생존성 강화를 위한 동적협동에 관한 연구

김기한°, 최명렬, 이진석
ETRI 부설 국가보안기술연구소
{ghkim1°, mrchoi, jinslee}@etri.re.kr

A Study on Dynamic Coalition for Survivability Enhancement

GiHan Kim°, MyeongRyeol Choi, JinSeuk Lee
National Security Research Institute in ETRI

요 약

프로그램에 취약성이 없다는 것을 증명하는 것은 거의 불가능하다. 또한 현재 보안을 위해서는 인증과 접근제어, 암호화를 이용하지만 이러한 단순한 보안 기술은 버퍼오버 플로우와 같은 프로그램의 취약성을 이용한 공격에 대해 적절한 방어 대응을 할 수 없다. 그러므로 현재 위협적인 공격으로부터 중요한 기능을 지속적으로 제공하여 시스템 방어능력의 향상을 위한 생존성에 대한 연구가 필요하다. 동적협동은 이러한 생존성 연구의 일부분으로 생존성 기능을 가진 각 프로그램들이 동적환경에서 협동할 수 있는 환경을 제공해주는 기술에 대한 연구이다. 본 논문에서는 동적협동에 대한 분석을 통해 동적협동의 아키텍처와 각 구성요소의 기능에 대해 제시한다.

1. 서 론

기존의 중앙집중적인 컴퓨팅 환경은 분산 컴퓨팅 환경으로 활발히 변경이 이루어 지고 있다. 그러나 중앙집중 환경과 달리 분산 환경에서 그룹 서비스를 고려하면 새로운 요구사항이 추가된다. 그룹서비스의 경우 그룹의 가입과 탈퇴에 따른 관리, 그룹간 멀티캐스트 통신 등과 같은 경우를 고려해야 한다.

이러한 멀티캐스트 통신과 그룹 통신을 위한 연구는 분산 시스템 분야에서 지속적으로 연구가 되어오던 분야이다. 동적협동은 이러한 연구의 연장선상에 동적환경에서의 그룹통신에 대한 기술을 포함한다.

그리고 동적협동은 일반적인 분산 환경에 필수적인 동적 그룹통신 뿐만 아니라 시스템 방어향상을 위한 생존성 프로그램에서 사용에 공통적으로 사용할 수 있는 보안 정책의 협상 기능에 대한 연구를 수행하고 있다. 이러한 보안 정책 협상을 위해서는 생존성 프로그램에서 공통적으로 이해될 수 있는 보안 정책 표현에 대한 기술이 필수적이다.

본 논문에서는 이러한 동적협동에 대한 분석을 통해 동적협동에서 필요한 기능을 추출하고 동적협동에서 필요한 기술에 대한 구성을 제시하는데 목적을 둔다.

본 논문의 구성은 2장에서 DARPA에서 연구중인 동적협동 프로젝트에 대해 알아보고 3장에서 생존성 강화를 위한 동적협동 아키텍처를 제시하고 4장에서 결론을 맺는 구성이다.

2. DARPA IA&S의 동적협동 프로그램

DARPA[1]의 IA&S(Information Assurance and Survivability) 프로젝트는 정보전에 대응하기 위한 정보보증 및 생존 기술 개발을 주도하고 있다[1]. 그 주요 내용은 여덟 가지 영역에 걸쳐 연구가 진행중인데 각 생존성 구성요소간에 협동을 위한 기술에 대한 연구가 바로 동적협동부분이다.

동적협동 프로그램은 위협적인 파트너가 증가하는 상황에서 잠재적인 위험을 최소화하기 위해서 작업의 동적인 설립을 위한 보안 협동을 목적으로 한다[2].

예를 들어, 전통적인 중앙집중적인 시스템에서 중심 시스템의 파괴로 모든 시스템이 정지되거나, 악성의 멤버들에 의한 전체 시스템의 비정상적인 행동을 막기 위함이다.

DARPA의 IA&S 프로젝트의 이전 프로젝트인 정보생존성(Information Survivability) 프로젝트의 기술을 이용하기 위해서 동적협동 프로그램이 IA&S에서 제시되었고 다차원 보안 정책 관리와 보안 그룹 관리부분, 마지막으로 협동 인프라스트럭쳐의 3가지 부분으로 나누어 진다.

다차원 보안 정책 관리 부분은 네트워크 중심 협동의 설립과 유지에 필요한 보안 정책 관리의 수행에 대해 관심을 가진다. 협동 정책은 로컬 시스템의 운영체제, 네트워크 성능, 지원되는 미들웨어 서비스와 어플리케이션과 같은 다차원으로 고려되어야 할 부분이 존재한다. 그리고 다차원 보안정책 관리부분은 네트워크 토폴로지와 협동의 크기, 협동 상대방의 능력, 등의 요소를 고려해야 한다.

그룹 통신은 멀티캐스트 프로토콜 혹은 협동 유니캐스트 프로토콜로 구현될 수 있다. 일반적인 유니캐스트 프로토콜에서는 추가적인 보안 요구사항이 필요하다. 추가적으로 필요한 요구사항은 구성원이 그룹에 가입하거나 탈퇴하는 경우의 관리 정책 그룹 통신에 필요한 사항이다. 그리고 새로 가입한 구성원에게 이전에 사용하던 키에 대한 접근에 대한 제한과 인증은 메시지를 받았을 때의 그룹 소속을 검증하는 것이 아니라 메시지를 보냈을 때의 그룹 소속을 검증해야 하는 요구사항을 가진다.

또한 그룹통신에서는 상이한 조직 내에서의 참여할 수 있는 그룹을 동적으로 생성하고 그 그룹에 포함된 모든 사용자와 모든 조직의 보안 정책에 합당한 보안정책으로 그룹을 관리해야 한다.

협동 인프라스트럭처는 협동의 성공을 위해서는 다양한 도메인과 다수의 사용자을 위한 보안 서비스에 대한 통합에 관계한 기술을 연구한다.

3. 동적협동 아키텍처

동적협동의 중요한 기능은 2장에서 언급한것과 같이 다차원 보안 정책 관리와, 보안그룹관리, 협동 인프라스트럭처로 구분할 수 있다.

다차원 보안관리는 운영체제, 네트워크 성능, 미들웨어 서비스, 어플리케이션 뿐만 아니라 협동의 크기, 협동 상대방의 능력과 같이 고려해야할 사항이 많이 존재한다. 예를 들어 효율적인 방어를 위해서는 기존의 IDS와 방화벽과 방화벽 내부의 호스트와 동적환경에서의 협동이 필요하다.

미들웨어에서 동적협동의 기술의 접목은 기존의 분산 컴퓨팅 환경을 제공해주는 CORBA, JINI와 같은 미들웨어에서 제공하는 분산 서비스에 대한 동적변화를 인식, 관리하는 부분에서 적용할 수 있다.

뿐만 아니라 기존의 인증에서도 동적협동 기술은 적용할 수 있다. 기존의 인증은 사용자 식별을 이용한다. 그러나 인증은 서브젝트의 식별을 위하려면 협동에 관계한 모든 서브젝트를 알아야 하지만 동적환경에서는 협동에 참가하는 서브젝트가 수시로 탈퇴와 가입이 이루어지기 때문에 어려움이 존재한다. 그러므로 사용자 식별에 기반한 인증이 아닌 속성 기반의 역할개념을 도입한 인증이 필요하다. 이러한 동적협동 환경에서의 인증방법의 변경은 현재의 DNSSEC, IPsec과 같은 네트워크 프로토콜의 변경이 필요하다.

또한 다차원 보안관리에서는 보안 정책의 관리을 위해 정책의 표현, 변환, 동의, 분배에 대한 기능이 필요하다.

정책 표현부분은 시스템의 보안을 관리하는 경우와 다른 시스템과 보안 정책을 통신할 때 도움을 준다. 이 정책부분은 또한 통신하는 시스템의 수에 관계없이 넓은 확장성을 가져야 하고, 사용자가 보안정책을 쉽게 작성할 수 있는 보안정책 편집기능과 추상적인 개념의 보안정책을 IDS, 방화벽, 라우터, 일반 호스트가 이해할 수 있는 하위 보안 정책으로 변경을 수행하는 보안 정책 컴파일러도 필요하다. 그리고 현재 적용하고 있는 보안 정책을 모델링을 수행하여 새롭게 적용하는 보안 정책이 기존에 적용하던 보안정책과 위반되는 사항은 없는지 보안 정책 모니터링을 수행하는 기능도 필요하게 된다.

그룹통신에 관계한 내용은 기존의 분산 컴퓨팅환경에서 연구되던 멀티캐스트 기술의 연장으로 동적협동의 크기와 관련이 많다. 현재의 멀티캐스트 기술로는 수만개의 협동은 지원할 수 없는 확장성에 문제가 존재한다. 그러므로 소문 기반 업데이트와 같은 방법을 이용하여 확장성을 향상시키는 기술에 대한 연구도 지속적으로 필요하다.

그리고 협동 인프라스트럭처 부분에서는 현재의 PKI 부분에서 동적환경에서 알맞지 않는 부분에 대한 개선과 cross-인증에 대한 부분을 포함한다.

예를 들어 기존의 PKI에서 기존의 CRL(Certification Revocation List)는 동적환경에서는 구성원의 탈퇴와 가입이 수시로 이루어지기 때문에 너무 방대한 양이 발생하기 때문에 동적협동에서는 적합하지 않는 면이 존재한다. 이런 동적환경에서 알맞은 PKI를 적용하는 부분도 동적협동 기술의 구성요소이다.

그림 1에 본 논문에서 제시하는 동적협동 아키텍처가 표현되어 있다.

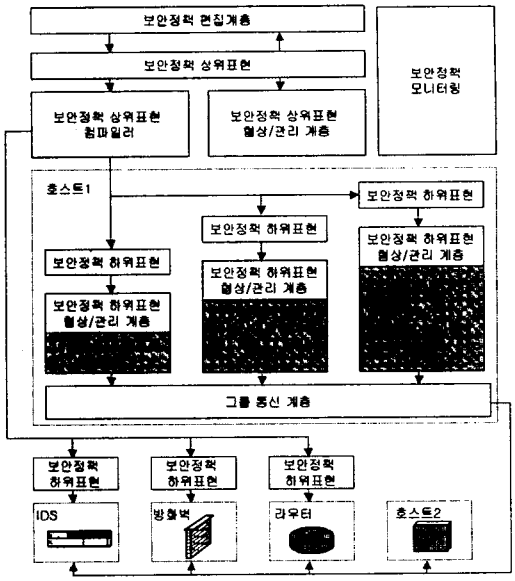

그림 1 동적협동 아키텍처

보안정책 편집계층에서는 사용자가 보안정책의 작성의 생성, 검색, 변경, 삭제를 용이하게 도와줄 수 있는 도구이다. 이러한 보안정책 편집계층을 이용하여 작성된 보안 정책은 특정 벤더의 IDS, 방화벽이 인식할 수 있는 구체적인 보안정책 하위표현을 직접 작성할 수도 있지만 전체적인 시스템의 보안 정책의 일관된 적용에 사용할 수 있는 보안정책의 상위표현이 된다. 보안정책 상위 표현은 협동 시에 동적으로 협상을 수행하는 경우 보안정책 상위표현 협상/관리 계층에서 그 기능을 담당하게 된다. 그리고 특정 IDS, 방화벽, 라우터에 적용할 수 있는 세부적인 보안정책으로 변경을 수행 할 수 있는 보안정책 상위표현 컴파일러가 필요하다. 보안정책 편집계층에서 작성된 보안정책 상위표현은 중간적인 언어로 사용자가 인식하기 좋은 정책으로 표현되어 있으나 실제 협동을 위해서 IDS와 방화벽, 라우터에서 통일된 표현으로 보안정책을 명세하는 표준이 존재하기 않기 때문에 이러한 보안 정책 하위표현으로의 컴파일 기능이 필요하다.

3.1 보안 정책 표현 기능

보안 정책은 동적협동 뿐만 아니라 다른 생존성 프로그램에서도 사용할 수 있는 부분이다. 현재의 보안 정책의 표현에 대한 표준화는 일부 이루어지고 있는 상황 이다. 예를 들어 IDS에서 침입에 대한 경보는 IDEF(Intrusion Detection Exchange Format)[3]와 같은 표준화 연구가 이루어졌지만 실제 모든 IDS에서 이 표준을 지원하고 있지 않는 상황이다. 또한 오브젝트에 대한

유기적인 보안을 제시하기 위해서는 IDS 뿐만 아니라, 방화벽, 라우터, 호스트와 같은 네트워크 구성요소와 네트워크 프로토콜, 미들웨어와 같은 소프트웨어 구성요소에 통일적으로 적용할 수 있는 보안정책에 대한 정의가 우선적으로 필요하다. 이러한 보안정책의 통일된 정의가 이루어지면 하나의 보안정책이 모든 오브젝트에 유기적이고 일관성있게 적용할 수 있기 때문이다.

그러나 현재 이러한 보안정책의 통일된 정의가 아직 부족하기 때문에 중간언어로 표현하고 보안정책상위표현 컴파일러를 통해 특정 벤더의 IDS, 방화벽, 라우터가 이해할 수 있는 보안정책으로 변경해주는 컴파일러가 필요하게 된다.

3.2 보안정책 모델링/ 협상/모니터링 기능

이러한 보안정책 표현을 협상하거나 모니터링하기 위해서 보안정책 모델링을 수행할 수 있는 기능이 필요하다. 보안정책 모델링을 수행하면 각 동적 협동자의 능력을 체계적으로 이해할 수 있고 이러한 이해를 바탕으로 협동시에 최선의 정책으로 협상을 수행할 수 있다. 이러한 보안정책의 협상은 보안정책상위표현과 보안정책하위표현 모두 협상 가능해야 한다.

보안정책 모니터링 부분에서도 보안정책 모델링을 수행하여 각각의 보안정책이 서로 위반하는 부분이 있는지 검사를 하는 기능을 수행한다. 이러한 보안정책 모니터링은 보안정책 상위표현과 보안정책 하위표현 모두 지원해주어야 한다.

3.3 그룹통신 기능

그룹 통신은 기존의 결함허용 부분에서 분산 컴퓨팅을 위해 꾸준히 연구되던 분야이다. 그러나 동적협동에서는 기존의 그룹통신부분 기능에서 확장성에 대한 부분에 대한 강화가 필요하다. 동적 환경에서 협동 구성원들의 가입과 탈퇴가 빈번한 상황을 지원할 수 있고 방대한 협동에 대한 통신 기능을 제공할 수 있는 그룹통신은 동적협동의 중요한 기능요소이다. 그리고 3.1절의 보안정책과 마찬가지로 그룹 통신부분은 다른 생존성 프로그램에서 공통적으로 사용할 수 있는 부분으로 활용도가 높은 부분이다.

3.4 동적협동이 포함된 네트워크 프로토콜 기능

ftp, pop3 등과 같은 네트워크를 사용하는 프로토콜은 평문으로 패스워드로 전송하는 경우가 많이 발생하여 많은 문제가 발생할 수 있다. 그리하여 현재의 접근방법은 공개키를 이용한 인증을 사용하여 암호화된 통신이 이루어지게 하는 부분으로 연구가 활발히 진행되고 있다. 그러나 통신을 수행하는 구성요소가 빈번히 변경되는 경우나 방대한 양이 통신을 통해 협동을 수행하는 경우 키 배포와 관리는 어려운 문제가 된다. 그러므로 동적환경에서 확장성을 보장해 줄 수 있는 인증방법에 대한 기술이 필요하다.

예를 들어 DNSSEC[4]은 최초에DARPA에서 개발된 기술로서 DNS간에 통신을 공개키를 이용하여 안전하게 수행하는 DNS의 확장이다. 그러나 이러한 DNS 통신을 위한 방대한 키 배포와 관리는 어려운 문제이다. 특히 DNS 와 같은 부분이 정적인 환경에서 이와 같이 공개키와 인증에 관계한 부분에서 동적협동 기술이 포함되어 더욱 향상된 확장성을 제공해주는 부분이 다양한 네트워크 프로토콜에 이루어져야 한다.

3.5 동적협동이 포함된 미들웨어 기능

분산 컴퓨팅 환경을 지원하는 미들웨어는 CORBA와 JINI 등이 존재한다. 이러한 분산 컴퓨팅 환경에서 지원하는 서비스에 대한 등록과 삭제가 빈번한 경우가 발생할 수 있다. 그리고 분산 컴퓨팅 환경에 참여하는 협동자의 수가 방대한 경우에 중앙집중적인 서비스 관리는 어려움이 존재할 수 있다. 그러므로 이러한 분산 컴퓨팅 환경을 지원한 미들웨어에서의 확장성에 대한 기술을 적용하기 위한 동적협동과 클라이언트와 서버와의 인증에서도 3.4절에 언급한 동적환경에서 확장성을 보장해줄 수 있는 인증방법도 미들웨어에 적용할 수 있다.

3.6 동적협동이 포함된 PKI 기능

현재 CA가 각각의 사용자가 인증을 폐기를 한 기록인 CRL(Certificate Revocation Lists)를 관리하고 있으나 이 방법은 대형 네트워크에서 확장성과 폐기정보에 대한 접근에 시간이 많이 드는 문제가 발생한다. 이러한 문제를 해결하기 기존의 PKI에 동적협동 기술이 접목될 필요성이 존재한다. 더 나아가 향상된 인증관리 인프라스트럭처를 지원하기 위해서는 서로 다른 보안 도메인에서 보안 정보를 검증할 수 있는 크로스 인증이 필요하다. 이 부분은 협동의 핵심적인 부분으로 현재는 크로스 인증은 오프라인으로 자동적이지 않은 방법으로 수행하고 있다. 미래의 네트워크 인프라스트럭처는 X.509, PGP 등과 같은 다양한 인증 인프라스트럭처를 지원해야 한다. 또한 동적협동 환경에서 권한부여 기술을 지원하기 위한 개발도 필요하다.

4. 결론

본 논문에서는 생존성을 위한 여러 기술 요소 중 동적협동에 대한 내용에 대한 분석을 통한 동적협동을 위한 개략적인 아키텍처를 제시하고 각각의 구성요소에서 지원해야할 기능을 정의했다. 동적협동 부분만으로 정보생존성의 모든 부분을 가질 수는 없지만 동적협동 부분은 생존성 프로그램간의 협동에 필수적인 기술요소이므로 매우 중요한 부분이다. 또한 동적협동의 보안정책의 표현/협상/관리/모니터링 부분과 확장성을 보장하는 그룹 통신 부분은 다른 생존성 프로그램에서도 필수적으로 사용되는 부분이다. 향후 연구방향으로는 다른 생존성 프로그램의 기술적 요소와 동적협동 부분의 통합에 대한 연구가 필요하다.

참고문헌

[1] http://www.darpa.mil
[2] http://www.afrlsn.afrl.af.mil/IA&S_topics.html#DC
[3] http://www.ietf.org/html.charters/idwg-charter.html
[4]http://www.ietf.org/html.charters/OLD/dnssec-charter.html