대한산업공학회/한국경영과학회 2002 춘계공동학술대회
한국과학기술원(KAIST) 2002년 5월 3일~4일

지리정보시스템 서비스 보안을 위한 프레임워크
A Framework for a Secure Geometric Information System

주운기.임기욱
선문대학교 벤쳐 및 산업공학

Abstract

This paper considers a security framework for geographic information System(GIS). The GIS is an information system for supporting fast decision associated spacial problems and the system has a role of infra structure of the information system. The security is also one of the major technology for information system. However, researches on secure GIS are presented little and this paper considers the secure GIS. This paper suggest a framework for the secure GIS based on derived requirements on the secure system. Analysis on security for a serial, parallel and hierarchical secure system is also added.

1. 서론

지리정보시스템(Geographic Information System : GIS)는 인간의 의사결정능력 지원에 필요한 지리 정보의 관측과 수집, 보존, 분석, 출력 등의 일련의 조작을 위한 소프트웨어와 장비를 총칭하는 정보시스템으로, 국가 경쟁력 강화와 행정 생산성의 제고 등에 기반이 되는 중요한 사회 간접자본 역할을 한다. 최근에는 정적인(static) 공간정보 위주인 GIS, 시간(time)관련 공간 정보 위주인 SIIS(Spatial Imagery Information System:공간영상정보시스템), 동적인(dynamic) 공간 정보를 주로 다루는 ITS(Intelligent Transport System : 지능형교통체계) 및 GNSS(Global Navigation Satellite System : 위성측위시스템)를 통합 관리하기 위한 4S(4 kinds of Spatial data) 연구도 시도되고 있다.[9]

GIS는 데이터베이스 구축 단계, 데이터베이스 관리 단계, 정보 분석 단계 및 정보 제공 단계를 통해서 서비스를 제공한다. 데이터베이스 구축 단계에서는 요구되는 각종 주제에 대한 도형 및 속성 자료를 수집하여 컴퓨터 데이터베이스에 저장하고, 데이터베이스 관리 단계에서는 저장된 데이터베이스를 지속적으로 분석 단계는 각종 수학적 분석, 통계적 처리, 공간적 분석을 통해 목적에 맞는 정보를 추출하는 단계로, GIS의 핵심 역할을 한다. 마지막으로, 정보 제공 단계에서는 목적에 맞게 추출한 정보를 사용자에게 다양한 포맷으로 컴퓨터를 이용한 다양한 매체를 통해서 제공하는 기능을 수행한다. GIS는 시설물 관리, 환경 개선, 토지 계획, 국방, 자원관리, 도시 계획 등의 각 활용분야 별 요구되는 GIS의 특성이나 구비 요건에 차이가 있다. 예를 들면, 시설물 관리(FM : Facility Management)의 경우, 상대적으로 높은 위치 정확도를 갖는 도형 정보 및 시설물 간 상호 간섭 등을 파악할 수 있는 삼차원적 그래픽 기능이 필요하고, 환경분야(EIS: Environment Information System)에서는 도형 정보의 정확도보다는 전반적인 환경 생태계의 분포를 파악하기 위한 항공사진과 인공위성 영상을 GIS 레이어와 혼합할 수 있는 방안이 필요하다. 그리고, 지적관리(LIS : Land Information System)에서는 지역별 전통적인 지적 관리 방식에 적합하고, 정밀 지적 측량 데이터의 입출력과 분석을 위한 기능 필요하고, 도시정보시스템(UIS : Urban Information System)을 위해서는 도시지역 주민의 복지 증진을 위한 기능이 필요하다. 이외에 국방정보시스템(DIS : Defense Information System) 및 전기 통신과 같은 주요 공공 시설물 관련 자료 관리 등에도 활용되고 있다.

본 논문은 다양한 GIS 서비스 보안을 위한 프레임워크(framework)에 대한 것으로, 날로 지능화 /복잡화되고 있는 보안 침해 기법에 대처할 수 있는 GIS 보안 시스템 프레임워크 수립을 위한 요구 사항을 도출하고, 적절한 보안성을 갖는 보안 시스템 구축을 위한 보안성 분석 방안을 제시한다. 정보 보호를 위한 프레임워크 및 표준화에 대한 연구는 진행되었으나([1,2,3,12]), GIS에 관한 연구는 현재 미미한 상태이다. 또한 보안성에 대한 연구로, 단순(직렬/병렬)구조의 정적인 분석 결과[6] 및 침입탐지율 계산 방안[6]은 제시되었지만, 본 논문에서와 같은 계층구조를 포함한 보안시스템에 대한 동적인 분석은 이루어지지 않은 상태이다.

2. GIS 정보 보호

정보보호(Information Security) 기술은 가용성(availability), 기밀성(confidentiality), 무결성(integrity)이 보장되지 않음으로 인해 받게 될 피해로부터 보호하는 것으로 정의할 수 있다. 여기서, 가용성(이용가능성)은 적시에, 인정된 방법으로 자료나 정보 접근하게 하는 것으로, 정보 접근의 지체 및 정보 자체의 파괴 등의 보안침해 공격이 있을 수 있다. 기밀성(은익성; 비밀성)은 인가된 사람 또는 기관이 인간된 시간이나 접근방법으로만 접근할 수 있게 하는 것으로, 정보의 불법적인 유출이나 공개를 통한 침해가 있을 수 있다. 그리고, 무결성(완전성;일관성)은 정확하고, 안전한 자료나 정보를 접근하게 하는 것이나, 자료의 변조를 하는 보안침해가 있을 수 있다. 이러한 정보 보호 기술은 국내외적으로 여러 가지 유형의 보안 시스템이 개발되고 있으나, 보안 기법에 대한 자세한 방안을 공개하지 않는 경우가 많고, 보안 기법의 적용 및 역할의 특성 상 자체 기술 확보가 필요하다. 정보 보호를 위해서는 보호를 위한 관리 데이터의 원활한 통신이 되어야 하므로 표준화도 중요한데, 우리 나라에서는 한국정보보호진흥원(KISA : Korea Information Security Agency)에서 전자서명 알고리즘 표준(KCDSA), 해쉬 알고리즘 표준(HAS-160), 128비트 블록암호알고리즘 표준(SEED) 등을 국내 표준으로 결정하여 발표하였다.[1] 여기서, KCDSA(Korean Certificate-based Digital Signature Algorithm)는 정보처리 시스템 및 정보통신망 환경에서 임의의 길이를 갖는 메시지 정보에 대해 부가형 전자서명을 생성 및 검증할 수 있게 해 주는 인증서 기반 부가형 전자서명 알고리즘으로, 1997년 6월에 발표되었다. HAS-160(Hash function Algorithm Standard)는 1998년 3월에 제정 발표된 것으로, 정보처리시스템 및 정보통신망 환경에서 임의의 길이의 비트 열을 고정된 길이(160비트)의 출력값인 해쉬코드로 압축시키는 해쉬 알고리즘이다. 그리고, 1999년 6월에 일반인에게 공지된 SEED(128-bit Symmetric block cipher)는 정보처리시스템 및 정보통신망 환경에서 임의의 키(비밀키)를 사용하여 블록단위로 데이터를 변환하는 암호알고리즘이다. 정보 보호 기술은 전자상거래, 전자정부, 차세대 인터넷 등 미래정보통신 산업의 안전성 보장을 위한 필수 기술이고, 이러한 사이버 공간에서의 개인 프라이버시 보장, 정보 범죄 차단. 신규 정보침해기술 출현에 대처하기 위해서는 지속적인 기술 개발이 필요한 분야이다. 이에 대한 중요성은 2001년 7월에 제정한 "정보통신기반 보호법 시행령"를 통해 주요 국가 정보통신기반시설을 지정하여 보호를 하는 정책을 추진하고 있다. 이 중 하나가 '국가지도통신망'이다. GIS는 도면정보 공유를 통해 인력 및 예산 절감 효과를 얻을 수 있고, 효율적인 시설물 관리 및 일반 국민에게 공간 정보를 제공하는 사회 인프라 성격을 갖고 있다.

GIS 정보보호에 대한 위협요소로는 GIS 시스템, 네트워크 및 응용 서비스에 대한 보안 침해가 있을 수 있다. 시스템 위협요소로는 OS 취약점, 서비스거부, 응용프로토콜 취약점, 바이러스, 신분위장, 불법침입 등의 있을 수 있고, 이를 통한 불법변조, 데이터 삭제 및 서버 정지 공격을 받을 수 있다. 네트워크는 전송중인 데이터에 대한 도청, 도청, 데이터 위변조, 트래픽 폭주 등을 통해 변조, 위장, 도청, 복제 등의 정보 보호 공격을 수행 할 수 있다. 이러한 위협 요소는 시간이 지남에 따라 새로운 침해 방법이 개발되므로, 다양한 침해 유형에 대해 유연성있게 대처할 수 있는 보안 프레임워크가 필요하다.

3. GIS를 위한 정보보호 framework

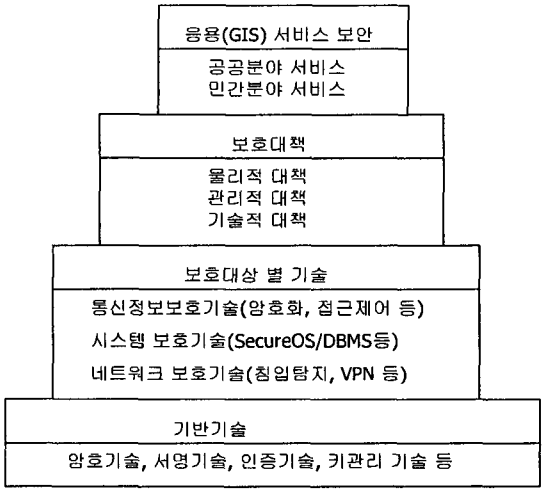
GIS 정보보호를 위해서는 정보보호 표준화 규약을 따라야하는데, 정보 보호 관련 표준화 기구로는 ISO/IEC JTC1/SC27(Joint Technical Committee 1/Sub Committee 27), ITU-T SG7(International Telecommunication Union : 국제전기통신연합)데이터통신망과 개방시스템 통신), IETF (Internet Engineering Task Force; 인터넷에 관련된 표준), 유럽의 ETSI(European Telecommunications Standards Institute)국제표준화 기구 등의 국제 표준화 기구가 있다. ISO/IEC JTC1는 ISO의 TC97(정보기술 표준화 담당)와 IEC의 TC83(정보처리 기기 표준화 활동 담당)를 통합하여 1987년 11월에 설립한 합동기술위원회로, 정보보호 관련 분과위원회 SC6에서는 물리계층, 데이터 계층에서의 암호적용 표준화 작업을 담당하고 있고, SC21에서는 OSI 보안 구조 및 개방형 시스템 보안 구조 표준화를 담당하고 있으며, SC27에서는 보안관련 서비스와 지침 및 일반적인 요구사항, 보안기술과 기법, 보안 평가 기준 등의 연구분석과 표준화 작업을 수행하고 있다. 우리나라는 SC27-Korea를 1992년에 기술표준원(구 국립기술품질원)산하에 구성하여 보안관련 서비스와 지침 및 일반적인 요구사항, 보안기술과 기법, 보안 평가 기준 등의 연구분석과 표준화 작업을 수행하고 있다. ITU는 유선 전신에 관한 국제협력을 위해 설립된 만국전신연합과 무선 분야 의 협력을 위해 설립된 국제무선전신연합이 1932년에 마드리드회의 에서 통합하여 탄생된 국제기구로, 그 중

IUT-T(Telecommunication, 전기통신표준화부문)는 CCITT(International Telegraph and Telephone Consultative Committee, 국제전신전화자문위원회)가 CCIR(International Radio Consultative Committee, 국제무선통신자문위원회)의 일부를 통합, 조정하여 1993년 세계전기통신표준화회의에서 개칭한 것으로, 14개의 연구그룹(SG : Study Group)과 하나의 TSAG(Telecommunication standardization Advisory Group)로 구성되어 있고, 이 중 SG7에서 개방시스템 통신에 관련된 정보보호 표준 개발을 위한 팩시밀리 표준화에 관한 암호기능 검토, ISDN 및 OSI 관련 표준화를 위한 보안 기능을 담당하고 있다.

국내 표준화 기구로, 한국정보통신기술협회(TTA)[2]는 국내·외 정보통신분야의 최신기술 및 표준에 관한 각종 정보를 수집/조사 연구 및 보급/활용하는 역할을 당당하고 있고, TC10 등 10개의 기술위원회와 30의 프로젝트 그룹으로 구성되어 있다. 이 중 TC(Technical Committee)10은 정보보호관리, 암호기술, 시스템 보안 등에 대한 표준화를 담당하고 있고, PG03(Project Group)은 국가지리정보시스템과 관련하여 2000년도 말까지 운용된 바 있다. 이외에 한국산업표준원(KISI)[3]에서는 산업표준 연구·개발, 표준화 국제협력 및 진흥, 북한표준 연구, 정보산업 표준화, 자본재 표준화, KSSN(한국표준정보망) 운영하고 있다.

GIS는 기반(infra) 특성이 강한 정보 시스템으로, 표준화의 필요성이 매우 크지만, 현재까지 국내외의 표준화 기관에서 GIS보안 관련 표준화 작업이나 권고안이 제시된 것은 없는 상태이다. 따라서, 본 논문에서는 일반적인 보안 시스템을 위한 권고안인 ISO 7498-2[12]을 기초로하는 GIS 보안 프레임워크를 요구 사항을 도출하고 보안 프레임워크를 <그림 1>과 같이 구성하였다.

GIS보안을 위해서는 먼저 정보 보호 기반 기술이 필요하고, 보안 대상 별 기술이 필요하며, 이들 보안 기술들을 종합 관리하는 보호대책이 필요하며, 이들 기반 하에서 GIS 정보보호가 이루어wu야 한다. 정보 보호 프레임워크를 위한 요구사항으로, ISO 7498-2의 Basic Reference Model 중 Part 2 : Security Architecture에서는 통신을 위한 각 계층에 보호서비스와 메커니즘 할당 시 고려 사항을 다음과 같이 규정하였다 : (1) 최소화된 방법으로 보호서비스가 구현되어야 한다. (2) 여러 계층에서 보호서비스가 제공되는 구조는 가능하지만, (3) 보호를 위한 추가기능은 OSI의 기존 기능과 중복되어서는 안된다. 그리고, (3) 계층의 독립성을 위반하면 안되고, (4) 보호해야 할 기능의 양은 최소화하고, (5) 한 실체가



<그림 1> GIS 보안 프레임워크

하위 계층의 실체에 의해 제공되는 정보보호 메커니즘에 종속적인 경우, 중간 계층들의 보호 정책에 위반되지 않아야 한다. 마지막으로, (6) 보호기능이 추가될 경우, 가능한 독립된 모듈로서 실현될 수 있도록 정의해야한다. 그러나, GIS 정보 보호를 위해 본 논문에서는 침입탐지시스템에 대한 분석[4,5,7,8]를 활용하여 다음과 같은 추가 요구사항을 도출하였다 : (7) 침입 탐지 자체는 시스템 운영자 및 보안 관리자의 별도 개입없이 동작해야한다. 즉, 대상 시스템에 대해 백 그라운드 상에서 동작해야한다. 그러나, 필요시 보안 담당자의 요청에 의해 내부적 작업에 대해 외부에서 이를 알 수 있어야 한다. (8) 시스템의 완전한 파괴를 피하기 위해 탐지시스템은 스스로 자신을 모니터링하여 방어시스템이 파괴되는 것을 방지할 수 있어야 한다. (9) 관리 기능과 GUI 기능에 문제가 발생하더라도 탐지기능을 포함한 주요 기능은 중단되지 않아야 한다. (10) 시스템에 걸리는 부하를 최소화해야 한다. 이를 위해서는 상황에 따라 수행하는 탐지 기능 모듈에 차별화를 한다. (11) 행위에 대해 정상적인 행위와의 차이를 관찰해야 한다. (12) 모든 시스템은 서로 다른 사용 패턴을 가지고 있으므로 방어 메커니즘도 이러한 패턴에 따라 적용될 수 있도록 침입탐지 시스템은 적용 시스템에 따라 쉽게 가공될 수 있어야 한다. (13) 새로운 응용 프로그램의 추가는 시스템 프로파일의 변화를 초래하므로 기존의 시스템 사용에 대한 허용 행위 여부 역시 변화해야 한다. (14) 침입에 의한 데이터 손실에 대응하기 위한 주기적인 데이터 백업 기능이 있어야 한다. (15) 침입에 대한 감시, 모니터링 외에 침입자의 신분을 확인할 수 있고, 침입자의 호스트에 직접 접근 가능해야 한다. 그리고, 좋은 탐지 시스템이 되기 위해서는 실제 침입이

아닌데 침입으로 판정하는 경우 및 실제 침입인데 탐지하지 못하는 경우가 작아야 하고, 기능 및 성능의 테스트가 용이하고, 공격을 탐지하여 탐지된 공격이 어떤 피해를 주는 지 결정하고 피해를 줄이며 공격으로부터 복구하는 것이다. 또한 오늘날의 네트워크에서 요구하는 크기에 변화할 수 있는 시스템의 개발이 필요하다. 이를 위해 본 논문에서는 보안 시스템의 보안성을 평가하고, 원하는 수준의 보안성 확보에 이용할 수 있는 분석을 수행하였다.

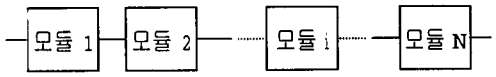
분석을 위해 먼저 다음을 정의하자.

$S_i(t)$: 보안 모듈 i의 시점 t에서의 보안성

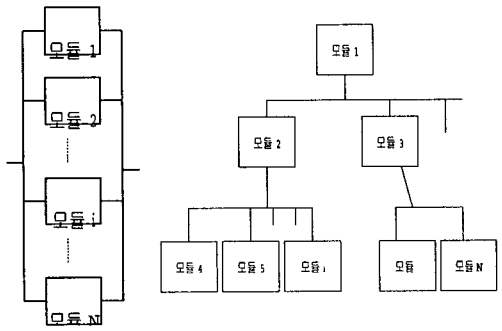
N : 병렬 또는 직렬 구조의 보안 시스템 구성 모듈 수

K : 계층 보안 경로 수

P_i : 보안 모듈 i를 통한 침입 확률



(a) 직렬구조



(b) 병렬구조 (c) 계층구조

<그림 2> 보안시스템 구조

보안 시스템에는 여러 개의 보안 모듈이 설치되어 운용되는데, 이를 위한 구조는 <그림 2>에서 보는 바와 같이 직렬(serial) 구조, 병렬(parallel) 구조 및 계층(hierarchical) 구조로 구성될 수 있다. 직렬 구조는 N개의 모듈이 모두 침해당하는 경우에 보안시스템 침해가 발생하고, 병렬 구조는 N개의 보안 모듈 중 하나라도 침해당하면 보안을 상실하는 시스템이다. 그리고, 계층 구조는 다양한 침해 유형에 대처하기 위한 다양한 보안 모듈을 설치한 경우로, 하위 계층의 모듈은 상위 계층의 모듈에 관리를 받고 있으면서, 임의의 계층 경로상의 모든 모듈이 침해당하는 경우 보안 시스템의 보안성을 상실하는 경우이다. 따라서, 이들 각 경우에 대한 보안성은 다음과 같이 평가 될 수 있다.

- 직렬 구조 : $1-\prod_{i=1}^{N} S_i(t)$

- P_i가 알려진 병렬구조 : $\min_{1\le i\le N}[S_i(t)]$, (P_i를 모르면, $\sum_{i=1=0}^{N} P_i \cdot S_i(t)$)

- 계층 경로 j의 침해 확률 P_j가 알려진 계층 구조 : $\min_{1\le j\le K}[H_j(t)]$ (P_j를 모르면, $\sum_{j=1}^{K} P_j \cdot H_j(t)$), 여기서, $H_j(t)= 1-\prod_{i=1}^{n_j} S_{ij}(t)$, $S_{ij}(t)$ = 계층 경로 j의 i 번째 모듈, i=1,2,..., n_j; j=1,2,...,K.

보안시스템의 보안성은 100%를 달성 목표로 하는 것은 바람직하지 않다[11]. 본 논문의 보안성 평가 방법은 계층구조를 포함한 보안 시스템의 동적인 분석을 수행하여, 원하는 수준의 보안성을 가지는 보안 시스템 구조(framework) 수립을 할 수 있을 것으로 기대한다.

4. 결론

GIS는 현실 세계를 구성하는 개체를 공간정보화하여 이를 입력, 저장, 관리, 분석할 수 있는 소프트웨어와 장비를 총칭하는 정보 시스템으로, 그 응용 분야는 교통망 관리, 교통시설 관리, 관광지 개발, 관광자원 관리, 도시시설물 관리, 하천 관리, 택지개발 관리, 재해예방 지원, 재무관리, 도로관리, 농정관리 등 매우 광범위하다. 따라서, 이에 대한 보안과 표준화가 필요한데, 현재까지 GIS 보안을 위한 표준화 및 연구나 연구는 미미한 수준이다. 본 논문에서는 GIS 보안의 특성을 파악하고, GIS 보안시스템의 요구사항을 도출하였으며, 이를 위한 보안 프레임워크를 제안하였다, 그리고, 보안 프레임워크 설계에 적용할 수 있는 보안성 분석 방안을 제시하였다. 향후, GIS 보안관련 표준화 동향을 고려한 개발이 되어야 할 것이며, GIS의 대량의 데이터 저장 및 전송 보안 방법에 대한 연구도 필요하다.

감사의 글 : 본 연구는 정보통신부가 지원한 대학 IT연구센터(ITRC) 육성.지원사업의 연구수행 결과의 일부이며, 이에 감사드립니다.

참고문헌

[1] 한국정보보호진흥원(KISA) 홈페이지, http//www.kisa.or.kr, 2002.

[2] 한국정보통신기술협회(TTA)홈 페이지, http://www.tta.or.kr, 2002.
[3] 한국산업표준원(KISI) 홈페이지, http://www.kisi.or.kr
[4] 김병구, 정태명, "침입탐지 기술의 현황과 전망", *정보과학회지*, 제28권 제1호, 2000, pp.29-39.
[5] 유신근, 이남훈, 심영철, "침입탐지시스템 평가 방법론", *한국정보처리학회 논문지*, 제7권 제11호, 2000, pp.3445-3461.
[6] 장화식, 이경현, "암호모듈 및 정보보호 시스템의 보안성 추정 모형", *1999년 한국멀티미디어학회 추계학술발표논문집*, pp.59-63.
[7] 정선이, 박정은, 유수연, 장성능, 채기준, 노병규, "네트워크 상에서의 침입차단시스템 영향력 분석", *통신정보보호학회 논문지*, 제10권 제 4호, 2000, pp.95-105.
[8] 주운기,임기욱, "정보보안을 위한 침입탐지 기술", *한국경영과학회/대한산업공학회 춘계공동학술대회*, 2001, pp.884-887.
[9] 한국전자통신연구원 공간정보기술센터, "제 3회 공간정보 워크샵", 2002, 코엑스 인터콘티넨탈호텔.
[10] S. Axelsson, "The Base-rate Fallacy and Difficulty of Intrusion Detection", *ACM Transactions on Information and Ststem Security*, Vol.3, No.3, 2000, pp.186-205.
[11] T.G. Beamsley, "Securing Digital Image Assets in Museums and Libraries : A Risk Management Approach", *Library Trends*, Vol.48, No.2, 1999, pp.359-378.
[12] S. Muftic et al., *Security Architecture for Open Distributed Systems*, John Wiley & Sons, 1993.