터넷 자원의 의존성(dependability)을 연구하고 있다.



(그림 1) 네트워크 영역관점의 보안 이슈

여기서 말하는 의존성은 시스템이 제공하는 서비스에 정당하게 부여되는 신뢰성, 즉 시스템의 믿을 수 있는 정도를 말한다. 의존성을 구성하는 일반적인 속성은 시스템의 사용 가능 정도에 대한 척도를 나타내는 가용도(availability), 서비스가 지속적으로 유지될 수 있는가에 대한 척도를 나타내는 신뢰도(reliability), 치명적인 재해가 발생하지 않는가에 대한 척도를 나타내는 안전성(safety), 그리고 사생활을 위협하거나 가치 있는 자산의 손실을 초래하는 사건을 피할 수 있는가에 대한 척도인 보안성(security) 등이다. 의존성 있는 시스템을 개발하기 위하여 결함(faults)을 공격(attack), 취약성(vulnerability), 침입(intrusion)으로 정의하고, 이에 대처하기 위한 방안으로 방지(prevention), 허용(tolerance), 제거(removal), 예측(forecasting)으로 구분하여 연구 개발을 추진하고 있다.

3. 교정 보안 프레임워크

현재의 인터넷은 DDoS 등의 공격으로 인하여 네트워크의 트래픽 폭주가 발생할 때, 신속하고 정확한 대응을 하기 위한 제어가 불가능한 태생적인 한계를 지니고 있으며, 현재의 보안 기술은 시스템과 네트워크 수준에서 대응하는데 그쳐, 안전하고 신뢰성 있는 인터넷 서비스를 제공하기 어렵다. 따라서, 인터넷 마비 사태에 대비한 신속한 복구와 개선이 가능한 네트워크 차원의 제어기술의 필요성이 증가하고 있다.

교정 보안 기술이란 외부의 공격이나 침입, 취약성에도 불구하고 사용자 서비스에 대한 신뢰성 보장을 위한 네트워크 보안기술로 정의할 수 있다.

3.1 교정 보안의 개념

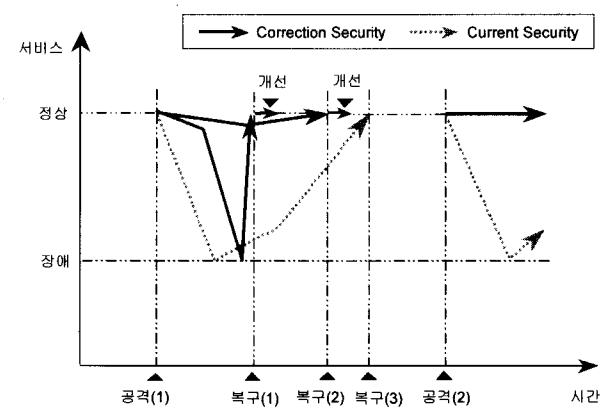
교정 보안 기술은 복구(recovery)와 개선(improvement) 기술을 이용한 네트워크 생존성과 장애 방지를 위한 네트워크 보안기술로 정의할 수 있다.

(그림 2)는 네트워크 차원의 복구기술과 개선기술을 이용한 교정 보안 기술의 개념을 나타낸 것으로서 현재 보안과의 차이를 보여준다.

현재 보안기술로는 외부의 공격이나 침입, 취약성 등의 장애 요인으로부터 급격한 네트워크 마비 사태가 초래되어 서비스 장애를 유발시키며, 정상 서비스로 복구되는 데 비교적 긴 시간이 소요된다. 그리고 현재 보안기술은 네트워크 마비를 초래한 장애 요인이 지속되거나 재발할 경우에도, 이에 대한 적절한 대응 방안이 없이 안정적인 서비스를 제공하지 못하는 한계점이 있다.

반면, 교정 보안 기술은 외부의 공격이나 침입, 취약성 등의 상황에 대하여 지속적인 개선작업으로 장애를 사전에 방지하고, 네트워크의 안전성이 위협 받는 상황에서도 정상적인 서비스를 제공할 수 있게 하며, 서비스 장애를 초래했다고 하더라도 이에 대한 빠른 서비스의 복원을 가능하게 하고, 기능 개선을 통하여 재발 방지를 포함하는 개념이다.

복구기술은 시스템 복구를 포함한 네트워크 차원의 복원 기술로서, 외부의 공격이나 침입, 취약성 등으로 인한 네트워크의 비가용성을 최소화 하기 위하여, 네트워크 차원에서 여분의 자원을 활용하여 최대한의 네트워크 서비스를 보장할 수 있도록 하는 네트워크 생존성 기술((그림 2)의 복구(2))과, 생존성 기술로는 대처가 불가능하여 네트워크 시스템의 장애가 발생한 경우, 빠른 서비스 복원을 가능하게 하는 네트워크 제어기술((그림 2)의 복구(1))이다.



(그림 2) 교정 보안 기술의 개념

개선기술은 복구기술의 한계를 보완하는 기술로서 네트워크 가용성의 저하를 초래하는 외부의 공격이나 침입, 취약성 등으로부터 장애발생을 사전에 방지하고, 장애요인이 지속되거나 재발할 경우에도 이를 방지할 수 있도록 한다. 구체적으로 타 시스템(취약성분석시스템, 망관리시스템, 통합보안관리시스템 등)으로부터 네트워크의 가용성을 저하시킨 원인을 전달받아 시스템의 기능을 동적으로 변경하여 개선하거나, 시스템 내부에 장애평가 및 처리기능을 가지고 동일한 침입에 대한 자체 방어기능을 보유하고 있다.

(그림 2)의 교정 보안과 기존 보안을 손실함수(Loss Function)로 표현하면 아래와 같다.

정상서비스 = 1, 공격(1) = $a(1)$, 공격(2) = $a(2)$, 복구(1) = $r(1)$, 복구(2) = $r(2)$, 복구(3) = $r(3)$, 시간 = t, 교정 보안 복구(1)의 보안함수 = $Y_1(t)$, 복구(2)의 보안함수 = $Y_2(t)$, current security의 보안함수 = $X(t)$라고 하고 $t < T$, $r(2) < T$, $N = r(n+2) < T$을 만족하는 최대정수 n이라 하면,

교정 보안의 손실함수는 다음과 같다.

$$L_y(t) = Min[\int_{a(1)}^{r(1)} (1 - Y_1(t)dt),\ \int_{a(1)}^{r(2)} (1 - Y_2(t)dt)]$$

Current security의 손실함수는 다음과 같다.

$$L_x(t) = \sum_{n=1}^{n} \int_{a(n)}^{r(n+2)} (1 - X(t))dt,\ \int_{a(N)}^{T} (1 - X(t))dt$$

이때, 교정 보안을 선택함으로써 얻게 되는 이득함수는,

$$G(t) = L_x(t) - L_y(t)$$

이며, 단위 시간당 손실비용을 라 하면 시간 동안에 발생하는 총 이득은 다음과 같다.

$$G(t) \times C = \left\{ \sum_{n=1}^{N} \int_{a(n)}^{r(n+2)} (1 - X(t))dt + \int_{a(N)}^{T} (1 - X(t))dt - Min[\int_{a(1)}^{r(1)} (1 - Y_1(t)dt),\ \int_{a(1)}^{r(2)} (1 - Y_2(t)dt)] \times C \right\}$$

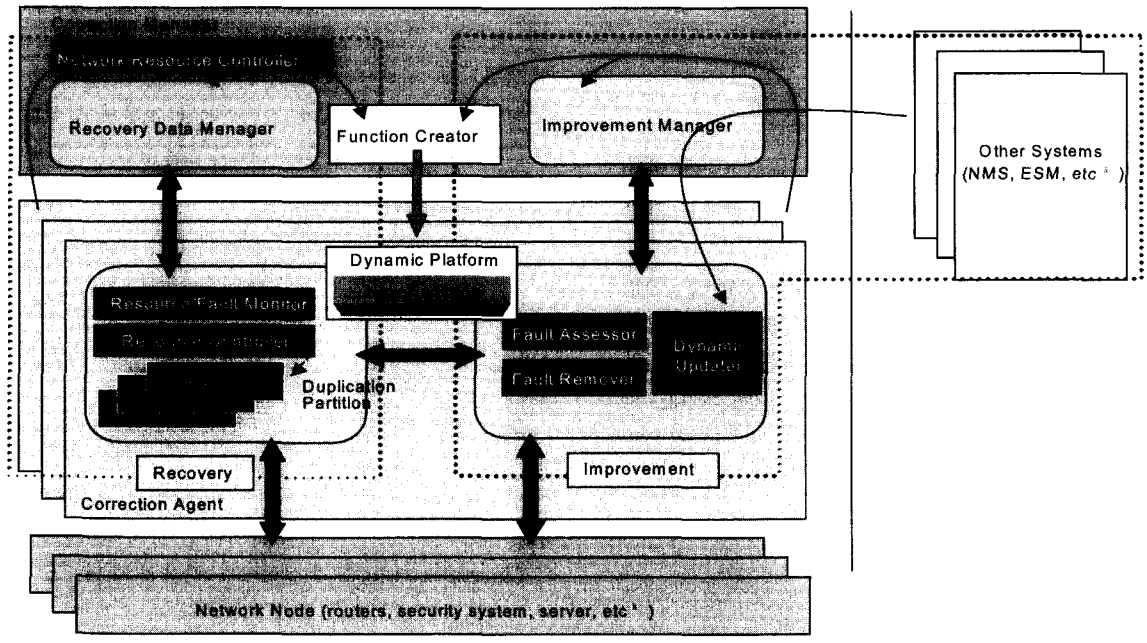
3.2 교정 보안 프레임워크

교정 보안 프레임워크는 (그림 3)과 같이 크게 교정 매니저와 교정 에이전트로 구성되며, 기능관점으로 복구(recovery)와 개선(improvement)영역으로 구분된다. 교정 매니저는 여러 개의 교정 에이전트들을 관리하며 전체적인 교정 제어를 담당한다. 교정 에이전트는 네트워크 노드(네트워크 장비, 네트워크 보안장비, 서버 등)내의 주요 기능의 복구와 개선을 위한 영역으로 구분된다. 교정 에이전트는 적용되는 네트워크 시스템 내에 존재할 수도 있고, 별도의 전용 시스템으로 구현될 수도 있다.

복구 영역은, 자원/장애 감시기(resource/fault monitor)로부터 장애감시와 자원의 상태를 파악하여 문제가 발생하면 우선, 개선영역의 장애 평가기(fault assessor)에서 장애수준을 평가하고 장애 제거기(fault remover)는 장애를 제거한다. 이러한 장애 제거 조치가 이루어지지 않으면, 복구영역의 자원 제어기(resource controller)는 여분의 자원을 재할당하고 분할하는 등의 과정을 통하여 시스템 내부의 주요 컴포넌트의 가용성을 보장하여, 교정 에이전트의 복구를 담당하는 핵심 기능을 제공한다.

이와 같은 조치로써 시스템의 성능회복이 어려우면, 교정 매니저의 네트워크 자원 제어기(network resource controller)에 의뢰하여 다른 교정 에이전트의 자원 상태를 파악하여 종합적인 대응방안을 모색한다. 그러나 이와 같은 방법에도 불구하고 가용성 확보가 불가능하여 장애가 발생하면, 해당 시스템에 대한 프로파일과 재설정 정보 등을 관리하는 복구 데이터 매니저(recovery data manager)로부터 장애가 발생한 일부 기능이나 시스템 전체에 대한 복구 메커니즘(reconfiguration, reconstitution 등)을 통하여 신속한 기능복원을 수행한다. 그리고 기능 생성기(function creator)에서는 복구에 요구되는 새로운 기능을 생성하고, 교정 에이전트로 전달하여 동적으로 실행될 수 있도록 한다.

개선 영역은, 타 시스템(취약성분석시스템, 망관리시스템, 통합보안관리시스템 등)과 연동하여 지속적으로 개선정보를 전달 받아 개선 매니저(improvement manager)에서 데이터 마이닝(data mining)과 상관관계 분석(correlation analysis) 등을 통하여 개선여부를 결정한 후, 개선 사항이라고 판단되면 해당 교정 에이전트로 전달하여 동적 업데이터(dynamic updater) 부분에서 동적으로 개선기능을 적용한다. 이러한 기능은 장애발생이전에 장애요인을 제거하여 장애유발을 방지하는 목적으로 수행된다. 그리고 개선영역에서는 복구영역에서 성능회복을 통하여 시스템의 가용성을 확보한 후, 동일한 장애의 발생을 방지하기 위하여, 매니저에 의해서 종합적으로 장애원인을 분석하여 해당 네트워크 노드의 기능개선을 수행한다. 그리고 개선에 필요한 새로운 기능이 요구되면, 교정 매니저의 기능 생성기에서는 해당 기능을 생성하고, 교정 에이전트로 전달하여 동적으로 실행될 수



(그림 3) 교정 보안 프레임워크

있도록 한다.

(그림 4)는 교정 보안의 동작흐름을 나타낸다.

3.2.1 장애사전방지 단계

장애사전방기 기능은 교정 매니저가 타 시스템과 연동하여 외부의 공격이나 침입, 취약성 등의 장애 요인에 대하여 지속적으로 시스템의 성능개선 정보를 수집하여 종합 분석한 후, 개선사항이 존재하면, 해당 시스템의 교정 에이전트로 통보하여 동적인 기능개선을 수행한다. 이 단계는 (그림 3)의 개선영역에서 수행된다.

3.2.2 장애허용 단계

장애요인을 사전에 제거하지 못하여 시스템 성능의 장애를 유발하기 시작했을 때, 장애를 감지하거나 시스템내의 자원의 상태를 모니터링하여 성능이 저하되고 있다고 판단되면, 장애의 수준을 평가하여 장애를 제거한다. 이러한 조치에도 불구하고 장애를 제거하지 못하면 우선, 시스템 내부의 자원을 재할당하여 시스템 성능을 정상적으로 유지시키고, 이러한 조치로써 성능회복이 불가능하면, 교정 매니저에 의한 네트워크기반의 자원 재할당을 수행하여 정상적인 서비스를 제공할 수 있도록 조치한다. 장애수준평가와 장애제거는 (그림 3)의 개선영역에서 수행되며, 그 이외의 기능은 복구영역에서 수행된다.

3.2.3 기능복원 단계

그러나 장애허용 단계에서 자원할당 방법에도 불구하고 시스템 기능이 제대로 동작하지 않으면, 교정 매니저는 교정에이전트에게 복구 메커니즘에 의해서 기능복원기능을 수행하도록 명령한다. 이 단계는 (그림 3)의 복구영역에서 수행된다.

3.2.4 장애재발방지 단계

장애재발방지 단계에서는 장애허용단계에서 장애를 제거하거나, 자원재할당에 의한 시스템 성능이 회복된 후, 동일한 장애발생 요인에 대하여 재발방지를 목적으로, 교정 매니저에 의해서 종합적으로 장애요인을 분석하여 기능개선을 수행한다. 이 단계는 (그림 3)의 개선영역에서 수행된다.

지금부터 교정 보안 프레임워크의 핵심 개념인 복구와 개선기술에 대하여 컴포넌트별 주요기술을 상세히 기술하고자 한다.

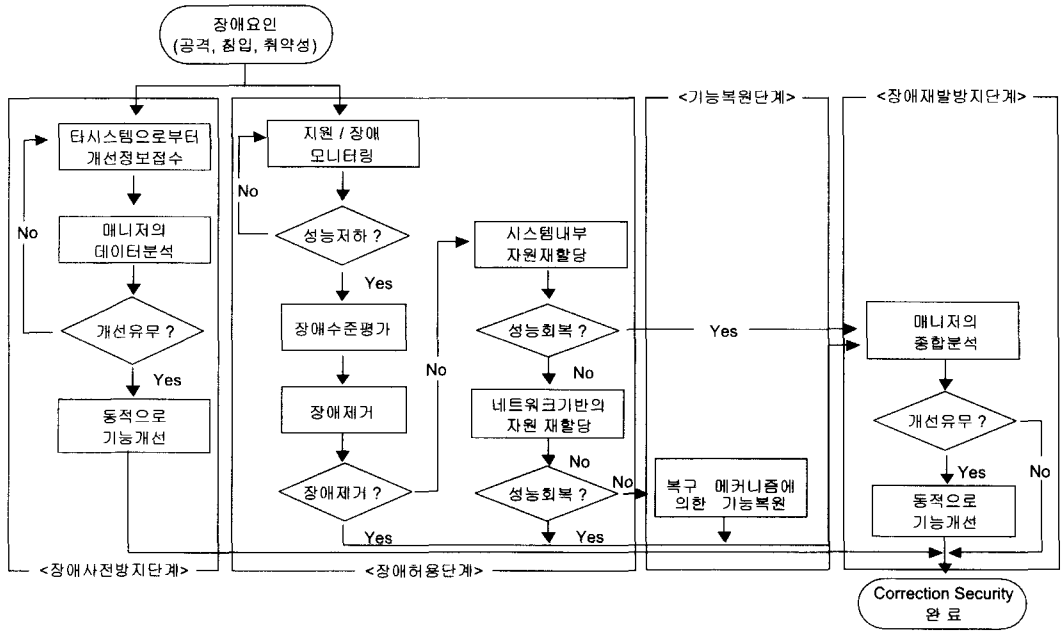
복구기술은 외부의 공격이나 침입, 취약성 등과 같은 서비스의 장애요인에도 불구하고 안정적인 서비스를 제공하기 위한 네트워크 차원의 생존성 및 제어기술로서, 자원 관리기술, 시스템 적응기술, 프로파일 저장 및 복제기술, 컴포넌트 랩핑기술, 동적 기능 적용기술 등이 있다.

● 자원 관리기술

외부의 공격이나 침입, 취약성 등으로부터 주요 자원 상태를 관리하며, 시스템의 성능 저하가 발생할 경우에 동일한 기능을 제공할 수 있도록 컴포넌트에서 네트워크에 이르는 자원 재할당, 자원 복제와 자원 동적 협동 등이 포함된다. 이 기술은 사용자의 무분별한 네트워크 자원 사용을 제한하여 보다 안정적으로 네트워크 서비스를 운용할 수 있는 방안도 포함한다.

● 시스템 적응기술

시스템 자체의 동적 적응 기술로서, 제한된 자원을 활용하여 최대한의 성능을 수행할 수 있도록 시스템내부에서 대응방안을 자체적으로 결정하고 수행한다.



(그림 4) 교정 보안 동작 흐름도

● 프로파일 저장 및 복제기술

시스템 장애로부터 시스템의 중요 프로파일 및 재설정 정보를 저장하고, 시스템의 최적의 설정상태를 복제하여 신속하게 시스템이 복구될 수 있는 메커니즘을 제공한다.

● 컴포넌트 랩핑기술

시스템 내 주요 기능을 수행하는 소프트웨어 컴포넌트 보호를 위한 기술로서 외부의 명령을 수행하기 전에 중간 계층에서 명령의 정당성 여부를 확인한다.

● 동적 기능 적용기술

교정 에이전트에서 새로운 복구기능을 전달 받아 동적으로 실행이 가능하도록 Open API, 동적 보안플랫폼 등의 환경을 제공한다.

개선기술은 복구기술의 한계를 보완하여 네트워크의 가용성을 저하시키는 외부의 공격이나 침입, 취약성 등의 장애발생 요인을 사전에 제거하거나 장애의 재발을 방지하는 기술로서, 시스템 연동기술, 데이터 마이닝기술, 장애 평가기술, 동적 기능 적용기술 등이 있다.

● 시스템 연동기술

네트워크에서 지원되는 자원과 기능의 성능에 대하여 취약성에 대한 정보를 수집하기 위한 타 시스템과의 연동기술이다. 네트워크 상태를 일정수준 이상으로 유지함으로써, 오동작 및 성능 저하를 초래할 수 있는 네트워크 공격을 사전에 차단하기 위한 핵심 기술이다.

● 데이터 마이닝기술

타 시스템으로부터 네트워크의 개선 정보를 전달받아, 해당 시스템에 적용하기 위하여 데이터를 종합적으로 분석하고 이들간의 상관관계를 판별하는 기능을 제공한다.

● 장애평가 및 제거기술

시스템내부의 자원상태나 장애감시로부터 시스템의 성능 저하로 판단되면, 시스템 차원의 대응을 위하여 현재 진행중인 장애 수준을 정확하게 평가하는 기술이다. 그리고 장애요인을 제거하기 위한 자체 장애 처리기술을 포함한다.

● 동적 기능 적용기술

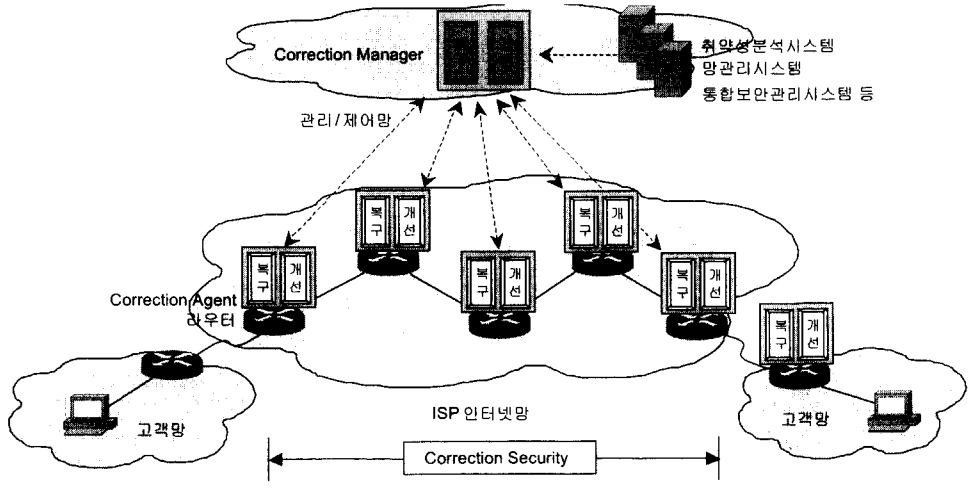
시스템의 기능과 성능을 지속적으로 개선하고 실시간으로 실행이 가능한 Open API, 동적 보안플랫폼 등의 환경을 제공한다.

3.3 적용 시나리오

(그림 5)는 ISP 인터넷망에 본 논문에서 제안하고 있는 교정 보안 프레임워크를 적용한 예이다. 교정 매니저는 관리/제어망에 위치하고 ISP망의 취약성분석, 망관리 및 통합보안관리 등을 담당하는 타 시스템과 연동되어 있으며, 교정 에이전트는 라우터내에 구현되거나 전용 에이전트 형태로 존재한다.

이러한 상황에서, 네트워크의 안전성을 위협하여 ISP망을 마비시킬 수 있는 DDoS 공격이 발생한다고 가정할 때, (그림 4)의 동작흐름을 참조하여 교정 보안의 대응과정을 살펴보기로 한다. 우선, 사전장애방지기능으로서, 취약성분석시스템, 망관리시스템, 통합보안관리시스템 등으로부터 DDoS 공격의 징후를 전달받고 교정 에이전트에서 DDoS 패킷을 폐기할 수 있는 기능을 동적으로 동작시켜서 장애발생을 방지한다.

그러나, 장애요인이 사전방지 단계를 통과하여 라우터가 장애요인에 노출되었을 때, 라우터의 프로세싱에 필요한 주요 자원인 메모리의 사용량을 증가시켜 라우터의 프로세싱 성능이 저하되면, 장애수준을 평가하여 장애요인이 되는 DDoS 패킷을 폐기하는 등의 장애제거기능을 통하여 장애허용단계를 수행하게 된다. 그러나 이와 같은 장애제거 조치에도 불구하고 라우터의 성능이 정상적으로 동작하지 않으면, 프로세싱을 수행하기 위해서 필요한 메모리량을 라우



(그림 5) 교정 보안 기술이 적용된 ISP 인터넷망의 보안구조

터내에서 재할당하고, 나아가서는 네트워크 차원에서 일부 패킷에 대해서는 이웃한 라우터로 경로를 변경하여 라우터 프로세싱 부하를 조절한다.

이와 같은 장애허용 조치에도 불구하고 라우터의 장애가 발생하여 정상적으로 기능이 동작하지 않으면, 교정 매니저에 저장되어 있는 라우터의 최적의 설정정보를 이용하여 신속하게 라우터의 기능을 정상화하는 기능복원 단계를 수행한다.

그리고 교정 매니저는 장애상황을 종합적으로 분석하여, 새로운 기능을 생성하거나 교정 에이전트에서 동적인 기능 개선을 통하여 장애의 재발생을 방지한다.

3.4 분 석

본 논문에서 제안한 교정 보안 프레임워크를 기존 연구 프로젝트와 비교하여 그 특징을 살펴보기로 한다.

첫째, 적용범위 관점에서 살펴보면 교정 보안은 단독 시스템 뿐만 아니라 대규모 네트워크를 구성하는 노드 시스템에 적용될 수 있는 반면, ITS, OASIS 등의 경우에는 단독 시스템에 국한되어 적용되며, MAFTIA의 경우 인터넷상에서 트랜잭션 서비스의 안전성을 보장하기 위하여 미들웨어 기반 아키텍처에 대한 연구가 진행되며 적용대상은 주로 네트워크 서버 노드와 같은 단독 시스템이다. FTN 프로젝트는 글로벌 네트워크에 적용되나 인터넷 프로토콜의 변경이나 능동 네트워크 기술과 같은 현재 적용 가능성이 적은 기술을 기반으로 하여 라우터를 비롯한 네트워크 장비에 직접 적용되기 때문에 현실성이 부족하다고 볼 수 있다.

둘째, 교정 보안은 개선기술을 적용하여 지속적으로 취약성 제거와 시스템 성능을 개선하여 장애에 대한 사전 방지 기능을 제공한다. FTN의 경우 침입탐지, 취약성분석 등과 같은 연구가 부분적으로 진행되고 있으나, 교정 보안과 같이 네트워크 장애의 사전 방지를 위한 네트워크 시스템 프레임워크에 대한 연구는 아니다.

셋째, 허용(tolerance)기능은 교정 보안을 비롯하여 기존 연구에서 모두 지원하고 있다. 즉, 외부의 침입 후에도 지속적인 시스템이나 네트워크의 동작을 보장한다. 그러나, 구현 관점에서 MAFTIA가 시스템의 침입허용에 관한 연구이며, 교정 보안의 복구기술은 이를 포함하여 네트워크 차원의 침입허용이라는 점이 특징이다. FTN의 경우 네트워크 기반의 서비스의 지속성을 보장하기 위한 프로토콜등에 관한 연구이며, ITS와 OASIS의 경우 침입에 대한 데이터의 무결성 보장과 시스템의 가용성 보장 측면에서 연구가 진행되고 있다.

넷째, 외부의 공격이나 침입, 취약성 등으로 인하여 발생한 장애로부터 시스템이나 네트워크의 기능을 복원할 수 있는 기능이다. 기존 연구 중에는 OASIS와 MAFTIA의 복원 기능은 시스템 차원의 에러 복구와 에러처리 방안으로 교정 보안과 유사하나, 시스템 재설정등과 같이 다소 소극적인 형태이며 교정 보안이 글로벌 네트워크에 적용될 수 있는 것과 비교하여 단독 시스템에 국한되어 있다. 그리고 FTN의 경우에는 기능 복원이 아니라 네트워크 장비의 장애 발생시 대체 경로 확보 방안에 관한 것이다.

다섯째, 장애를 유발시킬 수 있는 요인이 지속되거나 반복되었을 경우 이를 방지 할 수 있는 방안으로서, 교정 보안의 경우 개선(improvement)기술이 있으며, MAFTIA의 경우 소프트웨어 업그레이드나 보안 패치 적용 등의 장애 처리(treatment)기술이 있다. 교정 보안과 비교하여 MAFTIA는 재발방지 적용관점에서 신속성 떨어지고 체계적인 분석과 적용방안에 대한 연구가 이루어지지 않고 있다. FTN의 경우 침입대응 측면에서, 능동 네트워크 기반의 역추적 및 공격자 고립기술 등에 대하여 연구되고 있다.

여섯째, 네트워크의 안전성을 보장하기 위한 연구가 많이 진행되고 있으나, 대부분 시스템 관점에서 적용되어 왔다. 그러나 시스템의 신뢰성 향상이 네트워크의 안전성을 보장할 수 있을 지에 대해서는 의문점이 제기되고 있다. 즉, 실제 인터넷 서비스를 제공하는 공중망, ISP망 등에 적용하기에도 어려움이 있을 뿐만 아니라 그 결과에 대해서도 보장할 수 없다. FTN의 경우 네트워크 안전성과 관련된 연구가 있으나, 프로토콜이나 특정 서버 노드와 같이 네트워크를 구성하는 요소 기술에 대한 연구가 산발적으로 진행되고 있다.

<표 1>은 이를 요약하였다.

〈표 1〉 기존 연구와 교정 보안의비교

(○ : 제공함, △ : 보통, × : 제공않음)

구 분	FTN (DARPA)	ITS (DARPA)	OASIS (DARPA)	MAFTIA (EC)	Correction (ETRI)
적용범위	네트워크	단 독 시스템	단 독 시스템	단 독 시스템	단 독 시스템 + 네트워크
사전방지기능	△	×	×	×	○
허용기능	○	○	○	○	○
복원기능	△	×	○	△	○
재발방지기능	△	×	×	△	○
네트워크 안 전 성	△	×	×	×	○

종합적으로 분석하면, 교정 보안은 신뢰성 있는 서비스를 제공하기 위하여 네트워크의 안전성 확보를 목적으로, 네트워크를 구성하는 노드 시스템에 적용될 수 있는 프레임워크로써, 네트워크의 안전성을 위협하는 장애요인에 대한 사전 방지, 허용, 복원 및 재발 방지에 이르는 일련의 보안 방안을 제공한다. 반면, FTN의 경우 네트워크의 안전성 확보를 위하여 다양한 프로젝트에서 연구되고 있으나 특정 기능에 초점을 맞춰 개별 프로젝트 행태로 연구되며 기술의 현실성이 부족하다. ITS와 OASIS의 경우 주요 서비스를 제공하는 웹 서버와 같은 단독 시스템의 침입 허용에 대한 연구로 진행되고 있다. MAFTIA의 경우에도 인터넷 상에서 트랜잭션

서비스의 안전성을 목적으로 서버 노드의 미들웨어 기반의 분산 시스템 구조에 대하여 연구가 진행되고 있다.

4. 결 론

본 논문에서는 신뢰성 있는 인터넷 서비스를 제공하기 위한 차세대 보안기술로서 교정 보안 프레임워크를 제안하였다.

교정 보안의 핵심 개념으로서, 복구 기술은 네트워크의 생존성 기술과 이것으로 대처가 불가능 할 경우에는 신속하게 서비스 복원을 가능하게 하는 네트워크 제어기술을 포함하며, 개선 기술은 장애요인이 지속되거나 반복될 경우에도 이를 방지하기 위한 시스템 자체 개선기능과 타 시스템과 연동하여 동적으로 기능을 개선시킬 수 있는 방안을 포함한다.

본 논문에서 제안한 프레임워크는 타 시스템과 지속적인 연동을 통하여 단독 시스템은 물론 대규모 네트워크에 적용되어 장애에 대한 사전방지기능, 허용기능, 복원기능, 재발방지기능을 지원한다. 기존의 연구가 시스템 관점의 허용기술, 의존성 기술 혹은 네트워크 장비를 이용한 생존성 기술인 것과 비교하여, 교정 보안 프레임워크는 단독 시스템을 포함한 네트워크 차원의 허용기술, 의존성 기술, 생존성 기술이라는 특징이 있다. 이는 현재의 인터넷 뿐만 아니라 차세대 통합네트워크에서 신규 서비스의 도입과 보안성 강화 측면에서도 큰 역할을 할 수 있을 것으로 기대된다.

향후 본 연구를 통하여 제안된 프레임워크는 실제 적용성과 경제성 그리고 실효성을 높이기 위하여 시스템 구현 및 테스트 베드 구축 등을 이용한 보다 구체적인 연구를 계획하고 있다.

참 고 문 헌

[1] 남택용, 김숙연, 이승민, 지정훈, 손승원, "신뢰성 있는 차세대 네트워크 보안 시스템", 정보처리학회지, 제13권 제1호, 2003.

[2] Sook-Yeon Kim, Junghoon Jee, Taekyong Nam, Sungwon Sohn, and Cheehang Park "Framework of network security service for next generation," The International Workshop on Information Security Applications (WISA 2002), Jeju island, Korea, pp.123 -130, Aug., 2002.

[3] J. Pescatrore, M. Easley, R. Stiennon, "Network security platform will transform security markets," Gartner, Nov., 2002.

[4] "State of the NGN : Carrires and vendors must take security seriously," Gartner, March, 2003.

[5] DARPA FTN, http://www.iaands.org/iaands2002/ftn/index.html.

[6] DARPA ITS, http://www.tolerantsystems.org/its_projects/index.htm.

[7] DARPA OASIS, http://www.tolerantsystems.org/Project Summaries/Project_Summaries.html.

[8] IST MAFTIA, http://www.newcastle.research.ec.org/maftia/index.html#partners.

이 승 민

e-mail : todtom@etri.re.kr

1995년 고려대학교 산업공학과 공학사

1997년 한국과학기술원 산업공학과 공학석사

1997년~2001년 데이콤 종합연구소 연구원

2001년~현재 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀 연구원

관심분야 : 네트워크 보안, 인터넷, NGN

남 택 용

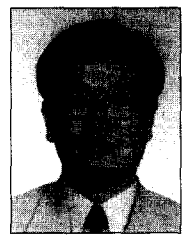
e-mail : tynam@etri.re.kr

1987년 충남대학교 계산통계학과 이학사

1990년 충남대학교 계산통계학과 이학석사

1987년~현재 한국전자통신연구원 정보보호연구본부 네트워크보안구조연구팀 팀장

관심분야 : 정보보호, 능동보안, 인터넷, 차세대네트워크구조



손 승 원

e-mail : swsohn@etri.re.kr

1984년 경북대학교 전자공학과 공학사

1994년 연세대학교 산업대학원 전자공학과 공학석사

1999년 충북대학교 컴퓨터공학과 공학박사

1983년~1986년 삼성전자 연구원

1986년~1991년 LG 전자(주) 중앙연구소 HI8mm 캠코더 팀장

1991년~현재 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 부장

관심분야 : 네트워크보안, 차세대 인터넷, Active Internet

한 치 문

e-mail : cmhan@hufs.ac.kr

1977년 경북대학교 전자공학과 공학사

1983년 연세대학교 전자공학과 공학석사

1990년 일본 동경대학교 전자정보공학과 공학박사

1977년~1983년 한국과학기술연구원(KIST) 연구원

1983년~1997년 한국전자통신연구원(ETRI) 계통연구부장(책임연구원)

1999년~2001년 한국외국어대학교 전자계산소 소장

1997년~현재 한국외국어대학교 전자정보공학부 교수

2002년~현재 한국외국어대학교 정보산업공과대학 학장

관심분야 : 차세대스위칭기술, 개방형네트워크기술, VoIP 기술, 네트워크보안기술