(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014 년 10 월 2 일 (02.10.2014)

WIPO | PCT

(10) 국제공개번호
WO 2014/157797 A1

(51) 국제특허분류:
G06F 21/57 (2013.01)

(21) 국제출원번호: PCT/KR2013/009389

(22) 국제출원일: 2013 년 10 월 21 일 (21.10.2013)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2013-0031955 2013 년 3 월 26 일 (26.03.2013) KR

(71) 출원인: **한국전자통신연구원 (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE)** [KR/KR]; 305-350 대전시 유성구 가정동 161 번지, Daejeon-city (KR).

(72) 발명자: **맹영재 (MAENG, Young-Jae)**; 305-810 대전시 유성구 전민동 339-15 번지 엔티스빌 402 호, Daejeon (KR). **이종후 (LEE, Jong-Hu)**; 305-793 대전시 유성구 관평동 테크노밸리아파트 1002 동 1403 호, Daejeon (KR). **박현동 (PARK, Hyun-Dong)**; 305-770 대전시 유성구 지족동 열매마을아파트 504 동 603 호, Daejeon (KR). **박상우 (PARK, Sang-Woo)**; 305-762 대전시 유성구 전민동 엑스포아파트 402 동 1001 호, Daejeon (KR). **박응기 (PARK, Eung-Ki)**; 305-777 대전시 유성구 상대동 682 한라비발디아파트 305 동 204 호, Daejeon (KR).

(74) 대리인: **한양특허법인 (HANYANG PATENT FIRM)**; 135-854 서울시 강남구 논현로 38 길 12 (도곡동, 한양빌딩), Seoul (KR).

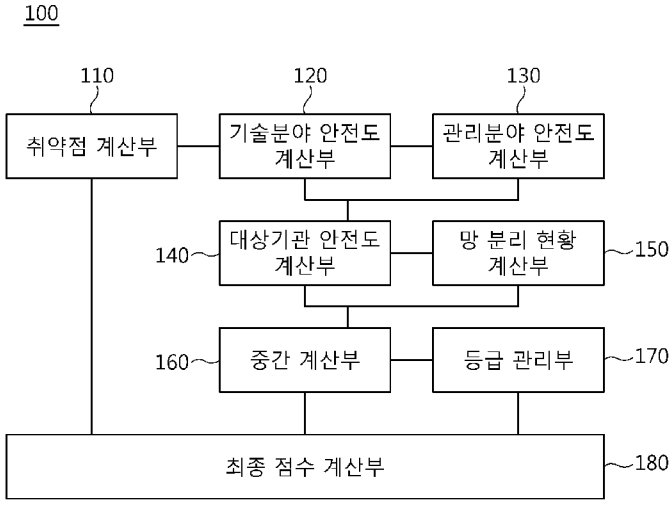
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC,

[다음 쪽 계속]

(54) **Title**: DEVICE FOR QUANTIFYING VULNERABILITY OF SYSTEM AND METHOD THEREFOR

(54) **발명의 명칭** : 시스템의 취약점 정량화 장치 및 그 방법



110 ... Vulnerability calculation unit
120 ... Technical field safety calculation unit
130 ... Management field safety calculation unit
140 ... Target organization safety calculation unit
150 ... Network separation status calculation unit
160 ... Intermediate calculation unit
170 ... Rank management unit
180 ... Final score calculation unit

(57) **Abstract**: The present invention relates to a device for quantifying the vulnerability of a system such that a state of the system can be intuitively and objectively expressed, and a method therefor. The device for quantifying the vulnerability of a system comprises: a vulnerability calculation unit for converting each system vulnerability identification result into a vulnerability score; a target organization safety calculation unit for calculating a target organization safety score corresponding to the system on the basis of a technical field safety score and a management field safety score among vulnerability scores; a network separation status calculation unit for converting a system separation status for an intranet and external networks into a network separation score; an intermediate calculation unit for calculating an intermediate score on the basis of the target organization safety score and the network separation score; and a final score calculation unit for quantifying the vulnerability of the system by calculating a final combined score of the system by using the intermediate score and a simulation hacking rank.

(57) **요약서**:

[다음 쪽 계속]

WO 2014/157797 A1

MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

규칙 4.17 에 의한 선언서:

— 특허출원 및 특허를 받을 수 있는 출원인의 자격에 관한 선언 (규칙 4.17(ii))

공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

본 발명은 시스템의 상태를 직관적 및 객관적으로 표현할 수 있도록 시스템의 취약점을 정량화하는 장치 및 그 방법에 관한 것이다. 시스템의 취약점 정량화 장치는 시스템의 취약점 식별 결과 각각을 취약점 점수로 변환하는 취약점 계산부, 취약점 점수 중 기술분야 안전도 점수와 관리분야 안전도 점수를 토대로 시스템에 해당하는 대상기관 안전도 점수를 계산하는 대상기관 안전도 계산부, 시스템의 업무망과 외부망의 분리 상황을 망 분리 점수로 변환하는 망 분리 현황 계산부, 대상기관 안전도 점수와 상기 망 분리 점수를 토대로 중간 점수를 계산하는 중간 계산부 및 중간 점수와 모의 침투 등급을 이용하여 최종적으로 시스템의 종합 점수를 계산하여 시스템의 취약점을 정량화하는 최종 점수 계산부를 포함한다.

명세서

발명의 명칭: 시스템의 취약점 정량화 장치 및 그 방법

기술분야

[1] 본 발명은 시스템의 취약점 정량화 장치 및 그 방법(APPARATUS AND METHOD FOR QUANTIFYING VULNERABILITY OF SYSTEM)에 관한 것으로, 특히 시스템의 상태를 직관적 및 객관적으로 표현할 수 있도록 시스템의 취약점을 정량화하는 장치 및 그 방법에 관한 것이다.

배경기술

[2] 정보통신 시스템에 대한 취약점을 분석하거나 평가하는 기술은 해당 시스템에 존재하는 취약점을 미리 식별하고, 식별한 결과를 통해 취약점을 제거하기 위함이다. 이와 같이, 시스템에 대한 취약점을 분석하거나 평가하는 기술은 취약점이 불법침해에 악용되기 이전에 제거함으로써, 궁극적으로 다양한 형태의 침해를 미연에 방지할 수 있다. 또한, 시스템에 대한 취약점을 분석하거나 평가한 결과는 해당 조직의 경영진에게 시스템의 안전 상태를 직관적으로 전달하는 방법에 적용할 수 있다.

[3] 한국등록특허 제0851521호는 네트워크 시스템에 대한 보안 기술로서 네트워크 및 시스템에 내재된 취약성을 탐지하고 분석할 수 있는 능동적이고 자동화된 통합적인 사이버 공격 모델을 제공하는 사이버 공격 시스템 및 그 공격 방법에 관한 기술을 소개하였다.

[4] 그러나, 이와 같은 종래의 취약점을 분석하거나 평가하는 기술은 취약성을 탐지하고 분석할 수 있는 능동적이고 자동화된 통합적인 사이버 공격 모델을 제공하고 있을 뿐, 취약점에 대한 직관적 또는 객관적인 평가 결과를 획득하는 기술에 관하여 제시하고 있지 못하다.

[5] 따라서, 시스템에 대한 취약점을 분석하거나 평가한 결과는 정량화되지 않으면 시스템의 상태를 대표값으로 표현하기 어렵다.

[6] 그리고, 취약점을 분석하거나 평가하는 것은 일회성으로 하는 것이 아니라, 주기적으로 수행하는 것이 일반적이다. 주기적으로 수행되는 업무의 결과를 표현할 때에는 현재의 결과 이외에 현재와 과거의 결과를 비교하여 설명하는 부분이 필요하다. 예를 들어, "특정 시스템은 패스워드 관리가 미비하고, 불필요한 서비스가 존재하는 등 접근통제가 미흡하여 위험한 상태이다"와 같은 결과는 청취자를 혼돈스럽게 한다. 이와 같은 경우에는 정량화를 통해 설명하는 것이 가능하다. 예를 들어, "2년 전에는 85점(우수 등급)이었으나, 이번에는 77점(미흡 등급)으로 취약점이 악화되어 있다"와 같이, 현재와 과거의 상황을 수치 또는 등급으로 비교, 설명함으로써 상세한 내용은 표현되지 않지만 현재의 상태를 직관적, 객관적으로 표현할 수 있다.

[7] 취약점을 분석하거나 평가한 결과의 정량화는 반드시 필요한 부분이나, 이를

위한 연구 및 개발은 이루어지지 않고 있다. 첫번째 이유는 취약점을 분석하거나 평가한 결과에 대한 수정 요구를 꼽을 수 있다. 기술적으로 취약점을 식별하고, 모의침투를 통해 취약점의 악용여부를 확인한 후 계산된 결과를 해당 시스템의 관리자가 수정해 달라고 요구하는 것이 일반적이다. 여기서, 시스템의 관리자는 낮은 점수가 경영진에게 보고되는 것을 원하지 않거나, 낮은 점수가 경영진에게 보고되게 함으로써 예산, 인력 등 자원 보충을 요구하기 위한 근거로 사용하려는 의도가 있기 때문이다. 두번째 이유는 취약점과 모의침투 결과를 수치화하는 방법, 그리고 이러한 방법의 객관성을 유지하는 방법에 대한 시도가 이루어지지 않았기 때문이다.

[8] 이전에도 나름대로의 방법으로 취약점을 분석하거나 평가한 결과를 수치화 하였으나, 객관성을 유지하기 어려웠다. 첫번째 원인은 점수 계산에 사용되는 취약점이 제한적이다. 식별된 취약점들 중에서 악용시 큰 영향을 발생시키는 소수의 특징적인 취약점만을 점수 계산에 활용하므로, 소수의 특징적인 취약점 이외의 취약점들은 점수화에서 배제된다. 두번째 원인은 분석자의 주관적 요소가 과다하게 개입될 수 있다. 동일한 시스템에 대해 동일한 취약점 식별 결과를 제공한 후에 점수화를 요구하는 경우에는 분석자마다 취약점들의 비중을 다르게 판단하므로, 사람마다 상이한 점수를 계산한다

[9] 이와 같은, 문제점으로 인하여 지금까지의 취약점을 분석하거나 평가한 결과는 객관성이 저하 되어있으며, 수정 요구에 반박할 수 있는 논리가 없어서 결과를 수정해 줄 수 밖에 없었다.

[10] 따라서, 시스템의 수준을 수치로 정량화하여 전달할 수 있는 기술의 필요성이 절실하게 대두된다.

발명의 상세한 설명

기술적 과제

[11] 본 발명의 목적은 시스템의 상태를 직관적 및 객관적으로 표현할 수 있도록 시스템의 취약점을 정량화하는 장치 및 그 방법을 제공하는 것이다.

과제 해결 수단

[12] 상기한 목적을 달성하기 위한 본 발명에 따른 시스템의 취약점 정량화 방법은

[13] 시스템의 취약점 식별 결과 각각을 해당 시스템의 취약점 식별 결과를 점수계산에 적용되도록 취약점 점수로 변환하는 단계; 상기 취약점 점수 중 상기 시스템에 해당하는 기술분야 안전도 점수와 관리분야 안전도 점수를 토대로 상기 시스템에 해당하는 대상기관 안전도 점수를 계산하는 단계; 상기 시스템의 업무망과 외부망의 분리 상황을 망 분리 점수로 변환하는 단계; 상기 대상기관 안전도 점수와 상기 망 분리 점수를 토대로 중간 점수를 계산하는 단계; 및 상기 중간 점수와 모의 침투 등급을 이용하여 최종적으로 상기 시스템의 종합 점수를 계산하여 시스템의 취약점을 정량화하는 단계를 포함한다.

[14] 이 때, 상기 대상기관 안전도 점수를 계산하는 단계는 상기 기술분야 안전도

점수와 상기 관리분야 안전도 점수를 설정한 비율에 따라 합산하여 상기 대상기관 안전도 점수를 계산하는 것을 특징으로 한다.

[15] 이 때, 상기 대상기관 안전도 점수를 계산하는 단계는 상기 시스템의 취약점 식별 결과 중에서 기술적으로 식별된 취약점을 상기 기술분야 안전도 점수로 변환하는 단계; 및 상기 시스템의 취약점 식별 결과 중에서 상기 시스템의 관리에 관한 취약점을 상기 관리분야 안전도 점수로 변환하는 단계를 포함한다.

[16] 이 때, 상기 기술분야 안전도 점수로 변환하는 단계는 상기 기술적으로 식별된 취약점에 해당하는 점수와 상기 취약점 점수의 합을 이용하여 하는 것을 특징으로 한다.

[17] 이 때, 상기 관리분야 안전도 점수로 변환하는 단계는 상기 시스템의 관리에 관한 취약점에 해당하는 점수와 상기 취약점 점수의 합을 이용하여 하는 것을 특징으로 한다.

[18] 이 때, 상기 시스템의 종합 점수를 계산하는 단계 이전에 상기 시스템의 취약점 식별 결과 각각에 해당하는 취약점을 조합하고, 조합한 취약점을 복수개의 경로의 모의 침투를 시도하는 단계; 및 상기 시도에서 성공한 모의 침투에서의 침투시도 위치 및 침투 결과에 따라 상기 모의 침투 등급을 산출하는 단계를 더 포함하는 것을 특징으로 한다.

[19] 이 때, 상기 시스템의 취약점을 정량화하는 단계는 상기 모의 침투 등급에 따라 상기 중간 점수에 가중치를 적용하여 상기 종합 점수를 계산하는 것을 특징으로 한다.

[20] 또한, 본 발명의 일실시예에 따른 시스템의 취약점 정량화 장치는

[21] 시스템의 취약점 식별 결과 각각을 해당 시스템의 취약점 식별 결과를 점수계산에 적용되도록 취약점 점수로 변환하는 취약점 계산부; 상기 취약점 점수 중 기술분야 안전도 점수와 관리분야 안전도 점수를 토대로 상기 시스템에 해당하는 대상기관 안전도 점수를 계산하는 대상기관 안전도 계산부; 상기 시스템의 업무망과 외부망의 분리 상황을 망 분리 점수로 변환하는 망 분리 현황 계산부; 상기 대상기관 안전도 점수와 상기 망 분리 점수를 토대로 중간 점수를 계산하는 중간 계산부; 및 상기 중간 점수와 모의 침투 등급을 이용하여 최종적으로 상기 시스템의 종합 점수를 계산하여 상기 시스템의 취약점을 정량화하는 최종 점수 계산부를 포함한다.

[22] 이 때, 상기 대상기관 안전도 계산부는 상기 기술분야 안전도 점수와 상기 관리분야 안전도 점수를 설정한 비율에 따라 합산하여 상기 대상기관 안전도 점수를 계산하는 것을 특징으로 한다.

[23] 이 때, 상기 시스템의 취약점 정량화 장치는 상기 시스템의 취약점 식별 결과 중에서 기술적으로 식별된 취약점을 상기 기술분야 안전도 점수로 점수화하는 기술분야 안전도 계산부; 및 상기 시스템의 취약점 식별 결과 중에서 상기 시스템의 관리에 관한 취약점을 상기 관리분야 안전도 점수로 점수화하는 관리분야 안전도 계산부를 더 포함한다.

[24] 이 때, 상기 시스템의 취약점 정량화 장치는 상기 시스템의 취약점 식별 결과 각각에 해당하는 취약점을 조합하고, 조합한 취약점을 복수개의 경로의 모의 침투를 시도하여, 상기 시도에서 성공한 모의 침투에서의 침투시도 위치 및 침투 결과에 따라 상기 모의 침투 등급을 산출하는 모 등급 관리부를 더 포함한다.

[25] 이 때, 상기 최종 점수 계산부는 상기 모의 침투 등급에 따라 상기 중간 점수에 가중치를 적용하여 상기 종합 점수를 계산하는 것을 특징으로 한다.

발명의 효과

[26] 본 발명에 따르면, 시스템의 취약점을 정량화하는 장치 및 그 방법은 수행자의 주관이 개입될 수 있는 부분을 최소화하여 사람에 따라 평가결과가 달라지는 문제점을 최소화하였다.

[27] 또한, 본 발명은 시스템의 취약점을 정량화하는 장치 및 그 방법은 시스템의 관리자에게 예를 들어, "어떠한 보호대책이 구현되면 종합 점수가 몇점까지 올라갈 수 있다"와 같이 가시적인 결과를 제공할 수 있다.

도면의 간단한 설명

[28] 도 1은 본 발명의 실시예에 따른 시스템의 취약점 정량화 장치를 개략적으로 나타내는 구성도이다.

[29] 도 2 내지 도 4는 본 발명의 실시예에 따른 시스템의 취약점 정량화 장치에 적용되는 참고도이다.

[30] 도 5는 본 발명의 실시예에 따른 시스템의 취약점을 정량화하는 방법을 나타내는 흐름도이다.

발명의 실시를 위한 형태

[31] 본 발명을 첨부된 도면을 참조하여 상세히 설명하면 다음과 같다. 여기서, 반복되는 설명, 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능, 및 구성에 대한 상세한 설명은 생략한다. 본 발명의 실시형태는 당 업계에서 평균적인 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되는 것이다. 따라서, 도면에서의 요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다.

[32] 이하, 본 발명에 따른 바람직한 실시예 따른 시스템의 취약점 정량화 장치 및 그 방법에 대하여 첨부한 도면을 참조하여 상세하게 설명한다.

[33] 도 1은 본 발명의 실시예에 따른 시스템의 취약점 정량화 장치를 개략적으로 나타내는 구성도이다. 또한, 도 2 내지 도 4는 본 발명의 실시예에 따른 시스템의 취약점 정량화 장치에 적용되는 참고도이다.

[34] 먼저, 시스템의 취약점 정량화 장치(10)는 시스템의 취약점을 분석하거나 평가한 결과(이하, "시스템의 취약점 식별 결과"라고도 함.)를 포함하거나, 외부로부터 전달 받을 수 있으며, 이에 한정되지 않는다.

[35] 도 1을 참고하면, 시스템의 취약점 정량화 장치(100)는 취약점 계산부(110), 기술분야 안전도 계산부(120), 관리분야 안전도 계산부(130), 대상기관 안전도

계산부(140), 망 분리 현황 계산부(150), 중간 계산부(160), 등급 관리부(170) 및 최종 점수 계산부(180)를 포함한다.

[36] 취약점 계산부(110)는 시스템의 취약점 식별 결과 각각을 해당 시스템의 취약점 식별 결과를 점수 계산에 적용되도록 취약점 점수로 변환한다. 여기서, 취약점 점수는 예를 들어, 0점에서 10점까지의 점수로 표현 할 수 있다.

[37] 예를 들어, 서버, 웹 응용프로그램에 대한 취약점 식별 결과는 CVSS(Common Vulnerability Scoring System) 2.0을 기반으로 계산하고, 관리 분야와 네트워크, DB 분야에 대한 취약점 식별 결과는 별도의 방법을 사용할 수 있다.

[38] 기술분야 안전도 계산부(120)는 시스템의 취약점 식별 결과 중에서 기술적으로 식별된 취약점을 종합하여 기술분야 안전도 점수를 계산한다. 여기서, 기술적으로 식별된 취약점은 시스템의 기술적인 부분에 관한 취약점을 분석하거나 평가한 결과이다.

[39] 구체적으로, 기술분야 안전도 계산부(120)는 수학식 1과 같이 기술분야 안전도 점수를 계산할 수 있다.

[40] [수학식 1]

[41] 기술분야 안전도 점수

[42] = 100 - (기술적으로 식별된 취약점 점수 / 최대 취약점 점수) * 100

[43] 수학식 1에서, 기술적으로 식별된 취약점 점수는 기술적으로 식별된 취약점을 점수로 변환한 결과이고, 최대 취약점 점수는 시스템의 취약점 식별 결과에 해당하는 취약점 점수의 합이다. 예를 들어, A 시스템이 유닉스 서버이고, 유닉스 서버의 취약점을 분석하거나 평가한 결과에 해당하는 취약점 점수의 합을 1000점이라고 가정한다. 여기서, 유닉스 서버의 기술적으로 식별된 취약점의 점수의 합을 80점이라고 하면, 수학식 1에 의해 A 시스템의 기술분야 안전도 점수는 92점이 된다.

[44] 관리분야 안전도 계산부(130)는 시스템의 취약점 식별 결과 중에서 관리분야에 해당하는 취약점을 종합하여 관리분야 안전도 점수를 계산한다. 여기서, 관리분야에 해당하는 취약점은 시스템의 관리에 관한 취약점을 분석하거나 평가한 결과이다.

[45] 구체적으로, 관리분야 안전도 계산부(130)는 수학식 2와 같이 관리분야 안전도 점수를 계산할 수 있다.

[46] [수학식 2]

[47] 관리분야 안전도 점수

[48] = 100 - (관리분야에 해당하는 취약점 점수 / 최대 취약점 점수) * 100

[49] 수학식 2에서, 최대 취약점 점수는 수학식 1의 최대 취약점 점수와 동일한 점수로, 시스템의 취약점 식별 결과에 해당하는 취약점 점수의 합이다.

[50] 대상기관 안전도 계산부(140)는 기술분야 안전도 점수와 관리분야 안전도 점수를 설정한 비율(α, β)에 따라 합산하여 대상기관 안전도 점수를 계산한다. 여기서, 설정한 비율 즉, 기술분야 안전도 점수에 적용하는 비율과 관리분야

안전도 점수에 적용하는 비율의 합(α + β)은 1이 되도록 설정한다.

[51] 대상기관 안전도 점수는 수학식 3과 같이 계산한다.

[52] [수학식 3]

[53] 대상기관 안전도 점수

[54] = (기술분야 안전도 점수 * α) + (관리분야 안전도 점수 * β)

[55] 망 분리 현황 계산부(150)는 시스템의 업무망과 외부망(예를 들어, 인터넷)의 분리 현황을 망 분리 점수로 변환한다.

[56] 예를 들어, 국가, 공공기관의 경우에는 구성원이 업무를 수행하는 업무망과 인터넷을 사용할 수 있는 외부망이 분리되어 있는 경우가 있다. 여기서, 망 분리 현황 계산부(150)는 업무망과 외부망이 분리되어 있는 형태(도 2의 망 분리 상황)에 따라 망 분리 점수를 도 2와 같이 할당할 수 있다.

[57] 중간 계산부(160)는 대상기관 안전도 점수와 망 분리 점수를 설정한 비율(γ)에 따라 합산하여 중간 점수를 계산한다.

[58] 등급 관리부(170)는 시스템의 취약점 식별 결과에 해당하는 취약점을 조합하고, 조합한 취약점을 복수개의 경로의 모의 침투에 적용하여 모의 침투 등급을 산출한다.

[59] 구체적으로, 등급 관리부(170)는 시스템의 취약점 식별 결과에 해당하는 취약점을 조합하여 복수개의 경로의 모의 침투를 시도한다. 다음, 등급 관리부(170)는 이와 같은 시도에서 성공한 모의 침투에서의 침투시도 위치 및 침투 결과에 따라 모의 침투 등급을 산출한다. 예를 들어, 등급 관리부(170)는 성공한 모의 침투에서의 침투 결과 및 침투시도 위치에 따라 도 3과 같이 모의 침투 등급을 산출한다. 여기서, 침투 결과는 관리자가 권한을 획득한 경우, 일반 사용자가 권한을 획득한 경우, 모의 침투로 인하여 시스템의 정상 운영에 방해가 가능한 경우 등을 포함할 수 있으며, 침투 시도 위치는 외부(인터넷), 시스템이 적용된 기관 내 타 시스템, 동일 시스템일 수 있다.

[60] 최종 점수 계산부(180)는 중간 점수에 모의 침투 등급을 적용하여 종합 점수를 계산한다. 구체적으로, 최종 점수 계산부(180)는 모의 침투 등급에 따라 중간 점수에 가중치(δ∈{80%, 85%, 90%, 95%, 100%})를 적용하여 종합 점수를 계산한다. 예를 들어, 최종 점수 계산부(180)는 도 4와 같이, 중간 점수가 94점인 경우에 모의 침투 등급에 따라 종합 점수를 계산한다.

[61] 다음, 시스템의 취약점을 정량화하는 방법을 도 5를 참조하여 상세하게 설명한다.

[62] 도 5는 본 발명의 실시예에 따른 시스템의 취약점을 정량화하는 방법을 나타내는 흐름도이다.

[63] 도 5를 참고하면, 시스템의 취약점 정량화 장치(100)는 시스템의 취약점 식별 결과를 취약점 점수로 변환변환한다(S510). 여기서, 취약점 점수는 예를 들어, 0점에서 10점까지의 점수로 표현 할 수 있다.

[64] 시스템의 취약점 정량화 장치(100)는 시스템의 취약점 식별 결과 중에서

기술적으로 식별된 취약점을 종합하여 기술분야 안전도 점수를 계산한다(S520). S520단계에서, 기술분야 안전도 점수는 수학식 1과 같이 계산된다.

[65] 시스템의 취약점 정량화 장치(100)는 시스템의 취약점 식별 결과 중에서 관리분야에 해당하는 취약점을 종합하여 관리분야 안전도 점수를 계산한다(S530). S530 단계에서, 관리분야 안전도 점수는 수학식 2와 같이 계산된다.

[66] 시스템의 취약점 정량화 장치(100)는 기술분야 안전도 점수와 관리분야 안전도 점수를 설정한 비율(α, β)에 따라 합산하여 대상기관 안전도 점수를 계산한다(S540). 여기서, 설정한 비율 즉, 기술분야 안전도 점수에 적용하는 비율과 관리분야 안전도 점수에 적용하는 비율의 합($\alpha + \beta$)은 1이 되도록 설정한다. S540 단계에서, 대상기관 안전도 점수는 수학식 3과 같이 계산된다.

[67] 시스템의 취약점 정량화 장치(100)는 시스템의 업무망과 외부망(예를 들어, 인터넷)의 분리 현황을 변환한다(S550). 여기서, 시스템의 취약점 정량화 장치(100)는 업무망과 외부망이 분리되어 있는 형태에 따라 망 분리 점수를 도 2와 같이 할당할 수 있다.

[68] 시스템의 취약점 정량화 장치(100)는 대상기관 안전도 점수와 망 분리 점수를 설정한 비율(γ)에 따라 합산하여 중간 점수를 계산한다(S560).

[69] 시스템의 취약점 정량화 장치(100)는 시스템의 취약점 식별 결과에 해당하는 취약점을 조합하여 복수개의 경로의 모의 침투를 시도하고, 시도한 결과 중 성공한 모의 침투에서의 침투시도 위치 및 침투 결과에 따라 모의 침투 등급을 산출한다(S570). 여기서, 시스템의 취약점 정량화 장치(100)는 침투시도 위치 및 침투 결과에 따라 도 3과 같이 모의 침투 등급을 산출할 수 있다.

[70] 시스템의 취약점 정량화 장치(100)는 중간 점수에 모의 침투 등급을 적용하여 종합 점수를 계산하여 시스템의 취약점을 정량화한다(S580).

[71] 이와 같이, 본 발명이 실시예에 따른 시스템의 취약점 정량화 장치(100)는 시스템의 취약점을 분석하거나 평가한 결과를 정량화함으로써, 시스템의 상태를 직관적 및 객관적으로 표현할 수 있다.

[72] 이상에서와 같이 도면과 명세서에서 최적의 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로, 본 기술 분야의 통상의 지식을 가진자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

청구범위

[청구항 1] 시스템의 취약점 식별 결과 각각을 해당 시스템의 취약점 식별 결과를 점수계산에 적용되도록 취약점 점수로 변환하는 단계;
상기 취약점 점수 중 상기 시스템에 해당하는 기술분야 안전도 점수와 관리분야 안전도 점수를 토대로 상기 시스템에 해당하는 대상기관 안전도 점수를 계산하는 단계;
상기 시스템의 업무망과 외부망의 분리 상황을 망 분리 점수로 변환하는 단계;
상기 대상기관 안전도 점수와 상기 망 분리 점수를 토대로 중간 점수를 계산하는 단계; 및
상기 중간 점수와 모의 침투 등급을 이용하여 최종적으로 상기 시스템의 종합 점수를 계산하여 시스템의 취약점을 정량화하는 단계
를 포함하는 시스템의 취약점 정량화 방법.

[청구항 2] 청구항 1에 있어서,
상기 대상기관 안전도 점수를 계산하는 단계는
상기 기술분야 안전도 점수와 상기 관리분야 안전도 점수를 설정한 비율에 따라 합산하여 상기 대상기관 안전도 점수를 계산하는 것을 특징으로 하는 시스템의 취약점 정량화 방법.

[청구항 3] 청구항 1에 있어서,
상기 대상기관 안전도 점수를 계산하는 단계는
상기 시스템의 취약점 식별 결과 중에서 기술적으로 식별된 취약점을 상기 기술분야 안전도 점수로 변환변환하는 단계; 및
상기 시스템의 취약점 식별 결과 중에서 상기 시스템의 관리에 관한 취약점을 상기 관리분야 안전도 점수로 변환하는 단계
를 포함하는 것을 특징으로 하는 시스템의 취약점 정량화 방법.

[청구항 4] 청구항 3에 있어서,
상기 기술분야 안전도 점수로 변환하는 단계는
상기 기술적으로 식별된 취약점에 해당하는 점수와 상기 취약점 점수의 합을 이용하여 하는 것을 특징으로 하는 시스템의 취약점 정량화 방법.

[청구항 5] 청구항 3에 있어서,
상기 관리분야 안전도 점수로 변환하는 단계는
상기 시스템의 관리에 관한 취약점에 해당하는 점수와 상기 취약점 점수의 합을 이용하여 하는 것을 특징으로 하는 시스템의 취약점 정량화 방법.

[청구항 6] 청구항 1에 있어서,

상기 시스템의 종합 점수를 계산하는 단계 이전에
상기 시스템의 취약점 식별 결과 각각에 해당하는 취약점을
조합하고, 조합한 취약점을 복수개의 경로의 모의 침투를
시도하는 단계; 및
상기 시도에서 성공한 모의 침투에서의 침투시도 위치 및 침투
결과에 따라 상기 모의 침투 등급을 산출하는 단계
를 더 포함하는 것을 특징으로 하는 시스템의 취약점 정량화 방법.

[청구항 7] 청구항 1에 있어서,
상기 시스템의 취약점을 정량화하는 단계는
상기 모의 침투 등급에 따라 상기 중간 점수에 가중치를 적용하여
상기 종합 점수를 계산하는 것을 특징으로 하는 시스템의 취약점
정량화 방법.

[청구항 8] 시스템의 취약점 식별 결과 각각을 해당 시스템의 취약점 식별
결과를 점수계산에 적용되도록 취약점 점수로 변환하는 취약점
계산부;
상기 취약점 점수 중 기술분야 안전도 점수와 관리분야 안전도
점수를 토대로 상기 시스템에 해당하는 대상기관 안전도 점수를
계산하는 대상기관 안전도 계산부;
상기 시스템의 업무망과 외부망의 분리 상황을 망 분리 점수로
변환하는 망 분리 현황 계산부;
상기 대상기관 안전도 점수와 상기 망 분리 점수를 토대로 중간
점수를 계산하는 중간 계산부; 및
상기 중간 점수와 모의 침투 등급을 이용하여 최종적으로 상기
시스템의 종합 점수를 계산하여 상기 시스템의 취약점을
정량화하는 최종 점수 계산부
를 포함하는 시스템의 취약점 정량화 장치.

[청구항 9] 청구항 8에 있어서,
상기 대상기관 안전도 계산부는
상기 기술분야 안전도 점수와 상기 관리분야 안전도 점수를
설정한 비율에 따라 합산하여 상기 대상기관 안전도 점수를
계산하는 것을 특징으로 하는 시스템의 취약점 정량화 장치.

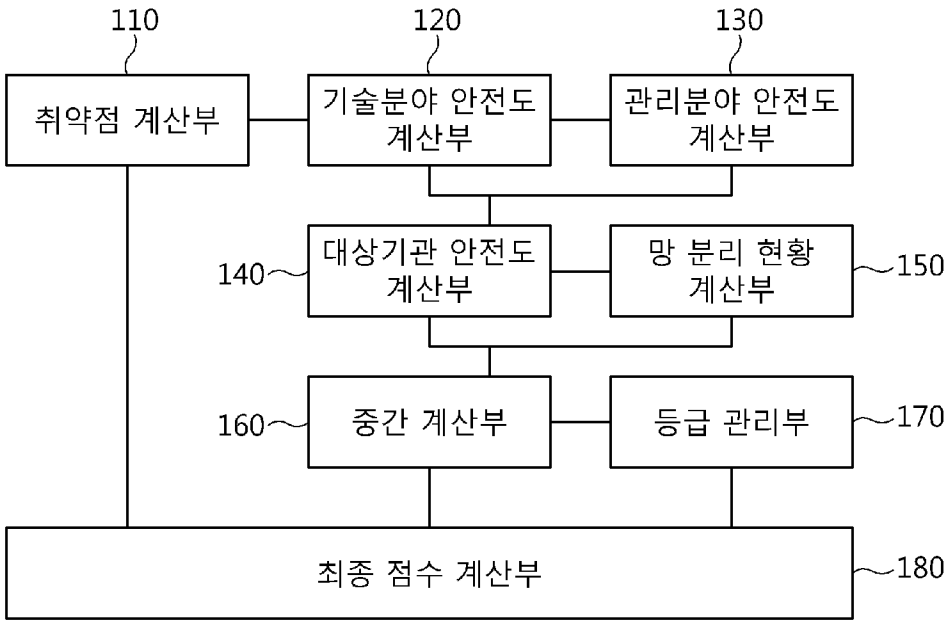
[청구항 10] 청구항 8에 있어서,
상기 시스템의 취약점 식별 결과 중에서 기술적으로 식별된
취약점을 상기 기술분야 안전도 점수로 변환하는 기술분야 안전도
계산부; 및
상기 시스템의 취약점 식별 결과 중에서 상기 시스템의 관리에
관한 취약점을 상기 관리분야 안전도 점수로 변환하는 관리분야
안전도 계산부

를 더 포함하는 시스템의 취약점 정량화 장치.

[청구항 11] 청구항 8에 있어서,
상기 시스템의 취약점 식별 결과 각각에 해당하는 취약점을 조합하고, 조합한 취약점을 복수개의 경로의 모의 침투를 시도하여, 상기 시도에서 성공한 모의 침투에서의 침투시도 위치 및 침투 결과에 따라 상기 모의 침투 등급을 산출하는 모 등급 관리부를 더 포함하는 시스템의 취약점 정량화 장치.

[청구항 12] 청구항 8에 있어서,
상기 최종 점수 계산부는
상기 모의 침투 등급에 따라 상기 중간 점수에 가중치를 적용하여 상기 종합 점수를 계산하는 것을 특징으로 하는 시스템의 취약점 정량화 장치.

[Fig. 1]



[Fig. 2]

망 분리 상황	점수
물리적으로 분리되어 있으며, 양 망간의 네트워크 연결이 전무함	1.0점
물리적으로 분리되어 있으나, 양 망의 특정자산들끼리는 연결되어 있음	0.9점
논리적으로 분리되어 있으며, 양 망간의 네트워크 연결이 전무함	0.8점
논리적으로 분리되어 있으며, 양 망의 특정자산들끼리는 연결되어 있음	0.7점
망이 분리되어 있지 않음.	0.6점

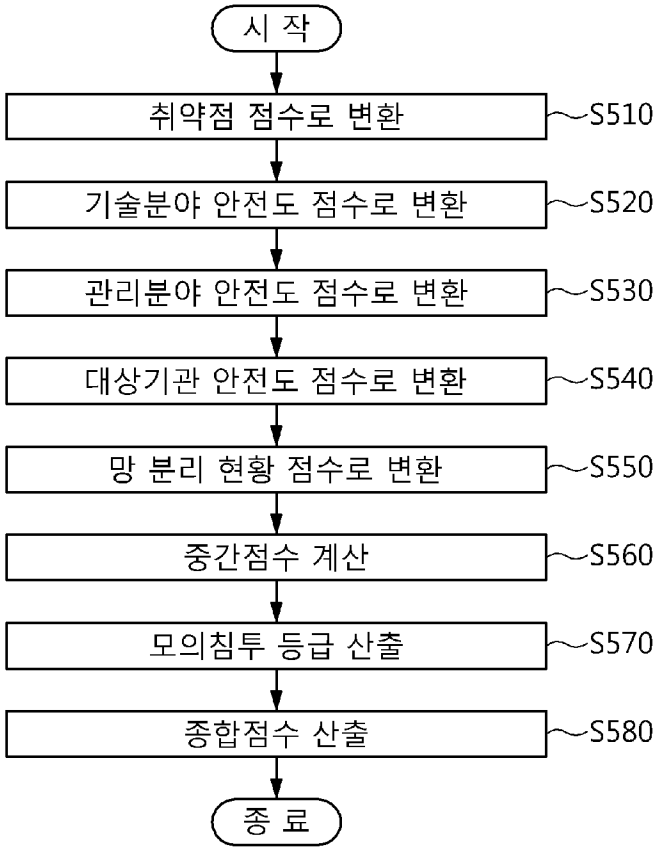
[Fig. 3]

침투시도 위치 / 침투 결과	외부(인터넷)	기관내 타 시스템	동일 시스템
관리자 권한 획득	1급	2급	2급
일반 사용자 권한 획득	1급	2급	3급
정상 운영 방해 가능	1급	3급	4급

[Fig. 4]

중간점수	모의침투 등급	종합점수
94점	1급	94점 x 80% = 75.2점
	2급	94점 x 85% = 79.9점
	3급	94점 x 90% = 84.6점
	4급	94점 x 95% = 89.3점
	모의침투 불가	94점 x 100% = 94점

[Fig. 5]


시 작
취약점 점수로 변환
S510
기술분야 안전도 점수로 변환
S520
관리분야 안전도 점수로 변환
S530
대상기관 안전도 점수로 변환
S540
망 분리 현황 점수로 변환
S550
중간점수 계산
S560
모의침투 등급 산출
S570
종합점수 산출
S580
종 료

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2013/009389

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/57(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/57; G06F 15/16; G06F 11/26; G06F 11/34; H04L 12/24; G06F 17/30; H04L 12/26; G06F 21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: system, safety grade, weak point, quantification, grade, network partition, and simulation penetration.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2009-0024663 A1 (MCGOVERN, Mark D.) 22 January 2009 See paragraphs 28-59; and figures 2-4.	1-12
A	US 2012-0151594 A1 (MCCLURE, Stuart C. et al.) 14 June 2012 See paragraphs 11-41; figures 3, 10-11; and claims 12, 15-21.	1-12
A	KR 10-1189967 B1 (SK C&C CO., LTD.) 12 October 2012 See paragraphs 6-20; and figures 3-5.	1-12
A	US 2009-0024627 A1 (KING, Nigel) 22 January 2009 See paragraphs 30-39; figure 1; and claim 1.	1-12
A	KR 10-2006-0067124 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 19 June 2006 See pages 2-3; and figure 1.	1-12

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 JANUARY 2014 (27.01.2014)	**28 JANUARY 2014 (28.01.2014)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2013/009389

Patent document cited in search report	Publication date	Patent family member	Publication date
US 2009-0024663 A1	22/01/2009	NONE	
US 2012-0151594 A1	14/06/2012	US 2007-0011319 A1	11/01/2007
		US 2009-0259748 A1	15/10/2009
		US 2012-0144476 A1	07/06/2012
		US 2012-0151595 A1	14/06/2012
		US 2012-0151596 A1	14/06/2012
		US 7543056 B2	02/06/2009
		US 8135830 B2	13/03/2012
KR 10-1189967 B1	12/10/2012	NONE	
US 2009-0024627 A1	22/01/2009	US 8166551 B2	24/04/2012
KR 10-2006-0067124 A	19/06/2006	US 2006-0129810 A1	15/06/2006

국 제 조 사 보 고 서

국제출원번호
PCT/KR2013/009389

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/57(2013.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/57; G06F 15/16; G06F 11/26; G06F 11/34; H04L 12/24; G06F 17/30; H04L 12/26; G06F 21/00

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 시스템, 안전도, 취약점, 정량화, 점수, 망분리, 및 모의침투.

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 2009-0024663 A1 (MARK D. MCGOVERN) 2009.01.22 단락 28-59; 및 도면 2-4 참조.	1-12
A	US 2012-0151594 A1 (STUART C. MCCLURE 외 7명) 2012.06.14 단락 11-41; 도면 3, 10-11; 및 청구항 12, 15-21 참조.	1-12
A	KR 10-1189967 B1 (에스케이씨엔씨 주식회사) 2012.10.12 단락 6-20; 및 도면 3-5 참조.	1-12
A	US 2009-0024627 A1 (NIGEL KING) 2009.01.22 단락 30-39; 도면 1; 및 청구항 1 참조.	1-12
A	KR 10-2006-0067124 A (한국전자통신연구원) 2006.06.19 페이지 2-3; 및 도면 1 참조.	1-12

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2014년 01월 27일 (27.01.2014)	2014년 01월 28일 (28.01.2014)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
변성철
전화번호 +82-42-481-8262

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2013/009389

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2009-0024663 A1	2009/01/22	없음	
US 2012-0151594 A1	2012/06/14	US 2007-0011319 A1	2007/01/11
		US 2009-0259748 A1	2009/10/15
		US 2012-0144476 A1	2012/06/07
		US 2012-0151595 A1	2012/06/14
		US 2012-0151596 A1	2012/06/14
		US 7543056 B2	2009/06/02
		US 8135830 B2	2012/03/13
KR 10-1189967 B1	2012/10/12	없음	
US 2009-0024627 A1	2009/01/22	US 8166551 B2	2012/04/24
KR 10-2006-0067124 A	2006/06/19	US 2006-0129810 A1	2006/06/15