프로그램 보안 솔루션 **MEGALOCK**

USB-C Type

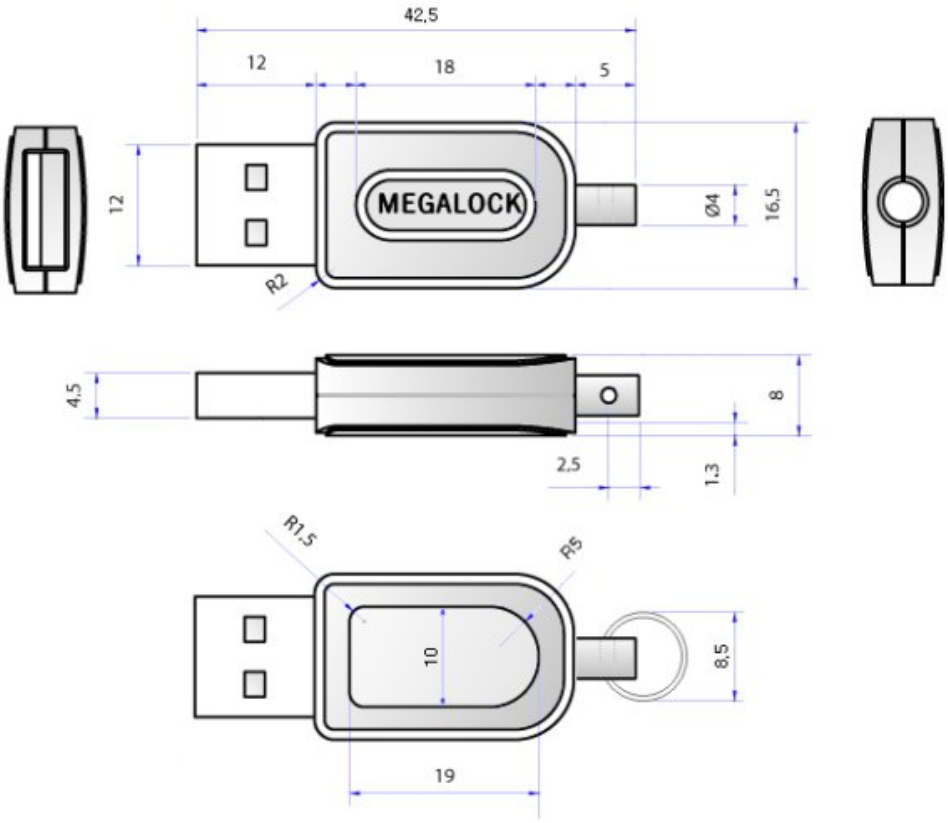
> 제품 개요

메가락은 한도컴퓨터에서 자체 개발한 강력한 불법복제 방지장치로서 USB 포트에 연결하는 일종의 보안키입니다. 응용프로그램에서 메가락의 기능을 체크하여 락이 없으면 프로그램 실행을 할 수 없도록 함으로써 프로그램의 불법 사용을 방지할 수 있습니다.

> 제품 상세설명

- 사용 용도 : Microsoft Windows 응용 프로그램용 보안키 또는 인터넷 인증키로 사용
- 사용 환경 : Win98SE~Window10(x32, x64)
- 운용 방식 : USB Version 1.1 Low Speed
- 장치드라이브 : 운영체제 내에 포함된 HID 드라이브 사용
- 장치 등록 : Plug and Play 방식으로 연결과 동시에 사용가능
- 메모리 사이즈 : 보급형 50Byte, 플러스형 50Byte + 2KByte
- 작동전압범위 : 4.75~5.25V
- 소모전류 : 50mA 미만
- 사용온도범위 : 0℃~70℃

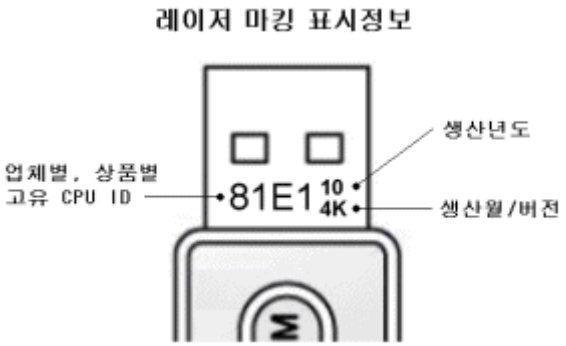
> 제품치수



> 레이저마킹

메가락은 내부 펌웨어가 업체마다 모두 다르게 생산되는 주문형 보안키이지만, 겉으로 드러나는 외형은 모두 동일한 형태라 이를 구분하기 위해 USB 컨넥터의 금속 부분에 업체별, 제품별 고유 CPU ID, 제조일, 버전이 마킹되어 출고됩니다.

출고되는 제품에 대해 전량 마킹 함으로써 위변조된 제품이 존재하기 어려우며, 부착된 스티커가 훼손되거나, 락이 고장난 경우에도 정품 확인을 하는데 큰 도움을 줄 것입니다.



> 함수 설명

unsigned int lock_init_usb(8);

프로그램 실행시 최초에 USB 메가락을 탐색하는 함수입니다.

결과값: 탐색된 메가락의 USB ID 0x81E1 값이 돌아오면 메가락 연결된 상태입니다.

CPU ID 81E1은 샘플락이 갖는 고유 ID입니다. 메가락을 정식 주문하시면 고정된 CPU ID를 부여해 드립니다.

unsigned char lock_check(0);

연결된 메가락과 직접적인 통신을 하면서, 메가락의 연결 유무를 가장 빠르고 간단하게 체크하는 함수입니다.

결과값: 0이면 연결 상태이고, 0 이외의 값은 통신오류 또는 연결해제 상태입니다.

unsigned char lock_version();

메가락의 펌웨어 버전을 읽어옵니다.

unsigned char lock_sn(0);~lock_sn(3);

메가락이 갖는 고유번호 4자리 값을 얻어옵니다.

모든 락은 각각의 고유번호가 있는데 그 값을 얻어오는 것입니다.

unsigned char lock_write(주소, 데이타);

기본 메모리 영역에 데이터를 기록합니다.

메모리 번지 0~50번지까지 사용할 수 있습니다. 데이터 값은 0~255 범위

주의:메모리 번지 58번지는 기본 메모리에 대한 쓰기 방지 시그널 영역이므로 기록범위가 넘지 않도록 주의하세요. 58번지의 데이터 값이 48(0x30)인 경우에만 쓰기가 가능합니다.

unsigned char lock_read(주소);

lock_write 함수로 기록한 값을 읽어옵니다.

int lock_write_ex(주소, 데이타);

확장 데이터 영역에 데이터를 기록합니다.

메모리번지 0~1024까지 사용할 수 있습니다. 데이터 값은 0~65535 범위

int lock_read_ex(주소);

lock_write_ex 함수로 기록한 값을 읽어옵니다.

void lock_write_enable(48);

확장 데이터 영역에 대해 쓰기 방지를 해제하거나, 설정합니다.

입력값이 48인 경우 쓰기 가능한 상태로 바뀌고, 이외의 값은 쓰기 불가능한 상태로 됩니다.

BOOL lock_receive(void);

USB와의 통신 중에 오류 여부를 확인하는 함수입니다.

Lock_read 함수 또는 lock_write 함수를 호출하여 결과값을 받은 다음 lock_receive 함수를 호출했을 때 FALSE이면 lock_read로 읽은 결과값을 오류 처리해야 합니다.

즉, 데이터 읽기를 할 때 데이터 값이 0인지 락이 제거되거나 오류가 생겨서 0인지를 구분하기 위해 이 함수를 사용합니다.

※ 데이터 영역 쓰기 방지 기능의 구분

- 기본 데이터영역 쓰기가능: lock_write(58,48);
- 기본 데이터영역 쓰기금지: lock_write(58,0);
- 확장 데이터영역 쓰기가능: lock_write_enable(48);
- 확장 데이터영역 쓰기금지: lock_write_enable(0);

※ 언급된 함수 이외의 함수는 패러럴용 메가락 관련함수이거나 더 이상 사용되지 않는 함수입니다.

> MFC 프로젝트 적용시 참고사항

- 제공된 예제는 VS2005로 만들어진 프로젝트로 32비트 64비트 컴파일이 모두 가능합니다. 상위버전에서도 컨버전이 가능합니다.
- 프로그램에 적용시 필요한 라이브러리는 l_mega32.lib 또는 l_mega64.lib가 전부입니다.
- 프로그램 링크시 추가로 필요한 라이브러리는 setupapi.lib(Visual Studio에 포함) 입니다.
- 프로그램 배포시에 추가되는 파일은 전혀 없습니다.

> MFC 프로그램에서의 참고사항

- lock_init_usb(8);은 메가락의 연결 여부를 운영체제에게 장치관리자에 등록되었는지 확인하는 것으로 패킷을 주고받는 것이 아니기 때문에 보안성은 없습니다.
결과값은 메가락의 존재여부를 신속하게 리턴하는 특성이 있으며, 결과값이 0인 경우에는 다른 함수를 호출하지 않도록 처리해주세요.
프로그램 실행시 최초에 1회 호출해야 되며, 락이 제거되어 팝업창을 표시한 경우 재연결 확인시에도 다른 함수 호출 전에 우선적으로 사용하는 것이 좋습니다.

- 통상적으로 락의 계속 연결여부는 lock_check(); 함수를 사용해야 하는데, 골프존에서는 키락과 컴퓨터를 1대1 대응하는 방식을 사용 있으니 lock_sn();함수의 고유번호를 체크하는 방법을 락의 계속 연결 여부를 확인하는 것이 좋겠습니다.

- 저장된 데이터를 연속으로 읽거나 쓰기를 할 때 lock_recive()함수를 적극적으로 사용해야 됩니다. 저장된 10바이트의 데이터를 읽어서 진위여부를 확인한다고 했을 때 오류가 없는 경우에는 응답이 매우 빠르지만, 오류가 생기면 1바이트(패킷) 읽는데 최대 2초까지 대기합니다. 따라서 오류가 생겼는데도 바로 탈출하지 않고 10바이트를 읽은 후에 비교를 할려고 하면 컴퓨터가 다운된 것처럼 20초를 기다리는 상황이 됩니다.

- lock_write(), lock_write_ex() 함수의 결과값은 USB에 기록한 다음, 다시 읽은 값을 되돌려 주므로 쓰기 기능에 대한 확인 값으로 사용하면 됩니다. 쓰기 방지 기능이 작동되는 중에는 이전에 저장된 값이 돌아옵니다.

>해킹방지와 관련한 몇가지 사항

1.해킹은 실행파일을 디스어셈블한 다음 락 펑션을 점프해서 제거하는 것이 대부분입니다. 해커는 우선 락펑션의 위치를 찾기 위해 애를 쓰는데, 이때 'lock not found' 같은 문자열이 소스에서 문자열 상수로 들어있다면 이 어드레스를 기준으로 찾게 됩니다.
  그래서 위와 같은 문자열은 프로그램 실행 후 변수로 만들어내는 것이 좋습니다.
간단한 예라면 'dnouf ton kcol'를 뒤집어서 사용하거나 암호화 하면 더 좋겠죠!

2. 통상적으로 락이 인지되지 않을 경우에 프로그램 실행 초기에 락을 연결하라는 팝업창을 띄우다보니 프로그램 시작부분에서 대체로 락 펑션을 찾아서 해킹합니다. 이런 유형의 해킹을 방지하려면 락이 없다고 해서 키를 연결하라는 메시지를 보여주는 것 보다는 프로그램의 처리를 데모버전으로 전환시키는 것이 좋습니다. 프로그램을 실행이 됐지만 파일 쓰기가 안된다든지, 인쇄를 못하게 하는 등의 방법입니다.

3. 메가락 체크 후에 오류 메시지를 바로 내지 말고 변수에 저장해 두었다가 다른 펑션들을 많이 실행한 후에 나중에 변수값을 체크해서 에러 메시지를 내보내는 것이 좋습니다. 디스어셈블 했을 때 거리가 멀면 연관관계를 짓기 힘들고, 디스어셈블러를 통한 해킹에서 상수값은 쉽게 파악이 되는데 변수값을 파악하기는 어렵습니다.

4. 실행파일을 통째로 압축해주는 실행파일압축(인터넷 검색가능)을 하면 디스어셈블이 좀 어렵습니다. 그런데 압축해제가 안되는 종류를 구해야 되겠죠.

5. 컴퓨터 바이러스가 붙어버리면 오히려 디스어셈블은 어려워질 수 있습니다.
이런 맥락에서 윈도우 코드사인인증(인터넷 검색가능)을 하면 디스어셈블이 어려워질 수 있습니다. www.certkorea.co.kr에서 1년 16만원인데, 귀사의 모든 프로그램을 1년동안 인증할 수 있습니다. 컴파일을 다시 하지 않으면 한번 인증한 프로그램의 인증기간은 1년과 관계없이 계속 유효합니다.