Security Policies
Confidentiality Policies

Kresten Jacobsen

Intro to System Security

Goals	**C-I-A**	**Threats**
Prevention	Confidentiality	Snooping
Detection	Integrity	Modification
Recovery	Availability	Spoofing
		Repudiation of Origin
		Denial of Receipt
		Delay

Security Policies

Requirements

- Common understanding (implicit / explicit)

- Trust (in people and computers)
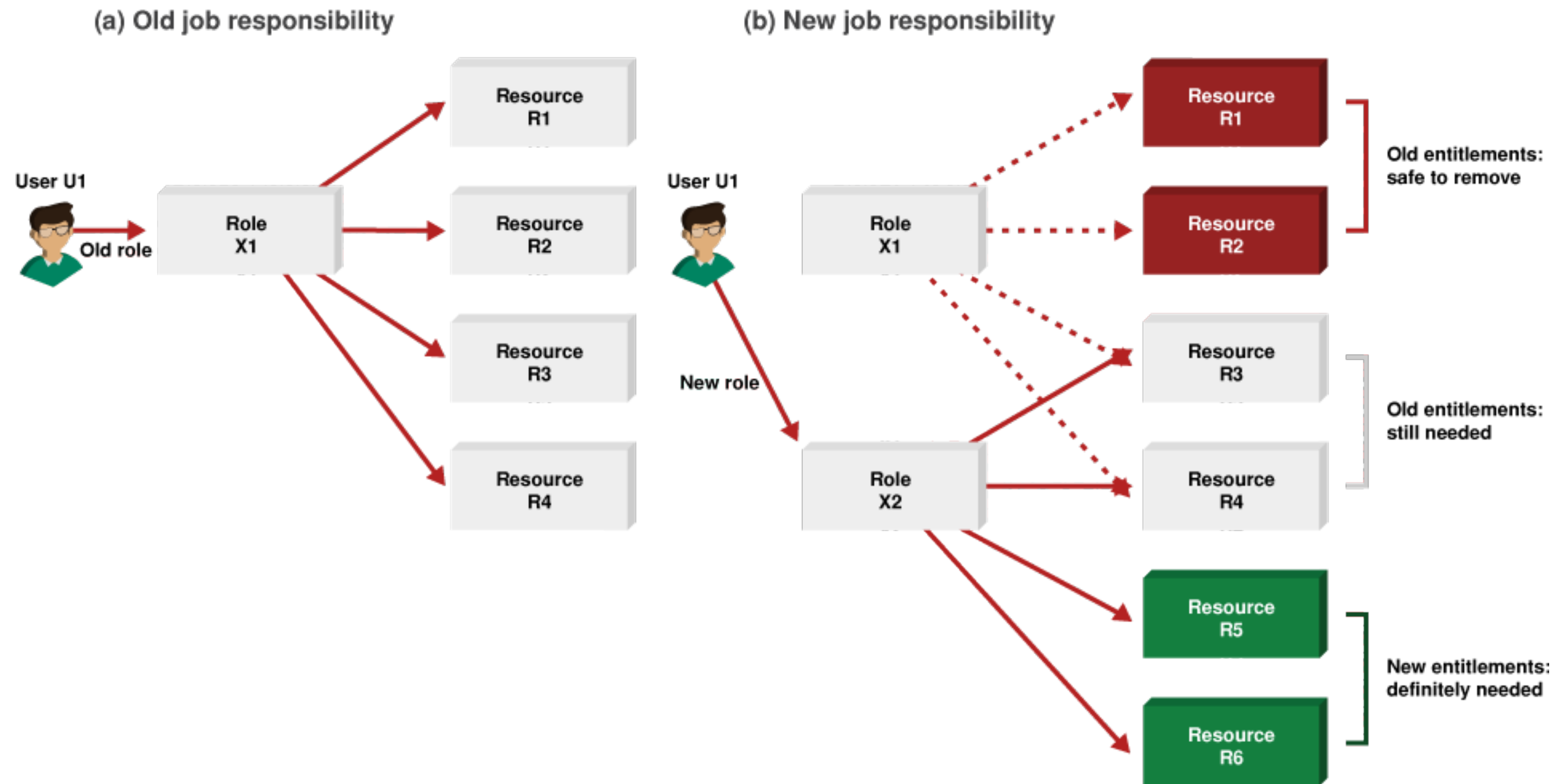
- Assumption (that policies are enforced)

Policy types

- Confidentiality

- Integrity Policy

- Availability Policy

Confidentiality Policies

- Discretionary Access Control (DAC)

- Mandatory Access Control (MAC)

- Role-Based Access Control (RBAC)

- Bell-LaPadula

Role-Based Access Control (RBAC)

(a) Old job responsibility

(b) New job responsibility

User U1 — Old role → Role X1 → Resource R1, Resource R2, Resource R3, Resource R4

User U1 → Role X1 (New role) → Role X2; Resource R1, Resource R2 (Old entitlements: safe to remove); Resource R3, Resource R4 (Old entitlements: still needed); Resource R5, Resource R6 (New entitlements: definitely needed)

Confidentiality Policies - Bell-LaPadula

- Policy to secure classification of documents (data)

"Read down; no read up.
Write up; no write down."

No read up

Top Secret

Secret

Confidential

Unclassified

No write down

Common understanding

Trust (in people and computers)

Assumption (that policies are enforced)

Policies

"Read down; no read up."

"Write up; no write down"

Bell-LaPadula
(Confidentiality)

Security Policies /
Confidentiality Policies

Discretionary Access Control
(Security)

Users can set permissions

Eg. Unix file system

Mandatory Access Control
(Security)

System controls permissions

Eg. SELinux

Role-based Access Control
(Security)

Permissions defined by roles

Eg. MS Advanced Directory