난수 대응 단순 전치암호를 이용한 선암호화 기법

(Pre-Encryption using Random Number Functional-related Transposition Cipher)

함 의 진 *
동 국 대 학 교 컴 퓨 터 공 학 과 *
(EuiJin Ham)*
Computer Science and Engineering, Dongguk University*

요 약 인간의 생활에서 접하는 정보처리장치들은 대부분 사용자를 식별하고 이에 대한 인증을 할 수 있도록 암호를 사용하고 있으며, 이에 대한 중요성은 계속해서 증대되는 추세이다. 그러나, 암호를 입력하는 과정에서 사용자는 휴먼 인터페이스 기기(키보드 혹은 터치 스크린 등)를 매개로 하는 입력을 할 수 밖에 없고, 이러한 과정에서 발생할 수 있는 여러 종류의 유출 위협으로부터 안전할 수 없다. 본 연구에서는 기존의 입력체계와는 독립적으로, 사용자의 입력과 동시에 암호화를 적용하는 선암호화 기법을 제안하고자 한다. 이는 입력 장치와 암호를 검증하기 위한 정보처리장치에 암호가 전달되기 전 이미 암호화된 상태에서 전달되도록 하는 방법으로, 암호를 처리하는 장치와 암호화하는 장치에 물리적 독립성(physical independence)을 부여함으로써 구현될 수 있다. 그리하여, 본 연구에서는 난수 대응과 단순 전치암호 등의 비교적 간단한 암호화 기법을 통해 실험하여 사용한 검증 과정과 선암호화 개념에 대한 메카니즘을 소개할 것이다.

키워드 : 선암호화, 물리적 독립성, 난수 대응, 전치 암호

Abstract The information processing devices in human life are mostly using passphrase for user identification and authentication and importance for it is a trend that continued to increase. However, the user has only to enter the passphrase to the human interface device (keyboard or touch screen, etc.) as parameters, cannot be protected from several types of threats that may occur in the outflow in the course of this process to enter a passphrase. In this study, as the traditional systems independently, It propose a technique for applying a encryption at the same time as the user's input. This is the method which transmits the passphrase to the processing device for verifying, in encryption state before action that users will take for input, and this is implemented by providing a physical independence to a input device for the passphrase and the processing device. Thus, this study will introduce the concept of mechanism on pre-encryption and process for proving, with the experiment using relatively simple techniques such as transposition cipher and its corresponding random number.

Key words : Pre-encryption, Physical independence, Random number, Transposition cipher

서 론

인간의 생활에서 접하는 대부분의 정보처리장치들은 사용자를 식별하고 이에 대한 인증을 수행하기 위해 다양한 형태의 암호를 사용하고 있으며, 이 중 다수는 문자열 기반의 내용을 사용하는 것이 일반적이다. 또한, 이에 필요한 암호화 알고리즘이나 시스템들의 중요성은 계속해서 증가하고 있다. 그러나, 암호를 입력하는 과정에서 사용자는 해당 시스템이 사용하는 특정한 인터페이스 기기(키보드 혹은 터치 스크린 등)를 매개로 하는 입력을 할 수 밖에 없으며, 이러한 입력 과정에서 발생할 수 있는 훔쳐보기, 지문 등을 이용한 입력흔 조합, 모니터링(터치스크린 기반의 입력장치를 사용하는 경우) 그리고 키로깅 등의 여러 종류의 유출 위협으로부터 안심할 만한 수준의 보안성을 기대할 수 없다. 본 연구에서는 기존의 입력체계와는 암호화 주체에 대해 독립적으로, 사용자의 입력과 동시에 암호화를 적용하는 선암호화 기법을 제안하고자 한다. 이는 암호를 입력하기 위한 인터페이스 장치와 암호를 검증하기 위한 정보처리장치에 암호가 전달되기 전 이미 암호화된 상태에서 전달되도록 하는 방법으로, 암호를 처리하는 장치와 암호화하는 장

치에 물리적 독립성(physical independence)을 부여함으로써 구현될 수 있다. 그리하여, 본 연구에서는 난수 대응과 단순 전치암호 등의 비교적 간단한 암호화 기법을 통해 실험하여 사용한 검증 과정과 선암호화 개념에 대한 메카니즘을 소개할 것이다.

관련 연구

정보처리장치에 대한 암호 입력에 있어서 새로운 입력 시스템에 대한 연구는 이미 많이 진행되어 왔다. 일반적으로 이러한 연구들은 다수의 경우에서 암호와 함께 제 2, 제3의 정보를 필요로 하였으며, 이를테면 암호로 이용되는 문자 혹은 숫자 이외에도, 문자의 색깔이나 입력 장치의 버튼의 위치 혹은 형태를 이용하여 인증 과정을 제공했다. 그러나, 이러한 방법들은 사용자로 하여금 보안성은 증대되나 입력에 많은 시간을 소비하게 하거나, 친근하지 않거나, 사용에 있어서 알아야 하는 정보가 많아 그 이용성이 떨어졌으며, 현존하는 여러 가지 공격방법에 있어서 맹점을 가지고 있는 경우가 다수를 차지했다.

대표적으로, Volker Roth의 'PIN-Entry' 기법을 들 수 있는데, 이는 흑과 백으로 구분된 버튼을 순서대로 선택하여 인증을 거치는 방법으로, 경우의 수가 극히 적어 Brute-Force에 매우 취약하다는 것을 직관적으로 알 수 있다.

암호 입력과 보안 위협

정보를 처리하는 다양한 기기를 사용함에 있어서 이를 이용하는 사용자가 타인과 독립된 환경 혹은 접근이 제한적인 환경 속에서 어떠한 특정 서비스를 누리기를 원하거나 또는 이러한 환경이 필수적으로 갖춰져야하는 서비스인 경우, 일반적으로 서비스 관리자는 사용자의 식별을 위한 사용자만이 유일하게 알 수 있는 제한된 정보를 입력하는 다양한 도구 혹은 수단을 사용한다. 국내의 NHN社 혹은 Daum-Kakao社 그리고 국외의 Google社에 이르기까지 이러한 '계정'을 통한 사용자 인증을 적용하고 있기에 위와 같이 합리성을 가지고 단언할 수 있다. 따라서, 수많은 서비스에 접근하기 위해 사용자는 계정과 이에 따른 암호의 입력을 필수적으로 수행하게되며, 무의미하거나 입력 장치에서의 단순 규칙성을 이용하는 경우를 제외하고 일반적으로 유일성을 띈 의미를 부여하기 위해 사용자는 자신의 개인적이거나 민감한 정보를 사용하는 경우가 다수 존재한다. 그러므로, 공격자가 다양한 방법을 통해 계정의 권한만을 탈취한 것이 아니라, 암호의 내용까지 탈취한다면 이는 '민감 정보의 유출'이라 일컬어질 수 있다. 이에 대해서는 이후 자세히 소개한다.

암호를 입력하는 과정에 있어서 보안적 위협은 다양하게 존재한다. 이러한 위협들은 크게 2가지로 분류하여 고려할 수 있으며, 이러한 분류는 다시 양분되어 질 수 있다. 첫 분류인 2가지는 입력장치에 물리적으로 공격자가 가까이 위치하는 경우(입력장치를 시각적으로 인지하거나 직접 접촉하는 것이 가능한 거리)와 공격자가 입력 장치가 연결된 처리장치와 물리적으로 먼 곳에서 원격 혹은 타 여러 수단을 통해 통신할 수 있는 경우이며, 이들을 각각 이하 '근거리 위협'과 '원거리 위협'으로 정의하여 사용할 것이다. 또한, 이들은 다시 처리장치의 화면 혹은 수용한 암호를 임시적으로 저장하는 기억장치에 접근할 수 있는 경우 혹은 입력 장치에 물리적으로 접근할 수 있는 경우와 같은 공통적 특성을 통해 재분류되는데, 전자는 '정보 위협'으로, 후자는 '장치 위협'으로 정의하여 사용할 것이다.

앞서 언급한 분류들은 암호 입력에 대한 여러 위협을 4가지의 종류로 나눈 것으로, 다시 나열하면 다음과 같다. 근거리 위협, 원거리 위협, 정보 위협 그리고 장치 위협이다.

근거리 위협의 경우, 공격자는 사용자가 입력하는 것을 관찰하거나 입력을 위해 사용자가 접촉한 위치를 지문 혹은 잔류할 수 있는 다양한 흔적 등의 입력흔(入力痕)을 토대로 여러 조합을 만들어 정보를 탈취할 수 있다. 비교적 단순하고 복잡하지 않은 시나리오라고 할 수 있으나, 모바일 기기 혹은 터치 스크린이나 패스워드 도어락 등에서 가장 많이 발생하고 있는 위협이다. 이러한 조합을 통해 공격자가 정보를 탈취하기 위해 시도해야하는 경우는 총 N 자리일 때, N의 계승과 같고, 다수의 기기가 4 자리의 PIN을 사용하고 있기에 24가지 정도의 시도라면, 누구든지 어렵지 않게 공격에 성공할 수 있다. 이러한 위협은 사용자의 행동과 독립적으로 입력장치에 대한 접근만으로 공격을 시도할 수 있는 장치 위협과 '사용자 관찰'의 측면에서 차이를 갖는다. 즉, 근거리 위협에 대해 장치 위협이 포함되어질 수 있다.

원거리 위협의 경우, 공격자는 사용자가 입력하는 것을 '키로깅' 혹은 '디스플레이 모니터링' 등의 방법을 통해 사용자의 입력을 관찰하거나, 암호를 처리 중인 장치에 대해 내부적으로 대조되는 과정에 대해 정보를 가로채는 행위 등을 통해 위협을 가할 수 있다. 이러한 과정에 있어서, 정보 위협은 앞서 근거리 위협에서 분류한 바와 같이 '사용자 관찰' 측면에서 차이를 가지며 원거리 위협에 포함되어 질 수 있다.

근본적으로, 본 연구에서는 암호 입력에 있어서의 보안성 증대를 위한 수단에 초점을 두고 있으며, 앞서

정의한 '정보 위협' 범주 내의 위협(암호 대조 과정 혹은 복호화 과정에 대한 위협)에 대한 보안성은 기존의 여러 암호화 알고리즘 혹은 해시 알고리즘을 통해 갖추어질 수 있으므로 고려하지 않았다.

선암호화 기법

선암호화(Pre-Encryption) 기법은 암호의 전달과정에 있어서 정보처리장치의 자원 활용없이 입력과 동시에 암호화가 적용되는 시스템으로, 암호가 입력되고 이를 기억장치에 적치하여 암호화를 진행하는 현 시스템들과는 암호화의 주체가 물리적 독립성(Physical Independence)을 갖는다는 점에서 큰 차이를 두고 있다. 본 연구에서는 이에 대한 예시로서 간단한 단순 전치 암호와 난수를 적용하여 암호화를 수행하고 있으며, 이에 대한 메카니즘은 다음과 같다.

<그림01> 추상화된 난수의 출력 예시

사용자는 암호 입력 인터페이스를 시각적으로 접하게 되는데, 이 때 인터페이스 기기에 속하는 모니터 등의 화면이나 다른 여러 장치(본 연구에서는 화면)를 이용하여 특정 길이의 난수를 추상화시켜 <그림01>과 같이 출력하게 된다. (인간의 통찰력이 필요한 숫자 이미지 인식 과정의 삽입을 통해 프로그램이나 기타 방법을 이용한 공격의 속도 저하를 도모) 사용자는 이를 확인하고 입력하려던 암호에 대한 단순 전치 결과를 사유(思惟)한다. 이를테면, 'A'를 입력해야하나 화면에 '3'이 출력되고 있다면, 원래의 문자로부터 세 번 전치된 'D'를 입력하게 되는 것이다. 이러한, 단순 전치는 각 문자를 단위로 다른 값의 난수를 적용하도록 구성되었으며, 이와 같은 과정을 통해 사용자가 알고있는 암호는 불변이나, 입력하는 암호는 매번 달라지기에 사용자를 관찰하는 키로깅(Key Logging)이나 훔쳐보기(Shoulder-Surfing), 입력흔 조합 추론 등은 선암호화에 있어서는 의미를 잃게된다. 또한, 무차별 대입 공격(Brute-Force) 의 경우에는 문자 단위로 갱신되는 난수로 인해 무차별 대입 알고리즘에 있어서 보다 많은 복잡도를 요구하게 되며, 속도와 복잡도에 대한 효율성이 가장 중요한 무차별 대입에 있어 큰 장애가 될 것으로 기대할 수 있다. 뿐만 아니라, 만일 공격이 성공한다고 하더라도 이로 인해 암호에 적용된 사용자의 개인적인 의미가 유출되는 것은 불가능할 것이다.

<그림02> 일반적 자물쇠와 QWERTY 키패드

무차별 대입을 적용함에 있어서 선암호화가 갖는 이점은 매우 크다. Brute-Force 공격의 기초적인 원리를 고려하면, <그림02> 좌측의 비밀번호 자물쇠의 경우, 최악의 경우 0000의 조합부터 9999까지의 조합으로, 10000개의 조합의 대입이 필요하다.

이는 단위 자리 당 10가지의 키(이하 (3)에서는 암호화의 키가 아닌 값의 의미로서)로 4자리를 입력하기 위한 조합의 수이다. 즉,

$$Variation = K^L (K : Keys, L : Length\,of\,Text)$$

이에 대해 선암호화가 적용된다면, 한 조합 당 한 번의 전치 과정이 필요하므로,

$$Complexity = LK^L$$

그러나, 위 자물쇠와 달리 가변적 길이의 문자열을 이용한 암호를 이용한다고 가정하여 일반화하여 대략적인 복잡도를 <그림02> 우측의 102키의 Qwerty 키패드에 적용하면 계산적으로 기존의 방식에 비해 상당히(컴퓨터보안적 관점에서 시간복잡도 및 효율성 면에서 합리적으로 안전하다고 할 수 있는 크기의) 큰 보안성을 갖는다.

선암호화의 일반화

본 연구에서의 기법은 단순한 암호화 기법인 전치암호(Transpositon Cipher)에 기반을 두고 있다. 그러나, 이는 해당 기법의 구조와 메카니즘의 소개를 위해 가장 간단한 한 가지의 예시를 제시한 것으로, 추가적 연구가 있다면 여러가지 암호화 알고리즘을 통해 다양하게 일반화되어 응용될 수 있다.

또한, 선암호화 기법은 사용자가 알고있는 문자열 등의 정보를 통해 인증 과정을 갖는 다양한 분야와 장치에 적용되어 질 수 있다. 그 대상이 Google社의 안드로이드의 암호 장치인 Pattern-Based Cipher이거나 일반 가정의 현관 잠금 장치일지라도, 소프트웨어적으로 이를 적용하거나 단순한 숫자 출력을 위한 8-segment chip 등을 사용하여 응용한다면 저비용으로 간단하게 적용이 가능하다는 것이다. 그리하여, 본 연구에서는 이를 소프트웨어적인 관점에서 선암호화를 적용한 프로그램을 구성하여 이를 검증할 수 있도

록 하였으며, 이는 이하 '실험 및 검증'에서 이어진다.

실험 및 검증

암호 입력 기법의 사용성이 사용자 편의성에 상당 부분 의존한다는 점은 널리 알려져 있다. 그러므로, 연구 검증에 앞서 사용성을 척도화하여 이를 비교할 수 있도록 다음과 같은 실험을 진행했다.

5명의 실험자를 대상으로 일반적으로 정렬된 숫자 키패드(일반적 키보드의 10 Keys), 임의 정렬 키패드(은행권 SW에서 이용되는 키 위치가 항상 다른) 그리고 선암호화 기법이 적용된 시스템에서 친숙한 4자리 PIN에 대해 입력에 소요되는 시간을 측정했고, 다음은 이를 30회 씩 반복하여 평균을 계산한 결과이다.

실험자/평균소요시간	General	Random Keypad	Pre-Encryption
1	0.552	3.253	7.112
2	0.621	3.545	7.502
3	0.875	3.881	8.051
4	0.733	3.665	6.994
5	1.020	5.459	7.443

<표01> 입력 소요시간 평균

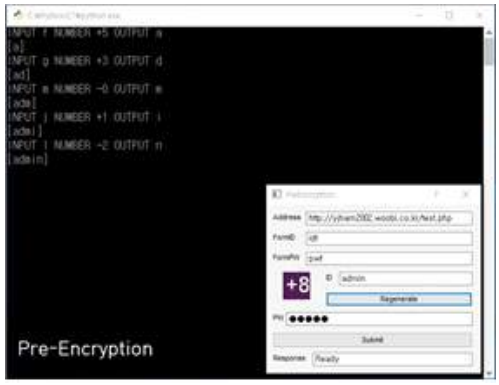
위 측정 결과와 같이 평균적 입력 시간의 총합은 순서대로 3.801sec, 19.801sec, 37.102sec으로, 각각 5.21배, 1.87배로, 은행권 등에서 사용되는 임의 정렬 키패드에 비해 2배가 되지 않는 소요시간으로 사용자에게 큰 불편을 주지 않을 것으로 기대할 수 있다.

선암호화의 소프트웨어적 적용을 통해 검증을 수행하기 위해 비교적 간단한 전치암호를 이용하였기에 몇 가지의 제약조건을 설정하였으며, 이들 조건은 다음과 같다.

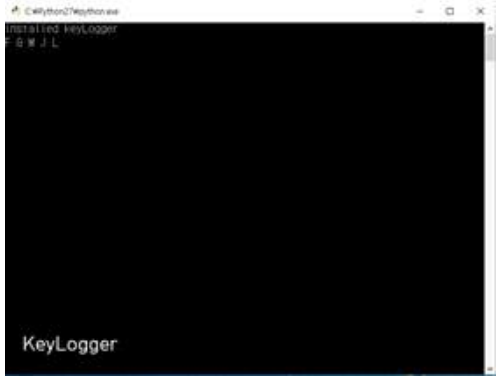
- 모든 문자를 수용한다.
- 한글은 키패드 상응 위치 알파벳으로 가정한다.
- 대소문자를 각각 폐포(Closure)로 취급한다.
- 알파벳 이외에는 전치하지 않는다.

위 조건들 중 대소문자를 폐포로 취급한다는 것은 입력해야하는 문자가 전치되어 알파벳 범위를 초과하였을 경우, 다시 첫 문자로 회귀하는 환형전치를 의미하며, 대문자는 대문자 이내의 범위에서 환형전치하며 소문자에도 동일하게 적용한다는 의미이다.

검증에는 위에서 언급한 조건을 통해 전치 암호 알고리즘을 적용한 선암호화 기법을 Python을 통해 구현한 GUI 기반 프로그램과 함께, 공격자 입장에서 암호를 입력중인 사용자를 관찰할 수 있는 한 가지의 예시인 간단한 키로거를 구현하여 보안성을 확인할 수 있도록 구성하였다. 키로거의 경우, 단순하게 Windows의 Hook Chain을 기본 API를 이용하여 Hooking하도록 함으로써 구현되었으며, 선암호화 프로그램의 경우, 실험을 위해 입력된 실제 문자와 사용자가 사유(思惟)를 통해 의도한 문자가 출력되도록 구성되어 있으며, 매우 간단히 문자열을 대조하여 Response를 보낼 수 있는 서버 페이지에 대한 전송과 Response의 수용과 출력을 할 수 있는 기능을 포함한다.



<그림03> 선암호화 프로그램과 이의 로그



<그림04> 키로거에 의해 기록된 사용자 입력

위 <그림03>과 <그림04>는 테스트를 위한 Passphrase인 "admin"의 입력을 선암호화 프로그램을 통해 입력한 모습이다. 각각 +5, +3, -0, +1, -2의 난수가 출력되어 f, g, m, j, l을 사용자가 입력한 결과이다. 또한, 정상적으로 admin이 각 문자에 대해 재전치되어 입력되었음을 알 수 있다. 키로거 또한 사용자가 입력한 허상 입력(Spurious Input)을 출력하게 되었으며, 이를 통해 위와 같은 실험을 위한 로그 출력이 없다면, 공격자는 사용자의 입력을 탈취하거나 사용자가 암호를 입력하기 위해 사용한 입력 장치의 입력흔을 조사하더라도 의미가 없는 값을 얻게 된다.

한 계

본 연구는 암호 입력에 대한 메카니즘에 대한 것이다. 따라서, 이에서 제안하는 방식은 사용자가 자신의 암호를 문자열을 입력할 수 있는 특정 인터페이스에서 이를 입력하는 시점에 대해 위에서 정의한 정보 위협을 제외한 원거리 위협과 근거리 위협에 따른 보안성을 제공하는데에 초점을 두고 있다. 그러므로, 해당 암호 정보가 이를 검증하는 서버 혹은 처리장치로 전달되는 일련의 과정, 이를 복호화하여 검증하는 과정 그리고 CAPTCHA를 이용하여 생성되는 추상화된 숫자 이미지 파일에 대한 접근 등에 있어서의 보안성과 저장된 암호에 대한 정보에 대한 보안성은 고려하지 않는다. 그러나, 해당 기법이 사용자에게 특정 난수를 전달하기 위해 디스플레이하는 과정에서 여러 경로를 통해 이 정보가 유출되어질 수 있으나, 이는 사용자가 어떤 키를 선택함에 있어서 터치스크린의 경우, 사용자가 선택하지 않은 대상을 선택한 것과 같이 보이는 허상 선택(Spurious Selection) 혹은 입력 스트림에 대한 허상 출력(Spurious Output)등을 통해 처리한다면 이러한 정보 유출은 공격자의 관점에서 의미를 잃기에 이는 한계가 아님을 명시한다.

결 론

본 연구에서 제안하고자 하는 바는 '전치 암호'가 적용된 선암호화가 아닌, 선암호화 기법의 개념에 대한 제안이다. 따라서, 암호화 주체와 처리장치에 대해 물리적인 독립성을 부여하는 데에 그 의미가 있다. 수많은 암호화 알고리즘과 암호 입력 시스템들은 다양한 수단과 공격 기법들에 의해 파괴되어져 왔으며, 발전해왔다. 이는 기억장치를 사용하는 정보처리장치에 암호에 대한 정보를 담거나 이들 정보를 처리하는 과정의 대부분을 의존하기 때문일 것이다.

알고리즘의 복잡화를 통해 얻어지는 보안성 특성은 거의 모든 경우에 있어서 계산적 안전성에 의존하기에, 빠른 속도로 발전하는 프로세서와 양자 컴퓨팅 기술로부터 안전할 수 없다. 그러므로, 구조적 관점 혹은 타 수단을 이용한 보안성 증대에 초점을 둔 발전이 필요할 것으로 보이며, 본 연구에서는 본 주제의 핵심 내용이라 할 수 있는 '암호화 주체의 물리적 독립성' 그리고 이에 기반한 '선암호화 기법'을 단순한 알고리즘을 이용한 새로운 메카니즘으로, 위에서 언급한 '타 수단'의 하나의 예시로서 제시하고자 하였다.

참 고 문 헌

[1] 김동화 외 4, "스도쿠 퍼즐을 이용한 훔쳐보기 방지용 비밀번호 입력 시스템", 한국정보과학회 학술발표논문집 38(2C), 2011, 195-198

[2] 조성문 외 1, "파이썬 해킹 입문 - 공격의 언어 파이썬을 이용한 해킹 연습", 프리렉, 2014

[3] Willam Stallings 외 1, "Computer security - Principles and practice", PEARSON, 2nd, 2013

[4] Volker Roth 외 2, "A PIN-Entry method resilient against shoulder surfing", Proc. CCS, 2004, 236-245