Algorithm for securing a system using RWFM / Access rules in RWFM

Input:

```
S  // set of subjects in the system
O // set of objects in the system
$\lambda: S \cup O \rightarrow L$ // labelling function that returns the current label of an entity
$A: L \rightarrow S$ // function that returns the first (administration) component of a label
$R: L \rightarrow 2^S$ // function that returns the second (readers) component of a label
$W: L \rightarrow 2^S$ // function that returns the third (writers) component of a label
```

Access rule for *read*: subject $s \in S$ requests read access to object $o \in O$

```
if ($s \in R(\lambda(o))$) then
    $a = A(\lambda(s))$
    $r = R(\lambda(s)) \cap R(\lambda(o))$
    $w = W(\lambda(s)) \cup W(\lambda(o))$
    $\lambda(s) = (a,r,w)$
    ALLOW
else
    DENY
```

Access rule for *write*: subject $s \in S$ requests write access to object $o \in O$

```
if ($s \in W(\lambda(o)) \wedge R(\lambda(s)) \supseteq R(\lambda(o)) \wedge W(\lambda(s)) \subseteq W(\lambda(o))$) then
    ALLOW
else
    DENY
```

Access rule for *create*: subject $s \in S$ requests creation of an object

```
new object o
$O = O \cup \{o\}$
$a = s$
$r = R(\lambda(s))$
$w = W(\lambda(s)) \cup \{s\}$
$\lambda(o) = (a,r,w)$
```

Access rule for *downgrade*: subject $s \in S$ requests to downgrade object $o \in O$ to (a,r,w)

```
if $(a=A(\lambda(s))=A(\lambda(o)) \wedge w=W(\lambda(s))=W(\lambda(o)) \wedge R(\lambda(s))=R(\lambda(o)) \wedge s \in R(\lambda(o)) \wedge$
    $(W(\lambda(o))=\{s\} \vee (r \supseteq R(\lambda(o)) \wedge r-R(\lambda(o)) \subseteq W(\lambda(o)))))$ then
        $\lambda(o) = (a,r,w)$
        ALLOW
else
        DENY
```

Access rule for *relabel*: subject $s \in S$ requests to relabel object $o \in O$ with (a,r,w)

```
if $(a=A(\lambda(s))=A(\lambda(o)) \wedge W(\lambda(s)) \supseteq W(\lambda(o)) \wedge R(\lambda(s)) \subseteq R(\lambda(o)) \wedge s \in R(\lambda(o)) \wedge$
    $w=W(\lambda(s)) \cup \{s\} \wedge r \subseteq R(\lambda(s)))$ then
        $\lambda(o) = (a,r,w)$
        ALLOW
else
        DENY
```