

Surface 및 Surface Pen에 대한 Threat Modeling 분석

김성겸

요 약

Bluetooth 4.0 기술 및 사용자에게 Surface간 효율적인 인터페이스를 제공하기 위해 부가적으로 같이 출시되는 Surface Pen을 통한 위협을 통해 취약점을 도출 해 냈으며, 공격자가 정확히 원하는 시간에 어플리케이션을 구동시키면서 사용자를 Pharming 사이트 및 원하는 타기중간의 통신을 하도록 유도할 수 있다. 다수의 Pen을 Surface에 연동 할 수 있는 것에서 기반 된 취약점으로 Pen에 대한 인증 시스템 및 사용자가 물리적으로 Pen의 구별이 가능 하다면 위협의 가능성을 대폭 줄일 수 있다.

I. Surface 및 Surface 에 대한 소개

I -1 Surface

Microsoft 사에서 Tablet과 Notebook의 중간정도에 위치하는 제품군의 주를 이루고 있는 제품이다. 2017년 5월을 기준으로 하여 Surface부터 Surface pro 4의 버전까지 하드웨어적인 향상 뿐 아니라 그에 맞춘 소프트웨어도 같이 개발되고 적용되어 왔다. 기존의 Tablet과는 다르게 개인용 컴퓨터에 사용되는 운영체제(OS, Operating System)를 그대로 사용할 수 있기 때문에 개인용 컴퓨터를 통해 할 수 있는 모든 작업이 Surface에서 가능하다. 뿐만 아니라 Surface와 함께 사용가능한 탈부착 가능한 Type Cover(Keyboard)는 필요시에는 Notebook과 같이 사용할 수 있게 제작 되어 있다.



[그림 1] Surface 및 Surface Pen

I -2 Surface Pen

Surface의 개발 및 기능향상과 더불어 Surface Pen 또한 변형을 같이 하였다. Surface 3세대와 함께 출시된 Surface Pen의 경우 wacom 사의 제품 BAMBOO Fineline 의 제품군을 많이 차용한 것으로 Microsoft 사와 wacom사가 합작으로 제작한 것이다. Surface 3세대의 Surface Pen의 경우, 종이 위에서 필기하는 동작에 디지털 작동의 이점을 결합하여 Surface에서 가장 최적화하여 사용가능 하다.

많은 버전의 Surface Pen 중에서 Surface 3세대 Pen에 대해 분석해 보았다.

Surface Pen 사양

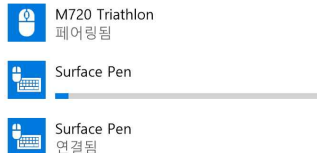
- 입력 감도 : 256 레벨(Levels)
- 연결 방식 : 블루투스 4.0(Bluetooth 4.0) 지원
- 호 환 : Surface 3, Pro3 이상부터 호환 가능
- 본체 크기 : 137 x 9.5(mm)
- 무 게 : 23g
- 전원 공급 : AAAA배터리 1개
- 지원 기능 : 단순 쓰기(상,하), 추가버튼 3개, Tilt 기능, 소프트웨어 및 응용 프로그램과 연동하여 사용가능.

I -3 Surface Pen 초기설정 및 기능

1) 초기 설정

Surface와 Pen의 통신은 Bluetooth 4.0을 통해서 이루어진다.

PC에서 검색하고 있으며 Bluetooth 장치에서 검색할 수 있습니다.



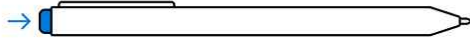
[그림 2] Surface Pen 과 Surface 간의 초기 연동 설정

Surface 와 Pen의 서로간의 페어링이 초기에 이루어지면 지속적으로 인증할 필요 없이 Surface에 운영체제(Windows10 Pro)가 구동되는 순간부터 사용이 가능해진다.

여기서 여러 개의 Surface Pen을 사용할 시에 사용자가 확인 하는 것은 단순히 장치의 이름인 “Surface Pen” 만 확인이 가능하며 여러 개의 Surface Pen을 등록 할 수 있다. 여러 개의 Surface Pen이 등록된 경우, 사용자는 공격자의 장비에 및 자신의 장비를 페어링 된 목록에서 구별이 불가능 하다.

펜 바로 가기

펜에 바로 가기 단추가 있는 경우 누를 때 수행할 작업을 선택하세요. 먼저 Bluetooth를 통해 펜을 연결해야 할 수 있습니다.



한 번 클릭

OneNote 2016

두 번 클릭

Windows Ink 작업 영역

화면 스케치

길게 누르기(일부 펜에서만 지원됨)

Windows Ink 작업 영역

스티커 메모

[그림 3] Surface Pen 기능 설정

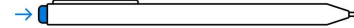
2) 제공 기능

마우스 등의 입력 기능 이외에도 Surface Pen의 경우 운영체제와 연동되어 특정 프로그램을 실행 시킬 수 있는 매크로기능이 추가 되어 있다.

Windows 10에서 Surface 펜과의 연동된 이후에는 측면 버튼을 이용하여 “지우기”, “마우스의 오른쪽 클릭”을 수행 할 수 있으며 펜촉의 반대 부분에 위치한 버튼을 세 가지 모션(한번, 두 번, 길게)을 통해 특정 앱을 실행 시킬 수 있다.

펜 바로 가기

펜에 바로 가기 단추가 있는 경우 누를 때 수행할 작업을 선택하세요. 먼저 Bluetooth를 통해 펜을 연결해야 할 수 있습니다.



한 번 클릭

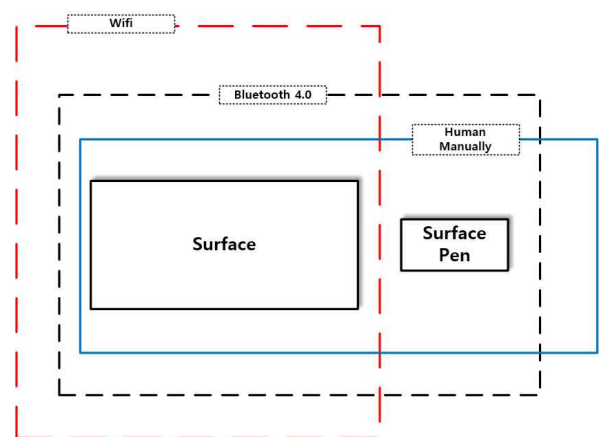
클래식 앱 실행

앱 선택

찾아보기

[그림 4] 특정 앱 실행 설정

이와 같은 설정 정보는 등록된 Surface Pen에 따라 설정 되는 것이 아니라 운영체제가 그 정보를 저장 하고 있으며, 페어링된 모든 Surface Pen에 대해 동일한 설정의 결과를 갖게 된다.



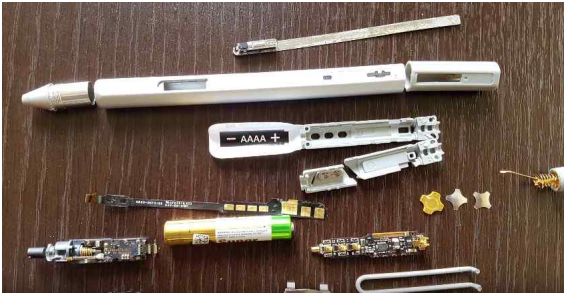
[그림 5] Surface와 Surface Pen 간의 통신 경계 (Wifi 포함)

II. 범위, 경계 및 공격자 모델의 설정

II-1 DFD(Data Flow Diagram)을 위한 경계 설정

Surface Pen의 경우, Surface와 연동된 이후에 다른 장비와의 통신을 하지 않는다. 경계의 설정은 Surface Pen 자체 및 Surface로 구성 하였다.

Surface Pen, Surface와 연관된 통신에 따른 경계를 표현 하였다. 경계에서 볼 수 있듯이 Surface Pen 자체는 Wifi의 경계에 속하지 않지만 Surface 기기를 통해서 Wifi 경계에 속할 수 있기 때문에 위와 같이 Wifi 경계 또한 포함 시켰으나 Wifi를 통한 대기중간의 통신은 고려 Object로 구성하지 않았다.



[그림 6] Data Flow 분석을 위한
동작원리 및 통신방법 분석

II-2 공격자 모델의 설정

공격자는 Surface의 물리적 접근을 지속적으로 수행 할 수는 없으나, 초기 설정 및 사용자에게서 물리적으로 근거리에 속할 수 있는 경우를 가정한다. [그림 5]에서의 경계에서 Human manually 경계는 최초 설정에 가능하고 이후에는 Bluetooth 4.0 경계에 속하는 공격자 이다. 뿐만 아니라, 공격자는 사용자의 화면을 근거리에서 확인이 가능한 것을 가정한다.

III. 연관된 자산

Hardware

연관된 자산 중 Hardware는 Surface, Surface Pen이 될 수 있겠다.

Hardware	
Surface Pen	자체에 대한 가치는 제품 자체의 가격(Price)이라고 볼 수도 있으나, Surface와의 통신 및 연동을 통해서 가 단순히 가격으로 평가하기 어렵다.
Surface	Surface는 다른 자산과의 연결 및 액세스 권한을 가진 것으로 다른 자산을 모두 포함 한 가치로 평가 받을 수 있다.

Software

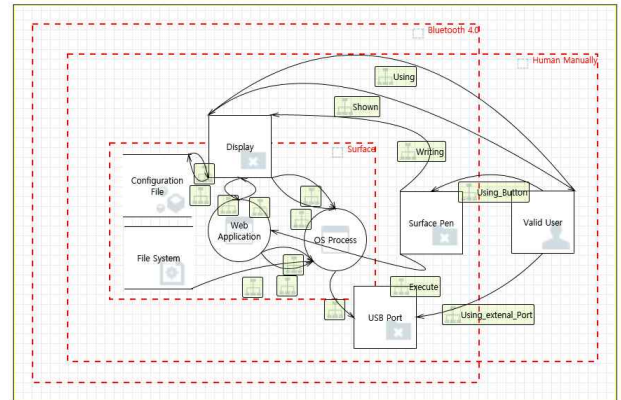
Hardware를 사용할 수 있게 도와주는 Software는 Hardware에 연관된 것으로 Surface를 운영하는 운영체제(Windows 10), 관련 앱 및 어플리케이션이 될 수 있겠다.

Software	
운영체제	모든 하드웨어와 소프트웨어를 관리 하는 시스템의 한 부분인 “실행 관리자”라고 정의 할 수 있다. 운영체제는 시스템을 사용할 수 있고, 어떻게 사용할 수 있는지를 관리하므로, 시스템의 보스(boss)라고 할 수 있다.
관련 앱 및 어플리케이션	운영체제의 도움을 받아 사용자가 원하는 것을 입력 받거나 그에 따른 결과를 출력해주는 기능을 사용자 친화적으로 구현 가능하다.

Data

Surface 사용간의 Data는 Surface 및 Cloud에 저장될 수 있으며, Surface Pen 및 Surface 간의 통신 또한 Data라고 볼 수 있다.

Data	
Surface 화면	Surface 화면의 경우 원하는 값의 출력뿐만 아니라 사용자의 입력도 가능하다.
Surface Pen 과 Surface 간 통신 데이터	Pen 과 Surface는 실시간으로 사용자의 입력을 주고 받게 설계 되어 있다.
Surface 저장공간	-
Cloud	Cloud 서비스를 사용하기 위해서는 Wifi 통신을 해야만 하는데, 현재 경계에서 Wifi 통신의 범위는 제외를 하였으므로 연관된 자산에서 제외 하였다.



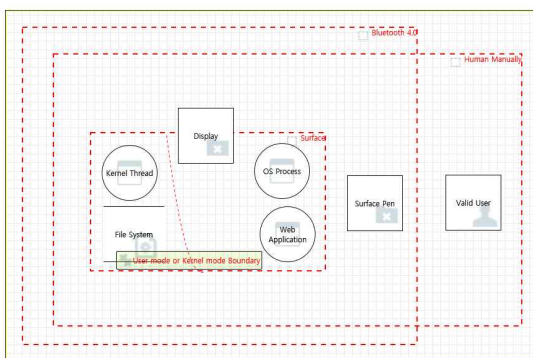
Data Flow의 경우 각각 통신의 성격에 따라서 속성을 정해 주었다. STRIDE와 직접적으로 영향이 있는 항목에 대해서만 적용해 주었으며, 그 항목은 다음과 같다.

IV. 위협 및 취약점 (Threat and Vulnerability)

IV-1 STRIDE Threat Model의 적용

Surface Pen 및 Surface 제품은 Microsoft의 제품으로서 Microsoft사에서 제공하는 Threat Modeling Tool을 사용하였다.

1. 설정한 자산 및 경계를 기준으로 작성한 Diagram



2. 실제 Data Flow의 입력

속한 경계간의 Data Flow만 가능 하므로 그것에 유의 하여 Data Flow를 작성 하였다.

- 1) 출발지의 인증
- 2) 도착지의 인증
- 3) 기밀성
- 4) 무결성
- 5) Forgery Protection의 유무

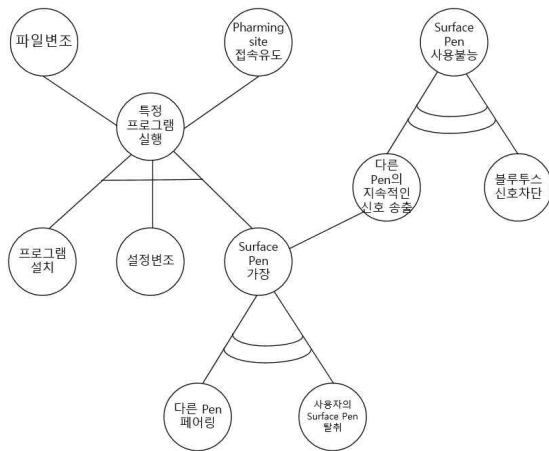
Surface 경계 안에서 생기는 Data Flow는 모두 동일하다고 가정 하였다. 즉 현재 Display라는 Object를 경유하면 모든 프로그램에 권한을 획득하여 Data를 얻어 낼 수 있다.

얻어낸 결과의 정리는 [부록-표]에 정리해 두었다.

IV-2 Attack Tree를 이용한 취약점 도출

취약점의 최종 목표는

1. 사용자를 Pharming site에 접속 하도록 유도
2. Surface 저장장치에 있는 파일의 변조
3. Surface Pen 장치 사용 불능 상태로 만들기



[그림 7] Surface Pen과 관련된 Attack Trees

IV-4 위험 분석 (DREAD를 사용)

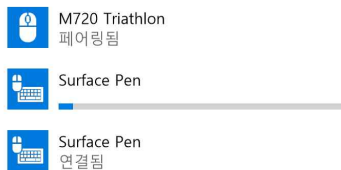
High : 3, Medium : 2, Low : 1

	파일 변조	Pharming site 접속 유도	Surface Pen 사용불능
Damage Potential	3	3	1
Reproducibility	3	3	3
Exploitability	1	2	3
Affected users	3	2	1
Discoverability	3	2	2
Total	13	12	10

V. 적절한 조치

1. 여러 개의 Surface Pen의 동시 사용을 막는다.

PC에서 검색하고 있으며 Bluetooth 장치에서 검색할 수 있습니다.



[그림 8] 동시 여러 개의 Pen의 페어링 및 사용이 가능

동시에 사용하는 Surface Pen의 사용을 허가 하는 것은 불필요한 장비에게 권한을 부여해주는 결과와 동일하다. 하나의 Pen을 사용한다고 하더라도 적합한 사용자가 서비스를 사용하는 것에 대한 문제점이 없다.

2. 사용자가 사용하는 각각의 펜에 고유 번호 부여

위에서 확인할 수 있듯이 페어링 된 다수의 Surface Pen에 대해서 식별 가능한 고유 번호가 아닌 “Surface Pen”으로만 나오게 되어있다. 뿐만 아니라 Pen의 형태는 외형적으로 색을 통한 분별을 제외 하고는 원래 사용자가 사용 했던 Surface Pen 이라는 인증을 할 수 없다. 이는, 일단 페어링 된 펜은 사용자가 임의로 제거 하지 않는 이상 지속적으로 시스템에 접속할 권한을 주는 것으로 사용하고 있는 Pen의 고유 번호를 확인 할 수 있도록 하여 인가 된(혹은, 처음에 페어링 된) Pen만 사용 가능 하도록 해야 할 것이다.

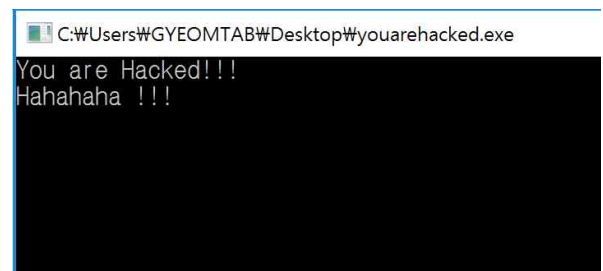
3. 펜을 통해서 사용할 수 있는 프로그램의 제한

길게 누르기(일부 펜에서만 지원됨)



[그림 9] 버튼의 모션에 따라서 지정할 수 있는 프로그램

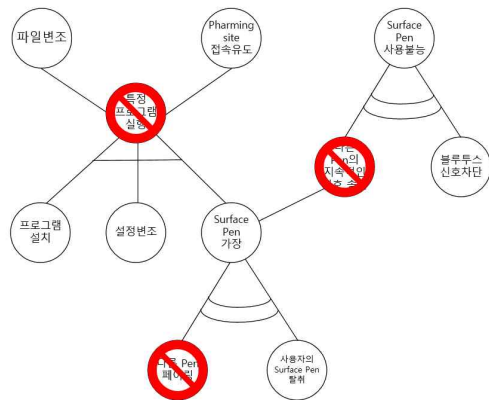
Surface Pen을 통해서 실행할 수 있는 프로그램의 제한이 전혀 없이 공격자는 [그림 9]와 같은 설정이 되어 있을 때 원하는 시간에 적절히 공격자가 원하는 프로그램을 실행 시킬 수 있다.



[그림 10] 버튼을 통한 프로그램 실행

따라서, 위와 같은 프로그램의 실행을 임의로 하지 못하도록 인가된 프로그램만이 버튼으로 등록이 될 수 있도록 해야 한다

VI. 조치에 대한 평가



[그림 11] 조치에 따른 불가능 위협

특정 프로그램 실행의 위협 : Surface Pen 설정 시에 인가된 프로그램만 등록이 가능 하도록 제한 하여 공격자가 원하는 프로그램의 실행을 막을 수 있다.

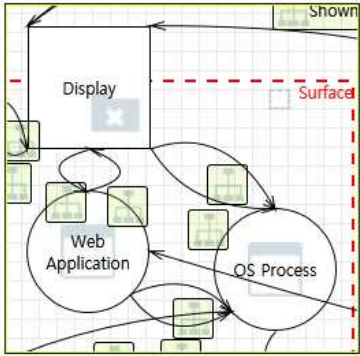
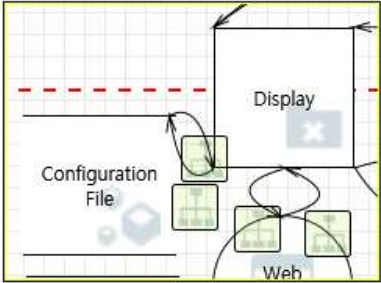
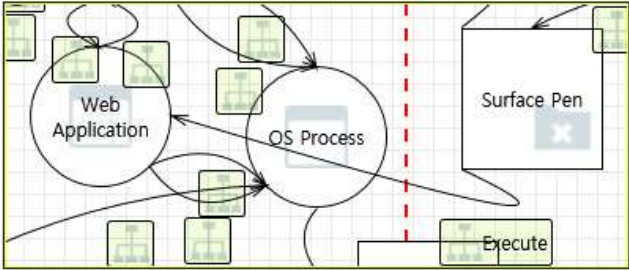
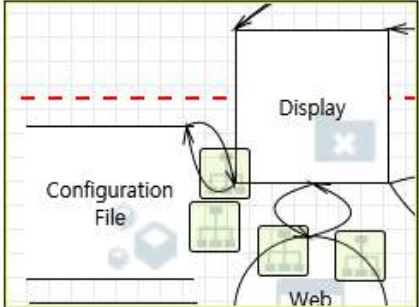
다수의 페어링 된 Pen의 사용 : 다수의 Pen이 동시에 Surface에 접근하지 못하도록 제한하면서 다수의 페어링 된 Pen의 사용을 막을 수 있다. 이는 공격자가 사용자의 Pen사용제한을 막을 수 있을 뿐만 아니라 사용자의 Pen을 가장(Spoofing)할 기회를 상실 시킬 수 있다.

다른 Pen의 지속적인 신호 송출 : 사용자는 자신의 Pen을 공격자와 물리적, 소프트웨어 적으로 구별 할 수 있게 되면서 비 인가된 Pen을 페어링 된 목록에서 제거 하면서 신호를 무시할 수 있게 된다. 이는 Bluetooth자체의 인증 방법에 기인한 것으로 인가된 Pen의 가용성(Availability)을 해치 기 어렵게 된다.

위와 같은 세 가지 위협 포인트는 앞서 제시한 적절한 조치를 통해서 제거 및 완화 시킬 수 있으며, 이 위협들은 목표한 취약점 도출에 있어서 중요한 다리 역할을 하고 있기 때문에 도출한 취약점을 일으킬 가능성을 제거하거나 줄일 수 있다.

VII. 부록

VII-표1

 	<p>종류 : Spoofing, Elevation Of Privilege</p> <p>Display를 통한 어플리케이션 사용에 있어서 Display는 사용자의 인증을 하지 않기 때문에 [자동 잠금이 설정 되지 않은 경우] 다양한 어플리케이션의 실행 위험이 있음</p> <p>여기서 사용자의 권한을 통해서 설정을 바꿀 수 있음</p>
	<p>종류 : Spoofing, Repudiation, Denial Of Service</p> <p>어플리케이션의 경우 Surface Pen을 통해 실행이 가능한데, 이는 초기 페어링 이후 지속적인 인증 과정이 없기 때문에 사용자 인척 가장 하여 프로그램을 실행 시킬 수 있다.</p> <p>뿐만 아니라, Surface Pen을 통한 정당한 요청이 단순히 신호 차단 또는 신호를 가로 채면서 가능해 질 수 있다.</p>
	<p>종류 : Information Disclosure</p> <p>Display를 통해서 손쉽게 설정 파일을 조작 할 수 있으며 어떤 설정이 되어 있는지 확인이 가능하다.</p>