창발 기반 보안 모델

Emergence-Based Security Model

고성범, 임기영
천안공업대학 전자계산과, 대전산업대학교 제어계측과
Sung-Bum Ko, Lim, Gi-Young
Department of Computer Science, Chonan National Technical College
Department of Control & Instrumentation, Taejon National University of Technology

요약

정의에 의해서, 창발적 개념은 보다 낮은 레벨의 하위 개념으로 환원될 수 없다. 따라서 해커의 입장에서 볼 때, 창발적 정보를 이면에서 훔치거나 공격하는 일은 구조적으로 어려운 일이다. 생명체는 대표적인 창발 시스템이며 생명체 패러다임으로 구축된 시스템은 보안의 관점에서 결정적인 유리함을 갖게 된다. 본 논문에서는 창발 이론에 기반한 생명체 모델 SAM을 제안한다. SAM 은 몇 가지 중요한 생명현상을 가질 수 있다. 본 논문에서는 SAM을 이용한 정보 시스템이 갖는 보안상의 특성과 유용성을 분석한다.

Ⅰ.서론

창발적 정보는 구조적으로 해킹이 어렵다. 왜냐하면 정의에 의해서 창발적 정보는 보다 낮은 레벨의 정보 개념으로 환원될 수 없기 때문이다. 창발 시스템의 하나인 인간의 두뇌도 컴퓨터와 마찬가지로 다양한 정보를 저장하고 관리하는 정보 시스템의 역할을 한다. 허지만 두뇌 시스템은 보안의 관점에서 볼 때 거의 완벽하며 두뇌 속의 정보를 해킹 한다는 것은 불가능에 가까운 일이다. 첫째로 뇌 세포 레벨에서 두뇌 시스템에 접근하는 일은 기술적으로 곤란하다. 둘째로 설사 그 일이 가능하다 해도 사람들이 사용하는 정보를 뇌 세포 레벨에서 찾아내는 일은 쉬운 일이 아니다. 셋째로 두뇌 속의 정보는 소위 자료 조작 자체가 간단치가 않다. 예를 들어, 두뇌 속의 정보를 왜곡하거나 파괴하거나 그 안에 트로이 목마를 숨겨 놓는 일 같은 전형적인 해킹 작업은 그 두뇌 당사자가 시도한다고 해도 여전히 어려운 일이다. 해킹을 방해하는 이런 속성들은 생명체가 갖는 생명 현상과 관련이 있다. 우리는 이점에 착안하여 생명체 패러다임을 따르는 정보 시스템 SAM 을 제안하였다. 우리는 SAM을 통하여 창발 기반 보안 모델의 유용성을 보여주고자 한다.

Ⅱ.창발적 관점[1][2]

본 장에서는 특히 보안이라는 측면에서 창발적 관점의 의미를 살펴보기로 한다.

[1]Global 적 관점

환원론적 패러다임에서는 전체 개념의 명료함은 부분 개념의 명료함에 근거한다. 반면 창발론적 패러다임에서는 부분은 전체(Global)를 통해서만 의미를 갖는다. 이처럼, 중요성의 축이 부분에서 전체로 이동했다는 것은 부분 전술을 사용할 수밖에 없는 해커로서는 그만큼 공격이 어려워진다는 의미가 된다.

[2]과정의 관점(비구조적 관점)

환원론적 패러다임에서의 구조는 시스템 구성의 정적인 틀이 된다. 반면 창발론적 패러다임에서는, 생명체의 진화과정에서 볼 수 있듯이, 구조 변화를 역동적인 것으로 간주한다. 생명체는 추상적으로 정의된 특별한 상태(항상성)를 유지하기 위하여 구조를 동적으로 바꿔 나간다. 구조에 대한 이러한 역동성은 해커의 공격 목표가 그만큼 불투명해진다는 의미가 된다.

[3]아날로그적 관점(근사치적 관점)

창발론적 정보들은 Global 한 관점에서는 거의 명료하고 일관된 개념을 제공할 수 있지만 Local 한 관점에서 보면 특정한 영역 내에서 역동적으로 요동하는 근사치 패턴을 보인다. 뛰어난 해커라도 아날로그 특유의 미세함을 흉내내는 일은 쉬운 일이 아닐 것이다.

[4]그물망적 관점

창발론적 패러다임에서는 뇌 세포의 예에서 보듯이

그물망적 구조를 사용한다. 그물망적 관점이 갖는 구조론적 의미는 철저한 분산 개념 즉 특별히 중요한 부분이 따로 없다는 것이다. 이러한 상황은 전체를 모두 공격할 수는 없는 해커의 입장을 곤란하게 할 것이다.

[5]인식론적 관점

창발은 논리적 귀결이 아니기 때문에 인식기를 전제하지 않을 수 없다. 즉, 다수의 개념들이 창발 공간에 뿌려지고 개념들이 창출해내는 패턴은 특정한 인식기에 의해 인식되어진다. 즉, 창발 개념 자체가 인식기에 종속적이라는 뜻이다. 이러한 '인식기 종속성'은 창발된 정보와 창발시킨 정보간의 매핑 관계를 복잡하게 만들 것이고, 해커는 공격 목표를 찾기가 곤란해질 것이다.

Ⅲ. 창발 정보 시스템[1][2]

본 장에서는 창발적 패러다임에 근거하여 만든 정보 시스템의 특징을 분석한다.

3.1 개념 정립

논의를 본격적으로 전개하기에 앞서 관련 개념들을 확실하게 정립해두고자 한다.

[정의 1] n 개의 정보들간의 상호관계에 의해서 창발된 정보를 창발 정보라고 정의하며 창발 정보를 제공하는 서버를 창발 정보 시스템이라고 정의한다.
[정의 2]정의1 에서 n이 무한대 값을 갖는 경우 이 시스템을 '이상적인 창발 정보 시스템' 이라고 정의한다.
[정의 3]창발 정보 시스템에 대한 해킹 효과는 r 로 표시하며 r 은 0.0 에서 1.0 사이 값을 갖는다.
[정의 4]창발 정보 시스템에서 일관성의 기준이 주어질 때, 그 값에 대응하는 n 값을 '창발 경계값' 이라고 정의한다.

창발 정보 시스템이 정상적인 서비스를 제공하려면 시스템 규모에 있어서 최소한 창발 경계값 이상의 n 값을 유지해야 할 것이다.

[공리 1]해커가 창발 정보 시스템을 공격할 때, 공격 대상이 되는 정보 집합의 크기 m 값은 유한하다.
[공리 2]해킹 효과 r 값은 m/n 에 대하여 단조 증가 관계에 있다. 단, m/n=0 에서 r=0 이고 m/n=1 에서 r=1.0 이다.

공리 2 와 관련하여 m/n 에 대한 해킹 효과는 일반적으로 비선형이다. 그 이유는 창발된 정보는 아날로그 적인 데 반해, 고객에게 제공되는 최종 정보는 일반적으로 디지털 적이기 때문이다.

[정리 1]창발 정보 시스템에서는 그것을 공격할 때 해킹 효과(r>0)를 얻을 수 있는 최소한의 m(단, m < n) 값이 존재한다. 이 m 값을 '해킹 경계값' 이라고 정의한다.
<증명> 공리 2 에 의해 m = 0 인 경우 해킹 효과 r 값은 0 이다. m 이 증가함에 따라 r 값은 단조 증가하며 n=m 인 경우 최대 값 1.0 에 이르게 된다. 따라서 해킹 효과 r 값이 0 이상의 값을 갖게되는 m 값이 반드시 존재해야 한다.

[정리 2]이상적인 창발 정보 시스템은 해킹이 구조적으로 불가능하다.
<증명> 이상적인 창발 정보 시스템의 경우 정의 2 에 의해 n 값은 무한하다. 또한 공리 1 에 의해 m 값은 유한하므로 m/n=0 이 된다. 공리 2 에 의해서 m/n=0 이면 해킹 효과 r 값도 0 이 된다.

3.2 창발 정보 시스템의 특성 실험

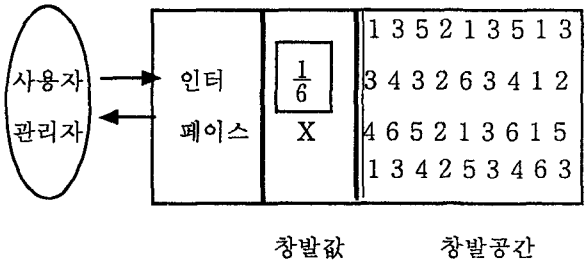

그림 3.1 창발 정보 시스템

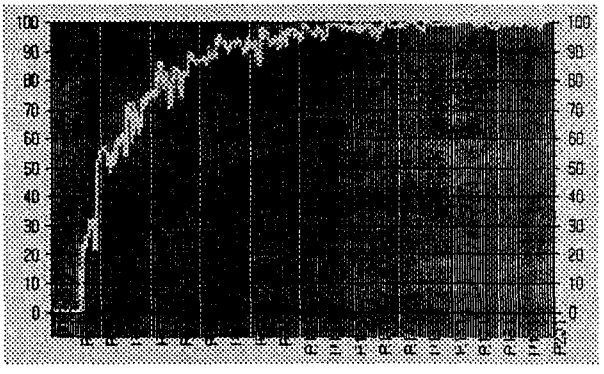

그림 3.2 창발 경계 값 측정

그림 3.1 은 창발 정보 시스템의 예이다. 이 정보 시스템은 고객에게 변수 X 값으로 1/6 을 제공한다. 창

발 공간은 n 개의 난수 값(1 에서 6 사이의 정수)으로 채워진다. n 개의 정수 집합에서 1 이 차지하는 비율이 구해지고 그 비율은 {k/6| k=0,1..,6} 중에서 가장 가까운 원소 값으로 바뀐다. 그림 3.2 는 n 을 변경하면서 정보 시스템의 효율을 측정한 결과이다. 여기서 서비스 값 1/6 에 대한 일관성을 효율 0.98 로 가정할 때 창발 경계값은 160 이 된다. 한편 상기의 창발 경계값(n=160) 조건에서 해킹 유형에 따른 해킹 경계값을 측정한 결과는 다음과 같다.

공격 유형	해킹 경계 값
훔치기	48(효율 0.8)
왜곡하기	16
파괴하기	16

즉, 해커는 160 개의 정보 중 최소한 16 개 이상을 파괴해야 해킹 효과를 얻어낼 수 있다. n 의 증가에 대하여 해킹 경계값은 훨씬 빠르게 증가한다. 예를 들어, n이 두 배로 증가하면 공격해야 할 대상은 거의 4 배인 63 개로 증가한다. 상기 예와는 달리, 보통은 왜곡하기와 파괴하기의 해킹경계 값은 서로 다르다.

Ⅳ. 생명체 및 생태계 모델[1][2][3]

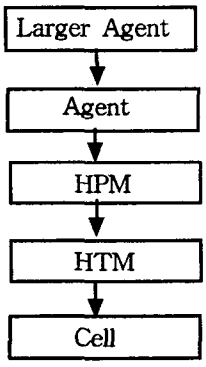

그림 4.1 인터넷 생태계 먹이 사슬

본 논문에서 제안하는 생태계 모델은 세 가지 기본 개념에 의존한다. 첫째는 가상 생명체가 살아가는 환경으로서의 인터넷, 둘째는 가상' 생명체를 구성하는 자원으로서의 컴퓨터와 액튜에이터 그리고 셋째는 가상 생명체 구현 메카니즘으로서의 생명체 모델이다. 우리가 고려하는 생명체 모형은 Cell, HTM, HPM, Agent 등 네 가지이다. 인터넷 생태계 관점에서 볼 때 먹이사슬의 가장 밑에는 Cell 이 존재한다. HTM 은 Cell 로 구성된 Support 위에서 정의된다. 이들은 고객의 요구를 Cell 수준으로 아웃소싱해서 먹고산다. 한편 HPM 은 학습이 가능하며 다른 HPM 과의 연합체를 구성할 수도 있고 필요하면 Agent 에 기생할 수도 있다. Agent 는 HTM 을 먹고산다. Agent 에게 잡아먹힌 HTM 들은 분해되고 소화되어 TM을 만드는 영양소가 된다. 한편 Agent 들이 모여서 보다 높은 레벨의 Agent를 구성할 수 있다. 이 경우 Agent 는 새로운 Agent 에 대해서는 TM 의 기능을 갖는다. 약육강식의 원리에 따라 Agent 는 보다 큰 Agent 의 먹이가 될 수 있다. 모든 생명체의 사체는 다른 생명체의 먹이가 되거나 분해되어 Cell 숲으로 환원된다.

Ⅴ. 생명체 모델에서의 보안

생명체 모델은 창발 모델의 속성들을 계승하지만 생명체 모델 고유의 특징들을 갖고 있다. 본 장에서는 특히 보안의 관점에서 생명체 모델을 분석한다.

5.1 생명체 모델에서의 자료 관리

일반적인 정보 시스템에서는 관리 모드가 지원되며 허가 받은 관리자는 일마든지 정보를 입력하고, 삭제하고 수정할 수 있다. 그러나 두뇌와 같은 창발적 정보 시스템의 경우는 자료 조작에 관한 한, 어느 것 한 가지도 쉽지 않다. 본 절에서는 Agent 개념을 이용해서 SAM 모델에서의 정보 조작 방법을 설명한다.

1.입력(Insert)

Agent 에게 특정한 정보를 입력시키기 위해서는 두 가지 단계가 필요하다. 첫째로 해당 정보를 갖는 이상적인 HPM을 제작해서 Agent 에게 제공한다. 둘째로 Agent 에게 그 정보를 반복적으로 요구한다. 그러면 Agent 는 제시된 HPM 에 대해서 식욕을 느끼게 되고 결국 그것을 먹게 될 것이다. 이 과정은 생명체 모델에서 약물 섭취 과정에 해당한다. 섭취된 HPM 은 소화 과정을 거쳐서 하나의 PM으로 자리 잡게된다.

2.수정(Modify)

Agent 가 갖고 있는 정보를 수정하는 일은 쉽지 않다. 일단 HPM을 이용하는 것은 좋은 방법이 아니다. Agent 는 HPM을 먹지 않으려 할 것이고 설사 다른 음식에 몰래 섞어 먹인다 해도 토해버릴 것이다. 왜냐하면 기존의 Belief 체계가 이질적인 정보에 거부 반응을 보일 것이기 때문이다. 따라서 이 경우는 정보를 HTM으로 만들어 먹여야 한다. HTM 은 특성 함수 값이 아주 작기 때문에 기존의 Belief 체계에 반하는 정보가 있어도 Agent 는 거부 반응을 보이지 않게 된

다. 그 다음, 새로운 정보에 대하여 집중적인 보상효과를 주는 Task를 연속적으로 맡긴다. 그러면 기존의 정보는 점점 약화되고 새로운 정보는 점점 강화되어 결국 기존의 정보는 새로운 정보로 바뀌게 될 것이다.

3.삭제(Delete)

Agent 가 소유하고 있는 정보를 당장에 삭제하는 명쾌한 방법은 없다. 가장 자연스러운 방법은 그 정보를 사용하지 않는 것이다. 그러면 PM 들의 학습 능력에 의해 서서히 그 정보의 가치가 소멸되어갈 것이다. 그러나 엄청난 숫자의 PM 들 모두가 그 정보를 완전하게 잊어주길 기대할 수는 없을 것이다. 왜냐하면 PM 은 자율성으로 인해 PM 들의 학습 메카니즘이 획일화되지 않기 때문이다. 이것은 인간의 경우도 마찬가지이다. 예를 들어 한번 각인된 불쾌한 추억은 아무리 시간이 흘러도 그 잔재가 남는 법이다.

5.2 해커의 공격과 SAM 의 방어

해커의 전형적인 공격 유형은 찾기, 훔치기, 파괴하기, 왜곡하기, 트로이목마 숨기기 등 대략 다섯 가지로 분류할 수 있을 것이다. 본 절에서는 각각의 행동이 SAM에 의해서 어떻게 저지되는지를 살펴본다.

[1]찾기(Find)

SAM 모델에서 Agent 레벨의 특정 정보는 n 개의 PM 들이 갖는 정보의 상호 관계에 의해서 창발 된다. 이때 n 은 일반적으로 큰 값을 갖는다. 더구나 창발된 정보에 대한 각각의 PM 들이 갖는 비중은 별로 차이를 보이지 않는다. PM 들은 기본적으로 자율적이어서 하나의 PM 정보는 다른 PM 들을 추적하는 일에 도움이 되지 못한다. 이처럼 뇌 세포와 비슷한 PM 들의 구조는 해커의 '공격 대상 찾기' 를 어렵게 할 것이다.

[2]훔치기(Steal)

SAM 모델은 대단히 동적인 특징을 갖기 때문에 비록 창발적 정보 자체의 일관성은 유지된다 할 지라도 그것을 창발시키는 n 개의 정보들은 수시로 변화하게 마련이다. 만일 해커가 어떻게든 이면 접근에 성공해서 하위 레벨의 특정 정보를 훔치는 데 성공하였다 해도 그 다음 순간 그 정보는 무의미한 정보가 되기 십상이다. 왜냐하면 하나의 패턴을 구성하는 데 사용되어진 정보는 다른 패턴 속에서는 아무런 역할을 하지 못할 것이기 때문이다.

[3]파괴하기(Destroy)

SAM 모델에서 정보 S를 창발해 내는 n 개의 정보분포는 성능 관점에서 정규 분포를 이룬다. 해커의 공격 목표는 당연히 최대 값을 갖는 PM 일 것이다. 그러나 그 PM 이 파괴되어 버린다해도 정규 분포의 속성상 창발된 정보가 크게 손상을 입지는 않는다. 더구나 파괴된 정규분포 부분은 SAM 모델 고유의 학습 기능에 의해 순식간에 메워져 버릴 것이다.

[4]왜곡하기(Distort)

SAM 모델에서 PM 들은 포텐셜을 교환하는 방법으로 애정과 갈등을 표현한다. 이를 감성 계층이라고 부른다. 해커가 정보를 왜곡시키는 데 성공하였다고 해도 그 왜곡된 정보가 시스템에 유의미한 피해를 주는 것이라면 그 효과는 지속되지 못한다. 왜냐하면 왜곡된 정보에 의해 창발된 정보의 평가 값이 떨어지게 되는 경우 그런 원인을 제공한 PM 은 집중적인 견제를 당할 것이기 때문이다. 이는 창발 현상에 대한 PM 들의 참여도가 공개되기 때문에 일어나는 일이다.

[5]트로이목마(Trojan Horses)

SAM 모델에서 PM 은 하나의 생명체로 유한한 수명을 갖는다. 즉, PM 은 태어나서 성장하고 늙어간다. 그리고 수명이 다하면 죽는다. 해커나 PM 속에 트로이 목마를 숨겨 놓는 데 성공한다 해도 그렇게 큰 의미는 없을 것이다. 결국 PM 은 늙어 죽을 것이며 따라서 트로이 목마도 함께 사라져갈 것이기 때문이다.

Ⅵ.결론

본 논문에서는 창발 이론에 근거한 생명체 모델 SAM을 제안하고 특히 보안의 관점에서 시스템 특성을 조사하였다. 우리의 결론은 다음과 같다. 즉, 정보 시스템을 SAM 과 같은 생명체 패러다임으로 구축하는 경우 보안의 관점에서 결정적인 이점을 얻을 수 있다. 즉, 보안 시스템을 따로 도입하지 않아도 창발적 시스템 자체가 해커의 공격을 어렵게 만든다는 것이다. 다만 생명체 패러다임은 자료 조작상의 어려움이라는 대가를 지불해야 한다. 설사 이런 단점을 감안한다 해도 응용 분야에 따라서는 보안상 유의미한 솔루션이 될 수 있다는 것이 우리의 주장이다.

참고문헌

[1]Sung-Bum Ko, Gi-Young Lim "The development of EBO System as a Life", Proceedings of KFIS Fall Conference, 295-306, 1999.

[2]고성범, "생태계로서의 인터넷", 한국생물공학회 춘계 학술 발표, S306, 2000.