

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control

Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Rewriting-Based Access Control Policies

Anderson Santana de Oliveira ¹

¹LORIA & INRIA

September, 2006

Outline

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- 1 Introduction
 - Access Control
 - Term Rewriting
- 2 Motivating Example
- 3 The Policy Environment
- 4 Rewriting Based Policies
- 5 Properties of Security Policies
- 6 Conclusions and Future Work

Outline

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- 1 Introduction
 - Access Control
 - Term Rewriting
- 2 Motivating Example
- 3 The Policy Environment
- 4 Rewriting Based Policies
- 5 Properties of Security Policies
- 6 Conclusions and Future Work

Outline

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- 1 Introduction
 - Access Control
 - Term Rewriting
- 2 Motivating Example
- 3 The Policy Environment
- 4 Rewriting Based Policies
- 5 Properties of Security Policies
- 6 Conclusions and Future Work

Outline

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- 1 Introduction
 - Access Control
 - Term Rewriting
- 2 Motivating Example
- 3 The Policy Environment
- 4 Rewriting Based Policies
- 5 Properties of Security Policies
- 6 Conclusions and Future Work

Outline

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- 1 Introduction
 - Access Control
 - Term Rewriting
- 2 Motivating Example
- 3 The Policy Environment
- 4 Rewriting Based Policies
- 5 Properties of Security Policies
- 6 Conclusions and Future Work

Outline

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- 1 Introduction
 - Access Control
 - Term Rewriting
- 2 Motivating Example
- 3 The Policy Environment
- 4 Rewriting Based Policies
- 5 Properties of Security Policies
- 6 Conclusions and Future Work

Access Control

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- A central issue in computer security
- Access control concerns stating which *actions*, *principals (or subjects)* are allowed to execute in order to manipulate the *objects (or resources)* of a given system.
- Some vocabulary: Request, Decision, Authorization, Deny, Permit (Grant), Policy, Mechanism

The Access Control Matrix

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- The most widespread form of access control specification and enforcement
- The lines of the matrix enroll the subjects, the columns list the resources of the system, and cells contain what rights (*read, right, execute, . . .*) are assigned to each case
- RBAC - Users, roles, and rights
- Is this enough?

The Access Control Matrix

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- The most widespread form of access control specification and enforcement
- The lines of the matrix enroll the subjects, the columns list the resources of the system, and cells contain what rights (*read, right, execute, . . .*) are assigned to each case
- RBAC - Users, roles, and rights
- Is this enough?

Principles of rewriting

- Terms are expressions built from variables, constant symbols and function symbols

$$0, x, s(0) + x, s(s(s(0)) + 0)$$

- Signature is a set of sorts \mathcal{S} together with a set of function symbols, each one associated to a natural number by the arity function ($\text{ar} : \mathcal{F} \rightarrow \mathbb{N}$).
- A rule describes a way of transforming a term into another term
- Normal forms: rules are successively applied until no rule can be used to transform the term anymore

Example of term rewriting system

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Example

$$\mathit{append}(\mathit{nil}, x) \rightarrow x$$
$$\mathit{append}(\mathit{cons}(y, x), z) \rightarrow \mathit{cons}(y, \mathit{append}(x, z))$$

Derivation

$$\mathit{append}(\mathit{cons}(0, \mathit{nil}), \mathit{cons}(s(0), \mathit{nil})) \xrightarrow{*}_R \mathit{cons}(0, \mathit{cons}(s(0), \mathit{nil}))$$

Example of term rewriting system

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Example

$$\mathit{append}(\mathit{nil}, x) \rightarrow x$$
$$\mathit{append}(\mathit{cons}(y, x), z) \rightarrow \mathit{cons}(y, \mathit{append}(x, z))$$

Derivation

$$\mathit{append}(\mathit{cons}(0, \mathit{nil}), \mathit{cons}(s(0), \mathit{nil})) \xrightarrow{*}_R \mathit{cons}(0, \mathit{cons}(s(0), \mathit{nil}))$$

Properties of term rewriting systems

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

A rewrite derivability relation $\xrightarrow{*}_R$ is defined on terms $t \xrightarrow{*}_R t'$ if there exists a rewriting derivation from t to t' . If the derivation contains at least one step, it is denoted by $\xrightarrow{+}_R$.

- Termination: A term rewriting systems is terminating if all reduction sequences are finite.
- Confluence: It is confluent if for all terms t, u, v , $t \xrightarrow{*}_R u$ and $t \xrightarrow{*}_R v$ implies $u \xrightarrow{*}_R s$ and $v \xrightarrow{*}_R s$, for some s .

Rewriting-Based Access Control Policies

Rewriting- Based Access Control Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

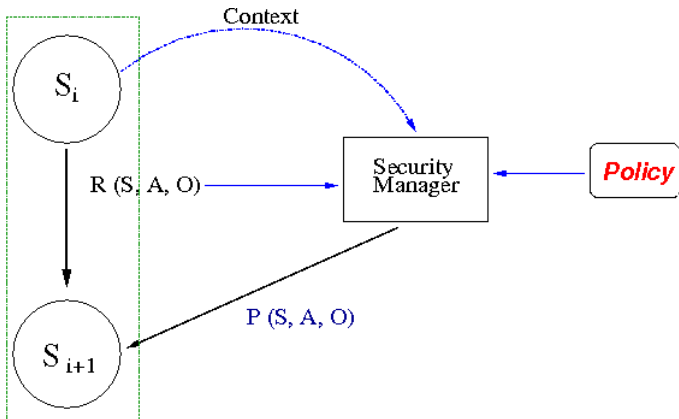
Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- Policies are represented as sets of rewrite rules whose evaluation produces authorization decisions
- Requests and the environment where policies are enforced are represented as algebraic terms
- The policy environment as a “fact base” under the form of a term, allowing to capture many dynamic aspects of the policy environment

General Schema



Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control

Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

A Medical System

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- 1 A person, identified by his or her patient number, may read any record for which he or she is the designated patient.
- 2 A person may read any record for which he or she is the designated parent or guardian, and for which the patient is under 16 years of age.
- 3 A physician may write to any medical element for which he or she is the designated primary care physician.
- 4 An administrator shall not be permitted to read or write to medical elements of a patient record.

Representing the policy environment

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- Policies are sentences about the current attributes of subjects and resources
- The policy environment contains the configuration of all elements relevant to access control.
- An arbitrary target system, noted as T is represented as a set of states and state transitions originated by access requests
- To each state s_i of T we associate an algebraic term containing the facts that are true in s_i .

The system state

Rewriting- Based Access Control Policies

Anderson
Santana de
Oliveira

Introduction

Access Control

Term Rewriting

Motivating Example

The Policy Environment

Rewriting Based Policies

Properties of Security Policies

Conclusions and Future Work

S_i	<pre>patient("Bart Simpson", 1, 14, guardian("Homer Simpson")) + record(patient("Bart Simpson", 1, 14, guardian("Homer Simpson")), physician("Julius Hibbert", 1), antibiotic, payment(visa)) + physician("Julius Hibbert", 1)</pre>
Request	<pre>request (physician("Julius Hibbert", 1), writeMedicalElements , record(patient("Bart Simpson", 1, 14, guardian("Homer Simpson")), physician("Julius Hibbert", 1) ,antibiotic, payment(Visa)))</pre>
S_{i+1}	<pre>patient("Bart Simpson", 1, 14, guardian("Homer Simpson")) + record(patient("Bart Simpson", 1, 14, guardian("Homer Simpson")), physician("Julius Hibbert", 1), antibiotic and aspirin, payment(visa)) + physician("Julius Hibbert", 1) .</pre>

The target system signature

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

```
fmod MEDICAL-SYSTEM-SIGNATURE is
  protecting STRING .
  protecting NAT .
  sort Patient Physician Record Administrator Guardian
  MedicalElements OtherElements .

  op patient : String Nat Nat Guardian -> Patient [ctor] .
  op administrator : Nat -> Administrator [ctor] .
  op guardian : String -> Guardian [ctor] .
  op physician : String Nat -> Physician [ctor] .
  op record : Patient Physician MedicalElements
  OtherElements -> Record [ctor] .

endfm
```

Subjects, Actions and Objects

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control

Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

```
fmod MEDICAL-SYSTEM-TERM-SIGNATURE is
    including MEDICAL-SYSTEM-SIGNATURE .
    including POLICY-SIGNATURE .
    subsort Physician < Subject .
    subsort Patient < Subject .
    subsort Guardian < Subject .
    subsort Administrator < Subject .
    subsort Record < Object .
    subsort MedicalElements < Object .
    subsort OtherElements < Object .
    op readRecord : -> Action .
    op writeRecord : -> Action .
    op readMedicalElements : -> Action .
    op writeMedicalElements : -> Action .
    op readOtherElements : -> Action .
    op writeOtherElements : -> Action .
endfm
```

Authorization Terms

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Requests implies on a system transition and have the following profile:

request : $Subject \times Action \times Object \rightarrow Request$

A decision w.r.t a request is taken according to the definition of the operator

auth : $Request \times Term \rightarrow Authorization$

which produces a decision for a request, based on the term representing the fact base.

Authorizations are terms built over the following signature:

$\{deny, permit\} : Subject \times Action \times Object \rightarrow Authorization$

Authorization Terms

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Requests implies on a system transition and have the following profile:

$$\textit{request} : \textit{Subject} \times \textit{Action} \times \textit{Object} \rightarrow \textit{Request}$$

A decision w.r.t a request is taken according to the definition of the operator

$$\textit{auth} : \textit{Request} \times \textit{Term} \rightarrow \textit{Authorization}$$

which produces a decision for a request, based on the term representing the fact base.

Authorizations are terms built over the following signature:

$$\{ \textit{deny}, \textit{permit} \} : \textit{Subject} \times \textit{Action} \times \textit{Object} \rightarrow \textit{Authorization}$$

Authorization Terms

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Requests implies on a system transition and have the following profile:

$$\textit{request} : \textit{Subject} \times \textit{Action} \times \textit{Object} \rightarrow \textit{Request}$$

A decision w.r.t a request is taken according to the definition of the operator

$$\textit{auth} : \textit{Request} \times \textit{Term} \rightarrow \textit{Authorization}$$

which produces a decision for a request, based on the term representing the fact base.

Authorizations are terms built over the following signature:

$$\{\textit{deny}, \textit{permit}\} : \textit{Subject} \times \textit{Action} \times \textit{Object} \rightarrow \textit{Authorization}$$

The policy signature

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control

Term Rewriting

Motivating
Example

The Policy
Environment

**Rewriting
Based
Policies**

Properties of
Security
Policies

Conclusions
and Future
Work

```
fmod POLICY-SIGNATURE is
    sort Object .
    sort Subject .
    sort Action .
    sort Term .
    sort Request .
    sort Authorization .
    subsort Subject < Term .
    subsort Object < Term .
    subsort Action < Term .
    op req : Subject Action Object -> Request [ctor] .
    op permit : Subject Action Object -> Authorization [ctor] .
    op deny : Subject Action Object -> Authorization [ctor] .
    op auth : Request Term -> Authorization .
    op _+_ : Term Term -> Term [assoc comm] .
endfm
```

Rewrite based policies

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Definition (Security Policy)

An access control security policy, \mathcal{P} , is a term rewriting system over $\mathcal{T}(\Sigma, X)$, with $\Sigma = \Sigma_T \cup \Sigma_P$, where the top symbol of the left hand side of each rule is the *auth* function.

The medical system policy

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

A person, identified by his or her patient number, may read any record for which he or she is the designated patient.

```
auth( req(p, readRecord, record(p, ph, me, oe)),  
      p + record(p, ph, me, oe) )  
=>  
permit(p, readRecord, record(p, ph, me, oe))
```

The medical system policy

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

An administrator shall not be permitted to read or write to medical elements of a patient record.

```
auth(req( adm, writeMedElem, record(p, ph, me, oe))  
      adm + record(p, ph, me, oe) )
```

=>

```
deny( adm, writeMedElem, record(p, ph, me, oe)) .
```

```
auth(req( adm, writeMedElem, record(p, ph, me, oe))  
      adm + record(p, ph, me, oe) )
```

=>

```
deny( adm, writeMedElem, record(p, ph, me, oe)) .
```

The medical system policy

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

An administrator shall not be permitted to read or write to medical elements of a patient record.

```
auth(req( adm, writeMedElem, record(p, ph, me, oe) )  
      adm + record(p, ph, me, oe) )
```

=>

```
deny( adm, writeMedElem, record(p, ph, me, oe) ) .
```

```
auth(req( adm, writeMedElem, record(p, ph, me, oe) )  
      adm + record(p, ph, me, oe) )
```

=>

```
deny( adm, writeMedElem, record(p, ph, me, oe) ) .
```

The medical system policy

```
mod POLICY1 is
  protecting MEDICAL-SYSTEM-TERM-SIGNATURE .
  var p : Patient .          var ph : Physician .
  var g : Guardian .        var adm : Administrator .
  var me : MedicalElements . var oe : OtherElements .
  vars s1 s2 : String .     var t : Term .     var n1 n2 : Nat .

  r1 [patReadRecord] : auth( req(p, readRecord, record(p, ph, me, oe)),
    p + record(p, ph, me, oe) + t )
    => permit(p, readRecord, record(p, ph, me, oe)) .

  r1 [gaurdReadRecord] : auth( req( g, readRecord,
    record(patient(s1, n1, n2, g), ph, me, oe )), patient(s1, n1, n2, g)
    + record(patient(s1, n1, n2, g), ph, me, oe) + t)
    => permit(g, readRecord, record(patient(s1, n1, n2, g), ph, me, oe)) .

  r1 [physWriteMedElem] : auth( req( ph, writeMedicalElements,
    record(p, ph, me, oe)),      record(p,ph, me, oe) + t)
    => permit(ph, writeMedicalElements, record(p, ph, me, oe)) .

  r1 [admReadMedElem] : auth(req( adm, readMedicalElements,
    record(p, ph, me, oe)), adm + record(p,ph, me, oe) + t )
    => deny(adm, readMedicalElements, record(p, ph, me, oe)) .

  r1 [admWriteMedElem] : auth( req( adm, writeMedicalElements,
    record(p, ph, me, oe)), adm + record(p,ph, me, oe) + t )
    => deny(adm, writeMedicalElements, record(p, ph, me, oe)) .

endm
```

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control

Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Termination

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction

Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- This will assure that every request evaluation is finite
- There are several tools available that check termination of term rewriting systems: CiMe, Approve, Cariboo, . . .
- The basic idea: a refinement discipline for policy deployment

Absence of conflict

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- The origin of the problem is the combined use of positive and negative authorizations
- Classical approaches for policy specification adopt either *closed policy* or *open policy*
- For rewriting-based policies, conflicts can be avoided if the corresponding term rewriting system is confluent: single response is produced for a given request

Completeness

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- Incompleteness happens when no authorization is specified for a certain request
- Completeness is usually achieved by assuming that one of either the open or closed policy operates as a default
- It is necessary to check the *sufficient completeness* of term rewrite system.

Completeness

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Alternatively, the user can make use of rules determining the default case to be applied in the case no redex exist for a request. These rules are either of the form

$$\mathit{auth}(\mathit{req}(s_1, a_1, o_1), t) \rightarrow \mathit{deny}(s_1, a_1, o_1)$$

or

$$\mathit{auth}(\mathit{req}(s_1, a_1, o_1), t) \rightarrow \mathit{permit}(s_1, a_1, o_1)$$

Trusted Policy

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

Definition (Trusted Security Policy)

A trusted access control security policy is **terminating** and *confluent* term rewriting system, \mathcal{P} , whose signature is $\mathcal{T}(\Sigma, X)$, with $\Sigma = \Sigma_T \cup \Sigma_P$, and **completely** defines the *auth* function.

Conclusion

Rewriting-
Based Access
Control
Policies

Anderson
Santana de
Oliveira

Introduction
Access Control
Term Rewriting

Motivating
Example

The Policy
Environment

Rewriting
Based
Policies

Properties of
Security
Policies

Conclusions
and Future
Work

- This talk presented a formalization for access control policies using term rewriting
- Future work:
 - To study problems related to **policy composition**
 - To investigate how to solve authorization conflicts using rewrite strategies
 - To develop analysis of access control policies: absence of conflict, completeness, . . .