Trusted Extensions 사용자 설명서

부품 번호: E25059
2011년 12월

ORACLE

120410@25097

목차

그림

표

머리말

Trusted Extensions 사용자 설명서는 Trusted Extensions 기능이 지원되는 Oracle Solaris 운영 체제(Oracle Solaris OS)에서 작업을 수행하기 위한 지침을 제공합니다.

본 설명서의 대상

본 설명서는 Trusted Extensions의 모든 사용자를 대상으로 합니다. 사용자는 Oracle Solaris OS 및 오픈 소스 GNOME 데스크탑에 익숙해야 합니다.

또한 조직의 보안 정책에 대해서도 잘 알고 있어야 합니다.

Trusted Extensions 설명서 구성 방식

다음 표에서는 Trusted Extensions 설명서에서 다루는 항목 및 각 설명서의 대상 사용자를 보여 줍니다.

설명서 제목	내용	대상
Trusted Extensions 사용자 설명서	Trusted Extensions의 기본 기능에 대해 설명합니다. 이 설명서에는 용어집도 포함되어 있습니다.	최종 사용자, 관리자 및 개발자
Trusted Extensions 구성 및 관리	I부에서는 Trusted Extensions 준비, 사용으로 설정 및 초기 구성 방법을 설명합니다. II부에서는 Trusted Extensions 시스템의 관리 방법을 설명합니다. 이 설명서에는 용어집도 포함되어 있습니다.	관리자, 개발자
Trusted Extensions Developer's Guide	Trusted Extensions로 응용 프로그램을 개발하는 방법에 대해 설명합니다.	개발자, 관리자
Trusted Extensions Label Administration	레이블 인코딩 파일에서 레이블 구성 요소를 지정하는 방법에 대해 설명합니다.	관리자
Compartmented Mode Workstation Labeling: Encodings Format	레이블 인코딩 파일에 사용되는 구문에 대해 설명합니다. 구문을 통해 올바르게 구성된 시스템 레이블에 다양한 규칙이 적용됩니다.	관리자

이 설명서의 구성

1 장, “Trusted Extensions 소개”에서는 Trusted Extensions 기능으로 Oracle Solaris 시스템에서 구현되는 기본 개념에 대해 설명합니다.

2 장, “Trusted Extensions에 로그인(작업)”에서는 시스템 액세스 및 Trusted Extensions 시스템 종료에 대한 절차를 설명합니다.

3 장, “Trusted Extensions에서 작업(작업)”에서는 Trusted Extensions를 사용하여 작업을 수행하는 방법에 대해 설명합니다.

4 장, “Trusted Extensions의 요소(참조)”에서는 Trusted Extensions 기능이 포함된 시스템의 주요 요소에 대해 설명합니다.

용어집에서는 Trusted Extensions에 사용되는 보안 용어에 대해 설명합니다.

Oracle Support에 액세스

Oracle 고객은 My Oracle Support를 통해 전자 지원에 액세스할 수 있습니다. 자세한 내용은 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info`를 참조하거나, 청각 장애가 있는 경우 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs`를 방문하십시오.

활자체 규약

다음 표는 이 책에서 사용되는 활자체 규약에 대해 설명합니다.

표 P–1 활자체 규약

활자체	설명	예
`AaBbCc123`	명령 및 파일, 디렉토리 이름; 컴퓨터 화면에 출력되는 내용입니다.	`.login` 파일을 편집하십시오. 모든 파일 목록을 보려면 `ls -a` 명령을 사용하십시오. `machine_name% you have mail.`
`AaBbCc123`	사용자가 입력하는 내용으로 컴퓨터 화면의 출력 내용과 대조됩니다.	`machine_name%` **`su`** `Password:`
aabbcc123	새로 나오는 용어, 강조 표시할 용어입니다. 명령줄 변수를 실제 이름이나 값으로 바꾸십시오.	`rm` *filename* 명령을 사용하여 파일을 제거합니다.

표 P–1 활자체 규약 (계속)

활자체	설명	예
AaBbCc123	책 제목, 장, 절	**사용자 설명서**의 6장을 읽으십시오. **캐시**는 로컬로 저장된 복사본입니다. 파일을 저장하면 **안 됩니다**. **주:** 일부 강조된 항목은 온라인에서 굵은체로 나타납니다.

명령 예의 셸 프롬프트

다음 표에는 Oracle Solaris OS에 포함된 셸의 기본 UNIX 시스템 프롬프트 및 수퍼유저 프롬프트가 나와 있습니다. 명령 예제에 표시된 기본 시스템 프롬프트는 Oracle Solaris 릴리스에 따라 다릅니다.

표 P–2 쉘 프롬프트

셸	프롬프트
Bash 셸, Korn 셸 및 Bourne 셸	`$`
수퍼유저용 Bash 셸, Korn 셸 및 Bourne 셸	`#`
C 셸	`machine_name%`
수퍼유저용 C 셸	`machine_name#`

◆ ◆ ◆ 1 장

1 Trusted Extensions 소개

이 장에서는 Trusted Extensions 기능을 통해 Oracle Solaris 운영 체제(Oracle Solaris OS)에 추가되는 레이블 및 기타 보안 기능을 소개합니다.

Trusted Extensions란?

Trusted Extensions는 Oracle Solaris 시스템에 특수 보안 기능을 제공합니다. 이러한 기능을 통해 조직은 Oracle Solaris 시스템에서 레이블 지정 보안 정책을 정의하고 구현할 수 있습니다. **보안 정책**은 사용자의 사이트에서 정보 및 기타 자원(예: 컴퓨터 하드웨어)을 보호하는 일련의 규칙이나 방침입니다. 일반적으로 보안 규칙은 어떤 사용자가 어떤 정보에 액세스했는지 또는 어떤 사용자가 이동식 매체에 데이터를 쓸 수 있도록 허용되었는지와 같은 문제를 처리합니다. **보안 실행**은 작업을 수행하기 위해 권장되는 절차입니다.

다음 절에서는 Trusted Extensions에서 제공하는 일부 주요 보안 기능에 대해 설명합니다. 텍스트는 어떤 보안 기능을 구성할 수 있는지 나타냅니다.

Trusted Extensions 침입자로부터 시스템 보호

Trusted Extensions는 침입자에 대한 보호 기능을 Oracle Solaris OS에 추가합니다. Trusted Extensions에는 또한 암호 보호와 같은 일부 Oracle Solaris 기능이 사용됩니다. Trusted Extensions에는 역할에 대한 암호 변경 GUI가 추가되었습니다. 기본적으로 사용자에게는 마이크 또는 카메라와 같은 주변 장치를 사용할 수 있는 권한이 부여되어야 합니다.

신뢰할 수 있는 컴퓨팅 기반에 대한 액세스 제한됨

신뢰할 수 있는 컴퓨팅 기반(*TCB*)은 보안과 관련이 있는 이벤트를 처리하는 Trusted Extensions의 일부를 말합니다. TCB에는 소프트웨어, 하드웨어, 펌웨어, 설명서 및 관리 절차가 포함됩니다. 보안 관련 파일에 액세스할 수 있는 유틸리티 및 응용 프로그램은 모두 TCB의 일부입니다. 관리자는 TCB와 함께 가질 수 있는 모든 잠재적 상호 작용에 대해 한도를 설정합니다. 이러한 상호 작용에는 작업을 수행해야 하는 프로그램, 액세스할 수 있는 파일 및 보안에 영향을 줄 수 있는 유틸리티가 포함됩니다.

필수 액세스 제어(MAC) 정보 보호

침입자가 시스템에 성공적으로 로그인할 경우 추가 장애물이 정보에 대한 액세스를 방지합니다. 파일과 기타 자원은 액세스 제어로 보호됩니다. Oracle Solaris OS에서와 같이 액세스 제어는 정보 소유자가 설정할 수 있습니다. Trusted Extensions에서 액세스는 시스템으로도 제어됩니다. 자세한 내용은 17 페이지 “Trusted Extensions에서 제공하는 임의의 액세스 제어 및 필수 액세스 제어”를 참조하십시오.

주변 장치 보호됨

Trusted Extensions에서 관리자는 테이프 드라이브, CD-ROM 드라이브, USB 장치, 프린터 및 마이크와 같은 로컬 주변 장치에 대한 액세스를 제어합니다. 액세스는 사용자별로 부여할 수 있습니다. 소프트웨어는 다음과 같이 주변 장치에 대한 액세스를 제한합니다.

- 장치는 기본적으로 사용하도록 할당해야 합니다.
- 사용자는 이동식 매체를 제어하는 장치에 대한 액세스 권한이 있어야 합니다.
- 원격 사용자는 마이크로폰 또는 CD-ROM 드라이브와 같은 로컬 장치를 사용할 수 없습니다. 로컬 사용자만 장치를 할당할 수 있습니다.

사용자를 속이는 프로그램으로부터 보호됨

"스푸핑"은 위조하는 것을 의미합니다. 침입자는 로그인 또는 기타 합법적인 프로그램을 스푸핑하여 암호 또는 기타 민감한 데이터를 가로챕니다. Trusted Extensions는 다음과 같이 화면 상단에서 쉽게 인식할 수 있는 허위 방지 아이콘인 **신뢰할 수 있는 기호**를 표시하여 악의적인 스푸핑 프로그램으로부터 사용자를 보호합니다.

그림 1–1 신뢰할 수 있는 기호

이 기호는 신뢰할 수 있는 컴퓨팅 기반(TCB)과 상호 작용할 때마다 표시됩니다. 이것은 보안 관련 트랜잭션을 안전하게 수행하도록 합니다. 잠재적인 보안 유출을 나타내는 기호는 볼 수 없습니다. 그림 1–1에서는 신뢰할 수 있는 기호를 보여줍니다.

Trusted Extensions에서 제공하는 임의의 액세스 제어 및 필수 액세스 제어

Trusted Extensions는 임의의 액세스 제어와 필수 액세스 제어를 모두 제공하여 어떤 사용자가 어떤 정보에 액세스할 수 있는지를 제어합니다.

임의 액세스 제어

임의의 액세스 제어(DAC)는 파일 및 디렉토리에 대한 사용자의 액세스를 제어하는 소프트웨어 메커니즘입니다. DAC는 파일 및 디렉토리의 설정 보호를 소유자 임의로 남겨둡니다. DAC의 두 가지 형식은 UNIX 권한 비트와 액세스 제어 목록(ACL)입니다.

소유자는 사용 권한 비트를 사용하여 소유자, 그룹 및 기타 사용자 별로 읽기, 쓰기 및 실행 보호를 설정할 수 있습니다. 일반 UNIX 시스템에서 수퍼유저 또는 `root` 사용자는 DAC 보호를 대체할 수 있습니다. Trusted Extensions에서 DAC 대체 기능은 관리자와 권한이 부여된 사용자에게만 허용됩니다. ACL은 액세스 제어에 대해 더 상세한 정보를 제공합니다. ACL을 사용하여 소유자는 특정 사용자와 특정 그룹에 대한 권한을 별도로 지정할 수 있습니다. 자세한 내용은 **Oracle Solaris 관리: ZFS 파일 시스템**의 8 장, “ACL 및 속성을 사용하여 Oracle Solaris ZFS 파일 보호”를 참조하십시오.

필수 액세스 제어

필수 액세스 제어(MAC)는 레이블 관계에 기반을 둔 시스템 강제 시행 액세스 제어 메커니즘입니다. 시스템은 프로그램을 실행하기 위해 만들어진 모든 프로세스에 민감도 레이블을 연결합니다. MAC 정책은 이 레이블을 사용하여 액세스 제어를 결정합니다. 일반적으로 프로세스는 대상 레이블이 프로세스 레이블과 같지 않는 한, 정보를 저장하거나 다른 프로세스와 통신할 수 없습니다. MAC 정책은 동일한 레이블의 객체 또는 하위 레이블의 객체에서 데이터를 읽을 수 있도록 프로세스를 허용합니다. 그러나 관리자는 하위 수준 객체가 거의 없거나 사용 가능한 하위 수준 객체가 없는 레이블이 지정된 환경을 만들 수 있습니다.

기본적으로 MAC 정책은 사용자가 볼 수 없습니다. 해당 객체에 대한 MAC 액세스 권한이 없는 한, 일반 사용자는 객체를 볼 수 없습니다. 모든 경우에 사용자는 MAC 정책과는 반대로 어떠한 작업도 수행할 수 없습니다.

민감도 레이블 및 클리어런스

레이블에는 다음과 같은 두 개의 구성 요소가 있습니다.

- 분류, **수준**이라고도 함

  이 구성 요소는 보안의 계층적 수준을 나타냅니다. 사람에게 적용될 때 분류는 신뢰도를 나타냅니다. 데이터에 적용될 때 분류는 필요한 보호 수준을 나타냅니다.

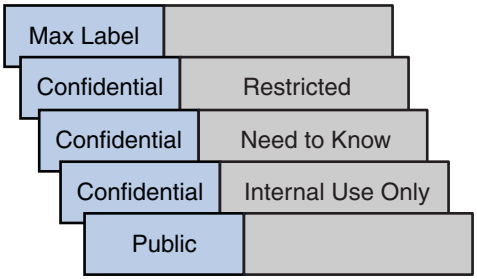
  미국 정부에서 정의한 분류는 TOP SECRET, SECRET, CONFIDENTIAL 및 UNCLASSIFIED입니다. 산업 분류는 표준화되어 있지 않습니다. 고유한 분류는 회사에서 설정할 수 있습니다. 예제를 보려면 그림 1–2를 참조하십시오. 왼쪽에 있는 용어는 분류입니다. 오른쪽에 있는 용어는 구획입니다.

- 구획, **범주**라고도 함

  구획은 작업 그룹, 부서, 프로젝트, 주제 등과 같은 그룹화를 나타냅니다. 분류에는 구획이 없어도 됩니다. 그림 1–2에서 Confidential 분류에는 세 개의 배타적 구획이 있습니다. Public 및 Max Label에는 구획이 없습니다. 그림에서와 같이, 이 조직에는 다섯 개의 레이블이 정의됩니다.

Trusted Extensions는 **민감도 레이블** 및 **클리어런스**라는 두 개의 레이블 유형을 유지관리합니다. 사용자는 하나 이상의 민감도 레이블에서 작업을 지울 수 있습니다. **사용자 클리어런스**라고 하는 특수 레이블은 사용자가 작업을 수행할 수 있도록 허용되는 최대 레이블을 결정합니다. 또한 각 사용자에게는 최소 민감도 레이블이 있습니다. 이 레이블은 기본적으로 다중 레벨 데스크탑 세션에 로그인하는 동안 사용됩니다. 로그인한 후 사용자는 이 범위 내의 다른 레이블에서 작업을 수행하도록 선택할 수 있습니다. 사용자는 최소 민감도 레이블로 Public을, 클리어런스로 Confidential: Need to Know를 할당할 수 있습니다. 첫 번째 로그인 시 데스크탑 작업 공간은 Public 레이블에 있습니다. 세션 중에 사용자는 Confidential: Internal Use Only 및 Confidential: Need to Know에서 작업 공간을 만들 수 있습니다.

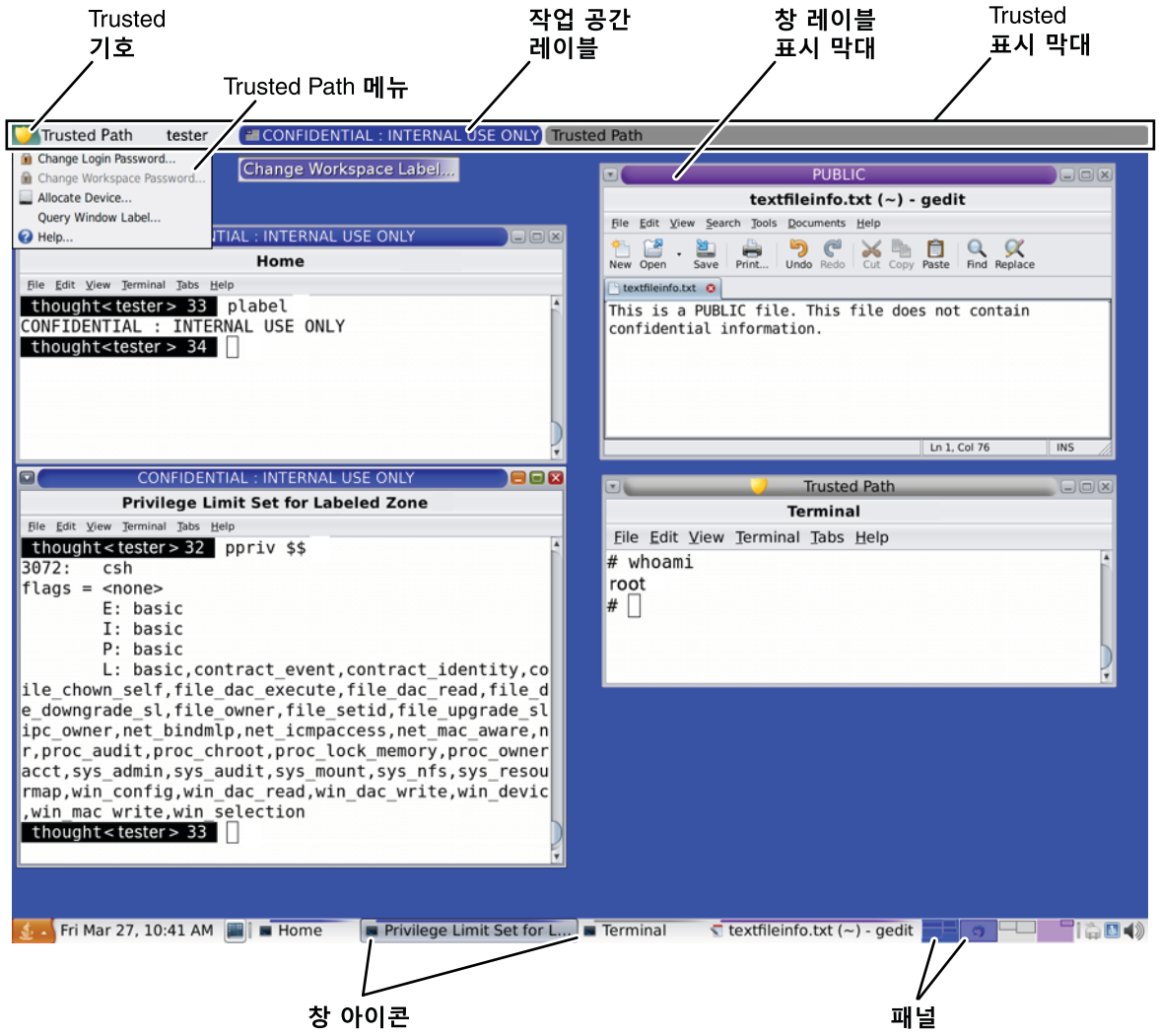
그림 1–2 일반적인 업계 민감도 레이블



모든 주체 및 객체는 Trusted Extensions로 구성된 시스템에 레이블이 있습니다. **주체**는 일반적으로 프로세스인 활성 엔티티입니다. 이 프로세스로 정보가 객체 간에 흐르거나, 시스템 상태가 변경될 수 있습니다. **객체**는 데이터 파일, 디렉토리, 프린터, 또는 기타 장치 등의 데이터가 들어있거나 수신되는 수동적인 엔티티입니다. 경우에 따라 프로세스는 한 프로세스에서 `kill` 명령을 사용할 때와 같이 객체일 수 있습니다.

그림 1–3은 일반적인 다중 레벨 Trusted Extensions 세션을 보여줍니다. 신뢰할 수 있는 스트라이프가 맨 위에 표시됩니다. 신뢰할 수 있는 스트라이프에서 Trusted Path(신뢰할 수 있는 경로) 메뉴가 호출됩니다. 역할을 수락하려면 사용자 이름을 눌러 역할 메뉴를 호출합니다. 맨 아래 패널의 작업 공간 스위치에는 작업 공간 레이블의 색상이 표시됩니다. 맨 아래 패널의 창 목록에는 창 레이블의 색상이 표시됩니다.

그림 1–3 일반적인 다중 레벨 세션



컨테이너 및 레이블

Trusted Extensions는 레이블을 지정하기 위해 컨테이너를 사용합니다. 컨테이너는 **영역**이라고도 합니다. **전역 영역**은 관리 영역이며 사용자에게 제공되지 않습니다. 비전역 영역을 **레이블이 있는 영역**이라고도 합니다. 레이블이 지정된 영역은 사용자에게 제공됩니다. 전역 영역은 일부 시스템 파일을 사용자와 공유합니다. 레이블이 지정된 영역에서 해당 파일을 볼 수 있는 경우, 이 파일의 레이블은 ADMIN_LOW입니다. 사용자는 ADMIN_LOW 파일의 내용을 읽을 수 있지만 변경할 수 없습니다.

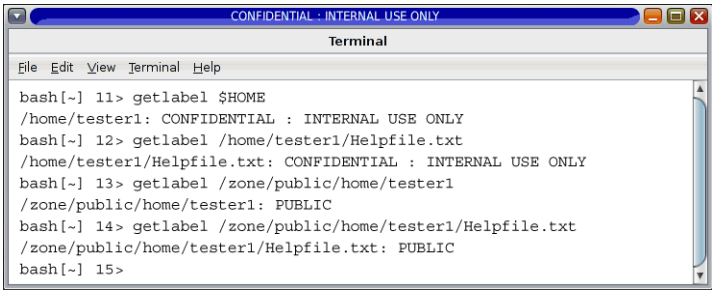
네트워크 통신은 레이블로 제한됩니다. 기본적으로 영역은 해당 레이블이 다르기 때문에 서로 통신할 수 없습니다. 따라서 한 영역은 다른 영역으로 쓸 수 없습니다.

그러나 관리자는 다른 영역에서 특정 디렉토리를 읽을 수 있도록 특정 영역을 구성할 수 있습니다. 다른 영역은 동일한 호스트 또는 원격 시스템에 있을 수 있습니다. 예를 들어 하위 수준 영역의 사용자 홈 디렉토리는 자동 마운트 서비스를 사용하여 마운트할 수 있습니다. 이러한 하위 수준의 홈 마운트에 대한 경로 이름 규약에는 다음과 같이 영역 이름이 포함됩니다.

`/zone/`*name-of-lower-level-zone*`/home/`*username*

다음 터미널 창에서는 하위 수준의 홈 디렉토리 표시를 보여 줍니다. 로그인 레이블이 `Confidential: Internal Use Only`인 사용자는 하위 수준의 영역을 읽을 수 있도록 자동 마운트 서비스를 구성할 때 `Public` 영역의 내용을 볼 수 있습니다. `textfileInfo.txt` 파일에는 두 개의 버전이 있습니다. `Public` 영역 버전에는 공개적으로 공유할 수 있는 정보가 포함되어 있습니다. `Confidential: Internal Use Only` 버전에는 회사 내에서만 공유할 수 있는 정보가 포함되어 있습니다.

그림 1–4 상위 레이블 영역에서 공개 정보 보기



레이블 및 트랜잭션

Trusted Extensions 소프트웨어는 시도된 모든 보안 관련 트랜잭션을 관리합니다. 소프트웨어는 주체의 레이블을 객체의 레이블과 비교한 다음 **지배**하는 레이블에 따라 트랜잭션을 허용하거나 허용하지 않습니다. 엔티티의 레이블이 다음과 같은 두 조건을 충족하는 경우 다른 엔티티의 레이블을 **지배**한다고 합니다.

- 첫 번째 엔티티 레이블의 분류 구성 요소는 객체의 분류와 같거나 객체의 분류보다 우위에 있습니다.
- 두 번째 엔티티 레이블의 모든 구획은 첫 번째 엔티티 레이블에 포함됩니다.

두 개의 레이블은 레이블에 동일한 분류와 구획 집합이 있을 경우 **동일**하다고 말합니다. 레이블이 같을 경우 레이블은 서로 지배합니다. 따라서 액세스가 허용됩니다.

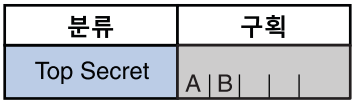
다음 조건 중 하나가 충족되는 경우 첫 번째 레이블은 두 번째 레이블을 **엄격하게 지배**한다고 합니다.

- 첫 번째 레이블의 분류는 두 번째 레이블의 분류보다 우위에 있습니다.
- 첫 번째 레이블의 분류는 두 번째 레이블의 분류와 같고 첫 번째 레이블은 두 번째 레이블의 구획을 포함하며 첫 번째 레이블에는 추가 구획이 있습니다.

두 번째 레이블을 엄격하게 지배하는 레이블은 두 번째 레이블에 대한 액세스가 허용됩니다.

어떤 레이블도 다른 레이블을 지배하지 않는 경우 두 레이블은 **분리**되었다고 합니다. 분리된 레이블 간의 액세스는 허용되지 않습니다.

예를 들어 다음과 같은 그림을 생각할 수 있습니다.



네 개의 레이블은 다음 구성 요소에서 만들 수 있습니다.

- TOP SECRET
- TOP SECRET A
- TOP SECRET B
- TOP SECRET AB

TOP SECRET AB는 자체를 지배하며 다른 레이블을 엄격하게 지배합니다. TOP SECRET A는 자체를 지배하며 TOP SECRET를 엄격하게 지배합니다. TOP SECRET B는 자체를 지배하며 TOP SECRET를 엄격하게 지배합니다. TOP SECRET A와 TOP SECRET B는 분리됩니다.

읽기 트랜잭션에서 주체의 레이블은 객체의 레이블을 지배해야 합니다. 이 규칙은 주체의 신뢰 수준이 객체에 대한 액세스 요구 사항을 충족시킵니다. 즉, 주체의 레이블에는 객체에 대한 액세스를 허용하는 모든 구획이 포함되어 있습니다. TOP SECRET A는 TOP SECRET A와 TOP SECRET 데이터를 읽을 수 있습니다. 마찬가지로 TOP SECRET B는 TOP SECRET B와 TOP SECRET 데이터를 읽을 수 있습니다. TOP SECRET A는 TOP SECRET B 데이터를 읽을 수 없습니다. 또한 TOP SECRET B는 TOP SECRET A 데이터를 읽을 수 없습니다. TOP SECRET AB는 모든 레이블에서 데이터를 읽을 수 있습니다.

즉, 쓰기 트랜잭션에서 주체가 객체를 만들거나 수정하면 그 결과 나타나는 객체의 레이블이 있는 영역은 주체의 레이블이 있는 영역과 같아야 합니다. 한 영역에서 다른 영역으로의 쓰기 트랜잭션은 허용되지 않습니다.

실제로, 읽기 및 쓰기 트랜잭션의 주체와 객체는 보통 동일한 레이블을 가지며 엄격하게 지배할 필요가 없습니다. 예를 들어 TOP SECRET A 주체는 TOP SECRET A 객체를 만들거나 수정할 수 있습니다. Trusted Extensions에서 TOP SECRET A 객체는 TOP SECRET A라는 레이블이 있는 영역에 있습니다.

다음 표는 미국 정부 레이블과 업계 레이블 집합 간의 지배 관계를 보여 줍니다.

표 1–1 Trusted Extensions의 레이블 관계 예

	레이블 1	관계	레이블 2
미국 정부 레이블	TOP SECRET AB	(엄격한) 지배	SECRET A
	TOP SECRET AB	(엄격한) 지배	SECRET A B
	TOP SECRET AB	(엄격한) 지배	TOP SECRET A
	TOP SECRET AB	지배(동등)	TOP SECRET AB
	TOP SECRET AB	분리	TOP SECRET C
	TOP SECRET AB	분리	SECRET C
	TOP SECRET AB	분리	SECRET A B C
업계 레이블	Confidential: Restricted	지배	Confidential: Need to Know
	Confidential: Restricted	지배	Confidential: Internal Use Only
	Confidential: Restricted	지배	Public
	Confidential: Need to Know	지배	Confidential: Internal Use Only
	Confidential: Need to Know	지배	Public
	Confidential: Internal	지배	Public
	Sandbox	분리	모든 기타 레이블

다른 레이블과 파일 간에 정보를 전송할 때 Trusted Extensions는 파일의 레이블을 변경할 권한이 있는지 여부를 확인 대화 상자에 표시합니다. 변경할 권한이 없는 경우 Trusted Extensions는 트랜잭션을 허용하지 않습니다. 보안 관리자는 사용자에게 정보를 업그레이드하거나 다운그레이드할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 44 페이지 “신뢰할 수 있는 작업 수행”을 참조하십시오.

데이터 보호에 대한 사용자의 책임

사용자는 파일과 디렉토리에 대한 보호 권한 설정을 담당합니다. 사용 권한을 설정하기 위해 수행할 수 있는 작업에서는 임의의 액세스 제어(DAC)라는 메커니즘을 사용합니다. `ls -l` 명령을 사용하거나 3 장, “Trusted Extensions에서 작업(작업)”에 설명된 대로 File Browser(파일 브라우저)를 사용하여 파일 및 디렉토리에 대한 권한을 확인할 수 있습니다.

필수 액세스 제어(MAC)는 시스템에서 자동으로 실행됩니다. 레이블이 있는 정보를 업그레이드하거나 다운그레이드할 권한이 있는 경우 정보 수준을 변경해야 할 필요가 있는지 확인해야 합니다.

데이터를 보호하는 또 다른 측면은 전자 메일과 관련되어 있습니다. 관리자로부터 전자 메일로 받은 지침을 따라서는 안 됩니다. 예를 들어, 사용자가 전자 메일의 지침에 따라 사용자의 암호를 특정 값으로 변경할 경우 사용자는 보낸 사람이 자신의 계정으로 로그인하도록 할 수 있습니다. 제한된 경우, 지침을 따르기 전에 별도로 지침을 확인할 수 있습니다.

Trusted Extensions 레이블별로 정보 구분

Trusted Extensions는 다음과 같은 방법으로 다른 레이블의 정보를 구분합니다.

- MAC는 전자 메일을 포함한 모든 트랜잭션에 강제 시행됩니다.
- 파일은 레이블에 따라 별도의 영역에 저장됩니다.
- 데스크탑은 레이블이 지정된 작업 공간을 제공합니다.
- 사용자는 단일 레벨 또는 다중 레벨 세션을 선택할 수 있습니다.
- 객체의 데이터는 객체를 다시 사용하기 전에 지워집니다.

단일 레벨 또는 다중 레벨 세션

Trusted Extensions 세션에 처음 로그인하는 경우 단일 레이블 또는 다중 레이블에서 작동할지 여부를 지정합니다. 그런 다음 **세션 클리어런스** 또는 **세션 레이블**을 설정합니다. 이 설정은 작동하려는 보안 수준입니다.

단일 레벨 세션에서는 현재 세션 레이블과 동일하거나 해당 레이블에서 지배되는 객체에만 액세스할 수 있습니다.

다중 레벨 세션에서는 세션 클리어런스와 동일하거나 낮은 레이블의 정보에 액세스할 수 있습니다. 작업 공간마다 다른 레이블을 지정할 수 있습니다. 또한 동일 레이블에서 여러 작업 공간을 가질 수 있습니다.

세션 선택 예제

표 1–2에서는 단일 레벨 및 다중 레벨 세션 간의 차이를 보여 주는 예를 제공합니다. 이 예는 `CONFIDENTIAL: NEED TO KNOW(CNF: NTK)`의 단일 레벨 세션에서 작동하도록 선택한 사용자를 `CNF: NTK`에서도 다중 레벨 세션을 선택한 사용자와 대조합니다.

왼쪽에 있는 세 개의 열은 로그인 시 각 사용자의 세션 선택을 보여 줍니다. 사용자는 단일 레벨 세션에 대해 **세션 레이블**을 설정하고 다중 레벨 세션에 대해 **세션 클리어런스**를 설정합니다. 시스템은 선택한 내용에 따라 올바른 레이블 구축기를 표시합니다. 다중 레벨 세션에 대한 샘플 레이블 구축기를 보려면 그림 3–4를 참조하십시오.

오른쪽에 있는 두 개의 열은 세션에서 사용할 수 있는 레이블 값을 표시합니다. 초기 작업 공간 레이블 열은 사용자가 시스템에 처음 액세스할 때의 레이블을 나타냅니다. 사용 가능한 레이블 열에는 세션 동안 전환하도록 허용된 레이블이 나열됩니다.

표 1–2 사용 가능한 세션 레이블의 초기 레이블 선택 효과

사용자 선택			세션 레이블 값	
세션 유형	세션 레이블	세션 클리어런스	초기 작업 공간 레이블	사용 가능한 레이블
단일 레벨	CNF: NTK	-	CNF: NTK	CNF: NTK
다중 레벨	-	CNF: NTK	Public	Public
				CNF: Internal Use Only
				CNF: NTK

테이블의 첫 번째 행에 표시된 대로 사용자는 CNF: NTK의 세션 레이블로 단일 레벨 세션을 선택했습니다. 사용자는 유일하게 작동할 수 있는 레이블이기도 한 CNF: NTK의 초기 작업 공간 레이블을 가지고 있습니다.

테이블의 두 번째 행에 표시된 대로 사용자는 CNF: NTK의 세션 클리어런스로 다중 레벨 세션을 선택했습니다. 사용자의 초기 작업 공간 레이블은 Public이 사용자의 계정 레이블 범위에서 가장 낮은 레이블이기 때문에 Public으로 설정됩니다. 사용자는 Public 및 CNF: NTK 간에 모든 레이블을 전환할 수 있습니다. Public은 최소 레이블이고 CNF: NTK는 세션 클리어런스입니다.

레이블이 지정된 작업 공간

Trusted Extensions 데스크탑에서 작업 공간은 하단 패널 오른쪽에 있는 작업 공간 패널을 통해 액세스됩니다.

그림 1–5 패널의 레이블이 지정된 작업 공간

각 작업 공간에는 레이블이 있습니다. 동일한 레이블을 여러 작업 공간에 할당할 수 있고, 여러 작업 공간에 각각 다른 레이블을 할당할 수도 있습니다. 작업 공간에서 시작된 창에는 해당 작업 공간의 레이블이 지정됩니다. 다른 레이블의 작업 공간으로 창이 이동되어도 창의 레이블은 원래대로 유지됩니다. 따라서 다중 레벨 세션에서는 서로 다른 레이블의 창을 하나의 작업 공간에 배열할 수 있습니다.

전자 메일 트랜잭션용 MAC 실행

Trusted Extensions는 전자 메일에 MAC를 적용합니다. 현재 레이블에서 전자 메일을 보내고 읽을 수 있습니다. 계정 범위 내의 레이블에서 전자 메일을 받을 수 있습니다. 다중 레벨 세션에서는 해당 레이블에서 전자 메일을 읽을 수 있도록 다른 레이블에서 작업 공간을 전환할 수 있습니다. 동일한 메일 읽기 프로그램 및 동일한 로그인을 사용합니다. 시스템은 사용자의 현재 레이블에서만 메일을 읽을 수 있도록 허용합니다.

객체를 다시 사용하기 전에 객체의 데이터 지우기

Trusted Extensions는 다시 사용하기 전에 사용자가 액세스할 수 있는 객체에서 기존 정보를 자동으로 지워 민감한 정보가 실수로 노출되지 않도록 방지합니다. 예를 들어 메모리 및 디스크 공간은 다시 사용하기 전에 지워집니다. 객체를 다시 사용하기 전에 민감도 데이터를 제거하지 못하면 부적절한 사용자에게 데이터가 노출될 위험이 있습니다. 장치 할당 해제를 통해 Trusted Extensions는 드라이버를 프로세스에 할당하기 전에 사용자가 액세스할 수 있는 모든 객체를 지웁니다. 하지만 다른 사용자가 드라이브에 액세스하도록 허용하기 전에 DVD 및 USB 장치와 같은 모든 이동식 저장소 매체를 지워야 합니다.

Trusted Extensions 보안 관리 사용

기존의 UNIX 시스템과 달리 수퍼유저(root 사용자)는 Trusted Extensions를 관리하는 데 사용되지 않습니다. 오히려, 고유한 기능이 있는 관리자 역할은 시스템을 관리합니다. 이러한 방법을 사용할 경우 어떠한 사용자도 시스템의 보안을 손상시킬 수 없습니다. **역할**은 특수 작업을 수행하는 데 필요한 권한이 있는 특정 응용 프로그램에 액세스하는 특수 사용자 계정입니다. 권한에는 레이블, 권한 부여, 권한 및 유효한 UID/GID가 포함됩니다.

다음 보안 실행은 Trusted Extensions로 구성된 시스템에서 적용됩니다.

- 사용할 필요성(need-to-use)을 기반으로 응용 프로그램에 액세스할 수 있는 권한을 부여받습니다.
- 관리자로부터 특수한 권한 부여 또는 특권을 부여받은 사용자만 보안 정책을 대체하는 기능을 수행할 수 있습니다.
- 시스템 관리 의무는 여러 역할로 구분됩니다.

Trusted Extensions의 응용 프로그램에 액세스

Trusted Extensions에서는 작업을 수행하는 데 필요한 프로그램에만 액세스할 수 있습니다. Oracle Solaris OS에서와 같이 관리자는 하나 이상의 권한 프로필을 사용자의

계정에 지정하여 액세스 권한을 제공합니다. **권한 프로필**은 프로그램 및 보안 속성의 특수 모음입니다. 이러한 보안 속성을 사용하면 권한 프로필에 있는 프로그램을 제대로 사용할 수 있습니다.

Oracle Solaris OS는 **권한** 및 **권한 부여**와 같은 보안 속성을 제공합니다. Trusted Extensions는 레이블을 제공합니다. 이러한 속성이 누락되면 프로그램이나 프로그램의 일부를 사용할 수 없게 됩니다. 예를 들어 권한 프로필에는 데이터베이스를 읽을 수 있는 권한이 포함될 수 있습니다. 데이터베이스를 수정하거나 `Confidential`로 분류된 정보를 읽으려면 다른 보안 속성이 포함된 권한 프로필이 필요할 수 있습니다.

연결된 보안 속성이 있는 프로그램이 포함된 권한 프로필을 사용하면 사용자가 프로그램을 잘못 사용하거나 시스템에서 데이터를 손상시키지 못하도록 방지할 수 있습니다. 보안 정책을 대체하는 작업을 수행해야 할 경우, 관리자는 사용자에게 필요한 보안 속성이 포함된 권한 프로필을 할당할 수 있습니다. 특정 작업을 실행하지 못하도록 방지할 경우 관리자에게 문의하십시오. 필요한 보안 속성이 누락되었을 수 있습니다.

또한 관리자는 로그인 쉘과 마찬가지로 프로필 쉘을 할당할 수 있습니다. **프로필 셸**은 특정 응용 프로그램 및 기능 집합에 대한 액세스를 제공하는 공통 셸의 특별 버전입니다. 프로필 셸은 Oracle Solaris OS의 기능입니다. 자세한 내용은 `pfexec(1)` 매뉴얼 페이지를 참조하십시오.

주 – 프로그램을 실행하고 **찾을 수 없음** 오류 메시지를 받거나 명령을 실행하고 **프로필에 없음** 오류 메시지를 받으면 이 프로그램을 사용하도록 허용되지 않을 수 있습니다. 보안 관리자에게 문의하십시오.

Trusted Extensions의 역할에 따른 관리

Trusted Extensions에서는 관리용 역할 사용을 권장합니다. 사용자의 사이트에서 어떤 사용자가 어떤 업무 세트를 수행하는지 알아야 합니다. 공통 역할은 다음과 같습니다.

- 루트 역할 – 주로 수퍼유저가 직접 로그인하지 못하도록 하는 데 사용됩니다.
- 보안 관리자 역할 – 장치 할당 권한 부여, 권한 프로필 지정 및 소프트웨어 프로그램 평가 등의 보안 관련 작업을 수행합니다.
- 시스템 관리자 역할 – 사용자 만들기, 홈 디렉토리 설정 및 소프트웨어 프로그램 설치 등의 표준 시스템 관리 작업을 수행합니다.
- 운영자 역할 – 시스템 백업을 수행하고 프린터를 관리하며 이동식 매체를 마운트합니다.

◆ ◆ ◆ 2 장

2 Trusted Extensions에 로그인(작업)

이 장에서는 신뢰할 수 있는 데스크탑 및 Trusted Extensions 시스템의 로그인 프로세스에 대해 설명합니다. 이 장에서는 다음 주제를 다룹니다.

Trusted Extensions의 데스크탑 로그인

Trusted Extensions에서 사용하는 데스크탑은 보호되어 있습니다. 레이블은 보호된 상태를 볼 수 있도록 표시됩니다. 응용 프로그램, 데이터 및 통신에는 레이블이 지정됩니다. 데스크탑은 Oracle Solaris 데스크탑의 신뢰할 수 있는 버전입니다.

로그인 화면에는 레이블이 없습니다. 로그인 프로세스에는 세션에 대한 레이블을 지정해야 합니다. 레이블을 선택한 후에는 데스크탑, 창 및 모든 응용 프로그램에 레이블이 지정됩니다. 또한 보안에 영향을 주는 응용 프로그램은 신뢰할 수 있는 경로 표시기로 보호됩니다.

Trusted Extensions 로그인 프로세스

Trusted Extensions로 구성된 시스템의 로그인 프로세스는 Oracle Solaris의 로그인 프로세스와 비슷합니다. 그러나 Trusted Extensions에서는 데스크탑 세션을 시작하기 전에 보안 관련 정보에 대한 몇 가지 화면을 검사합니다. 프로세스는 다음 절에 자세히 설명되어 있습니다. 다음은 간단한 개요입니다.

1. 식별 – Username(사용자 이름) 필드에 사용자 이름을 입력합니다.
2. 인증 – Password(암호) 필드에 암호를 입력합니다.

   확인 및 인증 단계를 성공적으로 완료하면 시스템에 대한 사용 권한이 확인됩니다.

3. 메시지 확인 및 세션 유형 선택 – Message Of The Day(오늘의 메시지) 대화 상자에서 정보를 확인합니다. 이 대화 상자는 사용자가 마지막으로 로그인한 시간과 관리자가 보낸 메시지 및 사용자 세션의 보안 속성을 표시합니다. 둘 이상의 레이블에서 작동이 허용된 경우 세션 유형인 단일 레벨 또는 다중 레벨을 지정할 수 있습니다.

주 – 계정이 한 레이블에서만 작동하도록 사용자를 제한하면 세션 유형을 지정할 수 없습니다. 이 제한 사항은 **단일 레이블** 또는 단일 레벨 구성이라고도 부릅니다. 예를 들어 24 페이지 “세션 선택 예제”를 참조하십시오.

---

4. 레이블 선택 – 레이블 구축기에서 사용자 세션에 있는 동안 작동하려는 최상위 보안 수준을 선택합니다.

주 – 기본적으로 원격 로그인은 Trusted Extensions의 일반 사용자용으로 지원되지 않습니다. 관리자가 Oracle Solaris Xvnc 소프트웨어를 구성한 경우 VNC 클라이언트를 사용하여 다중 레벨 데스크탑을 원격으로 표시할 수 있습니다. 이러한 절차는 34 페이지 “Trusted Extensions에 원격으로 로그인”을 참조하십시오.

로그인 시 식별 및 인증

로그인 중 식별 및 인증은 Oracle Solaris OS에서 처리됩니다. 처음에는 로그인 화면에 사용자 이름 프롬프트가 포함되어 있습니다. 이 로그인 프로세스 부분은 **식별**이라고도 합니다.

사용자 이름을 입력하면 암호 프롬프트가 표시됩니다. 이 프로세스 부분은 **인증**이라고도 합니다. 암호는 사용자가 사용자 이름을 사용할 권한이 있는 사용자임을 인증합니다.

암호는 시스템에 대한 사용자 ID를 확인하는 비공개 키입력의 조합입니다. 암호는 암호화된 형태로 저장되므로 시스템의 다른 사용자는 액세스할 수 없습니다. 다른 사용자는 이 암호를 사용하여 인증되지 않은 액세스를 얻을 수 없으므로 암호 보호의 책임은 사용자에게 있습니다. 사용자의 암호를 가진 타인이 확인이나 설명 없이 사용자의 모든 데이터에 액세스할 수 있으므로 절대로 다른 사람에게 암호를 적어주거나 공개하지 마십시오. 초기 암호는 보안 관리자가 제공합니다.

로그인 시 보안 속성 검토

보안 속성 검토는 Oracle Solaris OS가 아닌 Trusted Extensions에서 처리됩니다. 로그인이 완료되기 전에 Trusted Extensions는 MOTD(Message Of The Day)(오늘의 메시지) 대화 상자를 표시합니다. 이 대화 상자는 사용자가 검토할 수 있도록 상태 정보를 제공합니다. 상태에는 시스템을 마지막으로 사용한 시간과 같은 과거 정보가 포함됩니다. 또한 다음 세션에 영향을 주는 보안 속성을 검토할 수 있습니다. 계정이 둘 이상의 레이블에서 작동하도록 구성된 경우 단일 레벨 또는 다중 레벨 세션을 선택할 수 있습니다.

그런 다음 단일 레이블을 보거나 레이블 구축기에서 레이블 및 클리어런스를 선택할 수 있습니다.

Trusted Extensions에 로그인

다음 작업은 Trusted Extensions에 로그인하여 수행됩니다. 데스크탑에 연결하기 전에 보안 정보를 검토하고 지정할 수 있습니다.

▼ 시스템에서 사용자 식별 및 인증

1 **로그인 화면의 Username(사용자 이름) 필드에 사용자 이름을 입력합니다.**

관리자가 사용자에게 할당한 이름과 동일한 사용자 이름을 입력합니다. 철자와 대문자 표시에 유의하십시오.

입력을 실수한 경우 암호를 허위로 입력하십시오. Username(사용자 이름) 필드가 표시됩니다.

2 **입력한 내용을 확인합니다.**

Return 키를 눌러서 사용자 이름을 확인합니다.

주의 – 로그인 화면이 나타날 때 신뢰할 수 있는 스트라이프가 표시되면 **안 됩니다.** 로그인하거나 화면 잠금을 해제할 때 신뢰할 수 있는 스트라이프가 표시되면 암호를 입력하지 마십시오. 침입되고 있을 가능성이 있습니다. **스푸핑**은 침입자의 프로그램이 암호를 가로채기 위해 로그인 프로그램으로 가장하는 것입니다. 즉시 보안 관리자에게 문의하십시오.

3 **암호 입력 필드에 암호를 입력하고 Enter 키를 누릅니다.**

보안상의 이유로, 문자가 필드에 표시되지는 않습니다. 시스템은 로그인 이름과 암호를 인증된 사용자 목록과 비교합니다.

일반 오류 제공한 암호가 올바르지 않으면 화면에 다음 메시지가 표시됩니다.

```
Authentication failed(인증 실패)
```

OK(확인)를 눌러 오류 대화 상자를 닫습니다. 사용자 이름을 다시 입력한 후 올바른 암호를 입력하십시오.

▼ 메시지 확인 및 세션 유형 선택

사용자가 본인을 단일 레이블로 제한하지 않는 경우 다른 레이블에서 데이터를 볼 수 있습니다. 작동할 수 있는 범위는 세션 클리어런스에서 상한 끝으로, 관리자가 사용자에게 할당한 최소 레이블에서 하한 끝으로 제한됩니다.

1 MOTD 대화 상자를 확인합니다.

a. 마지막 세션의 시간이 정확한지 확인합니다.

정확하지 않은 시간과 같이 마지막 로그인에 대해 의심되는 사항이 없는지 항상 확인합니다. 시간이 정확하지 않다고 믿을 만한 이유가 있는 경우 보안 관리자에게 문의하십시오.

b. 관리자가 보낸 메시지를 확인합니다.

Message Of The Day(오늘의 메시지) 필드에는 일정이 잡힌 유지 관리 또는 보안 문제에 대한 경고가 포함될 수 있습니다. 이 필드의 정보를 항상 검토합니다.

c. 세션의 보안 속성을 검사합니다.

MOTD 대화 상자에는 사용자가 사용할 수 있는 역할, 최소 레이블 및 기타 보안 특성이 표시됩니다.

d. (옵션) 다중 레벨 세션에 로그인하도록 허용된 경우 단일 레벨 세션을 사용할지 여부를 결정합니다.

단일 레벨 세션에 로그인하려면 Restrict Session to a Single Label(세션을 단일 레이블로 제한) 버튼을 누릅니다.

e. OK(확인)를 누릅니다.

2 **레이블 선택을 확인합니다.**

사용자에게 레이블 구축기가 제공됩니다. 단일 레이블에서 로그인한 경우 레이블 구축기는 세션 레이블에 대해 설명합니다. 다중 레벨 시스템에서 레이블 구축기를 사용하면 세션 클리어런스를 선택할 수 있습니다. 다중 레벨 세션에 대한 샘플 레이블 구축기를 보려면 그림 3–4를 참조하십시오.

- **기본값을 사용하지 않을 특별한 이유가 없는 한, 기본값을 적용합니다.**
- **다중 레벨 세션의 경우 클리어런스를 선택합니다.**

  클리어런스를 변경하려면 Trusted Path 클리어런스를 누른 다음 원하는 클리어런스를 누릅니다.
- **단일 레벨 세션에 대해 레이블을 선택합니다.**

  레이블을 변경하려면 Trusted Path 레이블을 누른 다음 원하는 레이블을 누릅니다.

3 **OK(확인)를 누릅니다.**

신뢰할 수 있는 데스크탑이 표시됩니다.

▼ 문제 해결 로그인 문제

1 **사용자 이름 또는 암호를 인식하지 못하는 경우 관리자에게 문의하십시오.**

2 **레이블 범위가 워크스테이션에서 허용되지 않는 경우 관리자에게 문의하십시오.**

작업 공간은 세션 클리어런스 및 레이블의 한정된 범위로 제한될 수 있습니다. 예를 들어 로비의 워크스테이션은 PUBLIC 레이블로만 제한될 수 있습니다. 사용자가 지정한 레이블 또는 세션 클리어런스가 허용되지 않으면 관리자에게 문의하여 워크스테이션이 제한되어 있는지 확인합니다.

3 **쉘 초기화 파일을 사용자 정의했지만 로그인할 수 없는 경우 다음 두 가지 옵션을 선택할 수 있습니다.**

- **현재 문제를 해결하려면 시스템 관리자에게 문의하십시오.**
- **root가 될 수 있는 경우 비상 안전 세션에 로그인합니다.**

  표준 로그인에서 쉘 초기화 파일은 시작할 때 소스가 되어 환경을 사용자 정의합니다. 비상 안전 로그인에서는 기본값이 시스템에 적용되며, 쉘 초기화 파일은 소스가 되지 않습니다.

  Trusted Extensions에서는 비상 안전 로그인이 보호됩니다. root 계정만 비상 안전 로그인에 액세스할 수 있습니다.

  a. **로그인 화면에 사용자 이름을 입력합니다.**

b. **화면 하단의 데스크탑 메뉴에서 Solaris Trusted Extensions Failsafe Session(비상 안전 세션)을 선택합니다.**

c. **메시지가 표시되면 암호를 제공합니다.**

d. **추가 암호를 입력하라는 프롬프트가 표시되면 root에 대한 암호를 입력합니다.**

Trusted Extensions에 원격으로 로그인

VNC(가상 네트워크 컴퓨팅)는 랩탑 또는 홈 컴퓨터에서 중앙 Trusted Extensions 시스템에 액세스하기 위한 방법을 제공합니다. 사이트 관리자는 Trusted Extensions 서버에서 Oracle Solaris Xvnc 소프트웨어가 실행되도록 구성하고 클라이언트 시스템에서 VNC 뷰어가 실행되도록 구성해야 합니다. 서버에 설치된 레이블 범위 내의 모든 레이블에서 작동할 수 있습니다.

▼ 원격 Trusted Extensions 데스크탑에 로그인하는 방법

시작하기 전에 관리자가 Xvnc 서버를 설정했습니다. 관련 링크는 **Trusted Extensions 구성 및 관리**의 "원격 액세스를 위해 Xvnc를 사용하여 Trusted Extensions 시스템을 구성하는 방법"을 참조하십시오.

1 **터미널 창에서는 Xvnc 서버에 연결합니다.**

관리자가 Xvnc로 구성한 서버의 이름을 입력합니다.

```
% /usr/bin/vncviewer Xvnc-server
```

2 **로그인합니다.**

31 페이지 "Trusted Extensions에 로그인"의 절차를 따릅니다.

이제 VNC 뷰어에서 Trusted Extensions 데스크탑을 사용하여 작업할 수 있습니다.

◆ ◆ ◆ 3 장

3 Trusted Extensions에서 작업(작업)

이 장에서는 Trusted Extensions 작업 공간에서 작업을 수행하는 방법을 설명합니다. 이 장에서는 다음 주제를 다룹니다.

Trusted Extensions에 표시되는 데스크탑 보안

Trusted Extensions는 다중 레벨 데스크탑을 제공합니다.

Trusted Extensions로 구성된 시스템의 경우 로그인 및 화면 잠금 시를 제외하고는 항상 신뢰할 수 있는 스트라이프가 표시됩니다. 다른 경우에서는 모두 신뢰할 수 있는 스트라이프를 볼 수 있습니다.

스트라이프는 화면 상단에 있습니다. 신뢰할 수 있는 기호는 사용자가 TCB(신뢰할 수 있는 컴퓨팅 기반)를 사용할 때 신뢰할 수 있는 스트라이프에 표시됩니다. 예를 들어 암호를 변경할 때 TCB와 상호 작용합니다.

다중 헤드 Trusted Extensions 시스템의 모니터가 수평으로 구성된 경우 모니터 전체에서 하나의 신뢰할 수 있는 스트라이프가 나타납니다. 하지만 다중 헤드 시스템이 세로로 표시되도록 구성되었거나 모니터당 하나씩 별도의 데스크탑을 포함하는 경우 신뢰할 수 있는 스트라이프가 하나의 모니터에만 표시됩니다.

주의 – 두 번째 신뢰할 수 있는 스트라이프가 다중 헤드 시스템에 나타난 경우 해당 스트라이프는 운영 체제에 의해 생성되지 않습니다. 시스템에 허용되지 않은 프로그램이 있을 수 있습니다.

즉시 보안 관리자에게 문의하십시오. 올바른 신뢰할 수 있는 스트라이프를 확인하려면 42 페이지 "마우스 포인터를 찾는 방법"을 참조하십시오.

응용 프로그램, 메뉴, 레이블 및 데스크탑의 기능에 대한 자세한 내용은 4 장, "Trusted Extensions의 요소(참조)"를 참조하십시오.

Trusted Extensions 로그아웃 프로세스

워크스테이션을 로그인한 상태로 둔 채 자리를 비우는 것은 보안상 위험할 수 있습니다. 잠시 자리를 비우는 경우에는 항상 워크스테이션을 보호해 두는 것이 좋습니다. 곧 다시 사용하는 경우에는 화면을 잠급니다. 대부분의 사이트에서 지정한 유휴 기간이 지나면 화면이 자동으로 잠깁니다. 잠시 동안 사용하지 않을 경우나 다른 사람이 워크스테이션을 사용할 것으로 예상되는 경우에는 로그아웃합니다.

레이블이 있는 시스템에서의 작업

주의 – 신뢰할 수 있는 스트라이프가 작업 공간에서 누락된 경우 보안 관리자에게 문의하십시오. 시스템 문제는 심각할 수 있습니다.

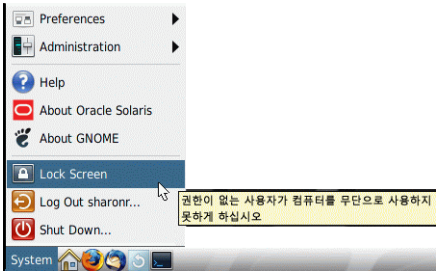
로그인 중이거나 화면을 잠글 경우 신뢰할 수 있는 스트라이프가 표시되지 않습니다. 신뢰할 수 있는 스트라이프가 표시되면 관리자에게 즉시 문의하십시오.

▼ 화면을 잠그고 잠금 해제하는 방법

워크스테이션에서 잠시 자리를 비우는 경우에는 화면을 잠급니다.

1 **주 메뉴에서 Lock Screen(화면 잠금)을 선택합니다.**

그림 3–1 Lock Screen(화면 잠금) 선택



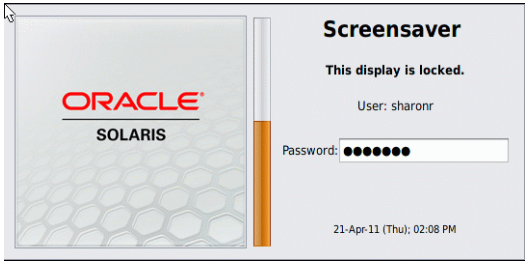
화면이 검은색으로 바뀝니다. 이 때, 사용자만 다시 로그인할 수 있습니다.

주 – 화면이 잠긴 상태에서는 신뢰할 수 있는 스트라이프가 표시되지 않아야 합니다. 스트라이프가 나타나는 경우 즉시 보안 관리자에게 알려야 합니다.

---

2 **화면을 잠금 해제하려면 다음을 수행합니다.**

a. **Screensaver(화면 보호기) 대화 상자가 표시될 때까지 마우스를 움직입니다.**



Screensaver(화면 보호기) 대화 상자가 표시되지 않으면 Return 키를 누릅니다.

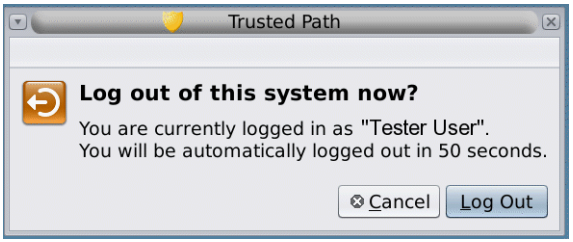
b. **암호를 입력합니다.**

이렇게 하면 세션이 이전 상태로 돌아갑니다.

▼ Trusted Extensions에서 로그아웃하는 방법

대부분의 사이트에서 지정한 유휴 기간이 지나면 화면이 자동으로 잠깁니다. 워크스테이션에서 잠시 자리를 비우는 경우 또는 다른 사람이 워크스테이션을 사용할 것으로 예상되는 경우에는 로그아웃합니다.

1 **Trusted Extensions에서 로그아웃하려면 주 메뉴에서 Log Out(로그아웃) *your-name*을 선택합니다.**



2 **로그아웃할지 확인한 후 Cancel(취소)을 누릅니다.**

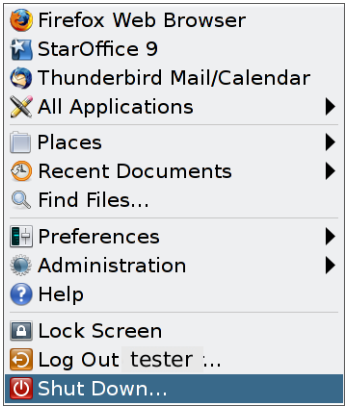
▼ 시스템을 종료하는 방법

로그아웃은 Trusted Extensions 세션을 종료하는 일반적인 방법입니다. 워크스테이션을 종료해야 할 경우 다음 절차를 사용합니다.

주 – 콘솔에서만 시스템을 종료할 수 있습니다. 예를 들어, VNC 클라이언트에서는 시스템을 종료할 수 없습니다.

시작하기 전에 사용자에게 Maintenance and Repair 권한 프로필이 지정되어 있어야 합니다.

- **주 메뉴에서 Shut Down(종료)을 선택합니다.**



종료를 확인합니다.

주 – 기본적으로 키보드 조합 Stop-A(L1-A)는 Trusted Extensions에서 사용할 수 없습니다. 보안 관리자는 이 기본값을 변경할 수 있습니다.

▼ 레이블이 있는 작업 공간에서 파일을 보는 방법

파일을 보려면 Oracle Solaris 시스템의 데스크탑에서 사용하는 것과 동일한 응용 프로그램을 사용합니다. 여러 레이블에서 작업하는 경우 작업 공간의 레이블에 있는 파일만 볼 수 있습니다.

- **터미널 창 또는 File Browser(파일 브라우저)를 엽니다.**
  - **털미널 창을 열고 홈 디렉토리의 내용을 나열합니다.**
    배경에서 마우스 버튼 3을 누릅니다. 메뉴에서 Open Terminal(단말기 열기)을 선택합니다.
  - **데스크탑 또는 데스크탑 패널에서 Home(홈) 폴더를 누릅니다.**
    폴더가 File Browser(파일 브라우저)에 열립니다. File Browser(파일 브라우저) 응용 프로그램은 현재 작업 공간과 동일한 레이블에서 열립니다. 응용 프로그램은 해당 레이블에 있는 파일에 대해서만 액세스됩니다. 다른 레이블에서 파일을 보는 자세한 내용은 20 페이지 “컨테이너 및 레이블”을 참조하십시오. 하나의 작업 공간에 있는 서로 다른 레이블에서 파일을 보려면 50 페이지 “다른 작업 공간으로 창을 이동하는 방법”을 참조하십시오.

▼ Trusted Extensions 매뉴얼 페이지에 액세스하는 방법

- **Oracle Solaris 릴리스의 터미널 창에서 `trusted_extensions(5)` 매뉴얼 페이지를 검토하십시오.**

```
% man trusted_extensions
```

Trusted Extensions에 적용되는 사용자 명령 목록은 **Trusted Extensions 구성 및 관리**의 부록 D, “Trusted Extensions 매뉴얼 페이지 목록”을 참조하십시오. 매뉴얼 페이지는 Oracle의 설명서 웹 사이트 (`http://www.oracle.com/technetwork/indexes/documentation/index.html`)에서도 제공됩니다.

▼ 모든 레이블에서 초기화 파일을 액세스하는 방법

다른 레이블에 파일을 연결하거나 파일을 복사하면 하위 레이블이 있는 파일을 상위 레이블에서 볼 수 있도록 할 경우 유용합니다. 연결된 파일은 하위 레이블에서만 쓸 수

있습니다. 복사된 파일은 각 레이블에서 고유하며, 각 레이블에서 수정할 수 있습니다. 자세한 내용은 **Trusted Extensions 구성 및 관리**의 ".copy_files 및 .link_files 파일"을 참조하십시오.

시작하기 전에 다중 레벨 세션에 로그인해야 합니다. 사이트의 보안 정책은 연결을 허용해야 합니다.

이 파일을 수정하는 경우 관리자에게 문의하십시오.

1. **다른 레이블에 연결할 초기화 파일을 결정합니다.**

2. **`~/.link_files` 파일을 만들거나 수정합니다.**
   한 줄당 하나의 파일에 항목을 입력합니다. 홈 디렉토리에 하위 디렉토리에 대한 경로를 지정할 수는 있지만, 선행 슬래시(/)는 사용할 수 없습니다. 모든 경로는 홈 디렉토리 내에 있어야 합니다.

3. **다른 레이블에 복사할 초기화 파일을 결정합니다.**
   초기화 파일을 복사하면 특정 이름의 파일에 항상 쓰는 응용 프로그램이 있고 다른 레이블에서 데이터를 구별해야 할 경우 유용합니다.

4. **`~/.copy_files` 파일을 만들거나 수정합니다.**
   한 줄당 하나의 파일에 항목을 입력합니다. 홈 디렉토리에 하위 디렉토리에 대한 경로를 지정할 수는 있지만, 선행 슬래시(/)는 사용할 수 없습니다. 모든 경로는 홈 디렉토리 내에 있어야 합니다.

예 3–1 .copy_files 파일 만들기

이 예에서 사용자는 레이블당 여러 개의 초기화 파일을 사용자 정의할 수 있습니다. 조직에서 회사 웹 서버는 `Restricted` 수준에서 사용할 수 있습니다. 따라서 `Restricted` 수준의 `.mozilla` 파일에서 다른 초기 설정을 설정합니다. 이와 유사하게, 특수 템플리트와 별칭이 `Restricted` 수준에 있습니다. 따라서 `Restricted` 수준에서 `.aliases` 및 `.soffice` 초기화 파일을 수정합니다. 가장 낮은 레이블에서 `.copy_files` 파일을 만든 후에는 이 파일을 손쉽게 수정할 수 있습니다.

```
% vi .copy_files
# Copy these files to my home directory in every zone
.aliases
.mozilla
.soffice
```

예 3–2 .link_files 파일 만들기

이 예제에서 사용자는 자신의 메일 기본값 및 C 셸 기본값을 모든 레이블에서 동일하게 유지합니다.

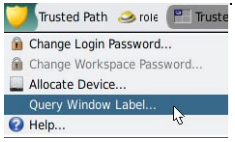
```
% vi .link_files
# Link these files to my home directory in every zone
.cshrc
.mailrc
```

일반 오류 이 파일은 비정상적 사항을 다루기 위한 보호 조치가 없습니다. 두 파일의 중복 항목이나 이미 다른 레이블에 있는 파일 항목으로 인해 오류가 발생할 수 있습니다.

▼ 창 레이블을 대화식으로 표시하는 방법

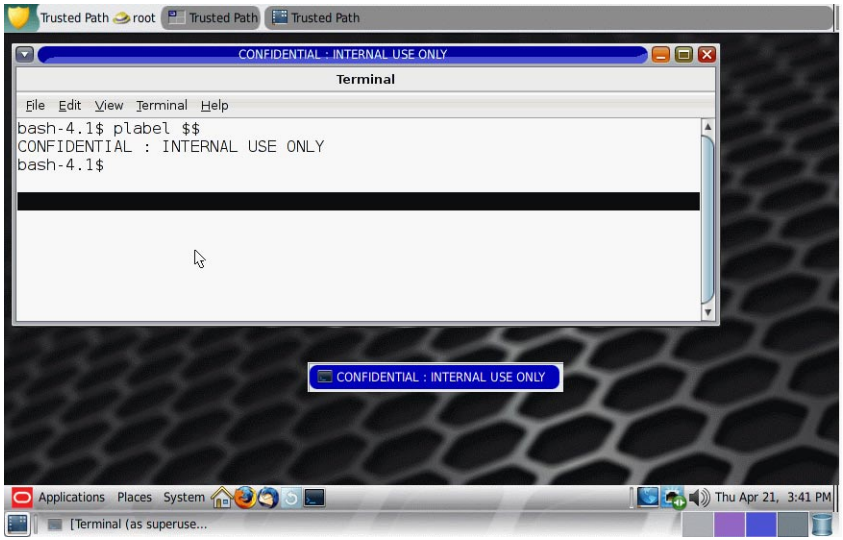
이 작업은 부분적으로 숨겨진 창의 레이블을 식별하는 데 유용할 수 있습니다.

1. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Query Window Label(창 레이블 쿼리)을 선택합니다.**



2. **포인터를 화면 주위로 이동합니다.**
   포인터 아래의 영역 레이블이 화면 가운데에 있는 작은 사각형 상자에 표시됩니다.

그림 3–2 창 레이블 쿼리 작업



3. **마우스 버튼을 눌러 작업을 종료합니다.**

▼ 마우스 포인터를 찾는 방법

신뢰할 수 없는 응용 프로그램은 키보드 또는 마우스 포인터에 대한 제어 권한을 얻을 수 있습니다. 포인터 찾기를 통해 데스크탑 포커스에 대한 제어 권한을 다시 확보할 수 있습니다.

1 **Sun 키보드에 대한 제어 권한을 다시 확보하려면 Meta-Stop을 누르십시오.**

키를 동시에 눌러 현재 데스크탑 포커스에 대한 컨트롤을 다시 얻습니다. Sun 키보드에서 스페이스바 양쪽에 있는 다이아몬드 키는 Meta 키입니다.

키보드 또는 마우스 포인터 잡기를 신뢰할 수 없는 경우 포인터는 신뢰할 수 있는 스트라이프로 이동합니다. 신뢰할 수 있는 포인터는 신뢰할 수 있는 스트라이프로 이동하지 않습니다.

2 **Sun 키보드를 사용하지 않는 경우 Alt-Break를 누르십시오.**

예 3–3 마우스 포인터를 신뢰할 수 있는 스트라이프로 강제 지정

이 예에서 사용자는 신뢰할 수 있는 프로세스를 실행하고 있지 않지만 마우스 포인터를 볼 수 없습니다. 신뢰할 수 있는 스트라이프의 중앙으로 포인터를 가져오려면 Meta-Stop 키를 동시에 누릅니다.

예 3–4 실제 신뢰할 수 있는 스트라이프 찾기

모니터가 각 모니터당 별개의 데스크탑을 표시하도록 구성된 다중 헤드 Trusted Extensions 시스템에서는 모니터당 하나의 신뢰할 수 있는 스트라이프가 표시됩니다. 따라서 Trusted Extensions 이외의 프로그램이 신뢰할 수 있는 스트라이프를 생성합니다. 다중 헤드 시스템이 모니터당 별개의 데스크탑을 표시하도록 구성된 경우 신뢰할 수 있는 스트라이프가 하나만 표시됩니다.

사용자가 작업을 중지하고 즉시 보안 관리자에게 연락합니다. 그런 다음 작업 공간 배경 위쪽과 같이 신뢰할 수 없는 위치에 마우스 포인터를 배치하여 실제 신뢰할 수 있는 스트라이프를 찾습니다. 사용자가 Alt-Break 키를 동시에 누르면 Trusted Extensions에서 생성된 신뢰할 수 있는 스트라이프로 포인터가 이동합니다.

▼ Trusted Extensions에서 일부 공통 데스크탑 작업을 수행하는 방법

일부 공통 작업은 레이블과 보안의 영향을 받습니다. 특히, 다음 작업은 Trusted Extensions의 영향을 받습니다.

- 휴지통 비우기
- 캘린더 이벤트 찾기

1 **휴지통을 비웁니다.**

데스크탑의 휴지통 아이콘 위에서 마우스 버튼 3을 누릅니다. Empty Trash(휴지통 비우기)를 선택한 다음 확인합니다.

주 – 휴지통에는 작업 공간 레이블에 있는 파일만 포함될 수 있습니다. 민감한 정보는 휴지통에 있는 즉시 삭제합니다.

---

2 **모든 레이블에서 캘린더 이벤트를 찾습니다.**

캘린더에는 캘린더를 연 작업 공간 레이블의 이벤트만 표시됩니다.

- **다중 레벨 세션에서 서로 다른 레이블이 포함된 각 작업 공간에서 캘린더를 엽니다.**
- **단일 레벨 세션의 경우 로그아웃합니다. 그런 다음 다른 레이블에서 로그인하여 해당 레이블에서 캘린더 이벤트를 확인합니다.**

3 **모든 레이블에서 사용자 정의된 데스크탑을 저장합니다.**

로그인하는 모든 레이블에 대해 작업 공간 구성을 사용자 정의할 수 있습니다.

a. **데스크탑을 구성합니다.**

주 – 사용자는 데스크탑 구성을 저장할 수 있습니다. 역할은 데스크탑 구성을 저장할 수 없습니다.

---

i. **주 메뉴에서 System(시스템) > Preferences(기본 설정) > Appearance(모양)를 누릅니다.**

ii. **창을 배열하고 글꼴 크기를 설정하며 다른 사용자 정의를 수행합니다.**

b. **현재 데스크탑을 저장하려면 주 메뉴를 누릅니다.**

i. **System(시스템) > Preferences(기본 설정) > Startup Applications(응용 프로그램 시작)를 누릅니다.**

ii. **Options(옵션) 탭을 누릅니다.**

iii. **Remember Currently Running Applications(현재 실행 중인 프로그램 기억)를 누른 다음 대화 상자를 닫습니다.**

다음에 이 레이블에 로그인하면 해당 구성에서 데스크탑이 복원됩니다.

신뢰할 수 있는 작업 수행

다음 보안 관련 작업에는 신뢰할 수 있는 경로가 필요합니다.

주의 – 보안 관련 작업을 시도하는 경우 신뢰할 수 있는 기호가 누락되면 즉시 보안 관리자에게 문의하십시오. 시스템에 심각한 문제가 있을 수 있습니다.

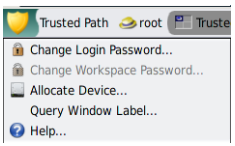
▼ Trusted Extensions의 암호를 변경하는 방법

Oracle Solaris OS와 달리 Trusted Extensions는 암호 변경을 위한 GUI를 제공합니다. GUI는 암호 작업이 완료될 때까지 포인터를 잡습니다. 포인터를 잡은 프로세스를 중지하려면 예 3–5를 참조하십시오.

1 **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Change Login Password(로그인 암호 변경) 또는 Change Workspace Password(작업 공간 암호 변경)을 선택합니다.**

암호 메뉴 항목을 선택하려면 신뢰할 수 있는 스트라이프에서 Trusted Path(**신뢰할 수 있는 경로**)를 누릅니다.

그림 3–3 신뢰할 수 있는 경로 메뉴



주 – 사이트에서 영역별로 별개의 이름 지정 서비스를 실행 중인 경우 Trusted Path(신뢰할 수 있는 경로) 메뉴 항목 Change Workspace Password(**작업 공간 암호 변경**)가 활성화됩니다.

2 **현재 암호를 입력합니다.**

이 작업은 사용자가 이 사용자 이름에 대한 적합한 사용자임을 확인합니다. 보안상의 이유로, 암호를 입력할 때 암호는 표시되지 않습니다.

주의 – 암호를 입력할 때 커서가 Change Password(암호 변경) 대화 상자에 있고 신뢰할 수 있는 기호가 표시되어 있는지 확인합니다. 커서가 이 대화 상자에 없으면 실수로 다른 사용자가 볼 수 있는 다른 창에 암호를 입력할 수 있습니다. 신뢰할 수 있는 기호가 표시되지 않으면 다른 사람이 암호를 도용하려고 시도했을 수 있습니다. 보안 관리자에게 즉시 문의하십시오.

3 **새 암호를 입력합니다.**

4 **암호를 다시 입력하여 확인합니다.**

주 – Change Password(**암호 변경**)를 선택했고 사이트에서 로컬 계정을 사용 중인 경우 영역 또는 시스템을 재부트하기 전까지 새 암호가 적용되지 않습니다. 영역을 재부트하려면 사용자에게 Zone Security 권한 프로필이 지정되어 있어야 합니다. 시스템을 재부트하려면 사용자에게 Maintenance and Repair 권한 프로필이 지정되어 있어야 합니다. 이러한 프로필이 사용자에게 지정되지 않은 경우 시스템 관리자에게 연락하여 재부트 일정을 잡으십시오.

예 3–5 암호 프롬프트를 신뢰할 수 있는지 테스트

Sun 키보드가 포함된 x86 시스템에서는 사용자에게 암호를 입력하라는 메시지가 표시됩니다. 마우스 포인터가 확보되어 Password(암호) 대화 상자에 배치됩니다. 프롬프트를 신뢰할 수 있는지 확인하려면 Meta-Stop 키를 동시에 누릅니다. 포인터가 대화 상자에 남아 있으면 암호 프롬프트를 신뢰할 수 있음을 확인할 수 있습니다.

포인터가 대화 상자에 남아 있지 않으면 암호 프롬프트를 신뢰할 수 없음을 확인할 수 있습니다. 그런 다음 관리자에게 연락해야 합니다.

▼ 다른 레이블에서 로그인하는 방법

첫 번째 로그인 후 후속 로그인 세션에 표시되는 첫 번째 작업 공간의 레이블은 레이블 범위 내의 모든 레이블에 대해 설정할 수 있습니다.

사용자가 로그인하는 모든 레이블에 대해 시작 세션 특성을 구성할 수 있습니다.

시작하기 전에 다중 레벨 세션에 로그인해야 합니다.

1 **모든 레이블에서 작업 공간을 만듭니다.**
자세한 내용은 49 페이지 “최소 레이블에서 작업 공간 추가 방법”을 참조하십시오.

2 **표시하려는 작업 공간에 대해 각 작업 공간을 구성합니다.**

3 **해당 레이블에 로그인할 때 표시하려는 레이블이 지정된 작업 공간으로 이동합니다.**

4 **현재 작업 공간을 저장합니다.**
자세한 내용은 42 페이지 “Trusted Extensions에서 일부 공통 데스크탑 작업을 수행하는 방법”을 참조하십시오.

▼ Trusted Extensions에서 장치를 할당하는 방법

Allocate Device(장치 할당) 메뉴 항목을 사용하면 독점적으로 사용할 장치를 마운트하여 할당할 수 있습니다. 장치를 할당하지 않은 상태에서 사용하려고 하면 "사용 권한이 거부되었습니다."라는 오류 메시지가 표시됩니다.

시작하기 전에 사용자는 장치를 할당할 권한이 있어야 합니다.

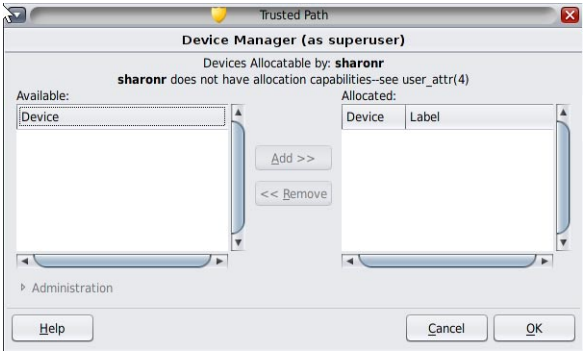
1. **Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Allocate Device(장치 할당)를 선택합니다.**

2. **사용할 장치를 두 번 누릅니다.**

   현재 레이블에서 할당이 허용된 장치가 Available Devices(사용 가능한 장치)에 나타납니다.

   - `audio`*n* – 마이크로폰 및 스피커를 나타냅니다.
   - `cdrom`*n* – CD-ROM 드라이브를 나타냅니다.
   - `floppy`*n* – 디스켓 드라이브를 나타냅니다.
   - `mag_tape`*n* – 테이프 드라이브(스트리밍)를 나타냅니다.
   - `rmdisk`*n* – 이동식 디스크(예: JAZ 또는 ZIP 드라이브) 또는 USB 핫플러그 가능 매체를 나타냅니다.

   다음 대화 상자에는 사용자가 장치 할당 권한이 부여되지 않은 것으로 표시됩니다.



3. **장치를 선택합니다.**

   사용할 수 있는 장치(Available Devices) 목록에서 할당된 장치(Allocated Devices) 목록으로 장치를 옮깁니다.

   - **Available Devices(사용 가능한 장치) 목록에서 장치 이름을 두 번 누릅니다.**
   - **또는 장치를 선택하고 Allocate(할당) 버튼을 눌러 오른쪽을 가리킵니다.**

이 단계는 지우기 스크립트를 시작합니다. 지우기 스크립트는 매체에 다른 트랜잭션의 데이터가 남아 있지 않는지 확인합니다.

현재 작업 공간의 레이블이 장치에 적용됩니다. 장치 매체에서 전송되는 모든 데이터는 이 레이블이 지배해야 합니다.

4 **지침을 따릅니다.**

지침은 매체에 올바른 레이블이 있는지 확인합니다. 예를 들어 마이크를 사용할 경우 다음과 같은 지침이 표시됩니다.

그런 다음 장치가 마운트됩니다. 이제 할당된 장치 목록에 해당 장치 이름이 나타납니다. 이 장치는 독점적으로 사용하도록 할당되었습니다.

일반 오류 사용할 장치가 목록에 나타나지 않으면 관리자에게 문의하십시오. 장치가 오류 상태에 있거나 다른 사람이 사용하고 있을 수 있습니다. 또는 장치를 사용할 권한이 없을 수 있습니다.

다른 역할 작업 공간으로 전환하거나 다른 레이블에서 작업 공간으로 전환하면 할당된 장치는 해당 레이블에서 작동할 수 없습니다. 새 레이블에서 장치를 사용하려면 초기 레이블에서 장치를 할당 해제한 다음 새 레이블에서 장치를 할당해야 합니다. Device Manager(장치 관리자)를 다른 레이블의 작업 공간으로 이동하면 올바른 컨텍스트를 반영하도록 Available Devices(사용할 수 있는 장치) 및 Allocated Devices(할당된 장치) 목록이 변경됩니다.

File Browser(파일 브라우저) 창이 표시되지 않으면 창을 수동으로 연 후 루트 디렉토리 /로 이동합니다. 이 디렉토리에서 할당된 장치로 이동하여 해당 내용을 봅니다.

▼ Trusted Extensions에서 장치를 할당 해제하는 방법

1 **장치를 할당 해제합니다.**

a. **Device Manager(장치 관리자)가 표시된 작업 영역으로 이동합니다.**

b. **할당된 장치 목록에서 할당 해제할 장치를 이동합니다.**

2 **매체를 제거합니다.**

3 **Deallocation(할당 해제) 대화 상자에서 OK(확인)를 누릅니다.**
이제 허용된 다른 사용자가 장치를 사용할 수 있습니다.

▼ Trusted Extensions에서 역할을 수락하는 방법

Oracle Solaris OS와 달리 Trusted Extensions는 역할을 가정하기 위한 GUI를 제공합니다.

1 **신뢰할 수 있는 기호의 오른쪽에서 사용자 이름을 누릅니다.**

2 **메뉴에서 역할 이름을 선택합니다.**

3 **역할 암호를 입력하고 Enter 키를 누릅니다.**
이 작업은 해당 역할을 합법적으로 수락할 수 있음을 확인합니다. 보안상의 이유로, 암호를 입력할 때 암호는 표시되지 않습니다.

주의 – 암호를 입력할 때 커서가 Change Password(암호 변경) 대화 상자에 있고 신뢰할 수 있는 기호가 표시되어 있는지 확인합니다. 커서가 이 대화 상자에 없으면 실수로 다른 사용자가 볼 수 있는 다른 창에 암호를 입력할 수 있습니다. 신뢰할 수 있는 기호가 표시되지 않으면 다른 사람이 암호를 도용하려고 시도했을 수 있습니다. 보안 관리자에게 즉시 문의하십시오.

역할 암호가 수락되면 현재 작업 공간이 역할 작업 공간이 됩니다. 사용자가 전역 영역에 있습니다. 사용자 역할에서 권한 프로필로 허용된 작업을 수행할 수 있습니다.

▼ 작업 공간 레이블을 변경하는 방법

Trusted Extensions에서 작업 공간 레이블을 설정하는 기능은 동일한 다중 레벨 세션 내의 서로 다른 레이블에서 편리하게 작업을 수행할 수 있는 방법을 제공합니다.

이 절차를 사용하여 다른 레이블의 동일한 작업 공간에서 작업을 수행합니다. 다른 레이블에서 작업 공간을 만들려면 49 페이지 “최소 레이블에서 작업 공간 추가 방법”을 참조하십시오.

시작하기 전에 다중 레벨 세션에 로그인해야 합니다.

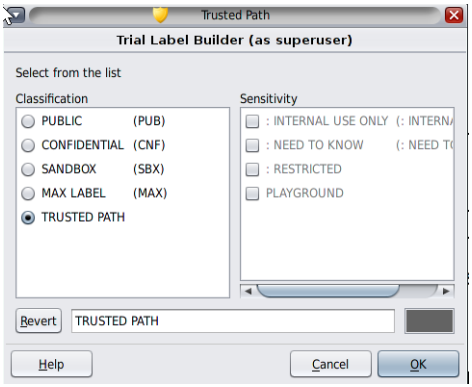
1 **신뢰할 수 있는 스트라이프에서 창 레이블을 누릅니다.**
작업 공간 패널을 누를 수도 있습니다.

2 **Change Workspace Label(작업 공간 레이블 변경)을 누릅니다.**

3 **레이블 구축기에서 레이블을 선택합니다.**

다음 그림에서는 Trusted Path(신뢰할 수 있는 경로) 버튼을 누르는 경우를 보여줍니다.

그림 3–4 레이블 구축기



이 버튼을 누른 다음에는 사용자가 사용자 레이블에서 선택할 수 있습니다. 작업 공간 레이블이 새 레이블로 변경됩니다. 레이블이 색상으로 지정된 시스템에서 새 창은 새 색상으로 표시됩니다.

4 **암호를 묻는 메시지가 표시되면 암호를 제공합니다.**

사이트가 영역당 별개의 이름 지정 서비스를 실행 중인 경우 새 레이블에서 작업 공간에 들어갈 때 사용자에게 암호를 묻는 메시지가 표시됩니다.

▼ 최소 레이블에서 작업 공간 추가 방법

Trusted Extensions에서 작업 공간 레이블을 설정하는 기능은 동일한 다중 레벨 세션 내의 서로 다른 레이블에서 편리하게 작업을 수행할 수 있는 방법을 제공합니다. 최소 레이블에서 작업 공간을 추가할 수 있습니다.

현재 작업 공간의 레이블을 변경하려면 48 페이지 “작업 공간 레이블을 변경하는 방법”을 참조하십시오.

시작하기 전에 다중 레벨 세션에 로그인해야 합니다.

1. **최소 레이블에서 작업 공간을 만들려면 다음을 수행하십시오.**

   a. **작업 공간 패널에서 마우스 버튼 3을 누릅니다.**

   b. **해당 메뉴에서 Preferences(기본 설정)를 선택합니다.**

   c. **Number of Workspaces(작업 공간 수) 필드에서 숫자를 늘립니다.**
   새 작업 공간이 최소 레이블에서 만들어집니다. 또한 이 대화 상자를 사용하여 작업 공간의 이름을 지정할 수 있습니다. 툴팁에 이름이 나타납니다.

   d. **(옵션) 작업 공간의 이름을 지정합니다.**
   작업 공간 패널 위로 마우스를 가져가면 이름이 도구 설명으로 표시됩니다.

2. **작업 공간 레이블을 변경하려면 작업 공간 패널을 선택하고 해당 레이블을 변경합니다.**
   자세한 내용은 48 페이지 "작업 공간 레이블을 변경하는 방법"을 참조하십시오.

▼ 다른 레이블에서 작업 공간을 전환하는 방법

시작하기 전에 다중 레벨 세션에 로그인해야 합니다.

1. **다른 색상의 작업 공간 패널을 누릅니다.**

2. **암호를 묻는 메시지가 표시되면 암호를 제공합니다.**
   사이트가 영역당 별개의 이름 지정 서비스를 실행 중인 경우 새 레이블에서 작업 공간에 들어갈 때 사용자에게 암호를 묻는 메시지가 표시됩니다.

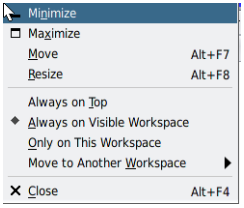
일반 오류 단일 레벨 세션에 로그인한 경우 다른 레이블에서 작업하려면 로그아웃해야 합니다. 그런 다음 원하는 레이블에 로그인합니다. 허용된 경우 다중 레벨 세션에 로그인할 수 있습니다.

▼ 다른 작업 공간으로 창을 이동하는 방법

창을 다른 레이블의 작업 공간으로 끌면 창이 원래 레이블에 유지됩니다. 해당 창의 모든 작업은 포함된 작업 공간의 레이블이 아닌 창의 레이블에서 수행됩니다. 창을 이동하면 정보를 비교하려는 경우 유용합니다. 또한 작업 공간 사이를 이동하지 않고 다른 레이블에서 응용 프로그램을 사용하려고 할 수도 있습니다.

1. **패널 표시에서 창을 하나의 패널에서 다른 패널로 끕니다.**
   끌어온 창이 두 번째 작업 공간에 나타납니다.

2 **모든 작업 공간에 창을 표시하려면 제목 표시줄의 오른쪽 버튼 메뉴에서 Always Visible(항상 표시)을 선택합니다.**



선택한 창은 이제 모든 작업 공간에 표시됩니다.

▼ 파일의 레이블을 결정하는 방법

일반적으로 파일의 레이블은 명확합니다. 그러나 현재 작업 공간보다 하위 레이블에서 파일을 보도록 허용된 경우 파일의 레이블이 명확하지 않을 수 있습니다. 특히 파일의 레이블은 File Browser(파일 브라우저)의 레이블과 다를 수 있습니다.

- **File Browser(파일 브라우저)를 사용합니다.**

참고 – 또한 Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Query Label(쿼리 레이블) 메뉴 항목을 사용할 수 있습니다.

▼ 레이블 간에 데이터를 이동하는 방법

Oracle Solaris 시스템에서와 같이 Trusted Extensions에서 창 사이에 데이터를 이동할 수 있습니다. 그러나 데이터는 동일한 레이블에 있어야 합니다. 다른 레이블이 있는 창 사이에 정보를 전송할 경우 해당 정보의 민감도를 업그레이드하거나 다운그레이드합니다.

시작하기 전에 사이트의 보안 정책은 이 전송 유형을 허용해야 하고, 포함된 영역은 레이블 다시 지정을 허용해야 하며, 사용자는 레이블 간에 데이터를 이동할 권한이 있어야 합니다.

따라서 관리자는 다음 작업을 완료해야 합니다.

- **Trusted Extensions 구성 및 관리**의 "레이블이 있는 영역에서 파일의 레이블을 재지정할 수 있게 설정하는 방법"
- **Trusted Extensions 구성 및 관리**의 "사용자가 데이터의 보안 수준을 변경할 수 있게 하는 방법"

다중 레벨 세션에 로그인해야 합니다.

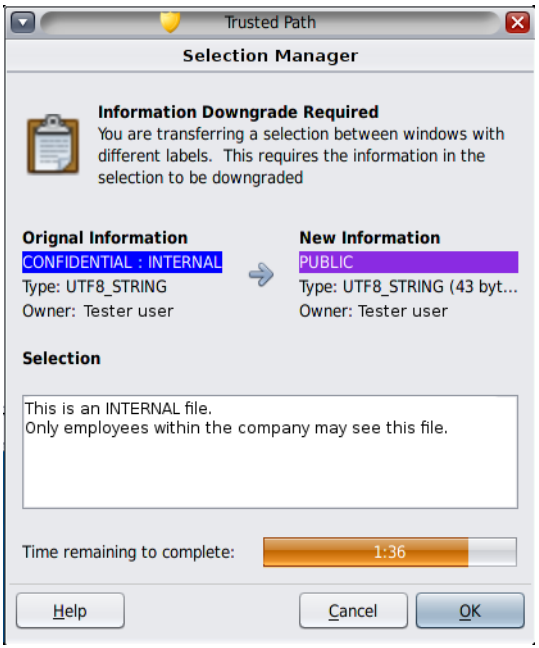
1. **두 레이블에서 작업 공간을 만듭니다.**
   자세한 내용은 49 페이지 “최소 레이블에서 작업 공간 추가 방법”을 참조하십시오.

2. **소스 파일의 레이블을 확인합니다.**
   자세한 내용은 51 페이지 “파일의 레이블을 결정하는 방법”을 참조하십시오.

3. **소스 정보가 있는 창을 대상 레이블의 작업 공간으로 이동합니다.**
   자세한 내용은 50 페이지 “다른 작업 공간으로 창을 이동하는 방법”을 참조하십시오.

4. **이동할 정보를 강조 표시하고 대상 창에 선택 내용을 붙여 넣습니다.**
   Selection Manager Confirmation(선택 관리자 확인) 대화 상자가 표시됩니다.

그림 3–5 선택 관리자 확인 대화 상자



5. **Selection Manager Confirmation(선택 관리자 확인) 대화 상자를 검토한 후 트랜잭션을 확인하거나 취소합니다.**
   이 대화 상자는 다음과 같습니다.
   - 트랜잭션을 확인해야 하는 이유를 설명합니다.
   - 소스 파일의 레이블과 소유자를 식별합니다.
   - 대상 파일의 레이블과 소유자를 식별합니다.

- 전송을 위해 선택한 데이터 유형, 대상 파일의 유형 및 데이터 크기(바이트)를 식별합니다. 기본적으로 선택한 데이터는 텍스트 형식으로 표시됩니다.
- 트랜잭션을 완료할 때까지 남아 있는 시간을 나타냅니다. 시간의 양과 타이머의 사용은 사이트 구성에 따라 결정됩니다.

◆ ◆ ◆ 4 장

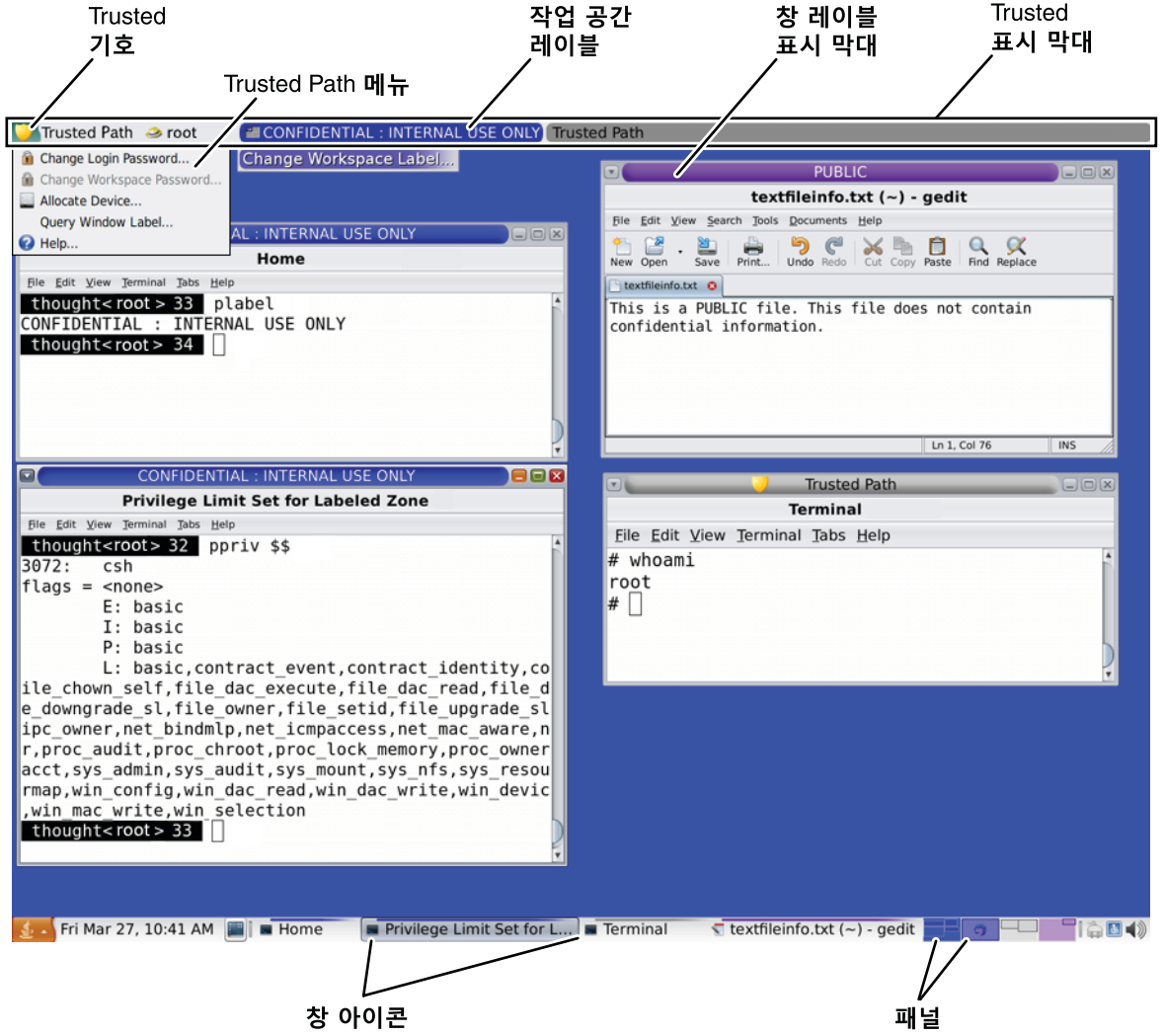
4 Trusted Extensions의 요소(참조)

이 장에서는 Trusted Extensions의 주요 요소에 대해 설명합니다. 이 장에서는 다음 주제를 다룹니다.

Trusted Extensions의 표시 기능

2 장, “Trusted Extensions에 로그인(작업)”에서 설명한 대로 로그인 프로세스를 성공적으로 완료한 후 Trusted Extensions 내에서 작업을 수행할 수 있습니다. 작업에는 보안 제한이 적용됩니다. Trusted Extensions에만 해당되는 제한 사항에는 시스템의 레이블 범위, 클리어런스 및 단일 레벨 또는 다중 레벨 세션 선택이 포함됩니다. 다음 그림에서와 같이 일부 기능에서는 Trusted Extensions로 구성된 시스템과 Oracle Solaris 시스템이 구분됩니다.

그림 4–1 Trusted Extensions 다중 레벨 데스크탑



- **레이블 표시** – 모든 창, 작업 공간, 파일 및 응용 프로그램에는 레이블이 있습니다. 데스크탑은 레이블 스트라이프 및 엔티티의 레이블을 표시하는 다른 표시기를 제공합니다.
- **신뢰할 수 있는 스트라이프** – 이 스트라이프는 특수한 그래픽 보안 메커니즘입니다. 모든 작업 공간에서 스트라이프는 화면 맨 위에 표시됩니다.
- **작업 공간에서 응용 프로그램에 대한 액세스 제한** – 작업 공간은 사용자의 계정에서 허용되는 응용 프로그램에 대한 액세스만 제공합니다.

- **Trusted Path(신뢰할 수 있는 경로) 메뉴 –** 신뢰할 수 있는 기호는 메뉴에 대한 액세스를 제공합니다.

Trusted Extensions 데스크탑의 레이블

17 페이지 “필수 액세스 제어”에 설명된 것처럼 Trusted Extensions의 모든 응용 프로그램과 파일에는 레이블이 있습니다. Trusted Extensions는 다음 위치에 레이블을 표시합니다.

- 창의 제목 표시줄 위의 창 레이블 스트라이프
- 창 목록에서 창 아이콘 위에 있는 레이블 색상 스트라이프
- 신뢰할 수 있는 스트라이프의 창 레이블 표시기
- 포인터 위치로 지정된 창의 레이블 또는 창 아이콘을 표시하는 Trusted Path(신뢰할 수 있는 경로) 메뉴의 Query Window Label(창 레이블 쿼리) 표시기

또한 패널 색상은 작업 공간의 레이블을 나타냅니다.

그림 4–2 다른 레이블에 있는 작업 공간을 나타내는 패널

그림 4–1에서는 Trusted Extensions 데스크탑에 레이블이 표시되는 방법을 보여줍니다. 또한 Query Window Label(창 레이블 쿼리) 메뉴 항목을 사용하여 창의 레이블을 표시할 수 있습니다. 이에 대한 그림은 그림 3–2를 참조하십시오.

신뢰할 수 있는 스트라이프

신뢰할 수 있는 스트라이프는 화면 맨 위에 표시됩니다.

그림 4–3 데스크탑의 신뢰할 수 있는 스트라이프

신뢰할 수 있는 스트라이프는 사용자의 세션이 정상적인 Trusted Extensions 세션인지를 시각적으로 보여줍니다. 이 스트라이프는 신뢰할 수 있는 컴퓨팅 기반(TCB)과 상호 작용하고 있을 때 표시됩니다. 또한 현재 작업 공간과 현재 창의 레이블도 표시합니다. 트러스트 스트라이프를 다른 윈도우나 대화 상자로 이동시키거나 숨길 수 없습니다.

신뢰할 수 있는 스트라이프의 요소는 다음과 같습니다.

- **신뢰할 수 있는 기호** – 화면 포커스가 보안과 관련되어 있을 때 표시됩니다.
- **창 레이블** – 화면 포커스가 보안과 관련되지 않았을 때 활성 창의 레이블을 표시합니다.
- **역할 표시자** – 신뢰할 수 있는 기호 오른쪽에는 계정 이름 앞에 해당 계정이 역할 계정인지를 나타내는 모자 아이콘이 표시됩니다.
- **현재 계정 이름** – 신뢰할 수 있는 기호 오른쪽에는 작업 공간에서 새 프로세스의 소유자 이름이 표시됩니다.
- **레이블 지정 창** – 작업 공간에 있는 모든 창의 레이블을 표시합니다.

신뢰할 수 있는 기호

TCB에 액세스할 때마다 신뢰할 수 있는 스트라이프 영역 왼쪽에 신뢰할 수 있는 기호가 표시됩니다.

마우스 포인터가 보안에 영향을 주지 않는 창 또는 화면 영역에 포커스되어 있는 경우 신뢰할 수 있는 기호가 표시되지 않습니다. 신뢰할 수 있는 기호는 위조하면 안 됩니다. 이 기호가 있으면 TCB와 안전하게 상호 작용하고 있는 것입니다.

주의 – 신뢰할 수 있는 스트라이프가 작업 공간에서 누락된 경우 보안 관리자에게 문의하십시오. 시스템 문제는 심각할 수 있습니다.

로그인 중이거나 화면을 잠글 경우 신뢰할 수 있는 스트라이프가 표시되지 않아야 합니다. 신뢰할 수 있는 스트라이프가 표시되면 관리자에게 즉시 문의하십시오.

창 레이블 표시기

창 레이블 표시기는 활성 창의 레이블을 표시합니다. 다중 레벨 세션에서 이 표시기는 같은 작업 공간에서 다른 레이블이 붙은 창을 식별하는 데 도움이 됩니다. 또한 이 표시기는 TCB와 상호 작용하고 있음을 보여 주기도 합니다. 예를 들어, 암호를 변경하면 신뢰할 수 있는 스트라이프에 신뢰할 수 있는 경로 표시기가 표시됩니다.

Trusted Extensions의 장치 보안

Trusted Extensions에서는 기본적으로 장치 할당 요구 사항에 의해 장치가 보호됩니다. 사용자는 장치를 할당하는 권한을 명시적으로 부여 받지 않고서는 장치를 사용할 수 없으며 할당된 장치는 다른 사용자가 사용할 수 없습니다. 특정 레이블에서 사용 중인 장치는 다른 레이블에서 사용할 수 없으며 첫 번째 레이블에서 할당을 해제한 후 두 번째 레이블에서 장치를 할당해야만 두 번째 다른 레이블에서 사용할 수 있습니다.

장치를 사용하려면 46 페이지 “Trusted Extensions에서 장치를 할당하는 방법”을 참조하십시오.

Trusted Extensions의 파일 및 응용 프로그램

Trusted Extensions의 모든 응용 프로그램에는 레이블로 표시된 민감도 수준이 있습니다. 응용 프로그램은 데이터 트랜잭션에서 **주체**에 해당합니다. 주체는 주체가 액세스하려고 하는 **객체**보다 우위에 있어야 합니다. 객체는 파일일 수 있으며 다른 프로세스가 객체일 수도 있습니다. 응용 프로그램에 대한 레이블 정보는 창 레이블 스트라이프에 표시됩니다. 이 레이블은 창이 열려 있을 때와 창이 최소화 상태일 때 표시됩니다. 응용 프로그램의 레이블은 포인터가 응용 프로그램 창에 있을 때 신뢰할 수 있는 스트라이프에도 표시됩니다.

Trusted Extensions에서 파일은 데이터 트랜잭션에서 객체에 해당합니다. 응용 프로그램 레이블이 파일 레이블보다 우위에 있는 응용 프로그램에서만 파일에 액세스할 수 있습니다. 파일은 파일과 레이블이 같은 창에서 볼 수 있습니다.

일부 응용 프로그램은 초기화 파일을 사용하여 사용자의 작업 환경을 구성합니다. 홈 디렉토리에 있는 두 개의 특수 파일이 모든 레이블에서 초기화 파일에 액세스하는 데 도움을 줍니다. 이러한 파일은 한 레이블의 응용 프로그램이 다른 레이블의 디렉토리에서 시작된 초기화 파일을 사용할 수 있도록 합니다. 이 두 개의 특수 파일은 `.copy_files`와 `.link_files` 입니다.

.copy_files 파일

`.copy_files` 파일에는 더 높은 레이블의 작업 공간으로 처음 변경할 때 복사할 파일 이름이 저장됩니다. 이 파일은 최소 레이블의 홈 디렉토리에 저장됩니다. 이 파일은 홈 디렉토리의 특정 이름의 파일에 항상 쓰는 응용 프로그램이 있을 때 유용합니다. `.copy_files` 파일을 사용하여 응용 프로그램이 모든 레이블의 파일을 업데이트하도록 지정할 수 있습니다.

.link_files 파일

.link_files 파일에는 더 높은 레이블의 작업 공간으로 처음 변경할 때 연결할 파일 이름이 저장됩니다. 이 파일은 최소 레이블의 홈 디렉토리에 저장됩니다. .link_files 파일은 특정 파일을 여러 레이블에서 사용해야 하지만 모든 레이블에서 내용이 동일해야 하는 경우에 유용합니다.

Oracle Solaris OS의 암호 보안

암호를 자주 변경하면 침입자가 불법적으로 암호를 알아낼 기회가 줄어듭니다. 따라서 암호를 자주 변경하도록 사이트의 보안 정책을 지정하는 것이 좋습니다. Oracle Solaris OS는 암호 내용에 대한 요구 사항을 설정하고 암호 재설정 요구 사항을 강제로 적용할 수 있습니다. 가능한 재설정 요구 사항은 다음과 같습니다.

- **최소 변경 기간** – 설정된 기간(일) 동안에는 아무도 암호를 변경할 수 없습니다.
- **최대 변경 기간** – 설정된 기간(일)이 지나면 암호를 변경할 것을 요청합니다.
- **최대 비활성 기간** – 암호를 변경하지 않은 경우 이 옵션에 설정된 기간이 지나면 계정을 잠급니다.
- **만료 날짜** – 특정 날짜가 되면 암호를 변경할 것을 요청합니다.

관리자가 위의 옵션 중 하나를 구현한 경우, 사용자는 마감일 이전에 암호를 변경하도록 경고하는 전자 메일 메시지를 받게 됩니다.

암호 내용에 대해 조건을 설정할 수 있습니다. Oracle Solaris OS에서 암호는 최소한 다음과 같은 조건을 충족해야 합니다.

- 암호는 최소 8자 이상이어야 합니다.
- 암호에는 최소한 두 개의 알파벳 문자와 하나 이상의 숫자 또는 특수 문자가 있어야 합니다.
- 새 암호는 이전 암호와 달라야 합니다. 이전 암호를 역순으로 사용하거나 문자를 순환해서 재사용하면 안 됩니다. 이 비교에서 대문자와 소문자는 동일한 것으로 인식됩니다.
- 새 암호에는 이전 암호와 다른 문자가 세 개 이상 있어야 합니다. 이 비교에서 대문자와 소문자는 동일한 것으로 인식됩니다.
- 암호는 추측하기 어려워야 합니다. 일반적인 단어나 고유한 이름은 사용하지 마십시오. 계정을 알아내려는 프로그램 및 개인이 목록을 보고 사용자의 암호를 추측하려고 할 수 있습니다.

Trusted Path(신뢰할 수 있는 경로) 메뉴에서 Change Password(암호 변경) 메뉴 항목을 사용하여 암호를 변경할 수 있습니다. 단계 설명은 44 페이지 “Trusted Extensions의 암호를 변경하는 방법”을 참조하십시오.

Trusted Extensions의 작업 공간 보안

Trusted Extensions에서 작업 공간 및 데스크탑 응용 프로그램은 레이블을 인식합니다. 응용 프로그램은 현재 작업 공간의 레이블에서 실행되며 응용 프로그램을 연 프로세스의 레이블에서만 정보를 표시합니다.

신뢰할 수 있는 데스크탑에 대한 보안 기능의 동작 및 위치는 다음과 같습니다.

- Trusted Path(신뢰할 수 있는 경로) 메뉴는 신뢰할 수 있는 스트라이프에서 사용할 수 있습니다.
- 패널의 작업 목록에 있는 창의 레이블 이름은 마우스를 해당 창 위에 올려 놓을 때 툴팁에 나타납니다. 마찬가지로 전환 영역에 있는 작업 공간의 레이블 이름도 툴팁에 나타납니다.
- 역할을 변경하려면 신뢰할 수 있는 스트라이프에서 계정 이름을 누르고 역할을 선택합니다.
- 특정 레이블에서 작업 공간을 추가하려면 기존 작업 공간을 선택하고 해당 레이블을 변경합니다.
- 데스크탑은 각 작업 공간에 사용자가 해당 작업 공간에서 사용 중임을 나타내는 레이블 색상이 반영되도록 구성되어 있습니다. 아래쪽 스트라이프의 패널에도 해당 레이블 색상이 표시됩니다.

용어집

Trusted GNOME 세션 관리자, 창 관리자 및 다양한 데스크탑 도구를 포함하는 레이블이 있는 그래픽 데스크탑입니다. 데스크탑은 완전히 액세스 가능합니다.

Trusted Path (신뢰할 수 있는 경로) 메뉴 전면 패널의 전환 영역 위를 마우스 버튼 3으로 누르고 있을 때 표시되는 Trusted Extensions 작업 메뉴입니다. 메뉴 옵션은 작업 공간 지향 선택 옵션, 역할 가정 선택 옵션 및 보안 관련 작업의 세 가지 범주로 구분됩니다.

감사 Oracle Solaris OS의 보안 기능입니다. 감사는 시스템의 사용자 활동 및 기타 이벤트를 캡처한 후 이 정보를 **감사 증적**이라는 파일 집합에 저장하는 프로세스입니다. 감사 중에는 사이트 보안 정책을 이행하기 위한 시스템 활동 보고서가 생성됩니다.

감사 ID (AUID) Oracle Solaris OS의 보안 기능입니다. 감사 ID는 로그인 사용자를 나타냅니다. AUID는 사용자가 역할을 할당받은 후에는 변경되지 않으므로 감사를 위해 사용자를 식별하는 데 사용됩니다. 감사 ID는 사용자가 유효 UID/GID를 획득할 때도 감사할 사용자를 나타냅니다. 사용자 ID(UID)를 참조하십시오.

객체 데이터 파일, 디렉토리, 프린터 또는 기타 장치와 같이 데이터를 포함하거나 수신하는 수동 엔티티입니다. 객체는 주체에 의해 작동합니다. 프로세스로 신호를 보낼 때와 같이 프로세스가 객체인 경우도 있을 수 있습니다.

게이트웨이 둘 이상의 네트워크 인터페이스가 있는 호스트입니다. 이러한 호스트는 둘 이상의 네트워크를 연결하는 데 사용할 수 있습니다. 게이트웨이가 Trusted Extensions 호스트이면 특정 레이블로 트래픽을 제한할 수 있습니다.

계정 레이블 범위 Trusted Extensions로 구성된 시스템에서 작업을 수행하기 위해 보안 관리자가 사용자 또는 역할에 대해 지정한 레이블 집합입니다. 레이블 범위는 사용자 클리어런스에 따라 상한이, 사용자의 최소 레이블에 따라 하한이 정의됩니다. 이 집합은 잘 구성된 레이블로 제한됩니다.

관리 레이블 관리 파일에만 사용되는 특수 레이블에는 `ADMIN_LOW`와 `ADMIN_HIGH`가 있습니다. `ADMIN_LOW`는 구획이 없는 시스템의 최하위 레이블입니다. 이 레이블은 시스템의 모든 레이블에서 완전히 지배됩니다. `ADMIN_LOW`의 정보는 모든 사용자가 읽을 수 있지만 역할 레이블에서 작업하는 **역할**의 사용자만 쓸 수 있습니다. `ADMIN_HIGH`는 모든 구획이 있는 시스템의 최상위 레이블입니다. 이 레이블은 시스템의 모든 레이블을 완전히 지배합니다. `ADMIN_HIGH`에서 작동하는 역할 내의 사용자만 `ADMIN_HIGH`의 정보를 읽을 수 있습니다. 관리 레이블은 역할 및 시스템에 대한 레이블 또는 클리어런스로 사용됩니다. 지배 레이블을 참조하십시오.

구획 레이블 구성 요소와 함께 사용하여 분류 또는 클리어런스을 형성하는 레이블의 비계층적 구성 요소입니다. 구획은 엔지니어링 부서 또는 여러 전문 분야에 걸친 프로젝트 팀과 같이 잠재적으로 이 정보에 액세스해야 하는 사용자 그룹을 나타냅니다.

구획 모드 워크스테이션 (CMW) **Security Requirements for System High and Compartmented Mode Workstations**, DIA 문서 번호 DDS-2600-5502-87에 제기된 신뢰 워크스테이션에 대한 정부의 요구 사항을 충족하는 연산 시스템입니다. 특히, 신뢰되는 UNIX 워크스테이션에 대한 X Window 시스템 기반 운영체제를 정의합니다.

권한 부여 Oracle Solaris OS의 보안 기능입니다. 권한 부여는 보안 정책으로 금지된 작업을 수행할 수 있는 권한을 사용자에게 부여합니다. 보안 관리자는 권한 프로필에 대한 권한 부여를 지정합니다. 그러면 권한 프로필이 사용자 또는 역할 계정에 할당됩니다. 일부 명령 및 동작은 사용자에게 필요한 권한이 부여되어야만 그 기능을 제대로 발휘할 수 있습니다. 특권을 참조하십시오.

권한 프로필 Oracle Solaris OS의 보안 기능입니다. 사이트의 보안 관리자가 보안 속성을 사용하여 명령을 묶을 수 있게 해주는 권한 프로필입니다. 사용자 권한 부여 및 권한과 같은 속성을 통해 명령을 성공할 수 있습니다. 권한 프로필은 일반적으로 관련된 작업을 포함합니다. 프로필은 사용자 및 역할에 지정할 수 있습니다.

그룹 ID (GID) Oracle Solaris OS의 보안 기능입니다. GID는 공통 액세스 권한이 있는 사용자 그룹을 식별하는 정수입니다. 임의의 액세스 제어(DAC)를 참조하십시오.

네트워크 인정 범위 네트워크에서 통신이 허용된 Trusted Extensions 호스트 내의 레이블 집합입니다. 이 집합은 네 개의 고유 레이블 목록일 수 있습니다.

다운그레이드된 레이블 레이블의 이전 값보다 우위가 아닌 값으로 변경된 객체의 레이블을 말합니다.

단일 레벨 구성 단일 레이블에서만 작업하도록 구성된 사용자 계정입니다. 단일 레벨 구성이라고도 합니다.

레이블 민감도 레이블이라고도 합니다. 레이블은 엔티티의 보안 수준을 나타냅니다. 엔티티란 파일, 디렉토리, 프로세스, 장치 또는 네트워크 인터페이스를 말합니다. 엔티티의 레이블은 특정 트랜잭션에서 액세스를 허용할지 여부를 결정하는 데 사용됩니다. 레이블에는 보안 계층 레벨을 나타내는 분류와 지정된 분류에서 엔티티에 액세스할 수 있는 사용자를 정의하기 위한 0개 이상의 구획이라는 두 가지 구성 요소가 포함됩니다. 레이블 인코딩 파일을 참조하십시오.

레이블 구축기 Trusted Extensions의 신뢰할 수 있는 응용 프로그램입니다. 이 GUI를 사용하여 세션 클리어런스나 세션 레이블을 선택할 수 있습니다. 클리어런스 또는 레이블은 계정 레이블 범위가 사용자에게 할당한 보안 관리자 내에 있어야 합니다.

레이블 범위 클리어런스 또는 최대 레이블에 따라 위쪽 끝에 바인딩되고, 최소 레이블에 따라서는 아래쪽 끝에 바인딩되며 잘 구성된 레이블로 구성되는 모든 레이블 집합입니다. 레이블 범위는 필수 액세스 제어(MAC)를 강제 시행하는 데 사용됩니다. 레이블 인코딩 파일, 계정 레이블 범위, 인정 범위, 네트워크 인정 범위, 세션 범위, 시스템 인정 범위 및 사용자 인정 범위를 참조하십시오.

레이블 보기 관리 레이블을 표시하거나 관리 레이블에 대해 미분류된 자리 표시자를 대신하는 보안 기능입니다. 예를 들어 보안 정책에 따라 `ADMIN_HIGH` 및 `ADMIN_LOW` 레이블을 노출하지 못하도록 금지할 경우 `RESTRICTED` 및 `PUBLIC` 레이블을 대신 사용할 수 있습니다.

레이블 인코딩 파일 보안 관리자가 관리하는 파일입니다. 인코딩 파일에는 모든 유효한 클리어런스 및 레이블에 대한 정의가 포함됩니다. 또한 이 파일은 시스템 인정 범위, 사용자 인정 범위 및 사이트 인쇄 출력에 대한 보안 정보를 정의합니다.

레이블이 있는 작업 공간 레이블과 연관된 작업 공간입니다. 레이블이 있는 작업 공간은 작업 공간의 레이블을 사용하여 작업 공간에서 실행되는 모든 활동에 레이블을 지정합니다. 사용자가 다른 레이블의 작업 공간으로 창을 이동하면 이동된 창은 원래 레이블을 계속 사용합니다. 신뢰할 수 있는 데스크탑의 모든 작업 공간은 레이블로 지정됩니다. 두 개의 작업 공간은 동일한 레이블과 연관될 수 있습니다.

민감도 레이블 레이블을 참조하십시오.

보안 관리자 Trusted Extensions로 구성된 시스템에서 보안 정책의 정의 및 강제 시행을 담당하는 사용자에게 할당된 역할입니다. 보안 관리자는 시스템 인정 범위의 모든 레이블에서 작업할 수 있으며, 잠재적으로 사이트의 모든 정보에 액세스할 수 있습니다. 보안 관리자는 모든 사용자 및 장비에 대한 보안 속성을 구성합니다. 레이블 인코딩 파일을 참조하십시오.

보안 속성 Oracle Solaris OS의 보안 기능입니다. 프로세스, 영역, 사용자 또는 보안 관련 장치와 같은 엔티티 특성입니다. 보안 속성에는 사용자 ID(UID) 및 그룹 ID(GID)와 같은 식별 값이 포함됩니다. Trusted Extensions와 관련된 속성에는 레이블 및 레이블 범위가 포함됩니다. 특정 보안 속성만 특정 유형의 엔티티에 적용된다는 것을 유의하십시오.

보안 정책 정보에 액세스할 수 있는 방법과 액세스하는 사용자를 정의하는 DAC, MAC 및 레이블 규칙 집합입니다. 고객 사이트에서 처리된 정보의 민감도를 정의하는 규칙 집합입니다. 정책에는 허용되지 않은 액세스로부터 정보를 보호하는 데 사용되는 방법이 포함됩니다.

분류 클리어런스 또는 레이블의 구성 요소입니다. 클리어런스는 `TOP SECRET` 또는 `UNCLASSIFIED`와 같은 보안의 계층 수준을 나타냅니다.

분리 레이블 지배 레이블을 참조하십시오.

사용 권한 어떤 사용자가 파일 또는 디렉토리(폴더)를 읽고 쓰거나 실행할 수 있도록 허용되었는지를 나타내는 일련의 코드. 사용자는 소유자, 그룹(소유자의 그룹) 및 기타(모든 사람)로 분류됩니다. 읽기 사용 권한(*r*로 표시)을 통해 사용자는 파일의 내용을 읽을 수 있으며, 디렉토리일 때는 폴더 내의 파일을 나열할 수 있습니다. 쓰기 사용 권한(*w*로 표시)을 통해 사용자는 파일을 변경할 수 있으며, 디렉토리일 때는 폴더에 파일을 추가하거나 삭제할 수 있습니다. 실행 사용 권한(*e*로 표시)을 통해 사용자는 파일이 실행 가능할 경우 파일을 실행할 수 있습니다. 파일이 디렉토리일 때 실행 사용 권한이 있으면 디렉토리의 파일을 읽거나 검색할 수 있습니다. UNIX 사용 권한 또는 사용 권한 비트라고도 합니다.

사용자 ID (UID) Oracle Solaris OS의 보안 기능입니다. UID는 임의의 액세스 제어(DAC), 필수 액세스 제어(MAC) 및 감사를 위해 사용자를 식별합니다. 액세스 권한을 참조하십시오.

사용자 인정 범위 보안 관리자가 특정 사이트의 사용자에게 할당할 수 있는 최대 레이블 집합입니다. 사용자 인정 범위에서 관리 레이블과 관리자만 사용할 수 있는 레이블 조합은 제외됩니다. 사용자 인정 범위는 레이블 인코딩 파일에 정의되어 있습니다.

사용자 클리어런스 보안 관리자가 할당한 클리어런스를 말합니다. 사용자 클리어런스는 사용자 계정 레이블 범위의 상한을 정의합니다. 사용자 클리어런스는 사용자 작업이 허용되는 최상위 레이블을 결정합니다. 클리어런스 및 세션 클리어런스를 참조하십시오.

선택 관리자 Trusted Extensions의 신뢰할 수 있는 응용 프로그램입니다. 이 GUI는 권한이 부여된 사용자가 정보를 업그레이드하거나 다운그레이드하려고 시도할 때 나타납니다.

세션 Trusted Extensions 호스트에 로그인하고 호스트에서 로그아웃하는 사이의 시간입니다. 신뢰할 수 있는 스트라이프는 모든 Trusted Extensions 세션에 표시되며 해당 사용자가 위조된 시스템에서 허위로 제공된 사용자가 아님을 확인합니다.

세션 범위 Trusted Extensions 세션 중에 사용자가 사용할 수 있는 레이블 집합입니다. 세션 범위는 사용자의 세션 클리어런스에 따라 상한이, 최소 레이블에 따라 하한이 정의됩니다.

세션 클리어런스 로그인할 때 Trusted Extensions 세션에 대해 레이블 상한을 정의하는 클리어런스 집합입니다. 사용자가 세션 클리어런스를 설정하도록 허가되면 사용자의 계정 레이블 범위 내의 어떤 값도 지정할 수 있습니다. 사용자 계정이 강제 시행되는 단일 레벨 세션용으로 구성되면 세션 클리어런스는 보안 관리자가 지정한 기본값으로 설정됩니다. 클리어런스를 참조하십시오.

속임수 시스템의 정보에 불법적으로 액세스하기 위해 소프트웨어 프로그램을 위조하는 것을 말합니다.

시스템 관리자 Oracle Solaris OS의 보안 기능입니다. 시스템 관리자 역할은 사용자 계정의 비보안 관련 부분의 설정과 같은 표준 시스템 관리 작업을 수행하는 사용자에게 할당될 수 있습니다. 보안 관리자를 참조하십시오.

시스템 인정 범위 사이트의 모든 유효 레이블 집합입니다. 여기에는 사이트의 보안 관리자 및 시스템 관리자가 사용할 수 있는 관리 레이블이 포함됩니다. 시스템 인정 범위는 레이블 인코딩 파일에 정의되어 있습니다.

신뢰할 수 있는 경로 신뢰할 수 있는 컴퓨팅 기반(TCB)과의 상호 작용이 허가된 작업 및 명령에 액세스하기 위한 메커니즘을 참조하십시오. 또한 Trusted Path(신뢰할 수 있는 경로) 메뉴, 신뢰할 수 있는 기호 및 신뢰할 수 있는 스트라이프를 참조하십시오.

신뢰할 수 있는 기능 관리 전통적인 UNIX 시스템에서 시스템 관리와 관련된 모든 활동, 분산 시스템의 보안 및 해당 데이터를 관리하는 데 필요한 모든 관리 활동을 말합니다.

신뢰할 수 있는 기호 신뢰할 수 있는 스트라이프 영역 왼쪽에 나타나는 기호입니다. 이 기호는 사용자가 신뢰할 수 있는 컴퓨팅 기반(TCB)에 액세스할 때마다 표시됩니다.

신뢰할 수 있는 스트라이프 화면의 예약 영역에 표시되는 화면 크기의 직사각형 그래픽입니다. 신뢰할 수 있는 스트라이프는 Trusted Extensions 모든 세션에 표시되어 Trusted Extensions 세션이 유효한 세션인지를 확인합니다. 신뢰할 수 있는 스트라이프에는 (1) 신뢰할 수 있는 컴퓨팅 기반(TCB)과의 상호 작용을 나타내기 위한 필수 신뢰할 수 있는 기호 및 (2) 현재 창 또는 작업 공간의 레이블을 나타내기 위한 레이블이라는 두 가지 구성 요소가 포함됩니다.

신뢰할 수 있는 응용 프로그램 특권이 하나 이상 부여된 응용 프로그램입니다.

신뢰할 수 있는 컴퓨팅 기반 (TCB) 보안에 영향을 주는 Trusted Extensions로 구성된 시스템의 부분입니다. TCB에는 소프트웨어, 하드웨어, 펌웨어, 설명서 및 관리 절차가 포함됩니다. 보안 관련 파일에 액세스할 수 있는 유틸리티 프로그램 및 응용 프로그램은 트러스트 컴퓨팅 기반의 모든 부분입니다.

아래로 읽기 주체가 지배하는 객체의 레이블을 볼 수 있는 주체의 기능입니다. 보안 정책은 일반적으로 아래로 읽기를 허용합니다. 예를 들어 `Secret`에서 실행하는 텍스트 편집기 프로그램에서는 `Unclassified` 데이터를 읽을 수 있습니다. 필수 액세스 제어(MAC)를 참조하십시오.

액세스 권한 대부분의 컴퓨터 시스템의 보안 기능입니다. 액세스 권한은 사용자에게 파일이나 디렉토리 이름에 대한 읽기, 쓰기, 실행 또는 보기 권한을 부여합니다. 임의의 액세스 제어(DAC) 및 필수 액세스 제어(MAC)를 참조하십시오.

액세스 제어 목록 (ACL) Oracle Solaris OS의 보안 기능입니다. ACL은 특정 사용자 및 특정 그룹에 적용되는 사용 권한 지정(ACL 항목) 목록을 사용하도록 임의의 액세스 제어(DAC)를 확장한 것입니다. ACL을 사용하면 표준 UNIX 사용 권한보다 좀 더 세부적으로 제어할 수 있습니다.

업그레이드된 레이블 레이블의 이전 값보다 우위에 있는 값으로 변경된 객체의 레이블입니다.

역할 Oracle Solaris OS의 보안 기능입니다. 역할은 특정 작업을 수행하는 데 필요한 보안 속성을 사용하여 해당 역할을 가정하는 사용자에게 특정 응용 프로그램에 대한 액세스 권한을 부여하는 특수 계정입니다.

완전한 지배 지배 레이블을 참조하십시오.

운영자 시스템 백업을 담당하는 사용자에게 할당할 수 있는 역할을 말합니다.

위장 채널 일반적으로 데이터 통신에 사용되지 않는 통신 채널입니다. 프로세스에서는 위장 채널을 사용하여 보안 정책 의도를 위반하는 방식으로 간접적으로 정보를 전송할 수 있습니다.

유효 UID/GID Oracle Solaris OS의 보안 기능입니다. 유효 ID는 특정 프로그램이나 프로그램의 옵션을 실행해야 할 때 실제 ID를 대체합니다. 보안 관리자는 특정 사용자가 명령이나 작업을 실행해야 할 때, 특히 명령을 루트로 실행해야 할 때 권한 프로필의 명령이나 작업에 유효 UID를 할당합니다. 유효 그룹 ID도 같은 방식으로 사용됩니다. 일반적인 UNIX 시스템을 사용할 때처럼 `setuid` 명령을 사용하면 특권이 필요하기 때문에 제대로 작동하지 않을 수 있습니다.

인정 범위 사용자 또는 자원 클래스에 대해 승인된 레이블 집합입니다. 시스템 인정 범위, 사용자 인정 범위, 레이블 인코딩 파일 및 네트워크 인정 범위를 참조하십시오.

일반 사용자 시스템의 표준 보안 정책에 따른 예외를 허용하는 특별한 권한이 없는 사용자입니다. 일반적으로 일반 사용자는 관리 역할을 가질 수 없습니다.

임의의 액세스 제어 (DAC) 파일 또는 디렉토리 소유자가 다른 사용자에게 액세스를 허용하거나 거부할 수 있도록 하는 액세스 제어 메커니즘입니다. 소유자는 소유자, 소유자가 속한 사용자 그룹 및 지정되지 않은 다른 모든 사용자를 나타내는 기타 범주에 읽기, 쓰기 및 실행 사용 권한을 할당합니다. 또한 소유자는 액세스 제어 목록(ACL)을 지정할 수도 있습니다. ACL을 사용하면 소유자가 추가 사용자 및 추가 그룹에 특수하게 사용 권한을 할당할 수 있습니다. 필수 액세스 제어(MAC)와는 대조됩니다.

작업 공간 레이블이 있는 작업 공간을 참조하십시오.

잘 구성된 레이블 범위에 포함될 수 있는 레이블을 말합니다. 이 레이블은 레이블 인코딩 파일의 모든 적용 가능한 규칙에 따라 허용됩니다.

장치 할당 가능한 장치를 참조하십시오.

장치 관리자 Trusted Extensions의 신뢰할 수 있는 응용 프로그램입니다. 이 GUI는 장치를 구성하고 장치를 할당 및 할당 해제하는 데 사용됩니다. 장치 구성에는 장치에 권한 부여 요구 사항 추가가 포함됩니다.

장치 할당 Oracle Solaris OS의 보안 기능입니다. 장치 할당이란 장치를 할당한 사용자 이외의 사용자가 액세스할 수 없도록 할당 가능한 장치의 정보를 보호하는 메커니즘입니다. 장치가 할당 해제되면 장치 정리 스크립트가 실행되어 다른 사용자가 장치에 액세스하기 전에 장치의 정보를 정리합니다. Trusted Extensions에서 장치 할당은 장치 관리자에서 처리됩니다.

주체 일반적으로 사용자 대신 실행하는 프로세스 또는 역할을 나타내는 활성 엔티티입니다. 주체는 객체 간의 정보 흐름을 일으키고 시스템 상태를 변경합니다.

지배 레이블 두 레이블을 비교할 때 해당 분류 구성 요소가 두 번째 레이블의 분류보다 높거나 같고 해당 구획 구성 요소가 두 번째 레이블의 모든 구획 구성 요소를 포함하는 레이블입니다. 구성 요소가 같으면 레이블이 서로 지배한다고 말하며 **동등**하다고 합니다. 한 레이블이 다른 레이블보다 우위에 있고 레이블들이 서로 동일하지 않을 경우 첫 번째 레이블이 다른 레이블을 **완전히 지배**한다고 합니다. 두 레이블이 동등하지 않고 지배 레이블이 없는 경우 두 레이블은 **분리**되었다고 합니다.

최소 레이블 사용자가 작업할 수 있는 레이블 집합의 하한으로서 사용자에게 할당된 레이블입니다. 사용자가 처음 Trusted Extensions 세션을 시작하면 최소 레이블이 사용자의 기본 레이블입니다. 로그인 시 사용자는 초기 레이블에 대해 다른 레이블을 선택할 수 있습니다.

또한 최하위 레이블은 관리자가 아닌 모든 사용자에게 허용됩니다. 최소 레이블은 보안 관리자가 할당하고 사용자 인정 범위의 하한을 정의합니다.

최소한의 특권 최소한의 특권 원칙을 참조하십시오.

최소한의 특권 원칙 작업을 수행하는 데 필요한 기능만으로 사용자를 제한하는 보안 원칙입니다. 이 원칙은 필요 시 기반에 따라 프로그램에 대한 권한을 부여하여 Oracle Solaris OS에 적용됩니다. 특권은 특정 용도로 필요할 때만 사용할 수 있습니다.

클리어런스 레이블의 상한을 정의하는 레이블 범위입니다. 클리어런스에는 분류 및 0개 이상의 구획이라는 두 가지 구성 요소가 포함됩니다. 클리어런스는 잘 구성된 레이블일 필요가 없습니다. 클리어런스는 반드시 실제 레이블이라기보다 이론적인 경계를 정의합니다. 사용자 클리어런스, 세션 클리어런스 및 레이블 인코딩 파일을 참조하십시오.

특권 Oracle Solaris OS의 보안 기능입니다. 특권은 보안 관리자가 프로그램에 부여하는 사용 권한입니다. 보안 정책의 일부 측면을 대체하는 데 특권이 필요할 수도 있습니다. 권한 부여를 참조하십시오.

특권 프로세스 Oracle Solaris OS의 보안 기능입니다. 특권 프로세스는 해당 권한이 부여된 상태로 실행됩니다.

평가할 수 있는 구성 정부의 보안 요구 사항 표준을 만족하는 컴퓨터 시스템. 확장된 구성을 참조하십시오.

폴백 메커니즘 `tnrhtp` 데이터베이스의 IP 주소를 지정하는 빠른 방법입니다. IPv4 주소의 경우 폴백 메커니즘에서 `0`을 서브넷에 대한 와일드카드로 인식합니다.

프로세스 실행 중인 프로그램입니다. Trusted Extensions 프로세스에는 사용자 ID(UID), 그룹 ID(GID), 사용자의 감사 ID(AUID) 및 권한과 같은 Oracle Solaris 보안 속성이 포함됩니다. Trusted Extensions는 모든 프로세스에 레이블을 추가합니다.

프로필 권한 프로필을 참조하십시오.

프로필 쉘 Oracle Solaris OS의 보안 기능입니다. 사용자가 보안 속성을 사용하여 프로그램을 실행할 수 있도록 허용하는 Bourne 쉘 버전입니다.

필수 액세스 제어 (MAC) 클리어런스 및 레이블을 사용하여 보안 정책을 강제 적용하는 시스템 적용 액세스 제어 메커니즘입니다. 클리어런스 또는 레이블은 보안 레벨입니다. MAC는 사용자가 실행하는 프로그램을 사용자가 세션에서 작업하도록 선택한 보안 수준과 연결합니다. 그러면 MAC는 동일하거나 더 낮은 수준에서만 정보, 프로그램 및 장치에 액세스하도록 허용합니다. 또한 MAC는 사용자가 낮은 레벨에서 파일에 쓰지 못하도록 합니다. 특별한 권한 부여 또는 권한 없이는 MAC를 덮어쓸 수 없습니다. 임의의 액세스 제어(DAC)와는 대조됩니다.

할당 가능한 장치 Oracle Solaris OS의 보안 기능입니다. 할당 가능한 장치는 한 번에 한 명의 사용자만 사용할 수 있으며 시스템에서 데이터를 가져오거나 내보낼 수 있습니다. 보안 관리자는 어떤 사용자가 어떤 할당 가능한 장치에 액세스할 수 있는지 결정합니다. 할당 가능 장치에는 테이프 드라이브, 플로피 드라이브, 오디오 장치 및 CD-ROM 장치가 있습니다 장치 할당을 참조하십시오.

할당 해제된 장치 Oracle Solaris OS의 보안 기능입니다. 할당 해제된 장치란 사용자에게 배타적으로 더 이상 할당되지 않는 장치를 말합니다. 장치 할당을 참조하십시오.

호스트 네트워크에 연결된 컴퓨터입니다.

호스트 유형 호스트를 분류한 것입니다. 이 분류 방식은 네트워크 통신에 사용됩니다. 호스트 유형의 정의는 `tnrhtp` 데이터베이스에 저장됩니다. 호스트 유형은 네트워크의 다른 호스트와 통신할 때 CIPSO 네트워크 프로토콜을 사용할지 여부를 결정합니다. **네트워크 프로토콜**은 통신 정보의 패키징에 대한 규칙을 나타냅니다.

호스트 템플리트 `tnrhtp` 데이터베이스에서 Trusted Extensions 네트워크에 액세스할 수 있는 호스트 클래스의 보안 속성을 정의하는 레코드입니다.

확장된 구성 수정된 부분 때문에 보안 정책이 위반되었으므로 더 이상 평가할 수 있는 구성에 속하지 않는 컴퓨터 시스템을 말합니다.

색인

로

루

만

문

민

변

보