적응적 보안등급을 이용한 컨텍스트-기반 보안정책 관리모델

서정철° 채종우 정목동
부경대학교 컴퓨터공학과
{baram78°, jwchae}@mail1.pknu.ac.kr, mdchung@pknu.ac.kr

Context-Based Security Policy Management Model Using Adaptive Security Level

Jungchul Seo°, Jongwoo Chae, Mokdong Chung
Dept. of Computer Engineering, Pukyong National University

요 약

최근 인터넷의 급성장을 기반으로 유비쿼터스 환경이 도래하면서 다양한 환경요소를 가진 자원들이 네트워크 상에 공존한다. 이러한 환경에서 적절한 보안 서비스를 제공하기 위해서는 자원의 환경정보를 제공하는 컨텍스트(Context)를 기반으로 적절한 보안정책을 결정하는 것이 필요하다. 본 논문에서는 유비쿼터스 환경에서 제공되는 상황정보를 통해 사용자의 선호도, 디바이스의 성능, 서비스의 가치 등 다양한 자원의 환경요소를 획득하여 MAUT와 간결한 휴리스틱스를 이용하여 자원에 적절한 보안 등급을 적응적으로 결정하는 알고리즘을 제안하고, 이를 바탕으로 유비쿼터스 환경에 적합한 보안정책 관리 모델을 제안한다.

1. 서 론

최근 인터넷의 급성장으로 유비쿼터스 환경이 도래하고 있다. 유비쿼터스 환경[1,2]이란 컴퓨터가 사람의 현실 공간으로 다가오는 개념으로, 컴퓨터가 도처에 편재하여 자원의 환경요소(물리적 상황: 위치, 디바이스 종류,성능, 정서적 상황: 선호도, 역사적 상황: 시간 등)인 상황 정보(Context Information)[3]를 서비스 받을 수 있음을 의미한다. 이러한 환경 요소에 관한 정보를 컨텍스트(context)[4]라 하며 컨텍스트-인지(Context-Awareness)[5]를 바탕으로 자동화된 서비스를 제공할 것이다.

유비쿼터스 환경에서는 자원들의 다양한 컨텍스트가 도처에 편재함에 따라 보안 및 프라이버시를 위한 기술성이 대두되고 있다[6]. 그러나 현재의 보안 서비스로는 시간과 상황에 따라 변화되는 유비쿼터스 환경에 그대로 적용하기 어렵다. 따라서 본 논문에서는 자원의 컨텍스트를 고려하여 적응적으로 보안등급을 결정하는 알고리즘을 제안하고, 이를 이용한 보안정책 관리 모델을 제안한다. 서론 이후의 논문의 구성은 다음과 같다. 2절에서 제안 모델의 관련 연구를 설명하고, 3절에서는 컨텍스트-기반의 보안정책 관리모델과 적응적 보안등급 결정 알고리즘을 제안한다. 4절에서는 사례연구와 프로토타입을 설명하고, 5절에서는 결론과 향후 연구에 대해서 논한다.

2. 관련 연구

2.1 컨텍스트-인지 컴퓨팅(Context-Aware Computing)

컨텍스트-인지 컴퓨팅은 유비쿼터스 환경에서 애플리케이션이 사용자의 컨텍스트를 감지하여, 사용자가 이용할 수 있도록 해주는 모바일 컴퓨팅의 패러다임[7]이다. 즉, 사용자에게 적절한 서비스를 제공하기 위해서 자원의 컨텍스트와 사용자의 입력정보가 결합되어 사용자가 처한 상황에 맞는 수준으로 조정하여 서비스를 제공하는 것을 말한다.

하지만 다양한 사용자의 정보가 노출된 유비쿼터스 환경에서 안전한 서비스를 제공하기 위해서는 컨텍스트-인지 컴퓨팅를 기반으로 동적으로 변하는 컨텍스트에 적절하게 대응할 수 있는 적응적인 보안 서비스가 필요하다.

2.2 MAUT(Multi-Attribute Utility Theory)

MAUT[8]는 다중변수에 대한 의사결정 문제(decision problem)에서 유틸리티(utility)를 통한 정략적인 의사결정 방법이다. 유틸리티 분석(utility analysis)은 의사 결정자(decision maker)가 원하는 제비뽑기(lottery)의 결과를 분석해주는 분야로서 의사 결정자는 이들 결과에 대한 개인의 선호도(preference)를 유틸리티 수(utility number)로 표현한다. 유틸리티는 0과 1사이의 상대적인 값으로서 가장 선호하지 않는 결과 유틸리티를 $u(x^0)=0$, 가장 선호하는 결과 유틸리티를 $u(x^*)=1$로 나타낸다. 그리고 결과에 대한 유틸리티 수의 대입은 의사결정자의 최적행동의 기준이 되는 기대 유틸리티(expected utility)를 최대화 시켜주는 쪽으로 이루어 진다

유비쿼터스 환경에서 다양한 변수에 기반 하여 의사결정을 하기 위해서는 사람마다 다른 만족도를 나타내는 유틸리티를 기반으로 MAUT 이론을 적용하는 것이 효율적일 수 있다[9,10].

2.3. 간결한 휴리스틱스(Simple Heuristics)

간결한 휴리스틱스(simple heuristics)[11]는 1995년 독일, 미국, 영국에서 심리학, 수학, 컴퓨터과학, 경제학, 생물학 등 학제간의 연구를 위해서 설립된 ABC(Adaptive Behavior and Cognition) 연구그룹의 주된 이론이다. 이 연구소에서는 제한적 추리(bounded rationality)와 불확실성 하에서 좋은 의사 결정에 관한 연구를 해오고 있다. 간결한 휴리스틱스(Simple Heuristics)를 이용하려는 이유는 보안 관련 특징 변수와 관련된 사용자들의 선호도를 개량적으로 정확히 예측한다는 것이 쉬운 일이 아니기 때

문이다. 간결한 휴리스틱스 중에서 대표적인 것은 Take The Best가 있는데, 이는 특정변수(cue)를 차례로 조사하여 두 개체를 차등화 시켜 줄 수 있는 변수를 발견하면 이 변수가 추론의 근거가 되고 나머지 특징변수는 모두 무시한다. Take The Best는 특히 훈련 집합의 규모가 적을 때 다중회귀(multiple regression)를 능가 한다[11].

3. 보안정책 관리 모델

3.1 적응적 보안정책 관리 모델의 구조

다음은 제안 모델의 구조와 흐름을 보여준다.

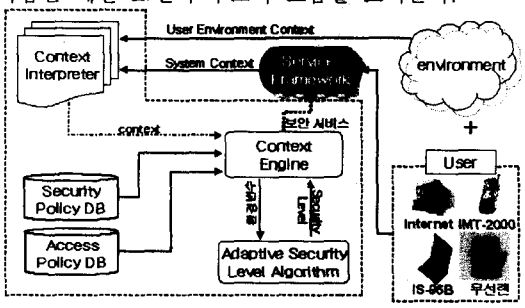

그림 1 보안정책 관리 모델의 구조

Environment와 User : 컨텍스트가 도처에 편재한 환경과 유·무선망을 기반으로 한 사용자를 나타낸다.

Service Framework : 증권거래, 계좌이체, 주문 등의 유·무선 응용서비스를 제공 시 정보에 대한 보안을 제공하는 Framework이다.

Context Interpreter : 획득한 컨텍스트를 수집하고 관리하며, 획득한 환경 변수를 정량적인 값으로 변환한다.

Secutiry PolicyDB와 Access PolicyDB : 보안정책은 보호되는 자원에 따라 알고리즘에 사용될 변수, 유틸리티 함수의 형태 등을 결정하고, 접근정책은 자원에 대한 접근을 허가 또는 거부를 결정한다.

3.2 적응적 보안등급 결정 알고리즘

MAUT와 간결한 휴리스틱스를 바탕으로 보안 등급을 환경 정보에 따라 동적으로 결정하는 알고리즘이다.

```
function SecuLevel(secureProblem) returns SL
 inputs: secureProblem:보안 등급 결정 문제
 step 1 // 영역 독립변수를 적용하여 보안 등급을 결정
   calculate SL
 step 2 // 영역 의존변수를 적용하여 보안 등급을 조정
   switch(UserSelection) //사용자의 선택에 따른 결정
     case MAUT:
       SL = MAUT(X);
     case S.Heuristics:
       SL = TakeTheBest(X)
return SL
```

```
function MAUT(X) returns SL
 static u(x1,x2,..,xn)=k1u1(x1) + k2u2(x2) +...+ knun(xn)
 //모든 i에 대해 ui(x°i) = 0, ui(x*i) = 1,
 //ki는 가중치, 사용자와의 질의를 통하여 가중치 ki를 결정한다.
  for i = 1 to n
    ui(xi) = GetUtilFunction(xi)
  end
 // 보안 등급 결정
  SL = ⌈ U*10 ⌉ /2, (SL = 0, 1, . . . , 5)
return SL
```

```
// Take the best, ignore the rest
function TakeTheBest(X) returns SL
 inputs u(x1,x2,..,xn) : 사용자의 기본 선호도
 // 가장 선호하는 것이 xi이면, xi 만 SL계산에 사용
 u(x1,x2,...,xn) is calculated by
      only considering the value of xi
return SL;
```

```
function GetUtilFunction(xi) returns u(x1,x2,..,xn)
 inputs xi : 영역 의존 변수
 local variables :
  uRiskProne : 주어진 xi에 대하여 사용자는 위험 선호
  uRiskNeutral : 주어진 xi에 대하여 사용자는 위험 중립
  uRiskAverse : 주어진 xi에 대하여 사용자는 위험 회피
  x : xi로부터 임의로 정한 값
  h : 임의로 선택한 상수
  <x+h, x-h> : <x+h>와 <x-h>사이의 lottery
  //lottery (x*, p , x°)는 확률 p로 x*, 확률 (1- p)로 x° 선택
  //p = 0.5는 <x+h>와 <x-h>의 선택 확률이 동일
 ask  user to prefer <x+h, x-h> or x // 사용자 선호도 질문
  if risk prone then b(2^cx -1)
  else if risk neutral then bx
  else if risk averse then blog2(x+1)// b,c>0 인 상수
return u(x1,x2,...,xn)
```

3.3.2 적응적 보안등급에 따른 보안 서비스

보안등급 SL은 0~5까지의 수로 나타내며, 0인 경우는 보안모델을 사용할 수 없는 경우이다. S_j는 암호알고리즘, A_l은 인증기법, R_m은 프로토콜을 나타낸다. 보안시스템의 속성 p_i는 아래의 표와 같은 다양한 보안속성(S_j,A_l,R_m)들의 조합으로 이루어진다.

표 1. 인증기법의 종류(A_l)

A_0	Password only
A_1	Certificate
A_2	Biometirc
A_3	Hybrid

표 2. 프로토콜 유형(R_m)

R_0	SPKI
R_1	Wireless PKI
R_2	PKI

표 3. 암호알고리즘들의 종류(S_i)

	대칭암호-키길이	공개키암호-키길이	MAC
S_1	DES	RSA-512	MD5
S_2	3DES	RSA-512	MD5
S_3	3DES	RSA-768	SHA
S_4	AES-128	RSA-1024	SHA
S_5	AES-192	RSA-1024	SHA

4. 사례 연구 및 프로토타입

사용자가 보호된 자원 A에 대해 읽기를 원할 때, 보안정책은 컨텍스트에 따라 표 4와 같이 정해 질수 있다.

표 4에서, 자원 A에 접근하기 위해서는 일정한 CPU 성능, 네트워크 전송속도, 암호 알고리즘의 강도를 요구하고, 알고리즘의 보안강도(X_{att}), 인증기법(X_{auth}), 자원의 보호수준(X_{res})등을 환경변수로 사용 한다. 보안등급을 결정하기 위해 각 변수를 표 5와 같이 정량적인 값으로 환산하고, 가중치 k_i를 결정하기 위해 정성적인 질문을 한다.

표 4. 보안정책의 예

A Security Policy for *Protected Resource A*
Action : reading
Utility Function : $u(x_{att}, x_{auth}, x_{res}) = k_{att}u(x_{att})+k_{auth}u(x_{auth})+k_{res}u(x_{res})$;
Security Contexts : comp ≥ 200MHz; nType ≥ 100Kbps; tType=PC/PDA/Cellphone;
User's Preference : $uRiskProne=2^{2(x-1)}$; uRiskNeutral=x; $uRiskAverse=\log_2(x+1)$

표 5. 환경 변수 유틸리티 환산표

변수 \ 값	0.2	0.5	0.8	1.0
x_{att}(보안강도)	$\geq 10^{0.5}$	$\geq 10^{3}$	$\geq 10^{7}$	$\geq 10^{11}$
x_{auth}(인증기법)	Password only	Certificate	Biometric	Hybrid
x_{res}(보호수준)	No	Low	Medium	High

가령 x^*_{auth}와 x^*_{res}보다 x^*_{att}을 더 선호하면 $k_{att}>k_{auth}+k_{res}$, $k_{att}>.5$이다. 또한 x^o_{res}에서 x^*_{res}로 되는 것 보다 x^o_{auth}에서 x^*_{auth}로 되는 것을 선호하면 $k_{auth}>k_{res}$이다. 만약 $k_{att}=.6$으로 평가되었다면 의사결정자는 $(x^*_{att},x^o_{auth},x^o_{res})$과 제비뽑기 $<(x^*_{att},x^*_{auth},x^*_{res}),.6,(x^o_{att},x^o_{auth},x^o_{res})>$ 사이의 어떤 결정도 무관하다는 것을 의미한다. 제비뽑기$<(x^*_{att},x^*_{auth},x^*_{res}),\ .6,\ (x^o_{att},x^o_{auth},x^o_{res})>$은 $(x^*_{att},x^*_{auth},x^*_{res})$일 확률 .6과 $(x^o_{att},x^o_{auth},x^o_{res})$일 확률 .4를 의미한다. k_{att}이 .6이므로 $k_{auth}+k_{res}=.4$이다. 이제 의사결정자가 $(x^o_{att},x^*_{auth},x^o_{res})$와 $<(x^o_{att},x^*_{auth},x^*_{res}),p,$

$(x^0_{att}, x^0_{auth}, x^0_{res})$>의 선택을 무관하게 할 수 있는 확률 p를 질의 한다. 만약 의사 결정자의 답이 .7이라면 공식 $k_{auth}=p(k_{auth}+k_{res})$[10]에 의해서 $k_{auth}=.28$이 된다. 그리고 $u_i(x_i)$를 결정하기 위해서 제비뽑기 $<x+h, x-h>$와 기대결과 x의 선호도를 질의한다. 만약 x를 선호하면 유틸리티 함수는 모험 회피이며 각 $u_i(x_i)$는 $b\log_2(x_i+1)$의 형태가 된다. 즉, $u(x_{att}, x_{auth}, x_{res})=.6\log_2(x_{att}+1)+.28\log_2(x_{auth}+1)+.12\log_2(x_{res}+1)$ 이 되고, 계산된 결과 값에 따라 아래와 같이 보안등급을 결정하고 표 1, 2, 3 과 같이 보안속성이 결정된다.

$$U=\sum_{i=1}^{n} k_i u_i(x_i), (0 \le U \le 1)$$

$$SL=\lceil U*10 \rceil /2, (SL=0,1,\ldots,5)$$

가령 보안강도가 $10^{0.5}$, 인증기법이 Biometric, 보호수준이 low라면, $u(x_{att}, x_{auth}, x_{res})=.6\log_2(.2+1)+.28\log_2(.8+1)+.12\log_2(.5+1)$ 이므로 $.6*0.263+.28*.849+.12*0.585=0.46572$ 이므로 보안등급은 3 등급으로 결정된다.

표 6. 접근정책의 예

An Access Policy for *Protected Resource A*
If ((SL≥2) **and** ((Role=administrator) **or** ((Role=user) **and** (Date=Weekdays **and** 8:00≤Time≤18:00))))
then resource A can be read
If ((SL≥3) **and** (Role=administrator))
then resource A can be written

그리고 자원에 대한 접근의 허가 또는 거부는 표 6과 같은 접근 정책에 따라 결정된다. 표 6에서, 보안등급이 3인 관리자인 경우에 자원 A에 대해서 읽기, 쓰기가 허가되며, 2등급의 일반 사용자인 경우는 08시~18시 사이에만 읽기가 허가된다는 것을 의미한다.

제시한 모델의 가용성을 실험하기 위해 표 7과 같이 5명의 사용자가 동적으로 결정된다고 가정하고 실험을 하였을 때 결과는 그림 2와 같다.

표 7 사용자의 환경 정보

	X_{att}	X_{auth}	X_{res}
A	$10^{0.5}$	Password only	No
B	$10^{0.5}$	Biometric	Low
C	10^{1}	Certificate	Low
D	$10^{0.5}$	Certificate	Medium
E	10^{1}	Biometric	Medium

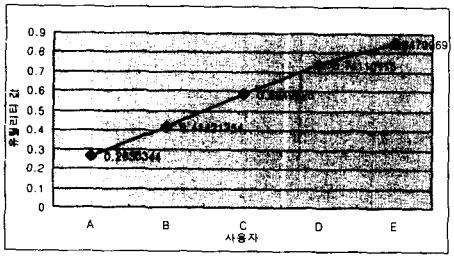

그림 2 프로토타입 결과

그림 2에서 각기 다른 컨텍스트 환경에 따라 유틸리티 값이 동적으로 결정됨을 알 수 있다. 즉, 동적으로 결정되는 유틸리티 함수의 값에 따라 보안등급이 결정되므로, 보안정책과 접근정책이 동적으로 결정됨을 의미한다.

이와 같이 다양한 환경 변수의 값을 정량화하여 정량적 의사 결정 이론인 MAUT와 Simple Heuristics를 사용함으로써 기존의 정적인 환경에서 해결하지 못했던 적응적 보안 서비스 사용의 어려움을 해결할 수 있을 것으로 예상한다. 즉, 기존의 정적인 보안 서비스 시스템에서는 다중의 환경 변수 중에서 특정 변수들의 동적인 변화를 적시에 반영할 수 없었기 때문에(정적으로만 반영) 자원의 효율적 활용이 어려웠지만 본 논문에서 제시하는 컨텍스트 기반 적응적 보안 모델에서는 이들 문제점을 효율적으로 해결 할 수 있을 것으로 기대한다.

또한 사용자의 환경에 따라 동적으로 적절한 보안등급이 결정되고 그에 따른 보안서비스를 제공받기 때문에 기존의 정적인 보안서비스를 이용함으로 열악한 환경의 사용자에게 무리한 시스템 자원이나 장기간의 대기시간을 요구하는 문제를 해결할 수 있을 뿐만 아니라 자원의 특성에 따른 접근정책으로 인해 악의를 가진 사용자로부터 자원을 안전하게 보호할 수 있을 것이다.

5. 결론

보안 시스템 속성이 고정된 현재 보안 시스템으로 인해 열악한 환경의 사용자는 상당히 긴 대기시간을 감수하거나 아니면 시스템의 이용을 포기하게 되는 문제점을 해결하기 위해서 정량적 의사 결정 이론인 MAUT와 Simple Heuristics를 사용하였다. 제안된 시스템은 기존의 정적인 환경에서 겪었던 적응적 보안 서비스 시용의 어려움을 해결할 수 있을 것으로 예상한다.

향후 연구 과제로서 보다 많은 환경 변수들을 이용하여 효율적인 보안 정책을 적용하고 사용자의 요구사항을 다 각도로 반영하는 MAUT에 대한 연구와 컨텍스트 정보에 따른 정량적 모델 개발과 제안 모델을 실제 환경에서 실험해 보는 것이 필요하다.

[참고문헌]

[1] Mark Weiser and John Seely Brown, THE COMING AGE OF CALM TECHNOLOGY, Xerox PARC, October 5, 1996
[2] M.Weiser, http://www.ubiq.com/weiser
[3] Guanling Chen, "A survey of context-aware mobile computing research", Dartmouth Univ.TR2000-38
[4] A. Dey., "Providing Architectural Support for Building Context-Aware Applications," Ph. D. Dissertation, Georgia Institute of Technology, 2000.
[5] 윤정로, 최장욱 역, 유비쿼터스, 21세기북스, 2003.
[6] D. Saha and A. Mukherjee, "Pervasive computing: A New Paradigm for Computing in 21st Century," IEEE Computer, Vol. 36, No. 3, 2003, pp. 25-31.
[7] R. Grimm.. " A system architecture for pervasive computing," ACM SIGOPS European Workshop,
[8] R.L.Keeney and H.Raiffa, Decisions with Multiple Objectives: Preferences and Value Tradeoffs, John Wiley & Sons, New York, NY, 1976.
[9] R. Schfer, "Rules for Using Multi-Attribute Utility Theory for Estimating a User's Interests," in Proceedings of the ninth GI-Workshop. ABIS-Adaptivitt und *Benutzermodellierung in interaktiven* software systemen, Dortmund, Germany, 2001.
[10] Mokdong Chung and Vasant Honavar, "A Negotiation Model in Agent-mediated Electronic Commerce," Proc of the IEEE International Symposium on Multimedia Software Engineering, Taipei, Dec. 2000, pp. 403-410.
[11] G.Gigerenzer et al., Simple Hueristics That Make Us Smart, Oxford University Press, New York, 1999.