A Mechanism for Risk Adaptive Access Control (RAdAC)

Machon Gregory
14 March 2007

National Information Assurance Research Laboratory (NIARL)

Motivation

- Need for new access control model, Risk Adaptive Access Controls
- Commonly deployed systems are incapable of supporting a policy with ability to change
- Technology exists with the ability to create a system capable of providing Risk Adaptive Access Controls

Outline

- Background
- Problem
- Solution
- Implementation
- Current Status
- Future Work

Background

- Risk Adaptive Access Control (RAdAC)
  - Global Information Grid
  - “Need to Know” ➔ “Need to Share”
  - Flexible (escalation and revoke privileges)
  - Access decisions based on changing risk
  - Risk is defined by numerous factors

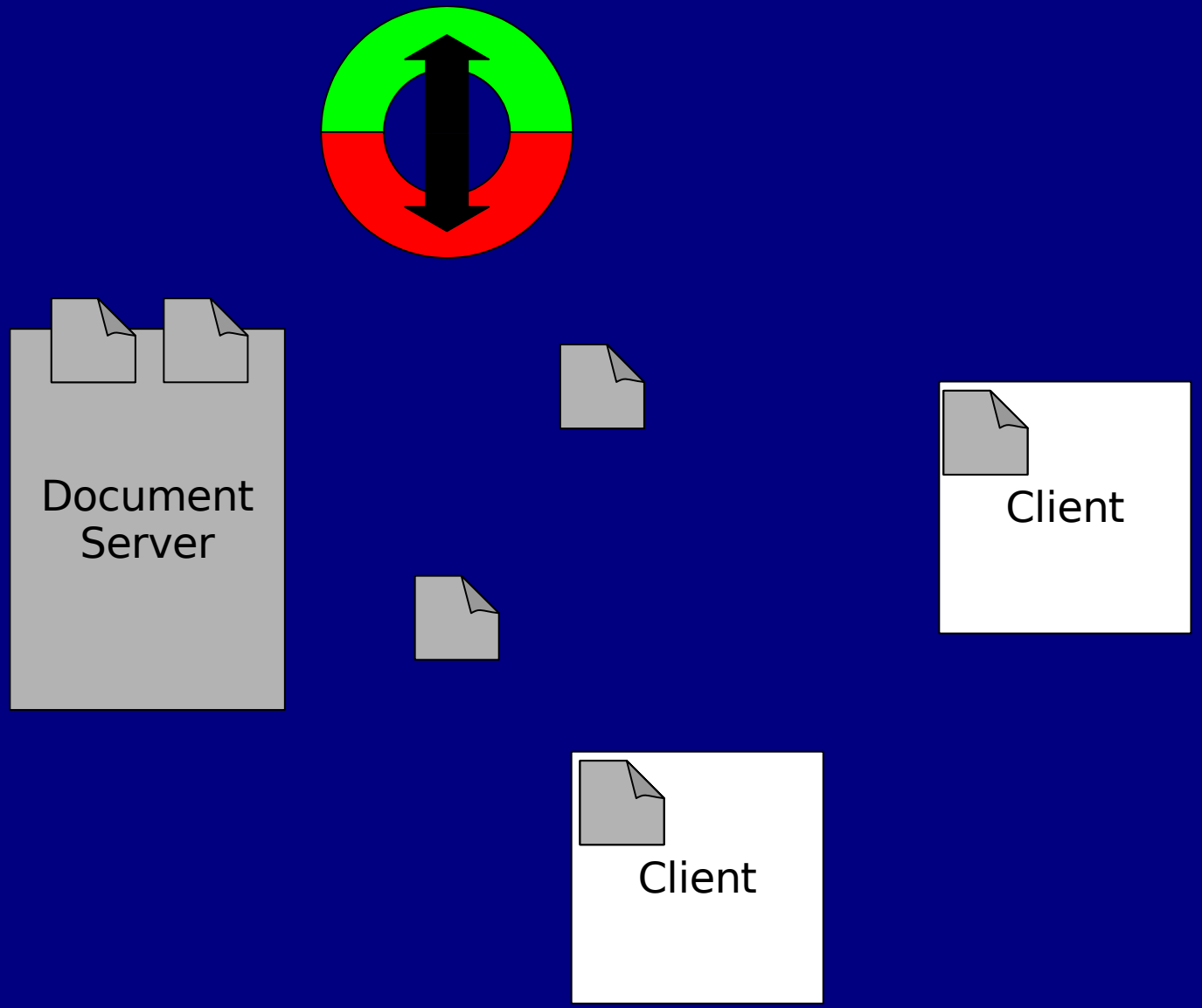
Problem

- What I want to do
  - Selectively Share Information
  - Maintain Originator Control
  - Flexible Access Controls
- Why I can't do it now
  - Trusted Computer
  - Access Control Limitation
  - State of the Remote System

Scenario

- Document Server/Document Viewer
- Protection of documents on remote machines
- Provide access controls over network objects
- Escalate and revoke privileges based on a risk knob

Scenario



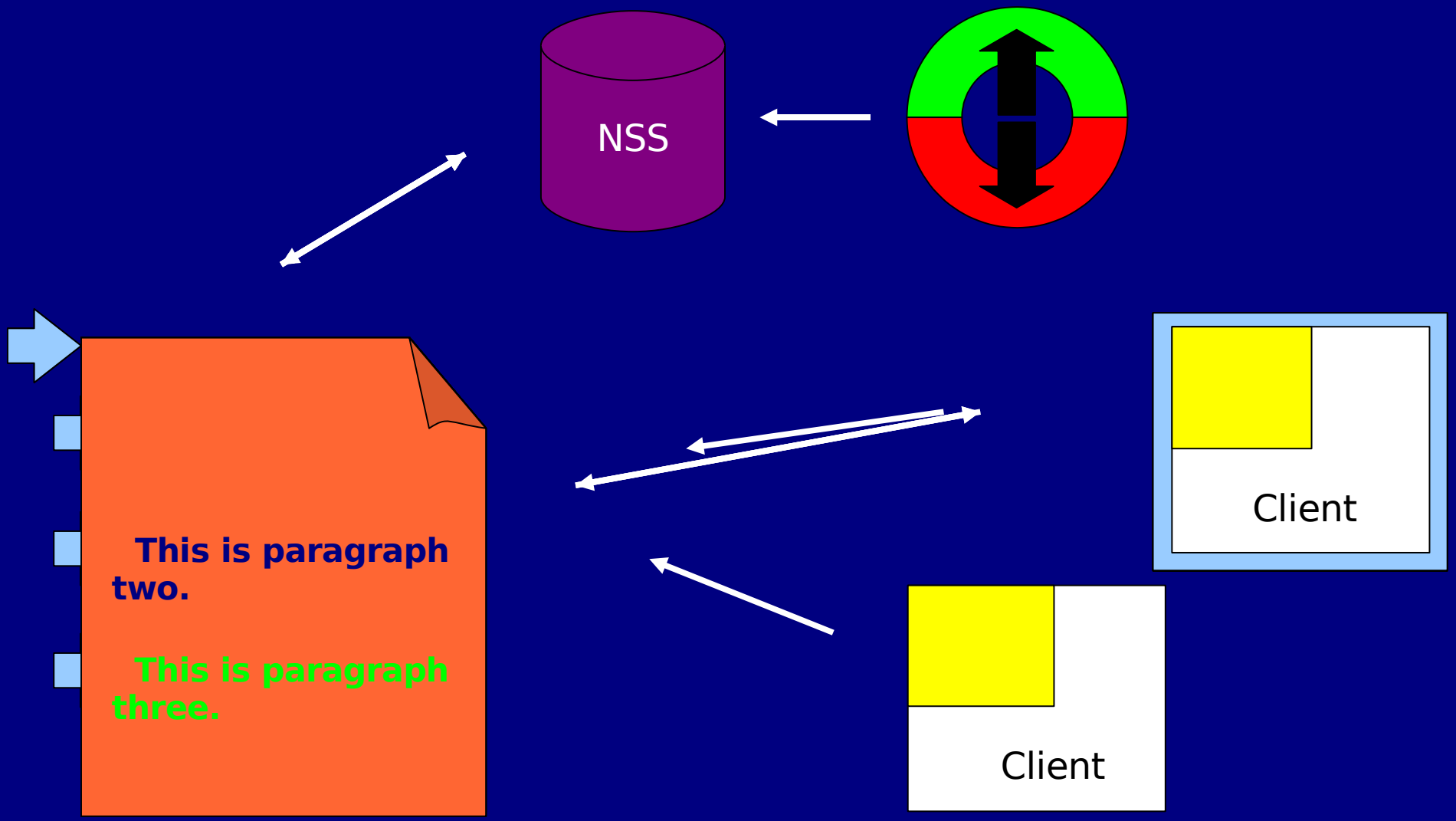
Solution

- Applications of the Flask Security Architecture
  - Client/Server (SELinux)
  - Policy over Network Object
- Least Privilege Environment
  - Prevents Release of Information
  - Provides a Level of Assurance
- IPSec Labeled Security Associations

Implementation

- User-space Security Server
- Document Server and Viewer
- IPSec with labeled security associations (SA)
- Translation Mechanism
- Mandatory Access Control Operating System
- Local and network policy

Implementation



Current Status

- Limited functionality application
- 3 static policies representing risk
- Policies for the system components

Future Work

- More robust application such as a Virtual Machine, Word Processor, or Streaming Media Server
- Incorporation of a more secure windowing environment
- Study the applicability of RAdAC concepts to real world applications

Questions?

Machon Gregory
mbgrego@tycho.nsa.gov