



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0012277
(43) 공개일자 2020년02월05일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01)

(52) CPC특허분류
G06F 21/577 (2013.01)

G06F 21/36 (2013.01)

(21) 출원번호 10-2018-0087371

(22) 출원일자 2018년07월26일

심사청구일자 2018년07월26일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

유혁

서울특별시 용산구 이촌로71길 10, 213동 1904호 (이촌동, 한가람아파트)

김영필

경기도 시흥시 월곶중앙로70번길 11, 111동 605호(월곶동, 진주마을 풍림1차 아이원)

(뒷면에 계속)

(74) 대리인

송인호, 윤형근, 최영중, 최관락

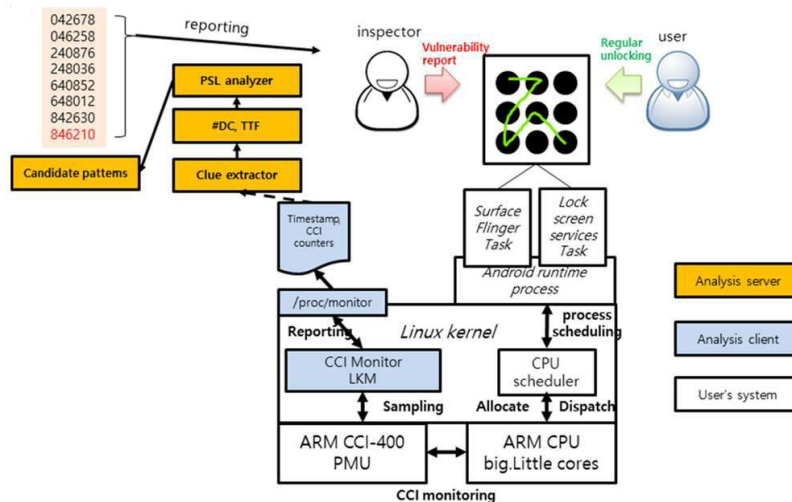
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도를 측정하는 장치 및 방법

(57) 요약

멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도를 측정하는 장치 및 방법이 개시된다. 개시된 장치는 사용자로부터 입력된 잠금 패턴을 구현하는 복수 개의 점(dot)의 터치와 관련된 캐쉬 일관성의 정보를 CCI(Cache Coherence Interconnect)로부터 독출하는 CCI 모니터부; 상기 독출된 캐쉬 일관성의 정보를 이용하여 복수 개의 유사 잠금 패턴 후보를 산출하는 산출부; 및 상기 복수 개의 유사 잠금 패턴 후보를 이용하여 상기 입력된 잠금 패턴의 보안 강도를 측정하는 측정부;를 포함한다.

대표도 - 도2



(72) 발명자

유시환

경기도 용인시 수지구 죽전로 152 단국대학교

이경운

서울특별시 성북구 보문로32길 86-7(동선동2가)
102호

이 발명을 지원한 국가연구개발사업

과제고유번호 20150002800041001

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신방송연구개발사업

연구과제명 (SW 스타랩) 성능 및 보안 SLA 보장이 가능한 차세대 클라우드 인프라SW 개발

기 여 율 1/2

주관기관 고려대학교산학협력단

연구기간 2018.01.01 ~ 2018.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호 20150002880041001

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보통신방송연구개발사업

연구과제명 SDN 2.0 실현을 위한 네트워크 가상화 플랫폼 핵심 기술 및 서비스 연구

기 여 율 1/2

주관기관 고려대학교산학협력단

연구기간 2018.01.01 ~ 2018.12.31

명세서

청구범위

청구항 1

멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도를 측정하는 장치에 있어서,
 사용자로부터 입력된 잠금 패턴을 구현하는 복수 개의 점(dot)의 터치와 관련된 캐쉬 일관성의 정보를 CCI(Cache Coherence Interconnect)로부터 독출하는 CCI 모니터부;
 상기 독출된 캐쉬 일관성의 정보를 이용하여 복수 개의 유사 잠금 패턴 후보를 산출하는 산출부; 및
 상기 복수 개의 유사 잠금 패턴 후보를 이용하여 상기 입력된 잠금 패턴의 보안 강도를 측정하는 측정부;를 포함하는 잠금 패턴 보안 강도 측정 장치.

청구항 2

제1항에 있어서,
 상기 산출부는,
 상기 산출부는 미리 저장된 사전 정보와 상기 독출된 캐쉬 일관성의 정보를 이용하여 상기 복수 개의 유사 잠금 패턴 후보들을 산출하되,
 상기 사전 정보는 미리 입력된 복수 개의 잠금 입력 패턴 각각에 따른 꺾임의 개수 및 상기 복수 개의 잠금 입력 패턴 각각의 전체 잠금 패턴의 길이를 포함하는 것을 특징으로 하는 잠금 패턴 보안 강도 측정 장치.

청구항 3

제2항에 있어서,
 상기 꺾임의 개수 및 상기 전체 패턴의 길이 각각은 그룹화되어 저장되되,
 상기 꺾임의 개수의 그룹의 경우, 동일한 꺾임의 개수를 포함하는 적어도 하나의 잠금 패턴의 형상 정보가 하나의 그룹으로 그룹화되고,
 상기 전체 패턴의 길이의 그룹의 경우, 동일한 전체 패턴의 길이를 가지는 하나 이상의 잠금 패턴의 형상 정보가 하나의 그룹으로 그룹화되는 것을 특징으로 하는 잠금 패턴 보안 강도 측정 장치.

청구항 4

제3항에 있어서,
 상기 산출부는,
 상기 독출된 캐쉬 일관성의 정보를 이용하여 상기 입력된 잠금 패턴에 따른 꺾임의 개수 및 상기 입력된 잠금 패턴의 전체 패턴의 길이를 산출하고,
 상기 입력된 잠금 패턴에 따른 꺾임의 개수를 이용하여 상기 꺾임의 개수의 그룹 중 하나의 그룹을 선택하고,
 상기 입력된 잠금 패턴의 전체 패턴의 길이를 이용하여 상기 전체 패턴의 길이의 그룹 중 하나의 그룹을 선택하며,
 상기 선택된 꺾임의 개수의 그룹에 포함된 적어도 하나의 잠금 패턴의 형상 정보 및 상기 선택된 전체 패턴의 길이의 그룹에 포함된 하나의 이상의 잠금 패턴의 형상 정보의 교집합인 잠금 패턴의 형상 정보의 적어도 일부를 상기 복수 개의 유사 잠금 패턴 후보로 산출하는 것을 특징으로 하는 잠금 패턴 보안 강도 측정 장치.

청구항 5

제1항에 있어서,

상기 측정부는 상기 입력된 잠금 패턴의 보안 강도가 강함인지 약함인지를 여부를 측정하되,

상기 입력된 잠금 패턴이 상기 복수 개의 유사 잠금 패턴 후보 중 어느 하나와 동일한 경우, 상기 입력된 잠금 패턴의 보안 강도를 약함으로 측정하고,

상기 입력된 잠금 패턴이 상기 복수 개의 유사 잠금 패턴 후보 중 전부와 동일하지 않는 경우, 상기 입력된 잠금 패턴의 보안 강도를 강함으로 측정하는 것을 특징으로 하는 잠금 패턴 보안 강도 측정 장치.

청구항 6

멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도를 측정하는 방법에 있어서,

사용자로부터 입력된 잠금 패턴을 구현하는 복수 개의 점(dot)의 터치와 관련된 캐쉬 일관성의 정보를 CCI(Cache Coherence Interconnect)로부터 독출하는 단계;

상기 독출된 캐쉬 일관성의 정보를 이용하여 복수 개의 유사 잠금 패턴 후보를 산출하는 단계; 및

상기 복수 개의 유사 잠금 패턴 후보를 이용하여 상기 입력된 잠금 패턴의 보안 강도를 측정하는 단계;를 포함하는 잠금 패턴 보안 강도 측정 방법.

청구항 7

제6항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

발명의 설명

기술 분야

[0001] 본 발명의 실시예들은 단말 장치에 적용되는 잠금 패턴의 보안 강도를 측정하는 장치 및 방법에 관한 것으로서, 보다 상세하게는 CCI(Cache Coherence Interconnect)로부터 얻을 수 있는 정보에 기반하여 멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도를 측정하는 장치 및 방법에 관한 것이다.

배경 기술

[0002] 최근의 스마트폰 등의 단말 장치는 다중 처리 및 고성능, 저전력을 위해 단일 CPU 아닌 다중 CPU의 환경을 제공하고 있으며, 특히 공유 캐쉬 메모리를 통한 효율적인 CPU 간 정보전달을 위해 멀티코어(multi-core) 환경을 지원한다. 특히, 멀티코어 환경의 단말 장치들이 패키징되어 있는 플랫폼에서는 CPU와 메모리 간의 효율적인 통신을 위해 내부 버스(internal bus)가 구축되어 있고, 분리된 코어 내에는 빠른 접근이 가능한 고성능 캐쉬 메모리(cache memory)가 존재한다. 멀티코어 환경에서는 캐쉬 메모리의 상태를 일관성 있게 유지하는 캐쉬 일관성(cache coherency) 기법과 이를 지원하는 장치인 CCI(Cache Coherency Interconnect)가 필요하다. 이러한 CCI는 캐쉬 상태를 추적하고, 관련 통계 데이터를 얻을 수 있는 인터페이스를 제공하고, 운영체제와 같은 시스템 소프트웨어는 관리 목적으로 CCI에서 독출한 정보를 활용할 수 있다.

[0003] 한편, 잠금 패턴 또는 PSL(Pattern Screen Lock)은 사용자가 안드로이드, iOS와 같은 단말 장치의 접근을 막기 위한 기법이다. 잠금 패턴은 그래픽컬 패스워드(graphical password)로 불리며, 손가락 제스처(finger gesture)를 기반으로 그래픽컬 패턴을 만들고, 이러한 패턴을 통해 사용자를 인증(authentication)한다. 안드로이드 기반의 단말 장치의 경우, 기본적으로 3x3 그리드의 9개의 점으로 잠금 패턴을 설정한다. 특히, 사용성이 중요한 모바일 장치의 경우, 잠금 패턴은 PIN(Personal Information Number)이나 일반 패스워드에 비해 기억이 쉽고 편리하기 때문에 많이 사용되고 있다.

[0004] 하지만, 잠금 패턴은 홈쳐보기(shoulder surfing), 카메라 공격(camera attack) 및 얼룩 공격(smudge attack)에 취약한 단점이 있으며, 잠금 패턴의 보안 강도를 측정하는 것이 중요한 이슈로 부각되고 있다.

발명의 내용

해결하려는 과제

[0005] 상기한 바와 같은 종래기술의 문제점을 해결하기 위해, 본 발명에서는 멀티코어 기반의 단말 장치에 구비된 CCI(Cache Coherence Interconnect)로부터 얻을 수 있는 정보에 기반하여 잠금 패턴의 보안 강도를 측정하는 장

치 및 방법을 제안하고자 한다.

[0006] 본 발명의 다른 목적들은 하기의 실시예를 통해 당업자에 의해 도출될 수 있을 것이다.

과제의 해결 수단

[0007] 상기한 목적을 달성하기 위해 본 발명의 바람직한 일 실시예에 따르면, 멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도를 측정하는 장치에 있어서, 사용자로부터 입력된 잠금 패턴을 구현하는 복수 개의 점(dot)의 터치와 관련된 캐쉬 일관성의 정보를 CCI(Cache Coherence Interconnect)로부터 독출하는 CCI 모니터부; 상기 독출된 캐쉬 일관성의 정보를 이용하여 복수 개의 유사 잠금 패턴 후보를 산출하는 산출부; 및 상기 복수 개의 유사 잠금 패턴 후보를 이용하여 상기 입력된 잠금 패턴의 보안 강도를 측정하는 측정부;를 포함하는 잠금 패턴 보안 강도 측정 장치가 제공된다.

[0008] 상기 산출부는, 상기 산출부는 미리 저장된 사전 정보와 상기 독출된 캐쉬 일관성의 정보를 이용하여 상기 복수 개의 유사 잠금 패턴 후보들을 산출하되, 상기 사전 정보는 미리 입력된 복수 개의 잠금 입력 패턴 각각에 따른 꺾임의 개수 및 상기 복수 개의 잠금 입력 패턴 각각의 전체 잠금 패턴의 길이를 포함할 수 있다.

[0009] 상기 꺾임의 개수 및 상기 전체 패턴의 길이 각각은 그룹화되어 저장되되, 상기 꺾임의 개수의 그룹의 경우, 동일한 꺾임의 개수를 포함하는 적어도 하나의 잠금 패턴의 형상 정보가 하나의 그룹으로 그룹화되고, 상기 전체 패턴의 길이의 그룹의 경우, 동일한 전체 패턴의 길이를 가지는 하나 이상의 잠금 패턴의 형상 정보가 하나의 그룹으로 그룹화될 수 있다.

[0010] 상기 산출부는, 상기 독출된 캐쉬 일관성의 정보를 이용하여 상기 입력된 잠금 패턴에 따른 꺾임의 개수 및 상기 입력된 잠금 패턴의 전체 패턴의 길이를 산출하고, 상기 입력된 잠금 패턴에 따른 꺾임의 개수를 이용하여 상기 꺾임의 개수의 그룹 중 하나의 그룹을 선택하고, 상기 입력된 잠금 패턴의 전체 패턴의 길이를 이용하여 상기 전체 패턴의 길이의 그룹 중 하나의 그룹을 선택하며, 상기 선택된 꺾임의 개수의 그룹에 포함된 적어도 하나의 잠금 패턴의 형상 정보 및 상기 선택된 전체 패턴의 길이의 그룹에 포함된 하나의 이상의 잠금 패턴의 형상 정보의 교집합인 잠금 패턴의 형상 정보의 적어도 일부를 상기 복수 개의 유사 잠금 패턴 후보로 산출할 수 있다.

[0011] 상기 측정부는 상기 입력된 잠금 패턴의 보안 강도가 강함인지 약함인지를 여부를 측정하되, 상기 입력된 잠금 패턴이 상기 복수 개의 유사 잠금 패턴 후보 중 어느 하나와 동일한 경우, 상기 입력된 잠금 패턴의 보안 강도를 약함으로 측정하고, 상기 입력된 잠금 패턴이 상기 복수 개의 유사 잠금 패턴 후보 중 전부와 동일하지 않는 경우, 상기 입력된 잠금 패턴의 보안 강도를 강함으로 측정할 수 있다.

[0012] 또한, 본 발명의 다른 실시예에 따르면, 멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도를 측정하는 방법에 있어서, 사용자로부터 입력된 잠금 패턴을 구현하는 복수 개의 점(dot)의 터치와 관련된 캐쉬 일관성의 정보를 CCI(Cache Coherence Interconnect)로부터 독출하는 단계; 상기 독출된 캐쉬 일관성의 정보를 이용하여 복수 개의 유사 잠금 패턴 후보를 산출하는 단계; 및 상기 복수 개의 유사 잠금 패턴 후보를 이용하여 상기 입력된 잠금 패턴의 보안 강도를 측정하는 단계;를 포함하는 잠금 패턴 보안 강도 측정 방법이 제공된다.

발명의 효과

[0013] 본 발명에 따르면, 잠금 패턴의 보안 강도를 정확하게 측정할 수 있는 장점이 있다.

[0014] 또한, 본 발명의 효과는 상기한 효과로 한정되는 것은 아니며, 본 발명의 상세한 설명 또는 특허청구범위에 기재된 발명의 구성으로부터 추론 가능한 모든 효과를 포함하는 것으로 이해되어야 한다.

도면의 간단한 설명

[0015] 도 1은 본 발명의 일 실시예에 따른 잠금 패턴의 보안 강도 측정 장치의 개략적인 구성을 도시한 도면이다.

도 2는 본 발명에 따른 CCI 모니터부의 개념을 도시한 도면이다.

도 3은 본 발명에 따른 전체 잠금 패턴의 길이의 개념을 도시한 도면이다.

도 4는 본 발명의 효과를 설명하기 위한 도면이다.

도 5는 본 발명의 일 실시예에 따라서, 멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도 측정 방

법의 흐름도를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0016] 본 명세서에서 사용되는 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "구성된다" 또는 "포함한다" 등의 용어는 명세서상에 기재된 여러 구성 요소들, 또는 여러 단계들을 반드시 모두 포함하는 것으로 해석되지 않아야 하며, 그 중 일부 구성 요소들 또는 일부 단계들은 포함되지 않을 수도 있고, 또는 추가적인 구성 요소 또는 단계들을 더 포함할 수 있는 것으로 해석되어야 한다. 또한, 명세서에 기재된 "...부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다.
- [0017] 이하, 본 발명의 다양한 실시예들을 첨부된 도면을 참조하여 상술한다.
- [0019] 도 1은 본 발명의 일 실시예에 따른 잠금 패턴의 보안 강도 측정 장치의 개략적인 구성을 도시한 도면이다.
- [0020] 도 1을 참조하면, 본 발명의 일 실시예에 따른 보안 강도 측정 장치(100)는 기술적 사상을 수행하기 위한 하드웨어 및 하드웨어를 구동하기 위한 소프트웨어의 기능적, 구조적 결합을 의미하는 모듈일 수 있으며, 멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도를 측정하는 장치로서, CCI 모니터부(110), 산출부(120) 및 측정부(130)를 포함한다. 이하, 각 구성 요소 별로 그 기능을 상세하게 설명하기로 한다.
- [0021] 먼저, CCI 모니터부(110)는 사용자로부터 입력된 잠금 패턴을 구현하는 복수 개의 점(dot)의 터치와 관련된 캐쉬 일관성의 정보를 CCI(Cache Coherence Interconnect)로부터 독출한다. 이 때, CCI는 멀티코어 각각에 구비되는 캐쉬 일관성의 정보를 CCI 이벤트로서 저장한다. 즉, CCI 이벤트는 이중 멀티코어 환경에서 캐쉬 일관성 유지를 위해 발생하는 이벤트이다.
- [0022] 보다 상세하게, CCI 모니터부(110)는 리눅스 커널 모델일 수 있으며, CCI 이벤트를 읽어 분석 가능한 로그를 생성한다. 도 2에서는 CCI 모니터부(110)의 개념을 도시하고 있다. CCI 모니터부(110)의 동작은 사용자가 잠금 패턴을 입력할 때 활성화되고, 운영체제(일례로, Android OS)에서 동작하는 리눅스 프로세스들이 이중 멀티코어에서 동작할 때 발생하는 캐쉬 일관성 정보를 CCI의 장치 레지스터에서 읽어들이며, "/proc/monitor"라는 특수 파일에 기록한다. 이 파일에는 타임 스탬프와 CCI의 카운터 값이 일정기간 기록되고, 기록 주기는 설정에 따라 조절될 수 있다.
- [0023] 다음으로, 산출부(120)는 독출된 캐쉬 일관성의 정보를 이용하여 복수 개의 유사 잠금 패턴 후보를 산출한다.
- [0024] 이 때, 유사 잠금 패턴 후보들은 사용자가 입력한 잠금 패턴과 유사한 복수 개의 잠금 패턴으로서, 일례로 20개의 잠금 패턴일 수 있으며, 아래에서 설명하는 바와 같이 사용자가 입력한 잠금 패턴의 보안 강도를 측정하기 위해 사용된다.
- [0025] 본 발명의 일 실시예에 따르면, 산출부(120)는 미리 저장된 사전 정보와 상기한 독출된 캐쉬 일관성의 정보를 이용하여 복수 개의 유사 잠금 패턴 후보들을 산출할 수 있다. 이에 대해 보다 상세하게 설명하면 다음과 같다.
- [0026] 산출부(120)는 상기한 독출된 캐쉬 일관성의 정보를 이용하여 사용자로부터 입력된 잠금 패턴에 따른 꺾임의 개수 및 사용자로부터 입력된 잠금 패턴의 전체 패턴의 길이를 산출한다.
- [0027] 여기서, 잠금 패턴에 따른 꺾임의 개수는 잠금 패턴의 방향 전환에 따른 꺾임의 개수를 의미한다. 예를 들어, 잠금 패턴의 형상이 '┐'자 형상 또는 '┌'자 형상인 경우 꺾임의 개수는 1개이고, 잠금 패턴의 형상이 'ㄷ'자 형상인 경우 꺾임의 개수는 2개이고, 잠금 패턴의 형상이 'ㄱ'자 형상인 경우 꺾임의 개수는 4개이다.
- [0028] 이러한 꺾임의 개수를 산출하기 위하여, 산출부(120)는 잠금 패턴을 구성하는 9개의 점으로 이루어진 3x3 그리드(grid)를 2차원의 유클리디안 좌표계(Euclidean coordinates)로 매핑하고, 입력된 잠금 패턴을 복수 개의 단위 벡터(unit vector)로 표현한다. 그리고, 복수 개의 단위 벡터 각각을 순차적으로 읽어 들여 벡터 합을 시도하고, 그 결과에 따라서 같은 방향과 다른 방향을 판단하는 판단식 f 을 적용한다. 이 때, 3개의 점인 (x_i, y_i) , (x_{i+1}, y_{i+1}) , (x_{i+2}, y_{i+2}) 를 사용한 수학적 식 1과 같은 판단식 f 을 사용한다.

수학식 1

$$f = \frac{\sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2} + \sqrt{(x_{i+2} - x_{i+1})^2 + (y_{i+2} - y_{i+1})^2}}{\sqrt{(x_{i+2} - x_i)^2 + (y_{i+2} - y_i)^2}}$$

[0030]

[0032]

여기서, 판단을 위해서 카운터 c를 유지한 후, $f > 0$ 이면, 카운터 c를 증가시킨다. 이 때, 잠금 패턴에 속한 벡터들을 모두 거쳤을 때 카운터 c값은 최소 1부터 최대 7내의 수가 산출되고 이는 꺾임의 개수가 된다.

[0033]

또한, 잠금 패턴에 따른 전체 잠금 패턴의 길이는 잠금 패턴이 정확하게(이상적으로) 점들을 지나갈 때의 전체 길이를 의미한다. 예를 들어, 가로 방향으로 인접하는 2개의 점의 길이 또는 세로 방향으로 인접하는 2개의 점의 길이를 '1'으로, 대각선 방향으로 인접하는 2개의 점의 길이를 $\sqrt{2}$ 로 정의하고, 전체 잠금 패턴의 길이는 점들을 지나는 잠금 패턴의 총합으로 정의된다. 이는 도 3에 도시된 바와 같다.

[0034]

이러한 전체 잠금 패턴의 길이를 산출하기 위하여, 산출부(120)는 잠금 패턴을 구성하는 9개의 점으로 이루어진 3x3 그리드(grid)를 2차원의 유클리디안 좌표계(Euclidean coordinates)로 매핑하고, 잠금 패턴에 속한 점들을 지난 길이를 구한다. 잠금 패턴의 총 길이는 잠금 패턴에 속한 점들을 2개씩 순차적으로 읽어들이고, 두 점간의 길이를 구하는 유클리디안 거리 계산식을 사용한다. 이를 위해, 각 그리드 점의 간격을 1의 단위 값으로 설정하고, 조합 가능한 모든 389,112개의 잠금 패턴들을 나열하여 계산해보면 전체 잠금 패턴의 길이는 '3'에서 '17.78'의 범위를 가진다.

[0035]

그리고, 산출부(120)는 미리 저장된 사전 정보와 상기한 독출된 캐쉬 일관성의 정보를 비교하여 복수 개의 유사 잠금 패턴 후보들을 산출한다.

[0036]

여기서, 사전 정보는 미리 입력된 복수 개의 잠금 입력 패턴 각각에 따른 꺾임의 개수 및 복수 개의 잠금 입력 패턴 각각의 전체 패턴의 길이를 포함할 수 있으며, 복수 개의 잠금 입력 패턴은 조합 가능한 모든 잠금 패턴일 수 있다. 즉, 사전 정보는 모든 잠금 패턴에 대한 꺾임의 개수 및 모든 잠금 패턴 각각에 대한 전체 잠금 패턴의 길이일 수 있다. 이 때, 사전 정보인 꺾임의 개수 및 전체 잠금 패턴의 길이는 상기에서 설명한 2차원의 유클리디안 좌표계의 매핑을 통해 산출되어 저장될 수 있다.

[0037]

그리고, 사전 정보인 꺾임의 개수 및 전체 잠금 패턴의 길이는 그룹화되어 저장될 수 있다. 이 때, 상기한 꺾임의 개수의 그룹의 경우, 동일한 꺾임의 개수를 포함하는 적어도 하나의 잠금 패턴의 형상 정보가 하나의 그룹으로 그룹화된다. 또한, 상기한 전체 패턴의 길이의 그룹의 경우, 동일한 전체 패턴의 길이를 가지는 하나 이상의 잠금 패턴의 형상 정보가 하나의 그룹으로 그룹화될 수 있다.

[0038]

예를 들어, 잠금 패턴의 형상이 '┐'자 형상 또는 '┌'자 형상인 경우 꺾임의 개수가 1개이므로, 이들은 제1 그룹으로 그룹화될 수 있고, 잠금 패턴의 형상이 'ㄷ'자 형상 또는 '┐'자 형상인 경우 꺾임의 개수는 2개이므로, 이들은 제2 그룹으로 그룹화될 수 있다. 따라서, 총 7개의 그룹이 생성될 수 있다. 또한, 전체 잠금 패턴의 길이는 최소 '3'에서 최대 '17.78'의 범위를 가지므로, 전체 잠금 패턴의 길이의 총 그룹의 개수는 273개고, 그룹에 속한 잠금 패턴들의 수는 8에서 12248개일 수 있다.

[0039]

한편, 본 발명의 일 실시예에 따르면, 산출부(120)는 사용자로부터 입력된 잠금 패턴에 따른 꺾임의 개수를 이용하여 꺾임의 개수의 그룹 중 하나의 그룹을 선택하고, 사용자로부터 입력된 잠금 패턴의 전체 패턴의 길이를 이용하여 상기 전체 패턴의 길이의 그룹 중 하나의 그룹을 선택한다. 그 후, 산출부(120)는 상기 선택된 꺾임의 개수의 그룹에 포함된 적어도 하나의 잠금 패턴의 형상 정보와, 상기 선택된 전체 패턴의 길이의 그룹에 포함된 하나의 이상의 잠금 패턴의 형상 정보의 교집합인 잠금 패턴의 형상 정보의 적어도 일부를 복수 개의 유사 잠금 패턴 후보로 산출할 수 있다.

[0040]

예를 들어, CCI 이벤트를 통해 산출된 상기 입력된 잠금 패턴에 따른 꺾임의 개수가 2개인 경우 산출부(120)는 꺾임의 개수의 그룹들 중 2개의 꺾임의 개수를 가지는 하나의 그룹(이하, 그룹 A)을 선택하고, CCI 이벤트를 통

해 산출된 상기 입력된 잠금 패턴에 따른 전체 잠금 패턴의 길이가 6인 경우 산출부(120)는 전체 잠금 패턴의 길이의 그룹들 중 6의 길이를 가지는 하나의 그룹(이하, 그룹 B)을 선택한다. 그리고, 산출부(120)는 그룹 A에 속하는 적어도 하나의 잠금 패턴의 형상 정보와 그룹 B에 속하는 하나 이상의 잠금 패턴의 형상 정보를 조합하여, 꺾임의 개수가 2개이고 전체 잠금 패턴의 길이가 6인 다수 개의 잠금 패턴의 형상 정보를 산출한다. 그 후, 산출부(120)는 다수 개의 잠금 패턴의 형상 정보 중 적어도 일부를 복수 개의 유사 잠금 패턴 후보로 산출한다.

[0041] 이 경우, 산출부(120)는 엔트로피(Entropy)를 이용하여 다수 개의 잠금 패턴의 형상 정보 중 적어도 일부를 선택할 수 있다.

[0042] 보다 상세하게, 본 발명에서 사용하는 엔트로피는 평균 혹은 기대하는 추측의 수(Average or Expected number of guesses)를 측정하기 위한 메트릭(metric)으로서, 추측의 수가 크면 엔트로피는 낮아지고, 유추가 어려워지므로, 해당 잠금 패턴이 취약하지 않음을 정량적으로 확인할 수 있다.

[0043] 이 때, 엔트로피를 통해 측정하는 것은 잠금 패턴을 찾기 위해서 최적화된 공격에 필요한 추측 동작의 평균 수와 대응되며, 이는 수학적 식 2와 같이 표현될 수 있다.

수학적 식 2

$$Entropy(\chi) = E[\#G(X \xrightarrow{R} \chi)] = \sum_{i=1}^N p_i i$$

[0045]

[0047] 여기서, X는 추측 대상이 되는 대상 잠금 패턴을 나타내는 랜덤 변수이고, i는 추측하여 선택한 잠금 패턴의 인덱스(index)로서 임의의 추측을 시도했을 때 증가한다. 그리고, χ 은 추측 대상이 되는 모든 잠금 패턴들의 분포를 가지고 있다. 즉, $X \xrightarrow{R} \chi$ 는 모든 잠금 패턴들의 분포에서 랜덤 추출하는 것을 의미한다. 또한, #G는 랜덤 추측에 필요한 연산의 총 수이며 본 발명의 경우, #G를 꺾임의 개수 및 전체 잠금 패턴의 길이로 사용할 수 있다.

[0048] 마지막으로, 측정부(130)는 복수 개의 유사 잠금 패턴 후보를 이용하여 사용자로부터 입력된 잠금 패턴의 보안 강도를 측정한다. 즉, 측정부(130)는 사용자로부터 입력된 잠금 패턴의 보안 강도가 강함인지 약함인지를 여부를 측정한다.

[0049] 본 발명의 일 실시예에 따르면, 상기 입력된 잠금 패턴이 복수 개의 유사 잠금 패턴 후보 중 어느 하나와 동일한 경우, 측정부(130)는 상기 입력된 잠금 패턴의 보안 강도를 약함으로 측정한다. 반대로, 상기 입력된 잠금 패턴이 복수 개의 유사 잠금 패턴 후보 중 전부와 동일하지 않는 경우, 측정부(130)는 상기 입력된 잠금 패턴의 보안 강도를 강함으로 측정한다.

[0050] 요컨대, 본 발명은 멀티코어 기반의 단말 장치에 구비된 CCI로부터 얻을 수 있는 정보에 기반하여 잠금 패턴의 보안 강도를 정확하게 측정할 수 있는 장점이 있다.

[0051] 이하, 도 4를 참조하여 본 발명의 효과를 상세하게 설명하기로 한다.

[0052] 도 4는 특정 잠금 패턴들에 대한 보안 강도를 정리한 표를 도시하고 있다.

[0053] 이 때, Pattern 열의 숫자들은 잠금 패턴의 3x3 그리드의 각 점에 0부터 8까지의 번호 매김을 하였을 때, 대상 잠금 패턴을 표현한 것이다. 그리고, #G는 엔트로피 평가의 척도인 잠금 패턴 추정 수를, Pattern length는 잠금 패턴에 사용된 점의 개수, #UPL은 전체 잠금 패턴의 길이, intersection은 잠금 패턴 내 교차점의 개수, overlaps는 잠금 패턴 내에서 겹치는 선의 개수를 각각 의미한다.

[0054] 상기한 요소들은 기존에 패턴의 보안 강도를 표현하는 척도들을 연구한 대표적인 세 가지 방법들을 적용해서 평가한 후 추출한 것이다. 기존에 잠금 패턴의 보안 강도를 평가하는 방법으로는 Pattern strength score, Pattern complexity 및 Pattern strength meter가 있다. Pattern strength score의 경우 그 점수를 구했을

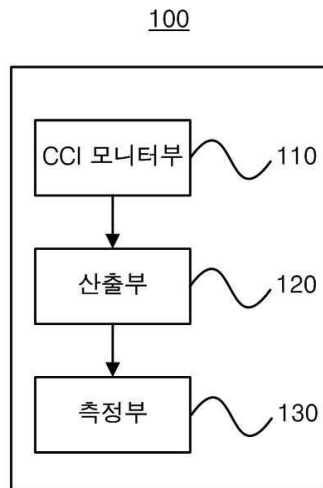
때, 40점 이상이면 가장 강력하고, 10점 이하면 약하며 그 중간대는 보통으로 평가한다. Pattern complexity는 pattern strength score의 총 범위를 동일한 크기의 3구간으로 나누어 Simple, medium, complex로 구분하였다. 그리고, Pattern strength meter에서는 기존의 pattern strength score를 수정하여 패턴에서 겹치는 구간의 비율을 적용하였고, 비슷하게 Weak, Medium, Strong으로 구분하였다.

- [0055] 도 4를 참조하면, 기존 방식에서 강력하다고 평가된 패턴이나 그렇지 않은 경우나 본 발명에 따르면 보안 강도가 낮은 것으로 확인되었다. 즉 가장 강한 보안 강도를 가지는 "40점 이상", "Complex", "Strong"인 패턴에 대해서도 최대 8번의 시도로 유사한 패턴을 찾아낼 수 있음을 확인할 수 있다. 따라서, 본 발명의 보안 강도 측정 방법이 더 우수함을 확인할 수 있다.
- [0057] 도 5는 본 발명의 일 실시예에 따라서, 멀티코어 기반의 단말 장치에 적용되는 잠금 패턴의 보안 강도 측정 방법의 흐름도를 도시한 도면이다. 이 때, 상기한 방법은 프로세서에서 수행될 수 있다. 이하, 각 단계 별로 수행되는 과정을 상세하게 설명한다.
- [0058] 먼저, 단계(510)에서는 사용자로부터 입력된 잠금 패턴을 구현하는 복수 개의 점의 터치와 관련된 캐쉬 일관성의 정보를 CCI로부터 독출한다.
- [0059] 다음으로, 단계(520)에서는 독출된 캐쉬 일관성의 정보를 이용하여 복수 개의 유사 잠금 패턴 후보를 산출한다.
- [0060] 본 발명의 일 실시예에 따르면, 단계(520)에서는 미리 저장된 사전 정보와 독출된 캐쉬 일관성의 정보를 이용하여 복수 개의 유사 잠금 패턴 후보들을 산출하되, 사전 정보는 미리 입력된 복수 개의 잠금 입력 패턴 각각에 따른 꺾임의 개수 및 상기 복수 개의 잠금 입력 패턴 각각의 전체 잠금 패턴의 길이를 포함할 수 있다.
- [0061] 이 경우, 사전 정보인 꺾임의 개수 및 전체 패턴의 길이 각각은 그룹화되어 저장되되, 꺾임의 개수의 그룹의 경우, 동일한 꺾임의 개수를 포함하는 적어도 하나의 잠금 패턴의 형상 정보가 하나의 그룹으로 그룹화되고, 전체 패턴의 길이의 그룹의 경우, 동일한 전체 패턴의 길이를 가지는 하나 이상의 잠금 패턴의 형상 정보가 하나의 그룹으로 그룹화될 수 있다.
- [0062] 그리고, 본 발명의 일 실시예에 따르면, 단계(520)는 독출된 캐쉬 일관성의 정보를 이용하여 상기 입력된 잠금 패턴에 따른 꺾임의 개수 및 상기 입력된 잠금 패턴의 전체 패턴의 길이를 산출하고, 상기 입력된 잠금 패턴에 따른 꺾임의 개수를 이용하여 상기 꺾임의 개수의 그룹 중 하나의 그룹을 선택하고, 상기 입력된 잠금 패턴의 전체 패턴의 길이를 이용하여 상기 전체 패턴의 길이의 그룹 중 하나의 그룹을 선택하며, 상기 선택된 꺾임의 개수의 그룹에 포함된 적어도 하나의 잠금 패턴의 형상 정보 및 상기 선택된 전체 패턴의 길이의 그룹에 포함된 하나의 이상의 잠금 패턴의 형상 정보의 교집합인 잠금 패턴의 형상 정보의 적어도 일부를 복수 개의 유사 잠금 패턴 후보로 산출할 수 있다.
- [0063] 마지막으로, 단계(530)에서는 복수 개의 유사 잠금 패턴 후보를 이용하여 상기 입력된 잠금 패턴의 보안 강도를 측정한다.
- [0064] 지금까지 본 발명에 따른 잠금 패턴의 보안 강도를 측정하는 방법의 실시예들에 대하여 설명하였고, 앞서 도 1 내지 도 4에서 설명한 잠금 패턴보안 강도 측정 장치(100)에 관한 구성이 본 실시예에도 그대로 적용 가능하다. 이에, 보다 상세한 설명은 생략하기로 한다.
- [0065] 또한, 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 일 실시예들의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0066] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되

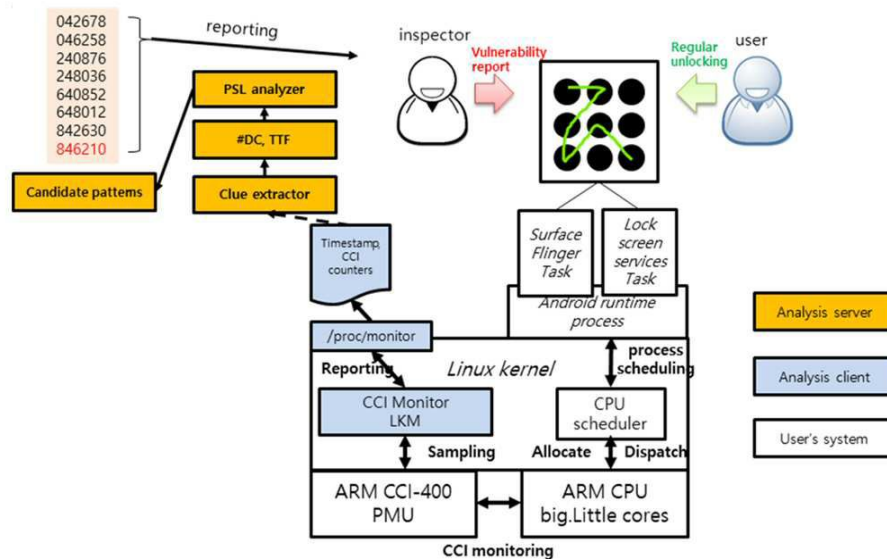
있으나 이는 본 발명의 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위 뿐만 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

도면

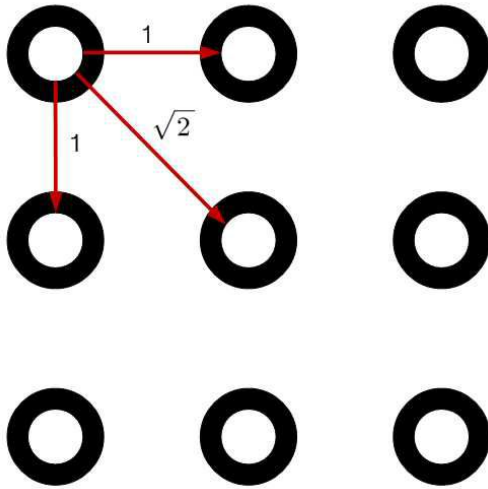
도면1



도면2



도면3



도면4

Pattern	# G	Pattern length	#UPL	Intersections	Overlaps	Pattern strength Score	Pattern complexity	Pattern strength meter
 462350817	8	9	17.78	6	1	41.68	Complex	Strong (0.83)
 426780	8	6	9.07	1	1	20.81	Medium	Medium (0.47)
 1025	8	4	4	0	1	9.28	Simple	Weak (0.31)

도면5

