(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0072210
(43) 공개일자 2013년07월01일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) *G06F 9/44* (2006.01)
(21) 출원번호 10-2012-7029352
(22) 출원일자(국제) 2011년05월06일
심사청구일자 없음
(85) 번역문제출일자 2012년11월08일
(86) 국제출원번호 PCT/EP2011/057345
(87) 국제공개번호 WO 2011/141388
국제공개일자 2011년11월17일
(30) 우선권주장
10305498.7 2010년05월11일
유럽특허청(EPO)(EP)

(71) 출원인
톰슨 라이센싱
프랑스 92130 이씨레뮬리노 루 잔다르크 1-5
(72) 발명자
알레씨오 다비드
프랑스, 렌네스 에프-35700, 루 데 푸제르 170
엘뤼아르 마르크
프랑스, 이씨-레-뮬리노 에프-92443, 루 잔다르크 1, 테크니컬러
매츠 이브
프랑스, 이씨-레-뮬리노 에프-92443, 루 잔다르크 1, 테크니컬러
(74) 대리인
문경진, 김학수

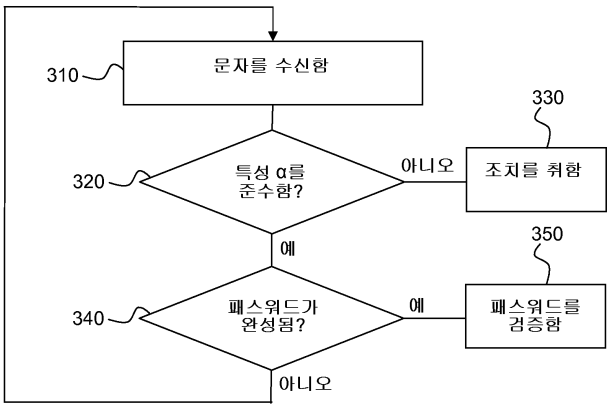
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **패스워드 생성 및 검증을 위한 방법들, 디바이스들, 및 컴퓨터 프로그램 지원들**

(57) 요 약

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안, 패스워드는 패스워드 문자를 반복적으로 수신하고(310); 수신된 문자가, 허용 가능한 패스워드들에 대한 적어도 하나의 요구 사항을 설정하는 미리 정의된 특성(α)을 준수하는 지를 검증함으로써 검증된다. 만약 이러한 경우가 아니라면, 이것은 맹목적인 집단 공격을 지시할 수 있으며, 적절한 조치가 취해질 수 있다. 특성은 사용자에 의존할 수 있다. 또한 해당 디바이스(120) 및 컴퓨터 프로그램 제품(140)이 제공된다.

대 표 도 - 도3



특허청구의 범위

청구항 1

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드의 검증의 방법으로서, 상기 방법은 프로세서(111, 121) 내에서,

입력 패스워드 중 적어도 하나의 문자를 수신하는 단계(310); 및

적어도 하나의 수신된 문자가, 허용 가능한 패스워드들에 대한 적어도 하나의 요구 사항을 설정하는 미리 정의된 특성(α)을 준수하는 것을 검증하는 단계(320);를 포함하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드의 검증의 방법.

청구항 2

제1항에 있어서, 입력 패스워드 및 입력 패스워드가 완전하다는 지시(indication)에 대한 모든 문자들이 수신되고, 상기 방법은 완성된 입력 패스워드가 실재물을 보호하는 패스워드에 해당한다는 것을 검증(350)하는 단계를 더 포함하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드의 검증의 방법.

청구항 3

제2항에 있어서, 상기 완성된 입력 패스워드는 제1의 부분 및 제2의 부분을 포함하고, 상기 특성은 제2의 부분으로 표현되며, 상기 특성에 대한 준수는 프로세싱된 제1의 부분이 제2의 부분과 매칭되는지의 여부를 확인하기 위해 제1의 부분을 프로세싱함으로써 검증되는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드의 검증의 방법.

청구항 4

제1항 또는 제2항에 있어서, 상기 특성은 사용자에 의존하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드의 검증의 방법.

청구항 5

제1항 내지 제4항 중 어느 한 항에 있어서, 맹목적인 집단 공격(brute force attack)이 사용자에 대한 특성을 고려하지 않는 입력 패스워드들의 미리 결정된 수 또는 입력 패스워드들의 부분들의 검출 시에 시도되었는지를 결정하는 단계를 더 포함하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드의 검증의 방법.

청구항 6

제5항에 있어서, 맹목적인 집단 공격이 시도되었는지에 대한 결정 시에 적절한 조치를 취하는 단계를 더 포함하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드의 검증의 방법.

청구항 7

제6항에 있어서, 적절한 조치는 관리자에게 경고를 발하는 것, 사용자에게 경고를 발하는 것, 시스템을 차단하는 것, 그리고 추가적인 로그온 시도들을 수용하기 이전에 미리 결정된 시간을 기다리는 것 중 적어도 하나를 포함하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드의 검증의 방법.

청구항 8

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드를 검증하기 위한 디바이스(110, 120)로서, 상기 디바이스(110, 120)는,

패스워드 문자들을 수신하기 위한 인터페이스(113, 114, 123, 124); 및

적어도 하나의 수신된 패스워드 문자가, 허용 가능한 패스워드들에 대한 적어도 하나의 요구 사항을 설정하는 미리 정의된 특성(α)을 준수하는지를 검증하기 위한 프로세서(111, 121);를 포함하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드를 검증하기 위한 디바이스.

청구항 9

제8항에 있어서, 상기 인터페이스는 입력 패스워드가 완전하다는 지시를 더 수신하기 위함이고, 상기 프로세서는 완성된 입력 패스워드가 실재물을 보호하는 패스워드에 해당하는 것을 더 검증하기 위함인,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드를 검증하기 위한 디바이스.

청구항 10

제9항에 있어서, 상기 완성된 입력 패스워드는 제1의 부분 및 제2의 부분을 포함하고, 상기 특성은 제2의 부분으로 표현되며, 상기 프로세서는 프로세싱된 제1의 부분이 제2의 부분과 매칭되는지의 여부를 확인하기 위해 제1의 부분을 프로세싱함으로써 상기 특성에 대한 준수를 검증하도록 적응된,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드를 검증하기 위한 디바이스.

청구항 11

제8항 또는 제9항에 있어서, 상기 특성은 패스워드의 사용자에 의존하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드를 검증하기 위한 디바이스.

청구항 12

제8항 내지 제11항 중 어느 한 항에 있어서, 상기 프로세서는 맹목적인 집단 공격이 사용자에 대한 특성을 고려하지 않는 입력 패스워드들의 미리 결정된 수 또는 입력 패스워드들의 부분들의 검출 시에 시도되었는지를 더 결정하기 위한,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드를 검증하기 위한 디바이스.

청구항 13

제12항에 있어서, 상기 프로세서는 맹목적인 집단 공격이 시도되었는지의 결정 시에 적절한 조치를 더 취하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드를 검증하기 위한 디바이스.

청구항 14

제13항에 있어서, 적절한 조치는 관리자에게 경고를 발하는 것, 사용자에게 경고를 발하는 것, 시스템을 차단하는 것, 그리고 추가적인 로그온 시도들을 수용하기 이전에 미리 결정된 시간을 기다리는 것 중 적어도 하나를 포함하는,

패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드를 검증하기 위한 디바이스.

청구항 15

소프트웨어 프로그램의 저장된 명령들을 갖는 컴퓨터 프로그램 제품(140)으로서, 상기 명령들은, 프로세서(111, 121)에 의해 실행될 때, 패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안,

입력 패스워드 중 적어도 하나의 문자를 수신하는 단계(310); 및

적어도 하나의 수신된 문자가, 허용 가능한 패스워드들에 대한 적어도 하나의 요구 사항을 설정하는 미리 정의된 특성(α)을 준수하는 것을 검증하는 단계(320);를 수행하는,

소프트웨어 프로그램의 저장된 명령들을 갖는 컴퓨터 프로그램 제품.

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 컴퓨터 시스템들에 관한 것이며, 특히 이러한 시스템들에서 로그온 시 패스워드의 취급(treatment)에 관한 것이다.

배 경 기 술

[0002] 본 절은 독자에게 다양한 양상의 기술을 소개하도록 의도되는데, 이는 아래에 설명 및/또는 청구된 본 발명의 다양한 양상들에 관한 것일 수 있다. 본 논의는 본 발명의 다양한 양상들에 대한 더 나은 이해를 촉진하기 위해, 독자에게 배경 지식을 제공하는 것에 있어서 도움을 줄 것이라고 믿어진다. 따라서 이러한 진술들은 종래 기술의 용인으로서가 아닌, 이러한 견지에서 읽혀져야 함이 이해되어야 한다.

[0003] 패스워드들은, 예를 들어 로그온에 있어서 사용자를 인증하기 위해, 오늘날의 컴퓨터 시스템들에 비일비재하다. 일반적인 정의로, 패스워드는 미리 정의된 알파벳(예를 들어 : PIN 코드를 위한 4개의 숫자 값들) 내에서 선택된 심볼들의 연속으로 구성된다.

[0004] '강력한' 패스워드들을 생성하기 위해, 선택된 패스워드가 미리 정의된 방침을 준수하는 것을 요구하는 것은 보편적이다. 이러한 방침은, 예를 들어 패스워드가 적어도 8개의 문자들 길이여야 한다는 것과, 이것이 적어도 하나의 대문자 및 &, (및 =와 같은 적어도 하나의 특수 문자를 포함해야 한다는 것일 수 있다. US2004/250139 및 US2009/158406는 이러한 패스워드들을 선택하기 위한 솔루션들을 제시한다.

[0005] 하지만 강력한 패스워드들을 사용하는 패스워드 보호 시스템들은 (모든 가능한 값을 반복적으로 시도하는) 맹목적인 집단 공격들(brute force attacks)에 의해, 또는 (선호되는 값들의 부분 집합을 시도하는) 사전 공격들(dictionary attacks)에 의해 공격을 받을 수 있다. 이하에서, 이들 공격들은 "자동화된 공격들(automated attacks)"이라 불려질 것이다. 이들의 구현을 간소화하기 위해, 이들 공격들은 인증 시스템의 사용자 인터페이스가 아닌 저-레벨 레이어들을 사용하여 운영된다. 이들 툴(tools) 중 일부, 예를 들어 더 존 더 리퍼 패스워드 크래커(the John the Ripper password cracker)는 인터넷에서 이용 가능하다.

[0006] 현재의 인증 시스템들은 자동화된 공격들과 사용자 실수들 사이를 식별할 수 없다. 디폴트(default)로서, 일부 인증 시스템들은, 두 개의 연속하는 요청들 사이에 지연을 삽입함으로써, 성공적이지 못한 시도들의 수를 제한함으로써, 또는 이 두 가지의 결합으로서, 자동화된 공격들의 위험을 최소화하기 위한 메커니즘들을 구현한다. PIN 코드들의 예시에 있어서, 성공적이지 못한 시도들의 수는 보통 3개로 고정된다.

발명의 내용

해결하려는 과제

[0007] 따라서 인증 시스템이 자동화된 공격을 검출하도록 허용할 수 있고, 이로써 본 시스템이 적절한 방침들에 따라 이러한 공격들에 반응하도록 허용할 수 있는 솔루션에 대한 필요가 있다는 것이 이해될 수 있다. 본 발명은 이러한 솔루션을 제공한다.

과제의 해결 수단

[0008] 제1 양상에 있어서, 본 발명은 패스워드에 의해 보호되는 실재물(entity)에 대한 사용자의 로그온 동안, 입력 패스워드의 검증의 방법에 관한 것이다. 프로세서는, 입력 패스워드 중 적어도 하나의 문자를 수신하고; 적어도 하나의 수신된 문자가, 허용 가능한 패스워드들에 대한 적어도 하나의 요구 사항을 설정하는 미리 정의된 특성을 준수하는 것을 검증한다.

[0009] 제1의 선호되는 실시예에서, 입력 패스워드 및 입력 패스워드가 완전하다는 지시(indication)에 대한 모든 문자들이 수신되고, 프로세서는 완성된 입력 패스워드가 실재물을 보호하는 패스워드에 해당되는 것을 더 검증한다. 한 변형에서, 완성된 입력 패스워드는 제1의 부분 및 제2의 부분을 포함하며, 제2의 부분으로 표현되는 특성 및 특성에 대한 준수(compliance)는, 프로세싱된 제1의 부분이 제2의 부분과 매칭되는지의 여부를 확인하기 위해

제1의 부분을 프로세싱함으로써 검증된다.

[0010] 제2의 선호되는 실시예에서, 특성은 사용자에 의존한다.

[0011] 제3의 선호되는 실시예에서, 프로세서는, 사용자에 대한 특성을 고려하지 않는 입력 패스워드들의 미리 결정된 수 또는 입력 패스워드들의 부분들에 대한 검출 시에, 맹목적인 집단 공격이 시도되었다는 것을 결정한다. 맹목적인 집단 공격이 시도되었다는 것의 결정 시에, 적절한 조치가 취해지는 것은 이롭다. 이러한 적절한 조치는 관리자(administrator)에게 경고를 발하는 것, 사용자에게 경고를 발하는 것, 시스템을 차단하는 것, 그리고 추가적인 로그온의 시도들을 수용하기 이전에 미리 결정된 시간을 기다리는 것 중 적어도 하나를 포함한다.

[0012] 제2의 양상에서, 본 발명은 패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 입력 패스워드를 검증하기 위한 디바이스에 관한 것이다. 디바이스는 패스워드 문자들을 수신하기 위한 인터페이스; 및 적어도 하나의 수신된 패스워드 문자가, 허용 가능한 패스워드들에 대한 적어도 하나의 요구 사항을 설정하는 미리 정의된 특성을 준수하는 것을 검증하기 위한 프로세서;를 포함한다.

[0013] 제1의 선호되는 실시예에서, 인터페이스는 입력 패스워드가 완전하다는 지시를 더 수신하기 위함이고, 프로세서는 완성된 입력 패스워드가 실재물을 보호하는 패스워드에 해당한다는 것을 더 검증하기 위함이다. 한 변형에서, 완성된 입력 패스워드는 제1의 부분 및 제2의 부분을 포함하며, 특성은 제2의 부분으로 표현되고, 프로세서는, 프로세싱된 제1의 부분이 제2의 부분과 매칭되는지의 여부를 확인하기 위해, 제1의 부분을 프로세싱함으로써 특성에 대한 준수를 검증하도록 적응된다.

[0014] 제2의 선호되는 실시예에서, 특성은 패스워드의 사용자에 의존한다.

[0015] 제3의 선호되는 실시예에서, 프로세서는, 사용자에 대한 특성을 고려하지 않는 입력 패스워드들의 미리 결정된 수 또는 입력 패스워드들의 부분들에 대한 검출 시에, 맹목적인 집단 공격이 시도되었다는 것을 더 결정하기 위함이다. 맹목적인 집단 공격이 시도되었다는 것의 결정 시에, 적절한 조치가 취해지는 것은 이롭다. 이러한 적절한 조치는 관리자에게 경고를 발하는 것, 사용자에게 경고를 발하는 것, 시스템을 차단하는 것, 그리고 추가적인 로그온의 시도들을 수용하기 이전에 미리 결정된 시간을 기다리는 것 중 적어도 하나를 포함한다.

[0016] 제3의 양상에서, 본 발명은, 패스워드에 의해 보호되는 실재물에 대한 사용자의 로그온 동안 프로세서에 의해 수행될 때, 입력 패스워드 중 적어도 하나의 문자를 수신하고; 적어도 하나의 수신된 문자가, 허용 가능한 패스워드들에 대한 적어도 하나의 요구 사항을 설정하는 미리 정의된 특성을 준수하는 것을 검증하는, 소프트웨어 프로그램의 명령들을 저장하는 컴퓨터 프로그램 제품에 관한 것이다.

[0017] 본 발명의 선호되는 특징들은 첨부된 도면들을 참조하여 비 제한적인 예시의 목적으로 설명될 것이다.

발명의 효과

[0018] 본 발명은, 맹목적인 집단 및 사전 공격들에 저항하고, 본 시스템이 공격하에 있는지의 여부를 판별하는 것을 가능하게 하며, 기존의 패스워드 기반의 인증 시스템들과 호환되고, 스케일링 가능하며(대문자 알파벳들로 이루어진 긴 패스워드들로 사용될 수 있으며), 특성 α가 상이한 환경들(PIN 코드, 텍스트형 패스워드들, 그래픽적인 패스워드들)에 적응할 수 있는, 패스워드들을 검증하는 방법을 제공할 수 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명이 구현될 수 있는 예시적인 시스템을 도시하는 도면.

도 2는 본 발명의 한 선호되는 실시예에 따른 패스워드 생성의 방법을 도시하는 도면.

도 3은 본 발명의 한 선호되는 실시예에 따른 패스워드 검증의 방법을 도시하는 도면.

발명을 실시하기 위한 구체적인 내용

[0020] 도 1은 본 발명이 구현될 수 있는 예시적인 시스템을 도시한다. 본 시스템은 계산하는 디바이스{("컴퓨터")110} 및 인증 서버(120)를 포함한다. 본 발명은 컴퓨터(110), 인증 서버(120), 또는 컴퓨터(110) 및 인증 서버(120) 모두 상에서 구현될 수 있다는 것이 이해될 것이다. 컴퓨터(110) 및 인증 서버(120)는, 표준 개인용 컴퓨터(PC) 또는 워크스테이션과 같은 계산들을 수행할 수 있는 임의의 종류의 적절한 컴퓨터 또는 디바이스일 수 있다. 컴퓨터(110) 및 인증 서버(120)는 각각 바람직하게 적어도 하나의 프로세서(111, 121), 램 메모리(112, 122), 사용자와의 상호 작용을 위한 사용자 인터페이스(113, 123), 및 연결(130)을 통해 다른 디바이스들과의 상호 작용

을 위한 제2의 인터페이스(114, 124)를 포함한다. 컴퓨터(110) 및 인증 디바이스(120)는 각각 또한 바람직하게, 프로세서에 의해 수행될 때, 아래에서 설명된 임의의 패스워드 방법들을 수행하는 명령들을 저장하는 디지털 데이터 지지부(140)로부터 소프트웨어 프로그램을 판독하기 위한 인터페이스를 포함한다. 당업자는, 도시된 디바이스들이 명료함을 위해 매우 간소화되었다는 것과, 추가적인 실제 디바이스들이 영구 저장 디바이스들과 같은 특징들을 포함한다는 것을 이해할 것이다.

[0021] 주된 개념은 특성 α {또한 '규칙(rule)' 또는 '함수(function)'라고도 불려짐}을 패스워드들의 집합 Ω에 추가하는 것이다. 이것은 완전한 패스워드 공간을 두 개의 구별된 부분 집합들로 분할할 것이다:

[0022] ● 특성을 고려하는 유효한 패스워드들의 부분 집합(즉 유효한 패스워드 공간)

[0023] $$\Omega_v = \{\omega \in \Omega | \alpha(\omega)\}$$

[0024] ● 특성을 고려하지 않는 무효한 패스워드의 부분 집합

[0025] $$\Omega_i = \{\omega \in \Omega | \neg \alpha(\omega)\}$$

[0026] 이것이 이미, 예컨데 패스워드가 하나의 문자 또는 하나의 숫자와는 다른 하나의 대문자 및 하나의 문자를 포함하는 적어도 8개의 문자들을 포함하도록 요구하는 일부 종래 기술 시스템들에서의 경우라는 것이 이해될 것이다. 하지만 이러한 요구 사항이, 사용자의 패스워드들을 사전 공격들에 덜 취약하게 하기 위해, 단지 이들을 다양화하도록 의도된다는 것을 깨닫는 것이 중요하다; 어떠한 방법으로도 이것은, 자동화된 공격들의 검출을 허용하지 않으며, 허용 가능한 문자들을 제안함으로써 사용자를 유효한 패스워드들로 안내하기 위하여 아무것도 수행하지 않는다.

[0027] 부분 집합들이 유리하게도 동적이라는 것과, 따라서 이들은 시간이 흐르면서 변할 수 있다는 것이 이해될 것이다. 이러한 역동설(dynamism)의 한 예시적인 설명은 무효한 부분 집합 Ω_i에 n번째로 가장 최근에 사용된 패스워드들을 넣는 것이다.

[0028] 부분 집합들이 개별적(distinct)이지만, 이들을 정의하는 규칙들은, 쉬운 구현을 위해, 오버래핑될 수 있는데, 이러한 경우에 한 가지 규칙이 다른 규칙에 우선해야만 한다. 예를 들어 사용자의 출생 연도의 사용을 금지하는 규칙은 유리하게도, 다른 점에서는 특정 결합을 허용할 임의의 규칙들을 무효화(overrule)시킨다.

[0029] 사용자가 사용자 인터페이스를 통하여 패스워드를 입력할 때, 그는 유효한 패스워드 공간 Ω_v에 제한된다. 본 시스템은 무효한 패스워드 공간 Ω_i(및 아마도 또한 제3의 부분 집합)으로부터의 임의의 요청을 공격으로서 간주하며, 이에 따라 반응할 수 있다.

[0030] 특성 α의 선택은 패스워드 엔트로피{password entropy(Ω_v의 사이즈)} 및 공격의 검출 가능성{detectability (Ω_i의 사이즈)} 사이의 절충(trade-off)이다.

[0031] 따라서 특성 α의 사용은 맹목적인 집단 공격들의 검출을 허용한다. 공격자가 체계적으로 모든 패스워드 값들을 시도할 경우, 이것은 반드시 Ω_i의 요소들을 포함할 것이다. 추가적으로 사전 공격들은, 알려진 또는 가능성 있는 사전 요소들(dictionary elements)을 Ω_i에 추가함으로써 반격될 수 있다.

[0032] 특성 α는 복소 함수일 수 있다. 이것은 완전한 패스워드에 적용될 수 있지만, 사용자 인터페이스에 의한 각각의 심볼 입력(symbol entry)에 대하여 바람직하게 보장되어야 한다. 이러한 경우에, 주어진 단계에서 입력될 수 있는 심볼들은 이전에 입력된 심볼들에 의존한다.

[0033] 바람직하게도, 특성 α는 패스워드 공간을, "완전 혼합형(well mixed)"이며 무시할 수 없는(non-negligible) 사이즈인 두 개의 섹션들로 분할하는데, 이는 무작위 패스워드 추측(random password guessing)이 무효한 부분 집합으로부터 패스워드를 사용하는 것에 대한 무시할 수 없는 확률(probability)을 갖는 것을 보장하기 위함이다.

[0034] 예를 들어 텍스트형 패스워드 입력에 있어서, 특성 α는 대문자와 소문자 사이에서 교체가 가능할 수 있다. 이

러한 경우에, 제1의 심볼에 대하여, 임의의 문자(대문자 또는 소문자)가 패스워드 생성 동안에 선택될 수 있다. 이후 사용자 인터페이스는 이전 것이 대문자였을 경우, 소문자들의 집합을 제안하고, 그리고 그 반대로도 가능하다. 따라서 특성 α는 패스워드 생성의 각 단계에서 검증된다.

[0035] 예를 들어 유효한 패스워드 공간 Ω_v과 무효한 패스워드 공간 Ω_i사이의 비율 r이 매우 작을 경우(r<<1), 유효한 패스워드들을 찾아내는 것은 어려우며, 본 시스템은 또한 규칙들의 일부 지식을 구비한 해커들로부터의 공격들에 취약할 수 있다. 다른 한편으로 r>>1일 경우, 거의 모든 패스워드들은 유효하며, 공격을 검출하는 것에 대한 가능성은 작다. 따라서 비율 $r \approx 1$, 즉 0.5<r<2는 눈대중으로서(as a rule of thumb) 사용될 수 있는 좋은 절충안(compromise)임이 드러날 것이다.

[0036] 특성 α는, 예를 들어 사용자 이름과 같은 다양한 요소들에 의존할 수 있다. 이러한 경우에, 두 명의 사용자들은 이들의 패스워드들을 구성하기 위해 상이한 규칙들을 가질 수 있다. 예를 들어 사용자 이름의 문자들 개수가 홀수(각각 짝수)일 경우, 패스워드는 대문자들(각각 소문자들)만을 포함해야 할 것이다. 혼합된 대문자들 및 소문자들로 구성된 임의의 요청이 공격으로서 간주될 것이다. 또 다른 예시는 사용자 이름 및 패스워드의 문자들 개수의 합이 짝수(또는 홀수) 이도록 요구하는 것이다.

[0037] 특성 α의 정의는, 많은 파라미터들을 고려하기 때문에, 매우 복잡할 수 있다. 하지만 너무 복잡한 특성은 다음의 결점들을 가질 수 있다: 결과적인 패스워드들은 기억하기에 어려울 수 있으며, 유효한 패스워드 집합 Ω_v의 사이즈는 너무 작아져서 충분한 엔트로피를 보장할 수 없다.

[0038] 본 시스템에 대한 보안의 전체 레벨은 특성 α의 비밀성(secrecy)에 의존한다. 이러한 특성을 아는 것 또는 추측하는 것은 유효한 패스워드 값들의 집합(Ω_v)을 구성하는 것을 허용하며, 검출되지 않고도 이러한 집합을 이용하여 사전 공격을 수행하는 것을 허용한다.

[0039] 공격자가 유효한 부분 집합 Ω_v을 재구성하는 것을 더 어렵게 하기 위해, 로그인 순간에 사용자 인터페이스에서의 제한(constraints)을 적극적으로 강조하지 않지만, 패스워드 구성 동안에 그렇게 행하는 것은 이롭다.

[0040] 게다가 인증 시스템에서 사용된 종래의 대응책{예컨데 올바르지 않은 패스워드 입력들 사이에 있어서의 시도들(tries) 및 부과된 지연(imposed delay)의 최대 개수}이 본 발명의 솔루션과 결합하여 사용될 수 있다.

[0041] **실례가 되는 예시**

[0042] 본 섹션은 PIN 코드의 사례 연구(study case)를 통해 본 발명의 개념을 설명한다. 본 예시는 또한, 예를 들어 사전 공격들을 피하는 종래의 대응책들의 일반화를 강조한다.

[0043] PIN 코드를 고려한다: {0,...,9}에서 선택된 일련의 4개의 숫자들.

[0044] 일반적으로, 패스워드 생성에 있어서 어떤 조건도 없는 종래 기술의 경우에, 패스워드 공간 Ω는 "0000" 및 "9999" 사이의 모든 (십진) 숫자들로 표현되는데, 즉 $\Omega = \{p_1p_2p_3p_4 \mid p_i \in \{0,...,9\}\}$이다.

[0045] 이하에서, PIN 코드는 p로 표시되며, $p = p_1p_2p_3p_4$이고, 여기서 $p_i \in \{0,...,9\}$이다.

[0046] 일반적인 경우에 있어서: $$\alpha : \begin{Bmatrix} \Omega_v = \Omega \\ \Omega_i = \Phi \end{Bmatrix}$$

[0047] 제1의 단계는 특정 집합, 너무 자주 사용되었거나, 또는 너무 간단한, 예를 들어 동일 숫자가 4번 반복되거나(예컨데 "7777") 또는 4개 숫자들이 증가하는 시퀀스에 속하는(예컨데 "1234") 결합들의 "사전"을 배제하는 것일 수 있다. 따라서 구현된 본 시스템은, 선택된 PIN 코드가 사전의 부분이 아니라는 것을, 패스워드 생성 동안, 검증할 것이며, 이러한 경우에, 선택된 PIN 코드를 유효화한다. 로그인(또는 다른 종류의 인증) 동안, 무효한 부분 집합 Ω_i으로부터의 PIN 코드가 입력된 경우에, 본 시스템은 예외를 발생시키고(raise an exception), 계획된 대응책들을 취한다.

$$\alpha' : \begin{cases} \Omega_v = \Omega \setminus \Omega_i \\ \Omega_i = \{p \mid p_1 = p_2 = p_3 = p_4 \text{ or } p_{j+1} = p_j + 1\} \end{cases}$$

[0048] 심볼들에 있어서:

[0049] 제2의 단계는 패스워드 공간 Ω을 유효한 부분 집합 및 무효한 부분 집합(후자는 "사전"과 결합될 것임)으로 분할하기 위해 함수 α를 적분(integrate)하는 것일 수 있다. 예를 들어 함수 α는, 모든 숫자의 패러티(parity)가 이전의 것에 대하여 변경되어야 함을 진술할 수 있다. 본 시스템은 자체 인터페이스를 개조함으로써, 그리고 유효한 숫자만을 선택적으로 도시함으로써, 생성 단계 동안, 이러한 규칙의 관찰(observation)을 선택적으로 강요한다. 패스워드 인증 동안, 본 시스템은 입력된 PIN이 규칙 α를 고려하는 지를 점검한다; 만약 그렇지 않을 경우, 예외가 발생되고, 본 시스템은 계획된 대응책들을 취한다.

[0050] 다시 한번, 심볼들에 있어서:

$$\alpha'' : \begin{cases} \Omega_v = \{p \in \Omega \mid p_{j+1} \text{ and } p_j \text{ have different parity}, \quad j = 1, \ldots, 4\} \setminus \Omega_i \\ \Omega_i = \{p \mid p_1 = p_2 = p_3 = p_4 \text{ or } p_{j+1} = p_j + 1, j = 1, \ldots, 4\} \end{cases}$$

[0051]

[0052] 이러한 예시에서, 함수 α"는 사전 조건에 의해 금지된 일부 결합들을 허용한다.

[0053] 이후 제3의 단계는, 패스워드 생성에 있어서, 인터페이스를 통한 활성 조건(active condition)을 실시하는 것이며, 또는 무효한 PIN 코드를 단순히 거부하는 것이다. 패스워드 인증 동안, 본 시스템은 양 조건들을 검증하며, 그렇지 않을 경우, 예외를 발생시키는 제2 및 제3 단계에서와 같이 진행된다.

[0054] 유효한 PIN 코드들의 변화성(variability)이 α에서부터 α"까지 감소하지만, 여전히 PIN 코드의 선택을 위해 유용한 사이즈를 유지하고 있음이 쉽게 검증될 수 있다. 또한 허용되고 금지된 PIN 코드 집합들이 무시할 수 없는 사이즈이고, "완전 혼합형"이라는 것이 관찰될 수 있다. 후자의 특성은 본 시스템을 공격하기 위해 사용된 툴들(tools)에도 또한 의존하며, 사용된 특정 α 함수에만 의존하는 것은 아니다.

[0055] 선택적으로, 이미 상술된 바와 같이, 사용자 이름에 의존하는 함수 α에 변화성을 추가하는 것이 가능하다.

[0056] 이러한 PIN 예시에 있어서, PIN 코드의 제1 숫자의 패러티는 사용자 이름 길이의 패러티와 상이함이 요구된다. $\log in$은 사용자에 의해 입력된 사용자 이름을 나타내고, $\#\{\log in\}$은 그 길이를 나타내며; 또한 p_0은 $\#\{\log in\}$의 패러티를 나타낸다.

[0057] 심볼들 안의 α에서 이러한 조건을 포함하는 것은 다음을 야기한다:

$$\alpha''' : \begin{cases} \Omega_v = \{p \in \Omega \mid p_{j+1} \text{ and } p_j \text{ have different parity}, j = 0, \ldots, 4\} \setminus \Omega_i \\ \Omega_i = \{p \mid p_1 = p_2 = p_3 = p_4 \text{ or } p_{j+1} = p_j + 1\} \end{cases}$$

[0058]

[0059] 도 2는 본 발명의 한 선호되는 실시예에 따른 패스워드 생성을 위한 방법을 도시한다. 본 방법은 컴퓨터(110) 또는 컴퓨터(110)와 상호 작용하는 인증 서버(120) 상에서 구현될 수 있다.

[0060] 우선적으로, 본 시스템은 가능한 문자들, 즉 단계(210)의 다음 사용자 입력을 위해 특성 α를 준수하는 문자들을 제안할 수 있다. 특히 제1의 문자에 대하여, 선택이 자유일 경우, 이번 단계는 건너뛸 수 있다. 본 단계는, 입력 문자가 특성 α를 준수하고, 이러한 경우가 아니라면, 문자를 수용하는 것을 거부하는 단계로 대체될 수 있다는 것이 이해될 것이다.

[0061] 이후 문자는 단계(220)에서 사용자로부터 수신되고, 패스워드가 완전한 지가 단계(230)에서 검증된다. 이것은 (사용자가 아이콘을 클릭하거나, 'Return'을 누르는 경우와 같은) 사용자 입력에 의해 지시될 수 있지만, 또한 암시적일 수도 있다. 패스워드가 완전할 경우, 본 방법은 단계(240)에서 종료되며; 그렇지 않을 경우, 본 방법은 단계(210)로 되돌아 간다.

[0062] 도 3은 본 발명의 한 선호되는 실시예에 따른 패스워드 검증의 방법을 도시한다. 패스워드 검증 방법은, 사용자

가 검증될 패스워드에 의해 보호되는 실재물{이용 계정(account), 디바이스, 서버 등)에 로그온할 때, 이롭게 수행된다. 패스워드 생성 방법과 마찬가지로, 본 검증 방법은 컴퓨터(110) 또는 인증 서버(120)에 의해 구현될 수 있다. 문자가 단계(310)에서 수신되고, 문자가 특성 α를 준수하는 지가 단계(320)에서 검증된다. 이러한 경우가 아니라면, 맹목적인 집단 공격이 시도되었는 지와, 적절한 조치가 단계(330)에서 취해질 수 있는지가 결정될 수 있다. 적절한 조치는, 예를 들어 관리자 및/또는 사용자에게 경고를 발하는 것, X의 순응하지 않는 패스워드들의 입력 이후에 시스템을 차단하는 것, 및 추가적인 시도를 수용하기 이전에 지연의 사용일 수 있다. 전체 패스워드가 입력될 때까지, 적절한 조치를 유보하는 것이 가능하며, 이러한 경우에 본 방법은 단계(340)를 계속한다는 것이 이해될 것이다. 특정 수의 올바르지 않은 패스워드들(즉 특성 α를 고려하지 않는 패스워드들)이 입력될 때까지, 적절한 조치가 또한 연기될 수도 있다; 올바르지 않은 패스워드들의 개수는 시간, 예컨데 최근 Y초에서의 올바르지 않은 패스워드들의 개수 X로 간주될 수 있다.

[0063] 단계(340)에서, 패스워드가 완전한 지의 여부가 검증되며, 이는 생성 방법의 단계(230)와 유사한 방식으로 수행된다. 이러한 경우가 아니라면, 본 방법은 단계(310)에서 다음의 문자의 수신을 기다린다; 하지만 이러한 경우이면, 특성 α가 고려되지 않는 경우, 엄밀히 말해 패스워드가 올바르지 못한 경우, 입력 패스워드가 필수적이지 않을지라도, 이것은 단계(350)에서 검증된다. 다른 말로, 입력 패스워드는 실재물을 보호하는 패스워드에 해당한다는 것이 검증된다. 상술된 바와 같이, 적절한 조치는 이 시점에서 취해질 수 있으며, 더 일찍 취해질 수도 있다. 또한 특성 α에 대한 준수(compliancy)가 이 단계까지 지연될 수 있다{즉 단계(320)는, 패스워드의 검증 이전 또는 패스워드의 성공적이지 못한 검증 이후에, 단계(350)까지 발생하지 않는다}는 것이 주목되어야 할 것이다.

[0064] **대안적인 실시예**

[0065] 특성 α를 표현하는 상이한 방법은, 사용자에 의해 통합적으로 선택된 패스워드의 끝에, "패딩 인증(authenticating padding)"으로서 서버에 의해 선택된 하나 이상의 문자들을 첨부하는 것이다. 문자들이, 사용자에 의해 입력된 패스워드, 사용자의 로그인, 및 서버 측 비밀 파라미터를 파라미터들로서 다루는 의사 난수 함수(pseudo-random function)의 결과인 것은 바람직하다. 이러한 솔루션의 단점은 사용자가 자신의 패스워드에 추가된 더 많은 문자들을 의무적으로 익혀야 한다는 것이다.

[0066] 후자의 예시로서, HMAC(해쉬 기반의 메시지 인증 코드) 기반의 솔루션이 있다: 생성 단계 동안, 사용자는 자신의 패스워드를 입력하고, 본 시스템은 이것의 HMAC를 계산하며, 사용자에 의해 입력된 패스워드와 HMAC의 제1 n 비트들을 묶음으로써 구성된 "완전한" 패스워드를 되돌린다. 인증 단계 동안, 사용자는 패스워드를 입력하는데, 이로써 본 시스템은 이것이 가능한 패스워드인지의 여부를 점검하여, 마지막 n 비트들이 HMAC 값에 해당하는 지를 검증한다.

[0067] 본 발명이,

[0068] ● 맹목적인 집단 및 사전 공격들에 저항하는,

[0069] ● 본 시스템이 공격 하에 있는지의 여부를 판별하는 것을 가능하게 하는,

[0070] ● 기존의 패스워드 기반의 인증 시스템들과 호환되는,

[0071] ● 스케일링 가능한(대문자 알파벳들로 이루어진 긴 패스워드들로 사용될 수 있는), 그리고

[0072] ● 특성 α가 상이한 환경들(PIN 코드, 텍스트형 패스워드들, 그래픽적인 패스워드들)에 적응할 수 있는,

[0073] 패스워드들을 검증하는 방법을 제공할 수 있다는 것이 이해될 것이다.

[0074] 본 개시 사항에 개시된 각각의 특징, (적절한 위치에 있는) 청구항들 및 도면들이 독립적으로 또는 임의의 적절한 결합으로 제공될 수 있다. 하드웨어로 구현될 것으로 설명된 특징들은 또한 소프트웨어로, 그리고 역으로 구현될 수 있다. 청구항들에서 등장하는 참조 번호들은 예시의 목적만을 위함이고, 본 청구항들의 범주를 제한하는 어떠한 영향도 끼치지 않을 것이다.

부호의 설명

[0075] 110 : 컴퓨터 111, 121 : 프로세서

112, 122 : 메모리 113, 123 : 사용자 인터페이스

114, 124 : 입력/출력 인터페이스 120 : 인증 서버

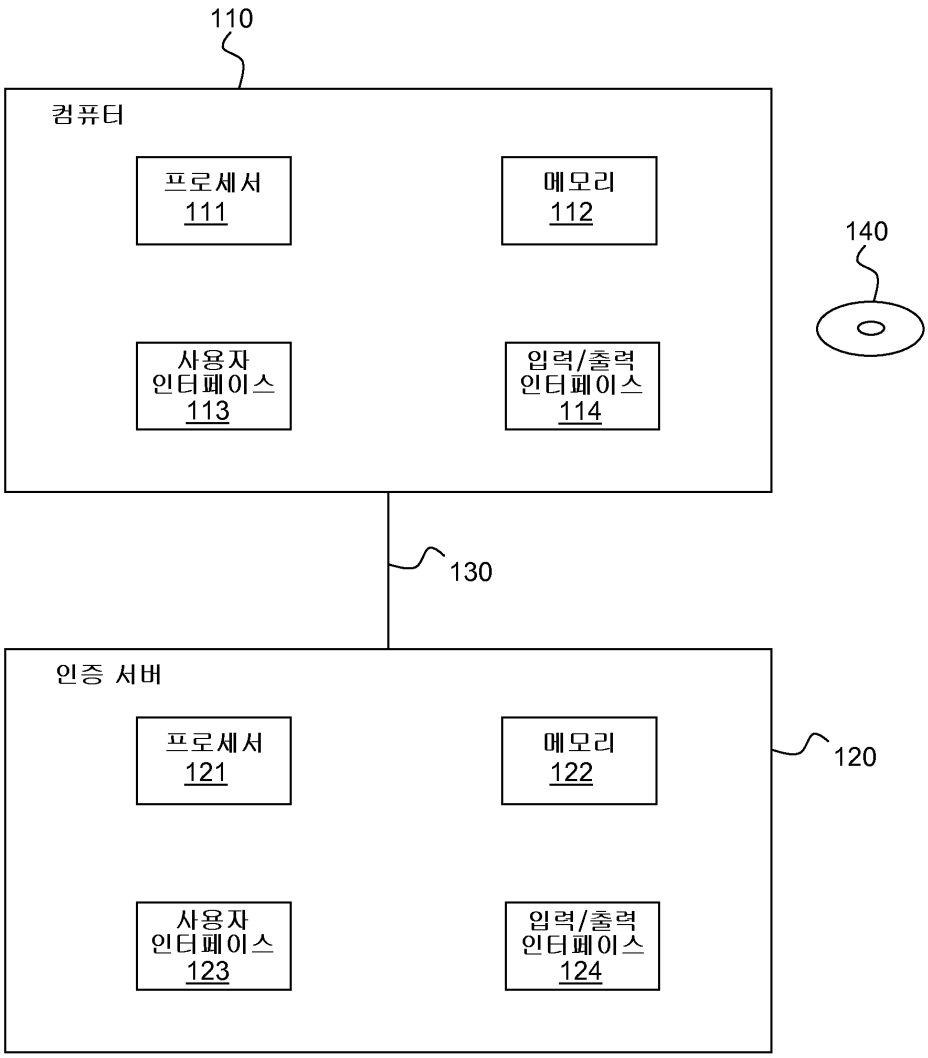
130 : 연결 210 : 제안 단계

220, 310 : 문자 수신 단계 230, 340, 350 : 검증 단계

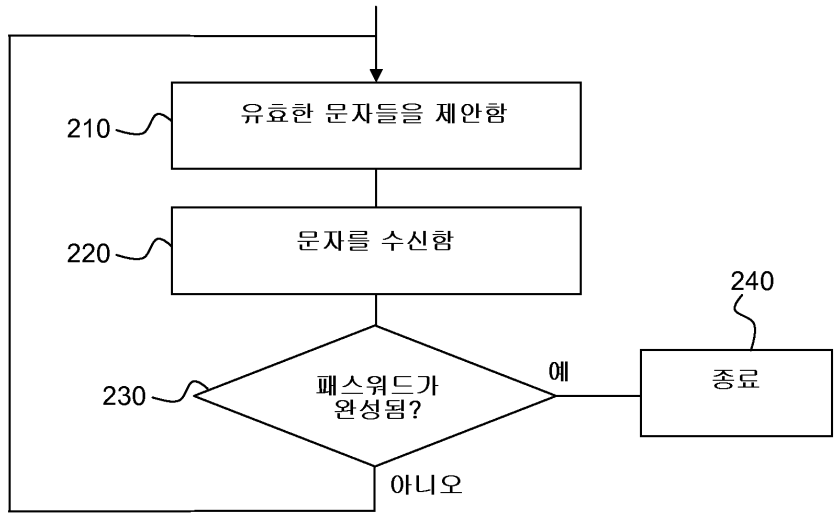
330 : 조치를 취하는 단계 240 : 종료 단계

도면

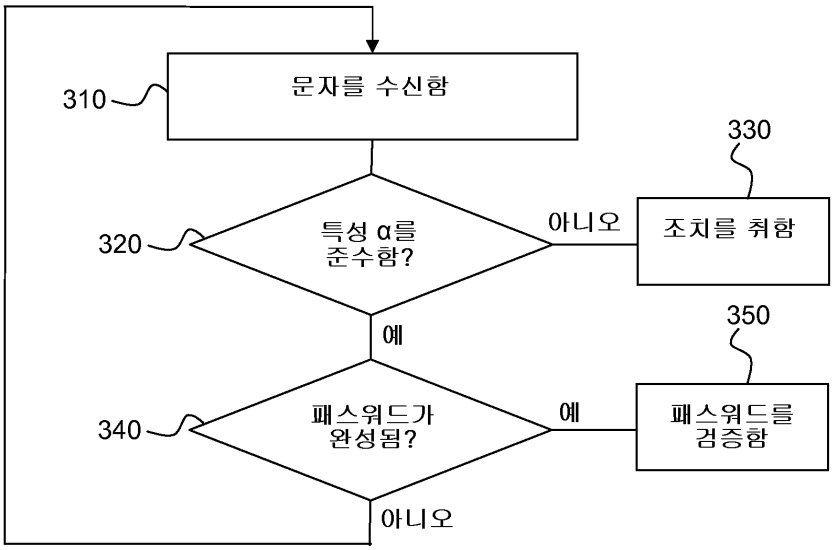
도면1



도면2


210
유효한 문자들을 제안함
220
문자를 수신함
240
230
패스워드가
완성됨?
예
종료
아니오

도면3


310
문자를 수신함
330
320
특성 α를
준수함?
아니오
조치를 취함
350
예
340
패스워드가
완성됨?
예
패스워드를
검증함
아니오