제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

Branch Instruction Trace Profiling Tool의 효과적인 가시적 방법

양수현, 김현우, 송은하, 정영식
원광대학교 컴퓨터공학과
e-mail : shyang@wku.ac.kr

Effective Visual Method for Branch Instruction Trace Profiling Tool

Su-Hyun Yang, Hyun-Woo Kim, Eun-Ha Song, Young-Sik Jeong
Dept. of Computer Engineering, Wonkwang University

요 약

최근 지식 정보화 사회에 있어서 컴퓨터 네트워크 개방화와 함께 컴퓨터 시스템의 보안 위협이 급증하였다. 또한 기본적으로 데이터 보호에 초점을 맞추고 있기 때문에 접근에 대한 제한이 없으며 응용 프로그램에 따라 보안 운영방식이 다르다는 취약점을 가지고 있다. 본 논문은 하드웨어 기반 보안상태 모니터링 가시화를 위하여 TCG에서 제안한 TPM 칩을 기반으로 동작하는 컴퓨팅 환경의 신뢰 상태 및 시스템 자원에 대한 상태 정보를 실시간으로 모니터링하고 분기 추적 모니터링을 통해 논리적 에러의 초기위치를 파악하여 가시화한다.

1. 서론

최근 컴퓨터 시스템의 보안 위협이 급증하고 점점 더 다양한 해킹 공격이 늘어나면서 기존 소프트웨어적 보안 취약점에 대한 공격이 기하급수 적으로 증가하고 있다. 이를 방지하기 위한 운영체제나 소프트웨어의 끊임없는 보안 패치는 필수 요소로 여겨지고 있다. 시스템에 구축된 방화벽을 뚫고 들어간 웜이나 스파이웨어를 통해 사용자의 키 입력을 직접 얻어오거나, 암호화된 패스워드나 페어 키를 가져와서 암호를 해제하고 악의적으로 사용하는 등 기존에 안전하다고 인식되었던 소프트웨어적인 보안 방식의 허점이 노출되고 있다.

하드웨어 기반 보안 기술들은 대부분 암호학적 이론에 근거한 알고리즘 및 프로토콜에 기반을 두고 동작되기 때문에 단말 인식 및 인증 기법, 암호학적 프리미티브에 대한 안전성 보장 기법 등에 관한 연구 방향으로 꾸준히 진행되고 있다. 이중에서 하드웨어를 이용하여 암호학적 프리미티브를 물리적으로 보호하는 기술들은 현재까지 가장 안전한 기술로 여겨지고 있다. 여기에 해당되는 대표적인 상용기술로 TCG(Trusted Computing Group)의 TPM(Trusted Platform Module)이 있다[1].

TPM은 신뢰 플랫폼을 구현하기 위한 핵심 기술로써 디바이스에 대한 식별 및 신용 정보를 별도의 하드웨어 모듈로 관리한다. 또한 최근 벤더들의 TPM칩 도입으로 IT시장에서 빠르게 보편화 되고 있으며 TPM칩을 이용한 하드웨어적 보안은 필수요소로 자리 잡고 있다[2-4].

그러나 현재까지 TPM을 기반으로 동작하는 PC의 보안 상태를 실시간으로 모니터링하기 위한 기술은 전무하다. 이에 본 논문은 웹을 기반으로 하여 시간과 장소에 구애받지 않고 실시간으로 특정 디바이스에 대한 신뢰상태와 자원상태를 모니터링하는 BiT Monitor를 제안함으로써 기존 보안의 취약점 해소와 하드웨어 보안을 기반으로 동작하는 PC에 대한 상태 모니터링을 지원하는 시스템 개발을 목적으로 한다.

2. BiT Profiling 기법

기존의 소프트웨어 관점에서의 보안은 이미 알려진 공격 패턴이나 방식에 대해서만 대처가 가능하고 새로운 공격에 대해서는 무기력하다. 또한 기존의 소프트웨어 수준에서의 보안은 시간의 지연과 성능 저하를 야기하는 문제점을 가지고 있다. 따라서 최근 하드웨어 관점에서의 보안 방법으로 Low level에 protection을 위치시킴으로써 좀 더 광범위한 영역 보호와 Architectural support를 통한 성능 저하의 문제점 해결을 기대할 수 있다.

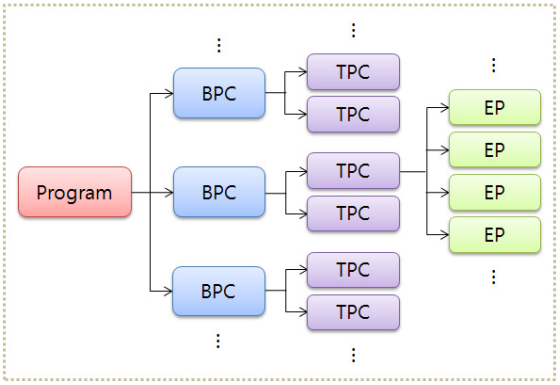
BiT(Branch Instruction Trace Profiling Tool)[5]의 Motivation으로는 공격이 어떻게 구현되든 간에 malicious execution trace가 명령어 레벨에서는 확인될 수 있다는 점과 프로그램 실행 시 명령 레벨의 행위는 시스템 모듈의 동작에 의해 영향을 받는다는 점이다. 또한 프로그램의

+ 본 연구는 지식경제부 및 한국산업기술평가관리원의 IT산업원천기술개발사업의 일환으로 수행하였음. [2011-KI002090, 신뢰성 컴퓨팅 (Trustworthy Computing) 기반 기술 개발]

실행 시간 동작으로부터 시스템 상태 안전은 분석될 수 있다.

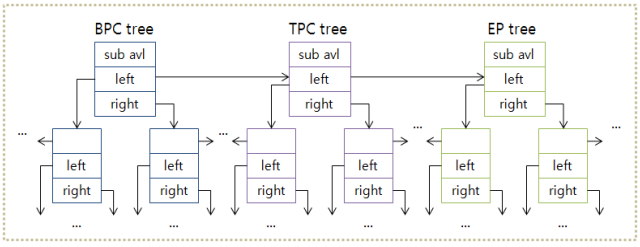
BiT는 기존의 CFA와는 다르게 control data뿐만 아니라 실행 경로까지 프로파일링 하며 계층적 구조를 통해 간접 분기와 그와 연관된 조건부 분기들의 정보를 계층적으로 보관하는 특징을 가지고 있다. 일반적으로 공격은 타겟 어드레스, PC 어드레스에 대한 참조를 우회한다. 그러나 이 두 가지를 결합함으로써 공격은 결합된 어드레스를 수정하지 않고는 변형을 시도할 수 없다. 따라서 BiT의 계층적 보관은 분기 추적을 위해 긴밀한 관계에 있으며 결과적으로 프로그램의 분기 명령 추적을 통한 논리적 에러의 초기 위치 파악으로 능동적인 대처가 가능하다.

BiT는 명령 추적을 모니터링하고, 처리에 대해 각각의 간접 분기와 관련된 조건부 분기를 선택한다. 각각의 간접 분기를 위한 여러 기준은 보안상 목적을 위해 정의되고 있다. BPC(Branch Program Counter)는 간접 분기 명령의 선형주소이고, TPC(Target Program Counter)는 BPC 값에 의해 색인된 간접 분기의 타겟 명령어 주소이다. EP(Execution Path)는 BPC값에 의해 색인된 간접 분기로 이어지는 조건 분기의 연속적인 결과(True or false)로 정의된다.



(그림 1) BiT의 구조

한 프로그램은 여러 개의 간접 분기(다수의 BPC)를 포함하고 있다. 이 간접 분기는 프로그램 실행에 따라 다른 실행 경로를 따른다. 즉 각 BPC에 다수의 TPC가 포함되는 것이 가능하다. 또한 간접 분기 타겟으로부터 다수의 조건 분기가 발생(EP)한다.

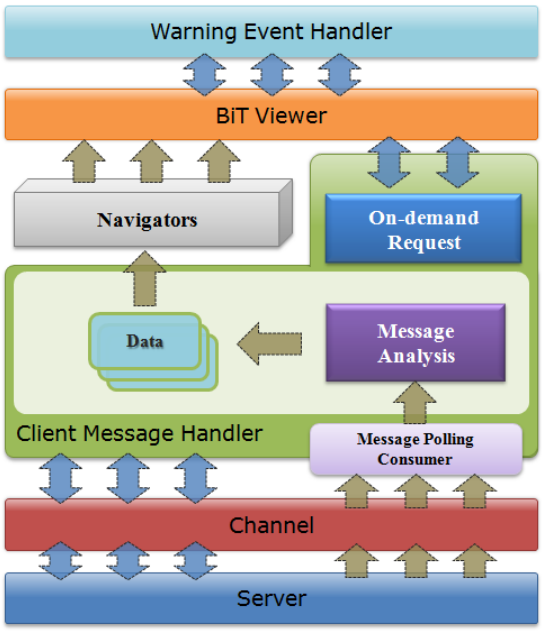


(그림 2) Signature table의 계층적 구조

대부분의 공격은 고유 분기주소 또는 타겟 위치를 유지하며 우회하지만 계층적 구조는 필연적으로 변경된다는 특징이 있으며, BiT는 BPC, TPC, EP가 상호 연관관계에 있으므로 해쉬 테이블은 (그림 2)와 같이 이러한 계층적 구조를 잘 표현할 수 있어야 한다.

3. BiT Monitor 설계

(그림 3)은 BiT Monitor의 전체적인 구조이다. Channel을 통해 서버와 통신을 하며 수집된 정보를 Viewer에서 보여준다. BiT Monitor는 모니터링 정보를 수집하기 위한 Client Message Handler와 가시화 뷰를 구성하는 BiT Viewer, 메시지 정보와 개체 정보를 분석하는 Analysis, Handler와 Viewer 사이에서 분석된 정보를 처리하는 Navigators 그리고 신뢰되지 못한 상태에 대해 경고를 알려주는 Warning Event Handler로 구성된다. Navigator는 Handler에서 올라온 정보를 모니터링하기 위해 정보를 분석하고 Viewer로 연결한다.

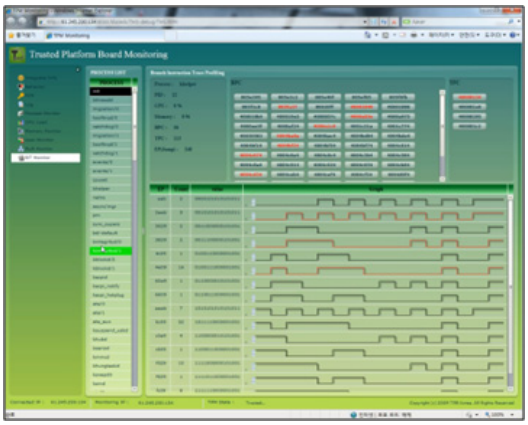


(그림 3) BiT Monitor의 구조

4. BiT Monitor 가시화 및 구현

(그림 4)는 BiT Monitor의 실행 화면이다. 왼쪽에서 Program을 선택하면 오른쪽 상단에 BPC의 리스트가 뜨고, 오른쪽 하단에는 선택된 Program을 중심으로 BPC들이 가지치기 형태로 나타나게 된다. 가지치기 형태로 나타난 BPC들을 선택하게 되면 마찬가지로 선택된 BPC를 중심으로 TPC들이 나타나게 된다.

(그림 5)는 BiT 추적 결과 화면으로 각 BPC, TPC, EP의 추적을 통해 논리적 에러의 초기 위치를 찾기 위한 모니터링이다. 상단에 각 BPC, TPC의 정보를 제공하고 하단에는 EP의 전체 결과를 제공한다. 논리적 에러의 초기 지점을 찾기 위해 해당 EP를 붉은색으로 표시하였다.



(그림 4) BiT Monitor의 실행 화면

(그림 5) BiT Monitor의 실행 화면

5. 결론

본 논문은 하드웨어 관점의 보안을 목적으로 연구, 개발된 TPM(Trusted Platform Module)칩이 탑재된 보드를 통해 접근 자체에 제한을 두고, 신뢰상태에 대한 상황을 실시간으로 모니터링하기 위한 것을 목적으로 하고 있다. BiT Monitor는 프로그램의 PC, TPC, EP의 추적을 통해 논리적 에러의 초기 위치 파악이 가능하고 그에 따라 능동적인 대처가 가능하며 웹을 기반으로 하는 모니터링 시스템을 제공함으로써 시간과 장소에 구애받지 않고 특정 디바이스를 모니터링 할 수 있다.

향후 프로그램 카운터 인코딩 컴파일러를 이용하여 응용 프로그램의 신뢰성을 강화하고, 단일 컴퓨팅을 비롯하여 모바일 및 클라우드 컴퓨팅 환경을 위한 다양한 신뢰성 기반 서비스를 제공하기 위한 연구를 하고자 한다.

참고문헌

[1] Trusted Computing Group Web Site, http://www.trusted computinggroup.org/home

[2] Trusted Platform Module Work Group Web Site, http://www.trustedcomputinggroup.org/groups/tpm/

[3] Steven L. Kinney, “Trusted Platform Module Basics Using TPM in Embedded System”, pp. 53-64, Aug. 2006

[4] David Challener, “A Practical Guide to Trusted Computing”, Dec. 2007

[5] Home page of BiT the Branch Instruction Trace Profiling tool.[online]. Available, http://arch.ece.uic.edue/BiT/index.htm