한국정밀공학회 2006년도 춘계학술대회논문집 pp. 417~418 KSPE 06S318

CAA를 이용한 CATIA V5 파일보안시스템 개발에 관한 연구

채희창*, 박두섭, 변재홍 (전북대 대학원 기계설계학과)

A study on development of CATIA V5 file security system using CAA

H. C. Chae, D. S. Park, J. H. Byun (Mech. Eng. Dept., CBU)

ABSTRACT

CATIA V5 is one of the most preferred softwares in product design for domestic and industrial use. But with the development of the IT industry, design data by CATIA V5 can easily be hacked and stolen especially via the internet and through assistance storage medium. The design data could be protected through executive, physical and technical security system. The best way to maintain confidentiality of data from unauthorized access is to have a cryptosystem of the technical security. In this paper, a cryptosystem for the protection of design data was being proposed.

The memory contains the file information made by the New and Open function of CATIA V5. No error can be expected even if the file changed before of after the application of Save and Open function, A cryptosystem was constructed in CATIA V5 by inserting crypto algorithm before and after the I/O process. The encryption/decryption algorithm of each function was based on the complex cipher, which applied permutation cipher and transpose cipher. The file security system was programmed in CAA V5 and Visual C++.

Key Words : CAA V5, Encryption (암호), Decryption (복호)

1. 서론

자동차 또는 항공기 업체와 같은 대형 제조업체들에서부터 중견기업에 이르기까지, 거의 모든 산업부문에서 생산되는 제품들이 CATIA를 통해 설계 및 제조되고 있다. 국외는 Boeing, Chrysler, BMW, Sony, Toyota 등과 국내는 현대/기아, 대우, 삼성, 삼립산업, 만도, 금호/한국 타이어 등이 CATIA 시스템이 설치되어 활용중이다. 그렇지만 Window/Unix를 바탕으로 CATIA V5가 설치된 수많은 컴퓨터들이 인터넷으로 상호 연결되어 정보의 공유가 가능해짐에 따라 외부인의 무단 자료 유출 가능성은 항상 내재되어 있으며 자료 보관을 목적으로 하는 보조기억매체에 의한 자료 유출 가능성은 더욱 가중되고 있다. 현재 CATIA V5 파일은 제도적, 행정적인 보호대책과 물리적인 보호대책을 사용하여 보호되고 있지만 혹시라도 자료가 유출되었을 경우 CATIA V5 또는 뷰어(Viewer)가 설치된 어느 장치에서든지 열고 정보를 빼낼 수 있기 때문에 이는 완벽한 대책이 아님에는 틀림이 없다. 이에 우연한 노출로부터 자료의 비밀성을 보장하는 가장 좋은 방법은 CATIA V5를 위한 암호시스템을 갖추는 것이라 하겠다.[11]

본 연구에서는 CATIA V5 파일의 최종 보호수단은 데이터 자체를 암호화하여 보관하는 것이라는 점에 착안, 소프트웨어 CAA(Component Application Architecture) V5와 Visual C++를 사용하여 암호시스템을 CATIA V5 자체에 구현함으로써 사용자가 암호시스템에 신경 쓸 필요 없이 원하는 데이터를 암복호화 되게 하는 파일보안시스템을 개발하고자 한다.

2. CAA V5 및 암호알고리즘

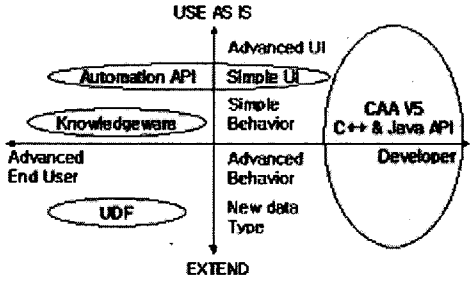

Fig. 1 CAA V5 Positioning

CAA V5는 CATIA, DELMIA, Deneb, CATweb 및 ENOVIA와 같은 다쏘시스템(Dassault Systems)사에서 개발된 모든 제품 라인에 대한 공통적인 애플리케이션 아키텍처로써 CATIA V5를 개발자가 원하는 방향으로 사용자정의(Customize) 할 수 있는 도구이다.[5] 이는 CATIA V5 자체에 일정 암호알고리즘을 거친 임의의 파일이 암복호화 되게 하는 암호시스템을 포함시킬 수 있음을 .의미한다. 파일보안시스템 개발에 사용된 암호화 방법은 대칭 암호화 방법의 종류인 치환암호(Permulation cipher)와 전치암호(Transpose cipher)를 응용한 암호를 사용하였다.

3. 보안시스템의 구현

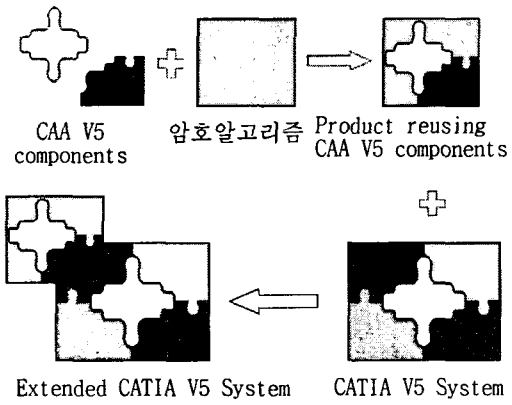

Fig 2 Security system construct

CAA V5에서 암호시스템이 CATIA V5에 삽입될 수 있는데 필요한 Components를 호출하여 원래의 (Original) CATIA V5 시스템에는 없는 새로운 기능 (Security Open, Security Save, Security Save As, Security Save All)을 추가하면 확장된(Extended) CATIA V5시스템이 된다. 새로운 기능을 추가하기 위해서는 CATIA V5에서 Save와 Open할 때 파일에 관한 정보가 관리되는 위치와 호출되는 함수를 알아야 한다. 이는 Save와 Open의 이벤트를 실행할 때 적절한 CAA V5의 Components를 호출하여 암호알고리즘을 적용해야 하기 때문이다.

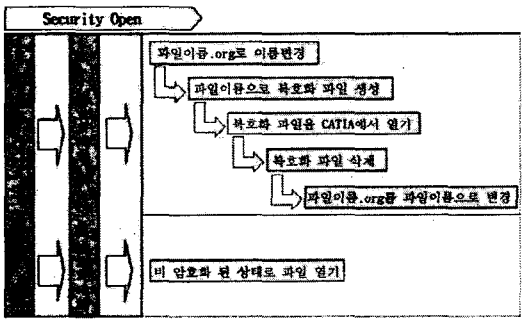

Fig 3 Algorithm of security open

암호시스템 설계에서 가장 핵심은 CATIA V5에서는 New에 의해 생성된 파일 또는 기존에 생성되어진 파일을 열기할 경우도 파일의 모든 정보가 메모리에서 관리된다는 것이다. 이는 CATIA V5에서 사용하고 있는 모든 파일의 정보는 메모리 상에 존재한다는 말이 되고, 만약 Save와 Open하기 전과 후에 파일(기존파일, 새로 만든 파일)을 조작하여도 오류가 나지 않는다. 암호시스템은 이 특성을 이용하여 임의의 파일을 저장과 열기할 때 각 이벤트 전후에 임의의 조작을 하여 암복호화 되도록 하였다.

4. 결론

본 연구는 현재 산업 현장에서 IT분야의 급속한 발달로 인하여 모든 산업의 데이터를 컴퓨터를 이용하여 처리, 관리, 전달하는 상황에서 그로 인해 발생되는 CATIA V5의 데이터파일 유출 및 도난 등의 예상 위험에서 데이터의 최종보호 수단은 파일자체를 암호화하여 보관하는 것이라는 점에 착안하여 사용자가 CATIA V5에서 임의의 파일을 로컬 디렉토리(Local Directory) 또는 파일서버(File Server)에 저장과 열기할 때 자동으로 암복호화 되도록 하는 파일보안 시스템을 개발하는 연구를 수행하였다. 암호시스템 개발에는 CATIA V5의 개발 API인 CAA V5, Visual C++과 암호알고리즘을 사용하였고 CATIA V5 자체에 개발된 보안기능을 편리하게 사용할 수 있도록 각 커맨드(Command)와 링크된 아이콘들을 포함한 툴바를 삽입하였다.

차후 연구로는, 현재 보안시스템은 관리자형으로써 보안기능 뿐만 아니라 기존의 CATIA V5에 있는 저장과 열기 기능이 아직도 메뉴의 풀다운(Pull-Down)과 기존툴바 안에도 존재하고 있어 사용자가 파일암호의 유무를 결정할 수 있다. 따라서 CATIA V5를 원래에 있는 저장과 열기 기능을 없애거나 기존기능을 보안기능으로 대체를 시켜 파일유출 가능성이 없는 사용자형을 만들어 향후 파일보안 시스템을 관리자형과 사용자형으로 구분하는 연구를 수행하고자 한다.

참고문헌

1. Douglas R. Stinson, "Crytography-Theory and Practice.", CRC Press, Inc., 1995
2. Alfres J. Menezes, Paul C.vaz Corschot, Scott A. Vanstrone, "Handbook of applied Cryptography.", CRC Press, 1997
3. Neal Koblitz, "Algebraic aspects of cryptography.", Kluwer Academic Publishers, 2000
4. William Stallings, Network and Internetwork Security, IEEE Press, 1995
5. Dassault Systems, CAA V5 Encyclopedia
6. Advanced Computer Aided Design User's Manual
7. 이임영, 송유진, "현대암호", 생능출판사, 1997
8. 박창섭, "암호이론과 보안", 대영사, 1999
9. 이민섭, "현대암호학", 교우사, 2001
10. 원동호, "현대암호학", 그린, 2003
11. 데이터파일의 보호를 위한 스트림 암호방식 설계와 해석, 한국 콘텐츠학회 2004년 춘계학술 발표회, 2004
12. 심정욱, 김진형, 황호연, 전경진, "항공기 형상 설계에서의 GUI 환경 구축 및 형상 데이터 추출을 위한 CAA V5의 활용", 항공우주학회 2001년 추계학술 발표회, 2001