김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제6호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 6 JUCHE105(2016).

승인된 대상들사이의 안전한 자료통신을 보장하기 위한 한가지 보안통신망구성방식

김철은, 한수남

최근에 국가망을 비롯한 공공통신망을 통하여 자료들을 서로 안전하게 주고받을수 있는 자료배포체계에 대한 요구가 제기되고있다.

선행연구[1]에서는 국가적인 원격교육망에서 정보내용물의 저작권보호를 목적으로 하는 보안망구성방식을, 선행연구[3]에서는 공공망우에 보안가상망을 구축하기 위하여 통신통제봉사기를 중심으로 하는 별형망형식의 구성방식을, 선행연구[4]에서는 P2P자료기지관리체계에서 안전한 자료교환을 위한 보안망구성방식을, 선행연구[2]에서는 특성이 각이한 마디들로 구성된 분산형정보감시체계의 구축을 목적으로 하는 P2P망구성방식을 제기하였다.

우리는 선행연구결과들에 기초하여 지난 시기와 달리 기밀성보장과 망접근통제, 감독가능성과 같은 중요한 보안요구들을 동시에 만족시킬수 있는 보안망구성방식을 제기하였다. 론문에서 제기하는 보안망은 한마디로 승인에 기초한 안전한 자료배포망으로 특징지을수 있으며 앞으로 이것을 ASDDN이라고 간단히 표시한다.

1. 기 본 구 조

ASDDN은 IP통신기반(공공통신망)우에 놓여있는 상부망으로서 그 역할에 따라 다음과 같이 구분할수 있는 통신마디들과 그것들사이의 안전한 통신경로로 이루어진다.

최종마디 최종사용자들이 리용하는 통신말단으로서 ASDDN에서는 통신자료의 출발점 혹은 종착점으로서의 지위를 차지한다.

중계마디 최종말단들사이에 배치되여 보안방책에 따라 통신을 차단하거나 중계해주는 통신중계점 및 통제시행점이다. 동시에 서로 다른 망을 련결하는 역할도 수행한다.

망관리마디 자료통신망의 일정한 부분을 관리령역으로 정하고 관리령역안의 각 마디들의 가동상태, 부하상태와 통신리력을 실시간적으로 감시하는 망관리말단이다. 망관리마디는 해당한 기능을 갖춘 특수한 중계마디들이다.

전송권한관리마디 ASDDN의 최종마디들의 전송권한을 규정하여 각 중계마디들에 시행하며 그 시행상태를 실시간적으로 감시하고 망관리마디들에 종합되는 정보에 기초하여 부하분산 및 통신안정성을 높이기 위한 중계마디들의 추가 및 삭제, 최종마디와 중계마디의 대응관계의 갱신 등 보안관리업무를 수행하는 관리말단이다. 전송권한관리마디는 중앙중계마디(뿌리마디)에 배치한다.

증명기관마디 자료통신망의 각 요소들의 인증과 암호통신에 리용할 전자증명서의 발급, 갱신, 폐기를 담당한 증명기관의 전자증명서봉사기이다. 증명기관마디들은 ASDDN의 보안하부구조의 중요한 구성부분인 PKI를 형성하며 ASDDN의 PKI설계에 따라 모든 최종

마디 혹은 중계마디들이 직접 혹은 다른 중계마디를 통하여 간접적으로 접근할수 있는 위치에 별도로 배치한다.

이상의 마디들은 모두 TCP/IP망으로 련결되여있다. 중계마디들은 전부 IP통신기반의 공공통신망우에 존재하게 되며 최종마디들은 공공통신망에 나와있는 하나의 통신말단 혹은 그것과 물리격폐기, 기관내부의 최종말단으로 이루어진 하나의 보안통신말단체계로 실현된다.

ASDDN에서 마디들은 서로 련결되여 하나의 뿌리(중앙중계마디)를 가진 나무를 형성한다. 전송권한관리기능을 가진 중앙중계마디는 차수가 2이상인 뿌리마디로 되며 차수가 1인 나무의 매개 잎들에는 최종마디가, 차수가 2이상인 마디들에는 중계마디가 배치된다.

뿌리마디를 0준위마디 또는 최고준위마디, 뿌리마디와의 거리가 n인 마디를 n준위마디라고 부른다. 매개 최종마디는 반드시 하나의 중계마디(부모마디)와 련결되여있다.

정의 1 ASDDN에서 증명기관마디들을 제외한 최종마디와 중계마디들로 이루어지는 보안통신망을 ASDDN자료통신망이라고 부른다.

ASDDN자료통신망은 마디(콤퓨터)들의 모임 V와 V우의 관계 $E:=\{(u,\ v)|\ v$는 u의 통신을 통제가능$\}$로 구성된 나무 $\mathbf{\Sigma}:=(V,\ E)$로서 다음과 같은 가정을 만족시킨다.

i) 차수가 2이상인 뿌리마디를 가진다.

ii) 임의의 잎마디의 높이는 1이상이다.

정의 2 $\mathbf{\Sigma}$의 차수가 2이상인 마디들을 중계마디라고 부르고 $\mathbf{\Sigma}$의 중계마디전부의 모임을 $R_{\mathbf{\Sigma}}$로 표시한다. $\mathbf{\Sigma}$의 차수가 1인 마디들을 최종마디라고 부르고 $\mathbf{\Sigma}$의 최종마디전부의 모임을 $T_{\mathbf{\Sigma}}$로 표시한다.

정의 3 $\mathbf{\Sigma}$의 마디 u와 v에 대하여 $u\neq v$이고 u가 뿌리마디 r로부터 v에 이르는 경로상에 놓이는 마디라면 $u\prec v$라고 정의하고 u를 v의 선조마디, v를 u의 자손마디라고 부르며 u와 v사이의 경로에 다른 마디가 존재하지 않는 경우에는 u를 v의 부모마디, v를 u의 자식마디라고 부른다.

보조정리 $\mathbf{\Sigma}$의 임의의 두 마디사이에는 유일한 경로가 존재하며 관계 $\prec$는 $V(\mathbf{\Sigma})$우의 반순서관계이다.

보조정리로부터 ASDDN자료통신망의 임의의 두 최종마디사이에는 유일한 경로가 존재한다. 이 경로는 비록 공공통신망우에 놓여있지만 ASDDN의 보안하부구조에 의하여 보안대책이 수립된 안전한 통신경로이다.

2. 마디식별자할당체계

IP통신기반에서 ASDDN자료통신망 $\mathbf{\Sigma}$의 매개 마디 u에는 DNS의 도메인이름과 같은 역할을 수행하게 되는 유일식별자 ID_u가 할당된다.

식별자명명규칙은 다음과 같다.

i) 뿌리마디의 식별자는 따로 설정하지 않는다.

ii) n준위마디의 식별자는 DNS의 도메인이름을 뒤집어놓은것과 같이 뿌리마디를 제외한 자기의 선조마디들의 식별자의 오른쪽에 일정한 구분기호(실례로 점)를 주고 그 마디의 최종고유식별자를 덧붙여 정의한다.

결국 마디 u와 v에 대하여 $u\prec v$이면 문자렬 ID_u는 문자렬 ID_v에 포함되며 식별자만 보고도 해당 마디로부터 뿌리마디에 이르는 경로상의 중계마디들의 개수와 그것들의

식별자를 알수 있다.(그림 1)

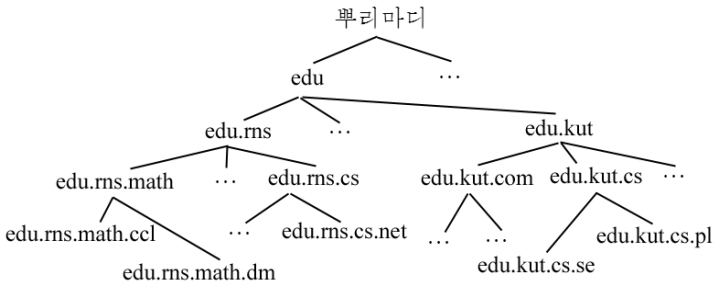

그림 1. ASDDN에서 마디식별자의 실례

구현을 쉽게 하기 위해 구분기호를 제외한 문자들은 대소문자를 구분하지 않는 원칙에서 영문자를 리용하며 될수록 사용자(관리자)들이 기억하기 쉽도록 3～4문자단위로 작성한다.

1준위마디들의 식별자는 최고준위마디의 관리자가 정하며 기타 마디들의 식별자에서 선조마디들의 식별자를 제외한 마지막부분은 해당 마디의 부모마디 혹은 어느 한 선조마디의 관리자가 해당기관의 내부에서 유일성을 보장하는 원칙에서 정하고 그 결과를 웃준위마디의 관리자에게 통지해주는 방식을 취하면 ASDDN에 망라된 모든 마디들의 식별자정의에서 유연성과 독자성을 보장할수 있을것이다.

ASDDN에서 모든 중계마디는 전송권한관리마디로부터 실시간적으로 자기의 자식마디들의 식별자와 IP주소사이의 대응표를 내리적재받아 자식마디들의 통신통제에 리용하게 된다. 중계마디는 자식마디들과 부모중계마디의 IP주소만을 알수 있다. 이 대응표를 간단히 해당 중계마디의 관리단위표라고 부른다. ASDDN에서 모든 최종마디는 부모마디의 IP주소만을 알수 있으며 통신상대방을 지적하는 유일한 수단은 그것의 식별자이다.

3. 전송권한의 표현

승인된 대상들사이의 통신만을 허용하는 보안목표를 달성하기 위한 수단으로서 ASDDN에서는 최종마디들의 자료전송권한을 전송권한관리마디(중앙중계마디)에서 통일적으로 규정하고 산하 중계마디들에 시달하여 그것에 따라 최종마디들의 통신을 통제하는것을 보안방책의 설정과 시행의 중요한 내용으로 설정하였다.

최종마디들의 자료전송관계를 규정하는 ASDDN의 보안방책을 다음과 같이 정의한다.

정의 4(전송권한방책) ASDDN자료통신망 $\boldsymbol{\Sigma}$의 최종마디전부의 모임을 $T_{\boldsymbol{\Sigma}}$라고 할때 전송권한방책 $\boldsymbol{\Pi}_{\boldsymbol{\Sigma}}$는 $T_{\boldsymbol{\Sigma}}$우의 관계 즉 $\boldsymbol{\Pi}_{\boldsymbol{\Sigma}} \subset T_{\boldsymbol{\Sigma}} \times T_{\boldsymbol{\Sigma}}$로서 $\boldsymbol{\Pi}_{\boldsymbol{\Sigma}} := \{(t,\ t') | t$는 t'에로 송신가능$\}$과 같이 정의한다. 최종마디 $t \in T$에 대하여 $\boldsymbol{\Pi}_t := \{(t,\ t') | (t,\ t') \in \boldsymbol{\Pi}_{\boldsymbol{\Sigma}}\}$를 t의 전송권한, 모임 $S_t := \{t' \in T | (t,\ t') \in \boldsymbol{\Pi}_{\boldsymbol{\Sigma}}\}$를 $t \in T$의 전송대상목록이라고 부른다. 그리고 중계마디 $r \in \boldsymbol{R}$에 대하여 $\boldsymbol{\Pi}_t := \{(t,\ t') | r \prec t \wedge t \in T \wedge (t,\ t') \in \Pi_{\Sigma}\}$를 r의 중계권한이라고 부른다.

전송권한방책과 최종마디의 전송권한, 중계마디의 중계권한 등은 빈모임이 될수도 있다.

정리 ASDDN자료통신망 $\boldsymbol{\Sigma}$의 최종마디모임 $T_{\boldsymbol{\Sigma}}$와 중계마디모임 $R_{\boldsymbol{\Sigma}}$가 주어졌을 때 다음의 결과들이 성립된다.

i) $\boldsymbol{\Pi}_{\boldsymbol{\Sigma}} = \bigcup_{t \in T_{\Sigma}} \boldsymbol{\Pi}_t$, $\boldsymbol{\Pi}_{\boldsymbol{\Sigma}} = \bigcup_{r \in R_{\Sigma}} \boldsymbol{\Pi}_r$

ii) $t,\ t' \in T_{\boldsymbol{\Sigma}} \wedge t \neq t' \rightarrow \boldsymbol{\Pi}_t \bigcap \boldsymbol{\Pi}_{t'} = \phi$

iii) $r,\ r' \in R_{\boldsymbol{\Sigma}} \wedge r \prec r' \rightarrow \boldsymbol{\Pi}_t \supseteq \boldsymbol{\Pi}_{t'}$

iv) $r,\ r' \in R_{\boldsymbol{\Sigma}} \wedge r \not\prec r' \rightarrow \boldsymbol{\Pi}_t \bigcap \boldsymbol{\Pi}_{t'} = \phi$

전송권한방책 $\mathbf{\Pi_{\Sigma}}$는 최종마디들의 식별자들로 구성된 표와 같은 형식의 전송권한표로 표현할수 있다.

표는 식별자 ID_{t_i}를 가진 마디 t_i가 식별자 ID_{t_j}를 가진 마디 t_j에로 송신가능하다는것을 보여준다.

표. 전송권한표

송신마디식별자	수신마디식별자
…	…
ID_{t_i}	ID_{t_j}
…	…

중앙중계마디에 배치된 전송권한관리마디는 전체 체계의 전송권한표를 작성하고 산하 중계마디들에 해당 마디의 중계권한표를 내려보낸다.

중계마디들은 최종마디로부터 수신마디식별자가 들어있는 자료전송요청을 접수한 후 그 마디와 수신마디식별자쌍이 중계권한표에 들어있는 경우에만 자료전송을 허가한다.

4. 보안하부구조

ASDDN에서 개별적마디들의 신분확인, 사용자확인, 암호통신, 중요한 자료의 안전한 보관 등을 담보하기 위하여 도입된 보안하부구조는 다음과 같은 요소들에 기초하고있다.

통과암호에 기초한 사용자관리 ASDDN의 각 마디에서 가동하게 되는 쏘프트웨어들은 자체의 사용자관리기능을 갖추고있다.

SSL 개별적마디의 신분인증, 통신내용의 기밀성과 무결성에 대한 요구를 동시에 만족시키기 위한 수단으로서 SSL을 ASDDN의 보안하부구조에 도입하였다.

PKI ASDDN을 국가망우의 상부망으로 구축하는 경우에는 국가망전자인증체계를 PKI로 쓸수도 있지만 국가망과 분리되여있는 기관망 혹은 부문망우에 구축하는 경우를 위하여 ASDDN에 따로 증명기관(CA)마디들을 배치하고 전자증명서의 발급과 폐기를 진행하는 자체의 PKI를 X.509v3에 기초하여 구축한다.

방화벽 ASDDN의 마디들은 고정된 포구주소를 리용하여 통신하게 된다. 마디들이 소속기관의 보안조치에 따라 기관내 방화벽뒤에 배치되는 경우에는 ASDDN용포구의 통화를 허용하도록 방화벽규칙을 설정하여 방화벽을 관통하는 직접통신을 보장하도록 한다.

방화벽밖에 놓여있는 마디들에서는 해당 조작체계준위 혹은 국가적으로 공인된 방화벽을 가동시키여 ASDDN용포구의 통화만을 허용하고 기타 통화는 모두 차단하도록 방화벽규칙을 설정한다.

자료기지암호화 전송권한관리마디를 비롯한 중계마디들에는 전송권한표나 관리단위표와 같은 중요한 자료들을 자료기지에 암호화하여 보관한다.

암호화된 사건기록 ASDDN에서는 책임추적성 및 감독가능성을 보장하기 위하여 모든 마디들이 통신과정에 발생하는 사건들에 대한 기록 및 통화내용을 암호화하여 보관하고 망관리마디의 요청에 따라 사건기록을 암호문으로 발송하는 기능을 보안하부구조에 도입하였다.

5. 최종마디들사이의 자료통신규약

ASDDN의 목적은 승인된 최종마디들사이의 안전한 통신을 보장하는것이다.

최종마디들사이의 통신의 전제조건은 ASDDN자료통신망의 모든 마디들 즉 최종마디들과 중계마디들이 고유한 식별자와 함께 전자증명서를 소유하는것이다.

ASDDN자료통신망 $\mathbf{\Sigma}:=(V,\ E)$에서 우의 전제조건이 만족되였다고 가정하자.

$s\in T_{\Sigma}$와 $d\in T_{\Sigma}$가 Σ의 최종마디일 때 s로부터 d까지 어떤 자료를 송신하는 과정은 크게 보안접속개설, 자료전송, 보안접속해제단계를 거치게 된다.

보안접속개설 이 단계에서는 전송가능성 즉 $(s,\ d)\in\Pi_{\Sigma}$인가를 확인하고 전송이 허용된 경우 s로부터 d까지의 보안통신로를 확보한다.

s로부터 d까지의 Σ에서의 유일한 경로상에 놓이는 중계마디들가운데서 뿌리마디까지의 거리가 가장 짧은 마디를 $r\in R_{\Sigma}$로 표시하고 s로부터 r에 이르는 Σ에서의 유일경로상에 놓이는 중계마디들을 차례로 $r_1^s,\cdots,r_k^s$로, r로부터 d에 이르는 Σ에서의 유일경로상에 놓이는 중계마디들을 $r_1^d,\cdots,r_l^d$로 표시하면 그림 2에서와 같이

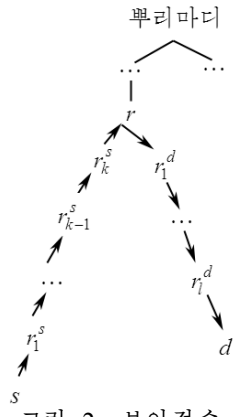

그림 2. 보안접속 개설과정

$$r\prec r_k^s\prec r_{k-1}^s\prec\cdots\prec r_1^s\prec s,\ \ r\prec r_1^d\prec\cdots\prec r_l^d\prec d.$$

1단계(s와 r_1^s 사이의 SSL접속개설) s는 자기가 알고있는 유일한 IP주소를 리용하여 자기의 부모중계마디 r_1^s에 SSL접속을 요청하는것으로 쌍방사이의 SSL악수규약실행을 개시한다. 성공적으로 끝나면 쌍방신분확인과 합의된 알고리듬에 의한 SSL접속 즉 보안통로가 개설된것이고 다음 단계로 전진한다.

2단계 r_1^s는 보안통로로 s에 전송대상목록을 송신한다. 이 단계는 선택적이다. 전송대상목록에서 변화가 없으면 이 단계는 뛰여넘는다.

3단계 s의 사용자는 사용자대면부에 표시된 전송대상목록에서 목적하는 수신측최종마디 d를 선택하고 $(\mathrm{ID}_s,\ \mathrm{ID}_d)$를 보안통로로 r_1^s에 보낸다.

4단계(올리접속개설) $r_{k+1}^s:=r$로 놓고 $i=1,\cdots,k$에 대하여 다음의 절차를 반복한다.

r_i^s는 자기가 가지고있는 전송권한표에 $(\mathrm{ID}_s,\ \mathrm{ID}_d)$가 있는가를 확인한다. 없으면 전송요청부결이라는 상태통보문을 보안통로로 s에까지 보내고 보안접속해제단계로 넘어간다. 있으면 IP주소를 알고있는 부모중계마디 r_{i+1}^s와 SSL접속을 개설하고 $(\mathrm{ID}_s,\ \mathrm{ID}_d)$를 전송한다. 상태통보문을 s로 보낸다.

5단계(내리접속개설) $r_0^d:=r$로 놓고 $i=0,\cdots,l-1$에 대하여 다음의 절차를 반복한다.

r_i^d는 자기가 가지고있는 전송권한표에 $(\mathrm{ID}_d,\ \mathrm{ID}_s)$가 있는가를 확인한다. 없으면 전송요청부결이라는 상태통보문을 보안통로로 s에까지 보내고 보안접속해제단계로 넘어간다. 있으면 ID_d의 왼쪽 부분과 가장 많이 일치되는 식별자를 가진 자식중계마디를 r_{i+1}^d로 선택하여 관리단위표에서 IP주소를 얻은 다음 그것과 SSL접속을 개설하고 $(\mathrm{ID}_s,\ \mathrm{ID}_d)$를 전송한다. 상태통보문을 s로 보낸다.

6단계 마지막중계마디 r_l^d는 관리단위표에서 ID_d를 검색한다. 성공하여 d의 IP주소를 얻으면 d와의 SSL접속을 시도한다.

7단계 d는 r_l^d와의 SSL접속이 개설된 후 접속성공통보문을 이미 확보된 보안접속경로를 통하여 s에 전송한다.

8단계 s는 d로부터 최종접속성공통보문을 접수한 후 완전보호방식의 SSL접속을 개설하는 경우에는 경로상의 중계마디들에 확보된 일반소케트렬을 통하여 d와 새로운 SSL

악수규약을 실행한다. 내용감독방식의 SSL접속을 개설하는 경우에는 s와 경로상에 설정된 감독마디들, d들사이에 각각 직통 SSL접속을 개설하는 과정을 다시 반복한다. 이 경우 감독마디가 아닌 중계마디들은 SSL소케트들을 일반소케트로 전환하여 단순중계자로 행동한다.

자료전송 최종마디들사이에 개설된 SSL보안접속을 통하여 자료를 주고받는다.

보안접속해제 통신쌍방중에서 어느 한 최종마디가 접속해제요청을 보내고 다른쪽이 동의하는 경우 혹은 오유가 발생한 경우 접속해제단계에 들어간다.

보안접속해제는 해제를 제기한 최종마디가 상대방의 동의를 받은 후 자기의 중계마디에 접속해제통보문을 보내고 접속을 해제하는것으로 시작한다. 상대측최종마디에 이를 때까지 같은 절차를 반복한다.

맺 는 말

론문에서는 국가망을 비롯한 공공통신망을 통하여 기관들사이 혹은 기관내 여러 부서들사이에 과학기술자료들을 비롯한 내부자료들을 서로 안전하게 주고받을수 있는 자료배포체계의 보안요구를 만족시킬수 있는 한가지 보안망구성방식을 제기하였다.

론문에서 제기한 보안망구성방식 ASDDN은 상부망구조, 통신마디들의 명확한 나무구조의 형성, 마디식별자할당체계에 의한 IP주소공개범위의 제한, SSL규약에 기초한 인증과 암호통신, 엄격한 전송권한관리 등에 기초하여 통신내용의 기밀성보장, 통신실체의 호상인증과 통신경로에 대한 통제가능성, 통화내용의 감독가능성과 같은 보안목표를 동시에 달성하면서도 충분한 통신속도를 보장할수 있다는것이 실험적으로 확증되였다.

ASDDN은 기관망, 부문망, 국가망 등 각이한 범위에서 승인된 대상들사이의 안전한 자료교환을 위한 보안망구축의 기초로 될수 있다.

참 고 문 헌

[1] H. Abie et al.; Int. J. Inf. Secur., 3, 113, 2004.

[2] B. Gedik et al.; IEEE Transactions on Computers, 54, 6, 767, 2005.

[3] T. Martin et al.; PCT/GB2007/004422, WO 2008/062169 A1, 29, May, 2008.

[4] S. Rahman et al.; Cryptology ePrint Archive: Report 2010/085, 2010.

주체105(2016)년 2월 5일 원고접수

Secure Network Architecture for Providing Secure Data Communication between Authorized Nodes

Kim Chol Un, Han Su Nam

We present secure network architecture for securely sending and receiving data between authorized nodes over a public network. The architecture can achieve the security goals of communication confidentiality, access control over communication paths and accountability.

Key word: secure network