(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 15/00 (2006.01)
G06F 13/00 (2006.01)

(11) 공개번호 10-2006-0048819
(43) 공개일자 2006년05월18일

(21) 출원번호 10-2005-0068468
(22) 출원일자 2005년07월27일

(30) 우선권주장 10/941,559 2004년09월15일 미국(US)

(71) 출원인 마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이

(72) 발명자 래저, 스텔링 엠.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
친타, 라메쉬
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
래츠, 폴 제이.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
브레작, 존 이.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내
플로, 에릭 알.
미국 98052 워싱턴주 레드몬드 원 마이크로소프트 웨이마이크로소프트 코포레이션 내

(74) 대리인 주성민
이중희
백만기

심사청구 : 없음

(54) 신뢰된 네트워크 노드들에 대한 액세스 권한을 제어하는방법 및 시스템

요약

컴퓨터에의 액세스를 제어하는 시스템 및 방법은, 네트워크에의 외부 액세스에 대하여는 강한 보안을 유지하는 한편, 로컬 네트워크 내부에서는 약한 보안을 제공한다. 일실시예에 있어서, 사용자는 로그인 패스워드를 선택, 입력, 및 기억할 필요 없이 비관리형 네트워크 내부의 보안된 그룹의 신뢰된 노드들에의 액세스 권한을 갖는다. 컴퓨터 상의 사용자에 대하여 이러한 보안상 안전한 블랭크 패스워드 또는 원클릭 로그온 계정을 설정하기 위하여, 강한 랜덤 패스워드가 생성 및 저장되

고, 계정은 블랭크 패스워드 계정으로 지정된다. 디바이스가 보안된 네트워크 그룹의 일부이면, 강한 랜덤 패스워드는 다른 신뢰된 노드들로 복사된다. 블랭크 패스워드 계정의 사용자가 컴퓨터에 로그온 하고자 하는 경우, 저장된 강한 랜덤 패스워드가 검색되어, 사용자가 인증된다.

대표도

도 3

색인어

랜덤 패스워드, 블랭크 패스워드, SSP, SAM, WinLogon

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 실시예가 구현될 수 있는, 소수의 컴퓨팅 장치들이 보안된 네트워크 그룹으로 형성되는 로컬 컴퓨터 네트워크를 나타낸 개략도.

도 2는 본 발명의 실시예에 따른, 사용자에 의한 새로운 원클릭 로그온 계정의 생성에 관한 단계들을 나타낸 플로우차트.

도 3은 본 발명의 일실시예에 따른 원 클릭 로그인 계정을 통해 머신으로의 사용자 로그인과 관련된 단계들을 나타낸 플로우차트.

도 4는 본 발명의 일실시예에 따라 구성된 컴퓨터들의 구성요소들을 나타낸 블록도.

<도면의 주요부분에 대한 부호의 설명>

100: 로컬 네트워크 102: 보안된 네트워크 그룹

106, 108, 110, 118: 디바이스 104: 허브/스위치

120: SSP 122: LSA

124: SAM 128: WinLogon

130: LogonUI 126: 보안 정보

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 컴퓨터 및 컴퓨터 네트워크들에 관한 것으로서, 특히 사용자가 로그인 패스워드를 선택, 입력, 및 기억할 필요없이, 무관리형(unmanaged) 컴퓨터 네트워크들의 신뢰된 노드들에 대하여 보안상 안전한 사용자 계정 액세스를 제공하는 방법 및 시스템에 관한 것이다.

대규모 컴퓨터 네트워크 특성은 사용자 액세스를 관리하는 관리 구조(administration schemes)를 복잡하게 하였다. 대규모 네트워크는 통상 다수의 도메인들을 포함하며, 그 각각은 도메인 내의 머신들에 대한 허가 정보, 사용자명, 및 패스워드와 함께 주 도메인 컨트롤러(main domain controller)를 갖는다. 인증된 사용자는 동일한 사용자명 및 패스워드를 사용하여 도메인 내의 어느 머신에나 로그온 할 수가 있다. 머신에 로그온 되는 동안 사용자에 의한 패스워드 변경은, 도메인 내의 다른 머신들에 의해 인식된다.

이와 대조적으로, 홈 네트워크와 같은 소규모의 로컬 네트워크는 일반적으로 무관리형(unmanaged)으로서, 중앙집중식의 자동화된 방식으로 계정 정보를 관리하기 위한, 전용의 "상주형(always-on)" 디바이스가 없다. 무관리형 네트워크의 머신들은 통상 동일한 허브 또는 라우터에 연결되어, 허술하게 구성된, P-P(peer-to-peer) 워크그룹으로 주로 동작한다. 이러한 네트워크는 특성상 사용자에게 불편하였다. 예컨대, 최근까지 사용자는 사용자가 액세스하고자 하는 네트워크의 각각 디바이스 상에 로컬 계정을 설정할 것이 요구되었다. 하나의 머신 상의 패스워드를 사용자가 변경시킨 경우, 그 변경은 그룹의 나머지 머신들에 대하여 자동적으로 복사되지 않았다.

컴퓨터 사용자들은 자신들의 데이터에 대한 무권한의 액세스에 대하여, 보안성과 편리성 모두를 요구한다. 통상 인가된 사용자들만이 네트워크의 머신에 대한 물리적인 액세스를 취득하므로, 홈 네트워크의 사용자들은 무권한의 외부 침입으로부터의 보호를 필요로는 하지만, 네트워크 내에서 높은 보안성을 기대하지는 않는다. 독립형 컴퓨터들 또는 소규모 네트워크의 사용자들은, 주로 보안을 위해서가 아니라, 데이터 분별 및 개별적인 사용자 편의를 위해서, 개별의 사용자 계정들을 갖는다. 따라서, 단일의 머신들에서, 사용자들은 일반적으로 패스워드에 의해 보호되지 않는 계정(더욱 자세하게는, 패스워드가 블랭크로 된 계정)의 편리성을 선호한다. 그러나, 마이크로소프트 윈도우즈® 운영체제에 기반한 것 등의 홈 네트워크들은, 사용자가 네트워크 내의 또 다른 머신으로부터 그 머신에의 액세스를 얻기 위해서는, 머신상에서 패스워드에 의해 보호되는 계정을 사용자가 가질 것을 요구하는 신뢰 모델(trust model)을 갖는다.

발명이 이루고자 하는 기술적 과제

사용자들은, 패스워드를 추출하는 무자비한 공격(brute force) 및 사전적 공격들(dictionary attacks)을 통한 무권한의 액세스에 대한 방호를 위해서, 비교적 복잡하거나 또는 "강한" 계정 패스워드를 채용할 것이 권고된다. 강한 패스워드는 길이로는 적어도 7개의 문자로서, 숫자와 부호를 포함한다. 그러나, 강한 패스워드는 비교적 기억하기 어렵고, 컴퓨터에 타이핑하기 어렵다. 일반적으로, 사용자들은 침입자들에게 취약할지라도 간단하고 기억하기 쉬운 패스워드를 선호한다. 홈 네트워크에 있어서, 사용자가 데이터에 원격으로 액세스하기를 원한다면, 사용자는 패스워드를 가져야 하지만, 사용자가 강한 패스워드를 채용하지 않는다면, 사용자의 데이터는 원하는 만큼 안전한 것은 아니다. 어떠한 컴퓨터 시스템은 "자동 로그온" 기능을 가져, 사용자의 패스워드가 저장되고, 사용자가 로그인 시에 검색되지만, 자동 로그온 계정은 사용자가 그 계정에 대하여 선택한 패스워드 만큼만 안전할 뿐이다.

발명의 구성 및 작용

본 발명은 무관리형 네트워크 내의 보안된 그룹을 형성하는 신뢰된 노드들과 같은 하나 이상의 컴퓨터들에의 액세스를, 네트워크에의 외부 액세스에 대하여 강한 보안성을 구비하지 않고서 로컬 네트워크 내의 약한 보안성의 장점이 얻어지는 방식으로, 제어하는 방법 및 시스템을 제공하는 것에 관한 것이다. 일실시예에 있어서, 네트워크의 머신들로의 물리적 액세스 권한을 갖는 사용자는 패스워드를 지정, 입력, 및 기억할 필요없이 임의의 신뢰된 노드로부터 데이터에 액세스할 수가 있다.

본 발명의 일 양태에 따르면, 보안된 네트워크 그룹의 노드에의 액세스를 제어하는 시스템이 제공된다. 본 시스템은, 보안된 네트워크 그룹을 형성하는 복수의 상호 신뢰된 노드들, 및 보안된 네트워크 그룹으로의 외부적인 액세스에 대하여는 강한 보안을 유지하는 한편, 보안된 네트워크 그룹 내에서는 약한 보안을 제공하는 메카니즘을 포함한다. 이러한 메터니즘은 보안된 네트워크 그룹 내의 사용자로 하여금 인증 기밀정보를 입력할 필요없이 다른 노드들로 액세스 하도록 한다.

본 발명의 다른 양태에 따르면, 사용자에게 하나 이상의 컴퓨터에의 액세스를 제공하는 방법이 개시된다. 제1 컴퓨터에서, 새로운 사용자 계정에 대하여 강한 랜덤 패스워드가 생성된다. 예컨대 플래그를 설정함으로써, 계정은 블랭크 패스워드 계정으로 지정되고, 강한 랜덤 패스워드는 데이터베이스 등에 저장된다. 일실시예에 있어서, 사용자는 블랭크 패스워드 계정 또는 종래의 계정을 설정하는 것을 선택할 수 있다. 컴퓨터가 신뢰된 노드들의 보안된 네트워크 그룹의 일부라면, 강한 랜덤 패스워드는 그룹 내의 다른 노드들에 복사된다.

본 발명의 또 다른 양태에 따르면, 컴퓨터에의 사용자의 액세스를 제어하는 방법이 제공된다. 사용자는 머신으로 로그온 하는 계정을 선택한다. 예컨대, 플래그를 체크함으로써, 선택된 계정이 블랭크 패스워드 계정인 것으로 판정되면, 예컨대, 데이터베이스를 조회함으로써 그 계정에 관련되는 저장된 강한 랜덤 패스워드가 검색된다. 그 후, 사용자는 그 패스워드에 기초하여 인증될 수도 있다. 계정이 블랭크 패스워드 계정이 아니라면, 사용자는 종래의 로그인과 같이 패스워드를 입력하도록 프롬프트 상태가 된다.

본 발명은 생체인식에 의해 인증되는 계정들로 설정된 사용자 계정들에 대하여 블랭크 패스워드 또는 원클릭 로그온 기능을 제공하는데 사용될 수도 있다. 본 발명의 실시예들은 무관리형 또는 관리형 네트워크들에서 구현될 수도 있으며, 독립형 머신들(standalonoe machines)에서 구현될 수도 있다. 보충적으로, 본 발명은 그 전체 혹은 부분에 있어서 하드웨어 또는 소프트웨어 또는 그 조합으로 구현될 수도 있다.

일반적으로 설명하면, 본 발명은, 네트워크에의 외부 액세스에 대하여 강한 보안을 구비하지 않고서도 로컬 네트워크 내에서 약한 보안의 장점을 성취하는 방식으로, 보안된 로컬 네트워크 그룹의 신뢰된 노드들과 같은, 컴퓨터에의 액세스를 제어하는 시스템 및 방법을 제공한다. 일실시예에 있어서, 네트워크의 머신들로의 물리적 액세스 권한을 갖는 사용자는 패스워드를 지정, 입력, 및 기억할 필요없이 임의의 신뢰된 노드로부터 데이터를 액세스할 수 있다. 이로서, 독립형 머신들의 블랭크 패스워드 계정들의 개방적이고 편리한 모델이 보안된 네트워크까지 확장된다. 사용자 계정이 블랭크 패스워드 계정으로 설정되는 경우, 암호학적으로 강한 랜덤 패스워드가 생성되고, 이 생성된 패스워드는 보안 계정 데이터베이스에 보안상 안전하게 저장된다. 본 발명의 실시예들에 있어서, 사용자는 사용자 타일 등을 단지 클릭함으로써 네트워크의 머신으로 로그인한다. 따라서, 본 발명에 따른 블랭크 패스워드 계정은 "원클릭 로그온" 계정으로 설명될 수 있다. 사용자 보안 계정 정보가 네트워크의 몇몇 머신들로 복사되므로, 사용자는 이러한 모든 머신들에 대한 원클릭 로그온 액세스 기능을 갖는다.

도 1을 참조하면, 본 발명의 일실시예는 소수의 컴퓨팅 장치들을 구비하는 무관리형 로컬 네트워크(100) 내에서 구현하기에 용이하다. 이러한 네트워크는 일반적으로 많은 홈 네트워크 및 소규모 사업용 네트워크들이 해당한다. 로컬 네트워크(100)는 도메인 컨트롤러 등의 중앙집중식 관리 구성요소를 갖지 않는다는 의미에서 무관리형(unmanaged)이다. 도시된 로컬 네트워크(100)는 네트워크 허브 또는 스위치(104)와, 이에 연결된 복수의 컴퓨팅 장치들을 갖는다. 컴퓨터들 간의 연결은 무선일 수도 있으며, 또는 유선일 수도 있다. 예컨대, 디바이스(116)는 액세스 포인트(114)를 통해 무선으로 네트워크와 통신한다. 로컬 네트워크(100)와 같은 네트워크에서 전개될 수 있는 컴퓨팅 장치들의 예로는, 이에 한하지 않지만, PC, 핸드헬드 컴퓨팅 장치, PDA, 랩톱 컴퓨터, 휴대 전화, 디지털 카메라, 프로세서 및 메모리를 갖는 전자 기기, 특수 목적의 컴퓨팅 장치, 등을 포함한다. 이러한 디바이스들의 세부적인 예들은 당업자에게 자명한 것으로서 더 이상 여기서 길게 설명할 필요는 없다.

도 1에 도시된 바와 같이, 네트워크(100)의 머신들의 부분집합, 즉 디바이스(106, 108, 110, 및 118)들은, (디바이스들을 연결하는 점선으로 개략적으로 나타낸 바와 같이) 보안된 네트워크 그룹(102)을 형성하여, 중앙집중형 관리 성분을 필요로 하지 않고, 사용자 액세스 및 리소스 공유에 대한 그룹 전체의 제어를 제공하였다. 본 발명의 문맥에서, "보안된 네트워크 그룹"이라는 것은, 사용자별로 그룹 내부에서 리소스들의 공유를 허용하는 한편, 그룹 외부의 컴퓨터 또는 사용자에 의한 무권한의 액세스 및 리소스의 사용을 막도록 그룹 전체에 걸쳐서 보안 정책(security policy) 및 액세스 제어가 구현되는 것을 의미한다. 보안된 네트워크 그룹의 디바이스들은 그들 사이에서 신뢰를 구축하고, 그 그룹내의 사용자 계정 데이터 및 사용자 프로파일 데이터와 같은 정보를 공유하였다. 보안된 네트워크 그룹은 특정의 네트워크 토폴로지에 의존하지 않는다. 새로운 디바이스가 보안된 네트워크 그룹(102)에 더해질 수도 있으며, 그룹내의 디바이스들이 보안된 그룹에 남아 있을 수도 있고, 특별한 경우에는, 그룹에서 축출될 수도 있다.

그룹(102)의 각 컴퓨팅 장치는, 사용자 계정 데이터를 포함하는 보안 정보 또는 그 등가물의 데이터베이스를 유지한다. 사용자 계정 데이터는, 각각의 인증된 사용자와 관련되며, 내부 프로세스에 의해 사용되어 사용자 계정을 식별하는, 고유한 보안 식별자(SID: Security Identifier)를 포함한다. 대표적인 실시예에 있어서, SID는 가변길이의 수치값이다. 보안된 네트워크 그룹이 형성되고 난 후에, 그룹의 각각의 머신에 대한 보안 정보는 그룹내의 다른 머신들에 대하여 복사된다. 보안 정보의 복사는, 정당한 계정을 갖는 사용자로 하여금, 그룹내의 임의의 컴퓨터에 로그온 할 수 있도록 한다. 컴퓨팅 네트워크 상의 보안 프로파일 정보의 복사에 대한 더욱 자세한 설명은 동일 출원인의 함께 계류중인 미국 특허출원 제10/414,354호 "Small-Scale Secured Computer Network Group Without Centralized Management"(2003년 4월 15일)에 제공되어 있으며, 이하 참조로서 본 명세서에 포함된다.

컴퓨터(118)와 같은, 보안된 그룹(102)의 디바이스는 로컬 보안 관리부(122)(LSA: Local Security Authority), 보안 지원 프로바이더(120)(SSP: Security Support Provider), 보안 계정 관리자(124)(SAM: Security Account Manager), 저장된 보안 정보(126), 인증 엔진(128)(예컨대, WinLogon), 및 사용자 로그인 표시부(130)(예컨대, LogonUI)를 포함한다. 이러한 구성성분들은 도 4를 참조하여, 이하 더 설명된다.

도 2는 본 발명의 일 양태에 따라서 새로운 원클릭 로그온 계정이 생성되는 절차를 나타낸다. 도 2에 있어서, 시작 블록 뒤에, 결정 블록(200)이 이어지는데, 여기서는 새로운 계정이 원클릭 로그온 계정인지 또는 종래의 사용자 선택의 패스워드 계정인지를 판정한다. 본 발명의 일실시예에서, 사용자가 특히 계정에 대하여 패스워드를 지정하도록 선택하지 않는 한,

원클릭 로그온 계정으로 새로운 사용자 계정이 설정된다. 새로운 계정이 원클릭 계정이 아니라면, 블록 202에서, 사용자는 패스워드를 입력하도록 프롬프트 상태가 된다. 그렇지 않으면, 블록 204에서, 새로운 계정에 대하여 암호학적으로 강한 랜덤 패스워드가 생성된다. 강한 랜덤 패스워드가 사용되므로, 계정이 생성되는 머신은 사전적 공격으로부터 또는 기타의 무권한의 외부 액세스로부터 보호된다. 블록 206으로 가서, 계정이 원클릭 로그온 계정임을 나타내는 데이터 플래그가 설정된다. 플래그는 계정에 대한 일련의 제어 플래그들 중 하나일 수도 있다. 블록 208에서, 생성된 강한 랜덤 패스워드를 포함하는, 사용자의 보안 프로파일 정보는 데이터베이스에 안전하게 저장된다. 다음, 프로세스는 종료 블록으로 간다. 그 후, 사용자 지정의 강한 랜덤 패스워드를 포함하는 사용자 계정 정보는, 보안된 네트워크 환경의 다른 신뢰된 머신들로 복사된다. 다음, 사용자는 패스워드를 입력할 필요없이 보안된 그룹의 임의의 신뢰된 머신으로 로그온 할 수 있다. 당업자라면 이러한 몇몇 단계들의 순서가 임의적일 수도 있으며, 본 발명의 본질을 벗어남이 없이 변경될 수도 있음을 알 수 있을 것이다.

도 3은 머신상에서 기존의 원클릭 계정에 사용자가 로그온 하는 절차를 나타낸다. 시작 블록 후에, 결정 블록 300으로 가서, 이 계정에 대한 원클릭 로그온 플래그가 설정되었는지를 판정한다. 플래그가 설정되지 않은 경우, 블록 302에서 사용자는 패스워드를 입력하도록 프롬프트 상태가 된다. 플래그가 설정된 경우, 로그인 사용자 인터페이스에 패스워드 입력 다이얼로그가 표시되지 않고, 블록 304로 가서, 사용자의 원클릭 계정에 관련된 강한 랜덤 패스워드에 대하여 데이터베이스에 조회한다. 블록 306에서 패스워드가 SSP 에 전달되고, 사용자는 이제 인증되어서, 블록 308에서 로그인을 완료한다. 그 후, 절차는 종료 블록으로 간다.

본 발명의 일실시예에 따라 구성된 컴퓨팅 장치의 구성성분들이 도 4의 블록도에 더 도시되어 있다. 컴퓨터(400)는 LSA(402)를 포함한다. 도시된 실시예에 있어서, LSA(402)는 로컬 시스템 보안 정책에 책임이 있는 사용자 모드의 프로세스이다. 보안 정책은 사용자 인증, 패스워드 정책, 사용자 및 그룹들에 부여되는 권한들, 및 시스템 보안 감사(security audit) 설정과 같은 작업들을 제어한다. SSP(404)는 바람직한 실시예에 있어서 어플리케이션에서 보안 프로토콜 패키지들이 활용가능하도록 하는 동적으로 링크된 라이브러리를 구비한다. SAM(406)은 보안 정보 데이터베이스(408)를 통해 사용자 계정 정보를 관리하는 서비스이다. 또한, 디바이스(400)는 LSA(402) 및 로그인 사용자 인터페이스(412)와 상호동작하는 사용자 인증 엔진(410)을 포함한다.

본 발명의 일 양태에 따르면, 사용자가 원클릭 계정을 통해 컴퓨터(400)에 로그온 하고자 하는 경우, 사용자 인증 엔진(410)은 로그인 사용자 인터페이스 성분(412)이 컴퓨터(400)와 관련된 사용자 계정들을 표시하도록 한다. 사용자 인터페이스(412)를 통해서, 사용자는 사용자 계정 타일(account tile)에 클릭하거나, 그 계정의 다른 표현에 클릭하며, 사용자 인터페이스 성분(412)은 사용자의 선택을 위해 사용자 인증 엔진(410)에 통신한다. 사용자 인증 엔진(410)은 사용자가 선택된 사용자 계정을 통해 로그온 하고자 함을 LSA(402)에 통지한다. LSA(402) 내부에서, SSP(404)는 원클릭 로그온 계정을 통해 머신(400)상에 로그온 하고자 하는 사용자를 인증하는데 사용되도록, SAM(406)을 통해 데이터베이스(408)로부터 패스워드를 검색한다.

본 발명의 실시예들은 생체인식으로 인증하는 계정에 사용될 수도 있다. 생체인식 계정 방호에 있어서, 지문과 같은 뚜렷한 물리적 특징을 입력 장치에 제공함으로써 사용자는 머신에 안전하게 로그온 한다. 본 발명의 일실시예에 따르면, 사용자가 생체인식 계정을 설정하는 경우, 그 계정에 대하여 강한 랜덤 패스워드가 생성되어, 전술한 원클릭 로그온 계정과 같이, 보안 계정 데이터베이스에 저장된다. 사용자가 머신에 로그온하고자 하는 경우, SSP는 데이터베이스에서 강한 랜덤 패스워드를 검색하고, 그 계정이 사용자 로그인에 대하여 인증된다.

무관리형 네트워크 환경뿐만 아니라, 관리형 네트워크 환경에도 본 발명의 기타의 실시예들이 포함된다. 본 발명은 패스워드 다이얼로그를 표시하지 않는 로그인 인터페이스와 같은, 간단화된 사용자 인터페이스에도 사용할 수 있도록 한다. 본 명세서에서 독립형 머신상의 블랭크 패스워드 계정에 한정시켰던 편리한 사용자 인터페이스는 본 발명을 통해 보안된 네트워크 그룹들에 활용 가능하도록 하였다.

발명의 효과

본 명세서에서, 본 발명을 실행하는데 있어서 발명자에게 알려진 최선의 모드를 포함하는, 본 발명의 바람직한 실시예들이 설명된다. 본 발명의 원리가 적용될 수 있는 많은 가능한 실시예들의 관점에서, 본 명세서에서 설명된 실시예들은 예시적인 의미일 뿐이며, 본 발명의 범주를 제한하고자 한 것은 아님을 이해하여야 한다. 당업자라면, 설명된 실시예들이 본 발명의 개념을 일탈함이 없이 그 구성과 세부사항에 있어서 변경될 수 있음을 알 수 있을 것이다. 따라서, 본 명세서에 설명된 바와 같은 본 발명은 이하의 청구범위와 그 균등물의 범주내에 있는 것으로서, 모든 실시예들을 포괄하는 것이다.

(57) 청구의 범위

청구항 1.

보안된 네트워크 그룹의 노드에의 액세스를 제어하는 시스템으로서,

상기 보안된 네트워크 그룹을 형성하는 복수의 상호 신뢰된 노드들; 및

상기 보안된 네트워크 그룹에의 외부 액세스에 대하여는 강한 보안을 유지하는 한편, 상기 보안된 네트워크 그룹 내부에서는 약한 보안을 제공하는 메커니즘

을 포함하는 것을 특징으로 하는 액세스 제어 시스템.

청구항 2.

제1항에 있어서,

상기 보안된 네트워크 그룹 내부에서 약한 보안을 제공하는 메커니즘은, 인증 기밀정보(credential)를 입력할 필요 없이, 상기 보안된 네트워크 그룹 내부의 사용자가 다른 노드들에 액세스 할 수 있도록 하는 메커니즘을 포함하는 것을 특징으로 하는 액세스 제어 시스템.

청구항 3.

제1항에 있어서,

상기 보안된 네트워크 그룹은 무관리형 네트워크의 보안된 네트워크 그룹을 더 포함하는 것을 특징으로 하는 액세스 제어 시스템.

청구항 4.

제1항에 있어서,

상기 보안된 네트워크 그룹 내부에서 약한 보안을 제공하는 메커니즘은, 각각의 노드에서,

원클릭 로그온 계정에 관련되는 강한 랜덤 패스워드를 저장하는 데이터베이스;

로컬 시스템 보안 관리부(security authority);

상기 원클릭 로그온 계정에 사용자가 로그인을 개시하는 때에, 상기 강한 랜덤 패스워드를 검색하는 보안 지원 프로바이더;

상기 보안 지원 프로바이더 및 상기 데이터베이스와 연계하여 동작하는 보안 계정 관리 서비스; 및

로그인 사용자 인터페이스 성분과 상기 로컬 시스템 보안 관리부와 연계하여상기 원클릭 로그온 계정에 대한 로그인을 단속하는 인증 엔진을 포함하는 것을 특징으로 하는 액세스 제어 시스템.

청구항 5.

사용자에게 하나 이상의 컴퓨터에의 액세스를 제공하는 방법으로서,

제1 컴퓨터에서,

상기 사용자의 새로운 계정에 대하여 강한 랜덤 패스워드를 생성하는 단계;

상기 새로운 계정을 블랭크 패스워드 계정으로 지정하는 단계; 및

상기 강한 랜덤 패스워드를 저장하는 단계를 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 6.

제5항에 있어서,

상기 강한 랜덤 패스워드를 저장하는 단계는 상기 패스워드를 보안상 안전하게 저장하는 것을 특징으로 하는 액세스 제공 방법.

청구항 7.

제5항에 있어서,

상기 새로운 계정이 블랭크 패스워드 계정이어야 하는지를 초기에 판정하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 8.

제7항에 있어서,

상기 새로운 계정이 블랭크 패스워드 계정이어야 하는 경우, 상기 사용자가 패스워드를 선택하도록 프롬프트 상태로 하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 9.

제7항에 있어서,

상기 새로운 계정이 블랭크 패스워드 계정인지를 초기에 판정하는 단계는, 상기 새로운 계정이 블랭크 패스워드 계정이 아님을 사용자가 나타내지 않는 한, 상기 새로운 계정을 블랭크 패스워드 계정으로 설정하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 10.

제5항에 있어서,

상기 새로운 계정을 블랭크 패스워드 계정으로 지정하는 단계는, 플래그를 설정하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 11.

제5항에 있어서,

상기 강한 랜덤 패스워드를 저장하는 단계는, 상기 강한 랜덤 패스워드를 데이터베이스를 통해 저장하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 12.

제5항에 있어서,

상기 하나 이상의 컴퓨터들이 복수의 링크된 컴퓨터들을 포함하는 경우, 상기 제1 컴퓨터 외의 상기 복수의 링크된 컴퓨터들의 각각에 상기 강한 랜덤 패스워드를 복사하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 13.

제12항에 있어서,

상기 강한 랜덤 패스워드를 복사하는 단계는, 상기 강한 랜덤 패스워드를 보안된 네트워크 그룹의 하나 이상의 신뢰된 노드들에 복사하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 14.

제13항에 있어서,

상기 보안된 네트워크 그룹에 대하여 적어도 블랭크 되지 않은 패스워드 계정 사용자와 동일한 액세스 권한을 상기 사용자에게 제공하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 15.

제5항에 있어서,

상기 새로운 계정에 대하여 상기 강한 랜덤 패스워드를 생성하는 단계는, 생체인식으로 인증되는 계정에 대하여 강한 랜덤 패스워드를 생성하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제공 방법.

청구항 16.

컴퓨터에의 사용자의 액세스를 제어하는 방법으로서,

상기 사용자에 의해 선택된 계정이 블랭크 패스워드 계정인지를 판정하는 단계;

상기 계정이 블랭크 패스워드 계정인 경우, 상기 계정에 관련되는 저장된 강한 랜덤 패스워드를 검색하는 단계; 및

상기 사용자를 인증하는 단계를 포함하는 것을 특징으로 하는 액세스 제어 방법.

청구항 17.

제16항에 있어서,

상기 계정이 블랭크 패스워드 계정인지를 판정하는 단계는, 상기 계정에 관련되는 플래그가 설정되는지를 판정하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제어 방법.

청구항 18.

제16항에 있어서,

상기 계정이 블랭크 패스워드 계정이 아닌 경우, 상기 사용자로 하여금 패스워드를 입력하도록 프롬프트 상태로 하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제어 방법.

청구항 19.

제16항에 있어서,

상기 저장된 강한 랜덤 패스워드를 검색하는 단계는,

데이터베이스에 조회하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제어 방법.

청구항 20.

제16항에 있어서,

상기 사용자에 의해 선택된 계정이 블랭크 패스워드 계정인지를 판정하는 단계는, 상기 계정이 생체인식으로 인증되는 계정인지를 판정하는 단계를 더 포함하는 것을 특징으로 하는 액세스 제어 방법.

청구항 21.

사용자에게 컴퓨터에의 액세스를 제공하는 컴퓨터 실행가능 명령어를 갖는 컴퓨터 판독가능 매체로서, 상기 명령어는,

상기 사용자의 새로운 계정에 대하여 강한 랜덤 패스워드를 생성하는 단계;

상기 새로운 계정을 블랭크 패스워드 계정으로 지정하는 단계; 및

상기 강한 랜덤 패스워드를 저장하는 단계를 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 22.

제21항에 있어서,

상기 컴퓨터가 네트워크를 통해 제2 컴퓨터에 연결되는 경우, 상기 강한 랜덤 패스워드를 상기 제2 컴퓨터에 복사하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 23.

제21항에 있어서,

사용자에 의한 상기 계정에 대한 후속의 로그인 요청이 블랭크 패스워드 계정 로그인 요청인지를 판정하는 단계;

상기 후속의 요청이 블랭크 패스워드 계정 로그인 요청인 경우, 상기 계정과 관련되는 상기 저장된 강한 랜덤 패스워드를 검색하는 단계; 및

상기 사용자를 인증하는 단계를 더 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

청구항 24.

보안된 네트워크 그룹의 노드에의 액세스를 제어하는 시스템을 구현하기 위한 구성성분들을 갖는 컴퓨터 판독가능 매체로서, 상기 시스템은,

원클릭 로그온 계정과 관련되는 강한 랜덤 패스워드를 저장하는 데이터베이스;

로컬 시스템 보안 관리부(authority);

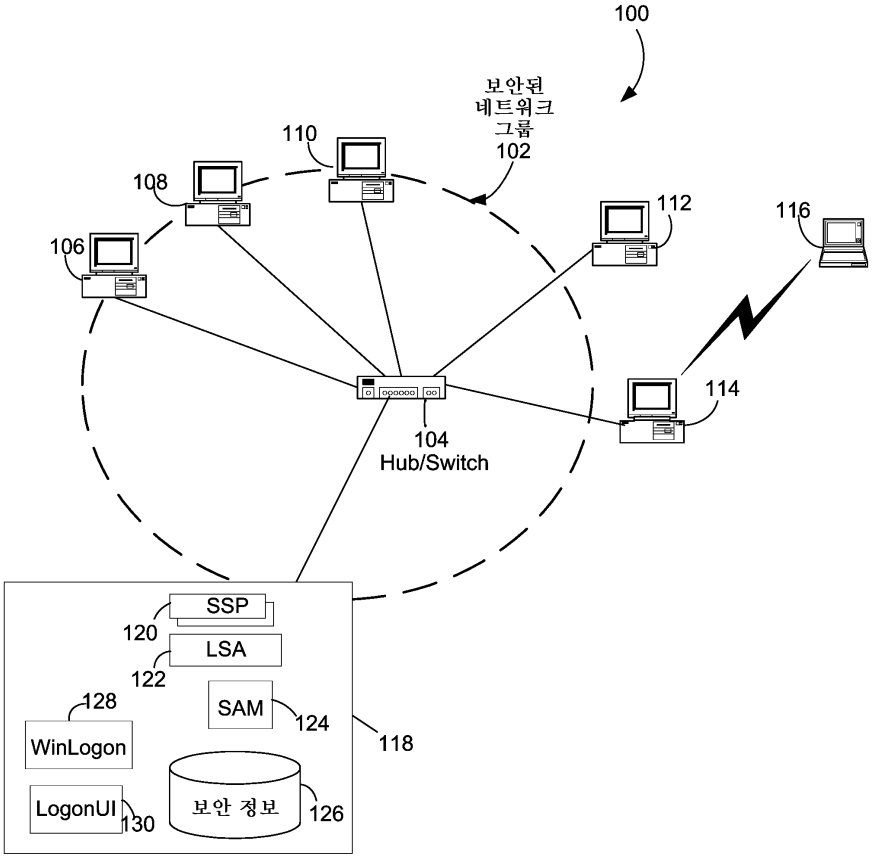
사용자가 상기 원클릭 로그온 계정에 로그인을 시작하는 경우, 상기 강한 랜덤 패스워드를 검색하는 보안 지원 프로바이더;

상기 데이터베이스 및 상기 보안 지원 브로바이더와 연계하여 동작하는 보안 계정 관리 서비스; 및

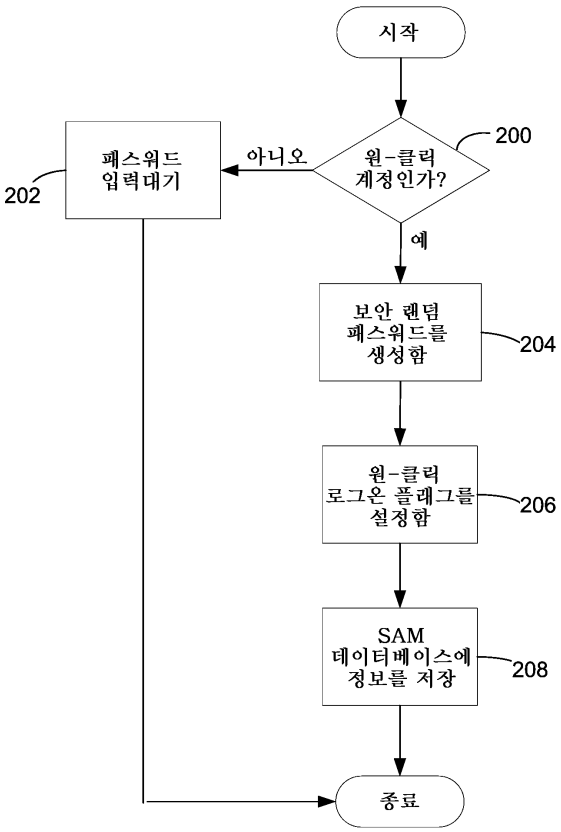
로그인 사용자 인터페이스 성분 및 상기 로컬 시스템 보안 관리소와 연계하여 상기 원클릭 로그온 계정으로의 로그인을 단속하는 인증 엔진을 포함하는 것을 특징으로 하는 컴퓨터 판독가능 매체.

도면

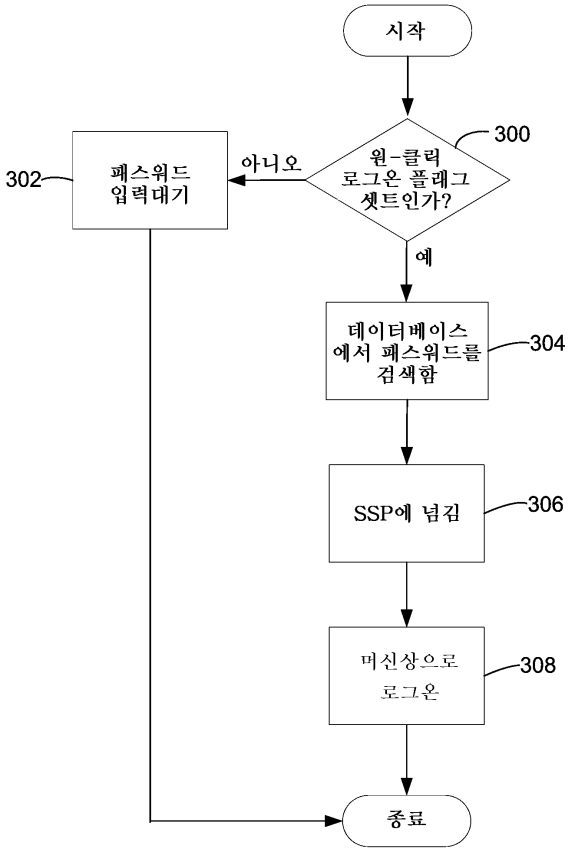
도면1


100
보안된
네트워크
그룹
102
110
108
106
112
116
114
104
Hub/Switch
SSP
120
LSA
122
128
SAM
124
118
WinLogon
LogonUI
130
보안 정보
126

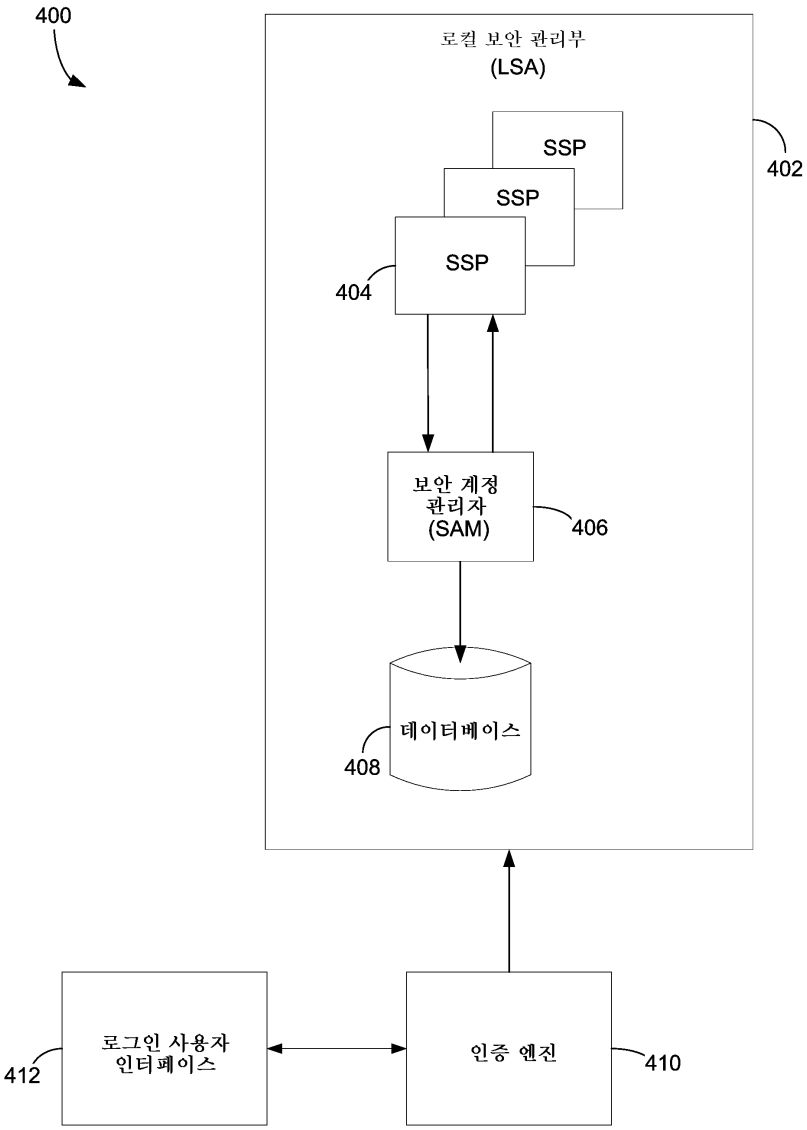
도면2


시작
원-클릭
계정인가?
200
아니오
패스워드
입력대기
202
예
보안 랜덤
패스워드를
생성함
204
원-클릭
로그온 플래그를
설정함
206
SAM
데이터베이스에
정보를 저장
208
종료

도면3


시작
300
원-클릭 로그온 플래그 셋트인가?
아니오
302
패스워드 입력대기
예
데이터베이스에서 패스워드를 검색함
304
SSP에 넘김
306
머신상으로 로그온
308
종료

도면4


400
로컬 보안 관리부
(LSA)
402
SSP
SSP
SSP
404
보안 계정
관리자
(SAM)
406
데이터베이스
408
로그인 사용자
인터페이스
412
인증 엔진
410