SECURITY IN PETRI NETS SHARING AND STORAGE: SUBNETS, PRIVACY, INTEGRITY, AUTHENTICATION AND NON REPUDIATION

Iñigo León Samaniego

Defensa de Tesis Doctoral

Universidad de La Rioja

Directores: Emilio Jiménez Macías, Juan Ignacio Latorre Biel

September 28, 2015

Introducción

Las Redes de Petri...

Las Redes de Petri...

- ...están muy extendidas para modelar sistemas
  - servicios y procesos logísticos
  - sistemas concurrentes
  - ...

Las Redes de Petri...

- ...están muy extendidas para modelar sistemas
  - servicios y procesos logísticos
  - sistemas concurrentes
  - ...
- ...están descritas de una manera exhaustiva, con información de toda la red

Las Redes de Petri...

- ...están muy extendidas para modelar sistemas
  - servicios y procesos logísticos
  - sistemas concurrentes
  - ...
- ...están descritas de una manera exhaustiva, con información de toda la red
- ...pueden ser modificadas sin control de integridad o autoría

Pero es posible que...

Pero es posible que...

- ...no queramos describir la red entera

Pero es posible que...

- ...no queramos describir la red entera
- ...parte del proceso sea secreto para personas no autorizadas

Pero es posible que...

- ...no queramos describir la red entera
- ...parte del proceso sea secreto para personas no autorizadas
- ...necesitemos validación de partes concretas por parte de determinadas personas

Pero es posible que...

- ...no queramos describir la red entera
- ...parte del proceso sea secreto para personas no autorizadas
- ...necesitemos validación de partes concretas por parte de determinadas personas
- ...queramos evitar cualquier modificación no autorizada

Justificación de la investigación

Sería interesante proveer de seguridad a las redes de Petri...

Justificación de la investigación

Sería interesante proveer de seguridad a las redes de Petri...

- ...ocultando partes concretas

Justificación de la investigación

Sería interesante proveer de seguridad a las redes de Petri...

- ...ocultando partes concretas
- ...detectando modificaciones no autorizadas

Justificación de la investigación

Sería interesante proveer de seguridad a las redes de Petri...

- ...ocultando partes concretas
- ...detectando modificaciones no autorizadas
- ...autenticándola (o una parte de ella)

Justificación de la investigación

Sería interesante proveer de seguridad a las redes de Petri...

- ...ocultando partes concretas
- ...detectando modificaciones no autorizadas
- ...autenticándola (o una parte de ella)
- ...evitando suplantación de identidades

Contribuciones

Mis **contribuciones originales** al conocimiento son:

Contribuciones

Mis **contribuciones originales** al conocimiento son:

1. Estudio en profundidad de subredes, abstrayendo su estructura interna del exterior a través de interfaces

Contribuciones

Mis **contribuciones originales** al conocimiento son:

1. Estudio en profundidad de subredes, abstrayendo su estructura interna del exterior a través de interfaces
2. Método para construir estas subredes e interfaces a partir de la representación matricial

Contribuciones

Mis **contribuciones originales** al conocimiento son:

1. Estudio en profundidad de subredes, abstrayendo su estructura interna del exterior a través de interfaces
2. Método para construir estas subredes e interfaces a partir de la representación matricial
3. Descripción de una posible extensión de PNML para la representación de subredes

Contribuciones

Mis **contribuciones originales** al conocimiento son:

1. Estudio en profundidad de subredes, abstrayendo su estructura interna del exterior a través de interfaces
2. Método para construir estas subredes e interfaces a partir de la representación matricial
3. Descripción de una posible extensión de PNML para la representación de subredes
4. Aplicación de técnicas de seguridad a las redes representadas de esta manera

Subredes

Conceptos y Definiciones

- Sea $R = \langle P, T, \alpha, \beta \rangle$ una red de Petri. Una subred de R es otra red $\overline{R} = \langle \overline{P}, \overline{T}, \overline{\alpha}, \overline{\beta} \rangle$ tal que $\overline{P} \subseteq P$ y $\overline{T} \subseteq T$, $\overline{\alpha}$ y $\overline{\beta}$ son restricciones de α y β sobre $\overline{P} \times \overline{T}$.

Conceptos y Definiciones

- Sea $R = \langle P, T, \alpha, \beta \rangle$ una red de Petri. Una subred de R es otra red $\overline{R} = \langle \overline{P}, \overline{T}, \overline{\alpha}, \overline{\beta} \rangle$ tal que $\overline{P} \subseteq P$ y $\overline{T} \subseteq T$, $\overline{\alpha}$ y $\overline{\beta}$ son restricciones de α y β sobre $\overline{P} \times \overline{T}$.
- Usando matrices:

$$C = \begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \end{array} \begin{array}{c} \begin{array}{cccccc} t_1 & t_2 & t_3 & t_4 & t_5 & t_6 \end{array} \\ \begin{bmatrix} -1 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \end{array} \xrightarrow[t_1, t_2, t_3]{p_1, p_3, p_4, p_5} C' = \begin{array}{c} \\ p_1 \\ p_3 \\ p_4 \\ p_5 \end{array} \begin{array}{c} \begin{array}{ccc} t_1 & t_2 & t_3 \end{array} \\ \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{bmatrix} \end{array}$$

Conceptos y Definiciones

- Sea $R = \langle P, T, \alpha, \beta \rangle$ una red de Petri. Una subred de R es otra red $\overline{R} = \langle \overline{P}, \overline{T}, \overline{\alpha}, \overline{\beta} \rangle$ tal que $\overline{P} \subseteq P$ y $\overline{T} \subseteq T$, $\overline{\alpha}$ y $\overline{\beta}$ son restricciones de α y β sobre $\overline{P} \times \overline{T}$.
- Usando matrices:

$$C = \begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \end{array} \begin{array}{c} \begin{array}{cccccc} t_1 & t_2 & t_3 & t_4 & t_5 & t_6 \end{array} \\ \begin{bmatrix} -1 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \end{array} \xrightarrow[t_1, t_2, t_3]{p_1, p_3, p_4, p_5} C' = \begin{array}{c} \\ p_1 \\ p_3 \\ p_4 \\ p_5 \end{array} \begin{array}{c} \begin{array}{ccc} t_1 & t_2 & t_3 \end{array} \\ \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & 1 & 0 \end{bmatrix} \end{array}$$

- $Q = \{R_1, R_2, ...R_k\}$ es una partición de R si
  - $R_1 \cup R_2 \cup ... \cup R_k = R$
  - $\forall i, j | 1 \leqslant i, j \leqslant k, i \neq j \ \Rightarrow \ R_i \cap R_j = \emptyset$

Descomposición en subredes

Los lugares de $\overline{P}$ y las transiciones de $\overline{T}$ pueden ser reordenadas poniéndolas al principio de la matriz de incidencia[1]...

$$C = \begin{array}{c} \\ p_1 \\ \vdots \\ p_r \\ p_{r+1} \\ \vdots \\ p_n \end{array} \begin{array}{c} \begin{array}{cccccc} t_1 & \cdots & t_s & t_{s+1} & \cdots & t_m \end{array} \\ \left[\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1s} & a_{1(s+1)} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{r1} & \cdots & a_{rs} & a_{r(s+1)} & \cdots & a_{rm} \\ \hline a_{(r+1)1} & \cdots & a_{(r+1)s} & a_{(r+1)(s+1)} & \cdots & a_{(r+1)m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{ns} & a_{n(s+1)} & \cdots & a_{nr} \end{array}\right] \end{array}$$

dividiéndola en 4 partes:

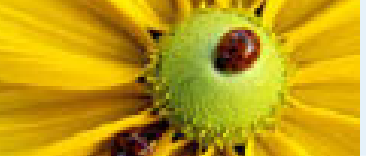
[1] Se prueba que es una relación de equivalencia

Descomposición en subredes

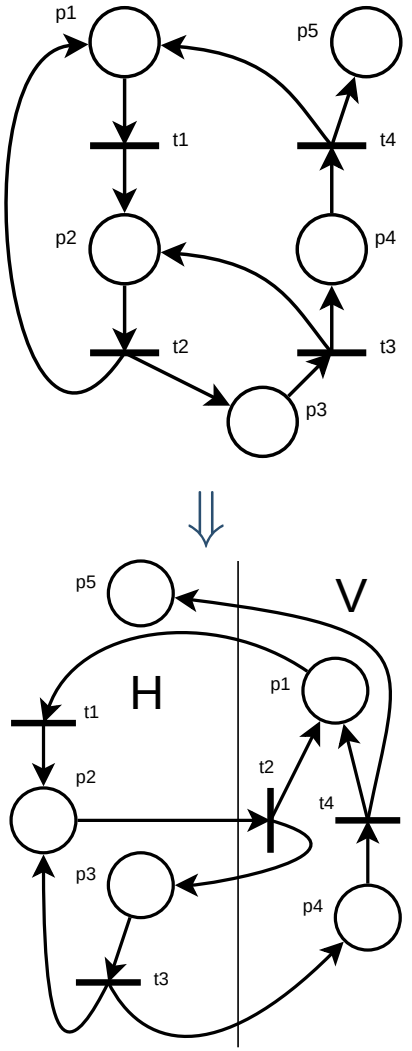
$$C = \begin{pmatrix} N_1 & PIM_{12} \\ TIM_{12} & N_2 \end{pmatrix}$$

- N_1 es la subred formada por los lugares y las transiciones que queremos agrupar en una subred
- N_2 es la subred complementaria de N_1 y formada por el resto de lugares y transiciones
- PIM_{12} (Places Influence Matrix) define la interacción entre lugares de N_1 y transiciones de N_2
- TIM_{12} (Transitions Influence Matrix) define la interacción de las transiciones de N_1 y los lugares de N_2

PIM_{12} y TIM_{12} se utilizarán para crear el front-end de N_1



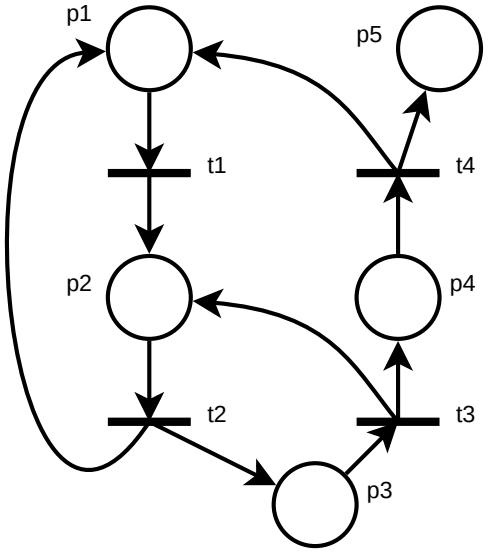
Descomposición en subredes



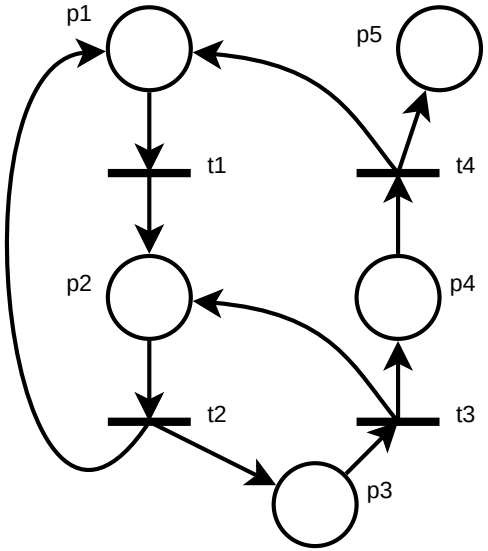
$$
\begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \end{array}
\begin{array}{c}
\begin{array}{cccc} t_1 & t_2 & t_3 & t_4 \end{array} \\
\left[\begin{array}{cccc}
-1 & 1 & 0 & 1 \\
1 & -1 & 1 & 0 \\
0 & 1 & -1 & 0 \\
0 & 0 & 1 & -1 \\
0 & 0 & 0 & 1
\end{array}\right]
\end{array}
$$

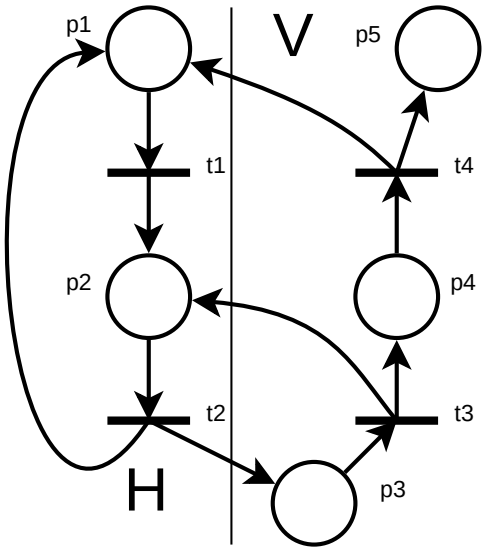
$$
\begin{array}{c} \\ p_2 \\ p_3 \\ p_5 \\ \hline p_1 \\ p_4 \end{array}
\begin{array}{c}
\begin{array}{cccc} t_1 & t_3 & t_2 & t_4 \end{array} \\
\left[\begin{array}{cc|cc}
1 & 1 & -1 & 0 \\
0 & -1 & 1 & 0 \\
0 & 0 & 0 & 1 \\ \hline
-1 & 0 & 1 & 1 \\
0 & 1 & 0 & -1
\end{array}\right]
\end{array}
$$

Descomposición en subredes

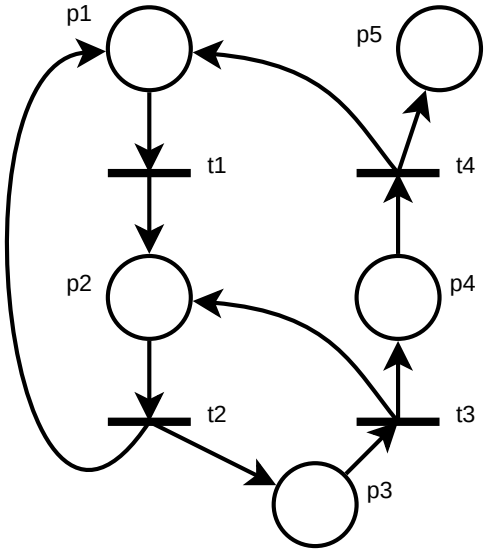


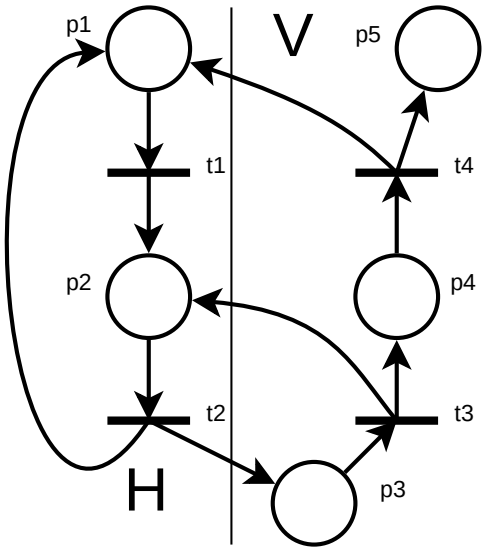
Descomposición en subredes

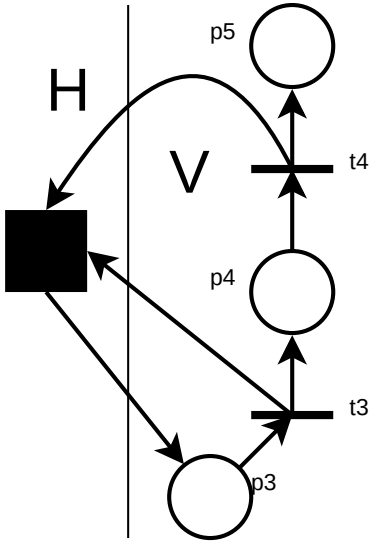




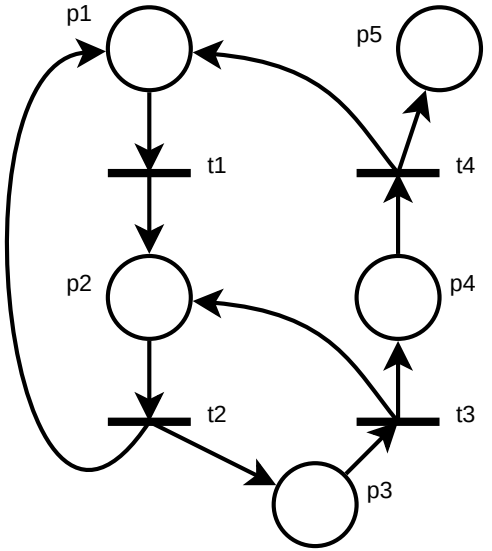
Descomposición en subredes

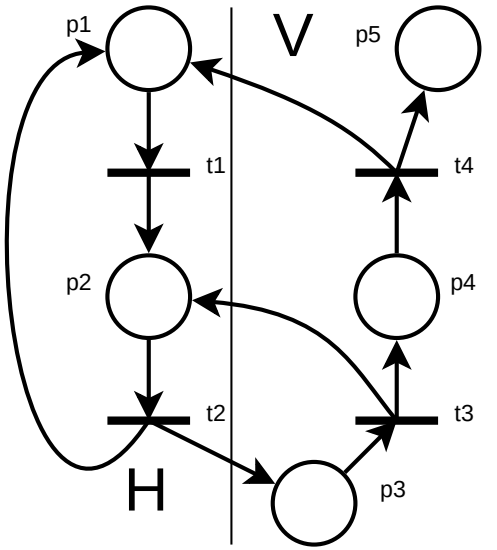


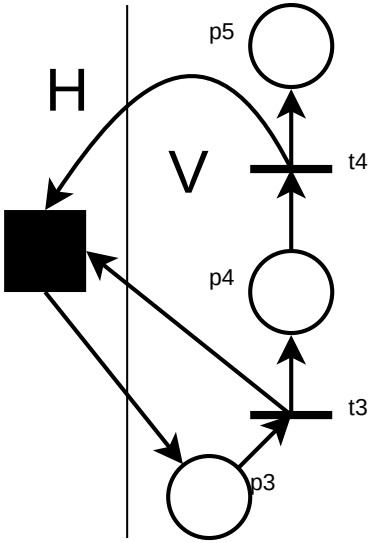




Descomposición en subredes



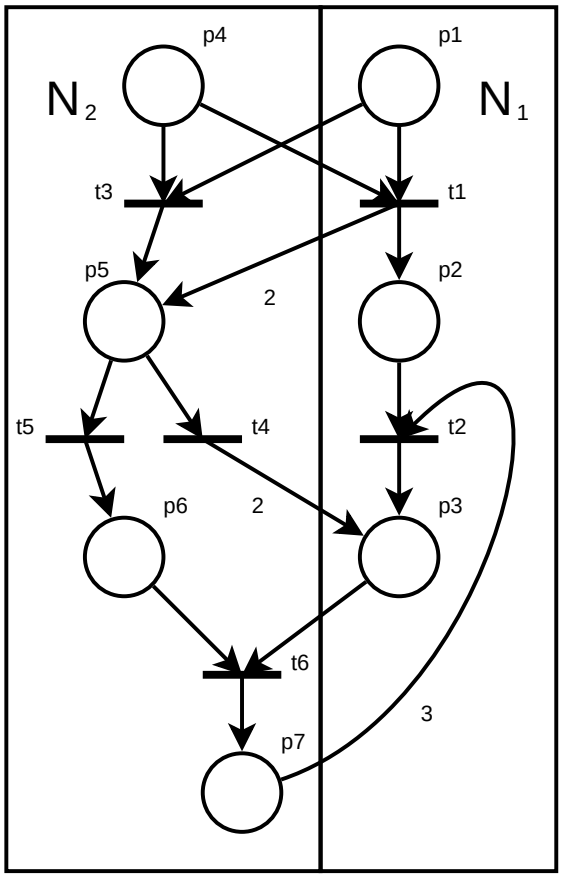




¿Cómo representar esto?

Front-end

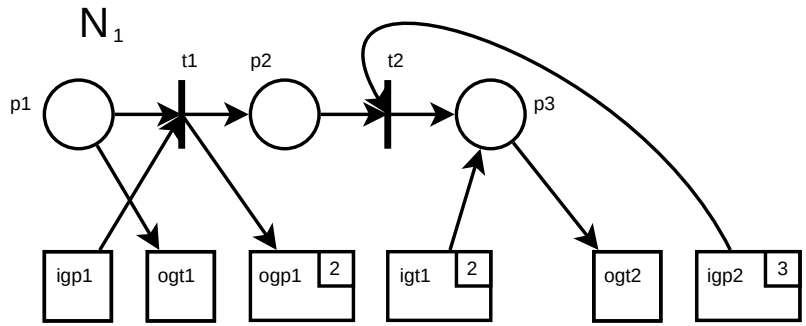
Sea la siguiente red de Petri y su matriz de incidencia



$$C = \begin{array}{c|cc|cccc} & t_1 & t_2 & t_3 & t_4 & t_5 & t_6 \\ p_1 & -1 & 0 & -1 & 0 & 0 & 0 \\ p_2 & 1 & -1 & 0 & 0 & 0 & 0 \\ p_3 & 0 & 1 & 0 & 2 & 0 & -1 \\ \hline p_4 & -1 & 0 & -1 & 0 & 0 & 0 \\ p_5 & 2 & 0 & 1 & -1 & -1 & 0 \\ p_6 & 0 & 0 & 0 & 0 & 1 & -1 \\ p_7 & 0 & -3 & 0 & 0 & 0 & 1 \end{array}$$

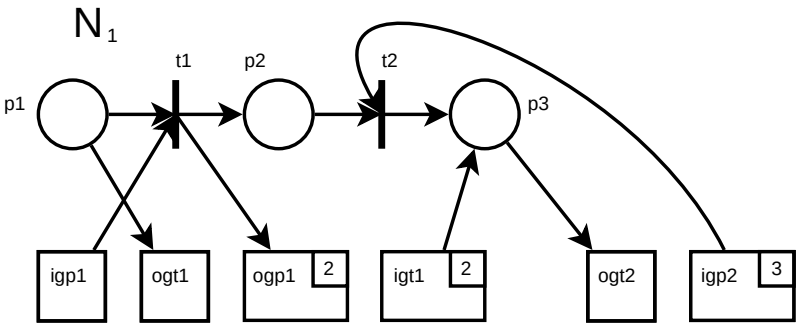
Front-end

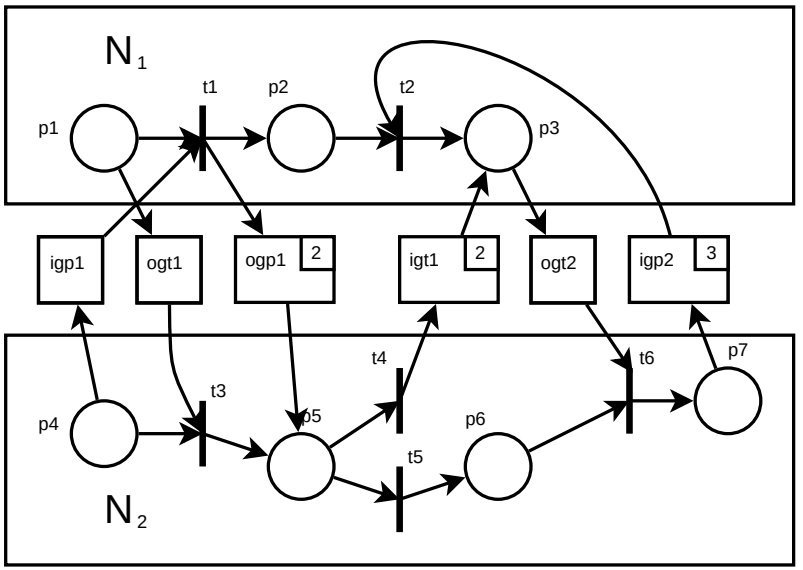
- $\left\{ \begin{array}{l} \text{Input} \\ \text{Output} \end{array} \right\}$ gate $\left\{ \begin{array}{l} \text{Place} \\ \text{Transition} \end{array} \right\}$ (igp, igt, ogp, ogt)



Front-end

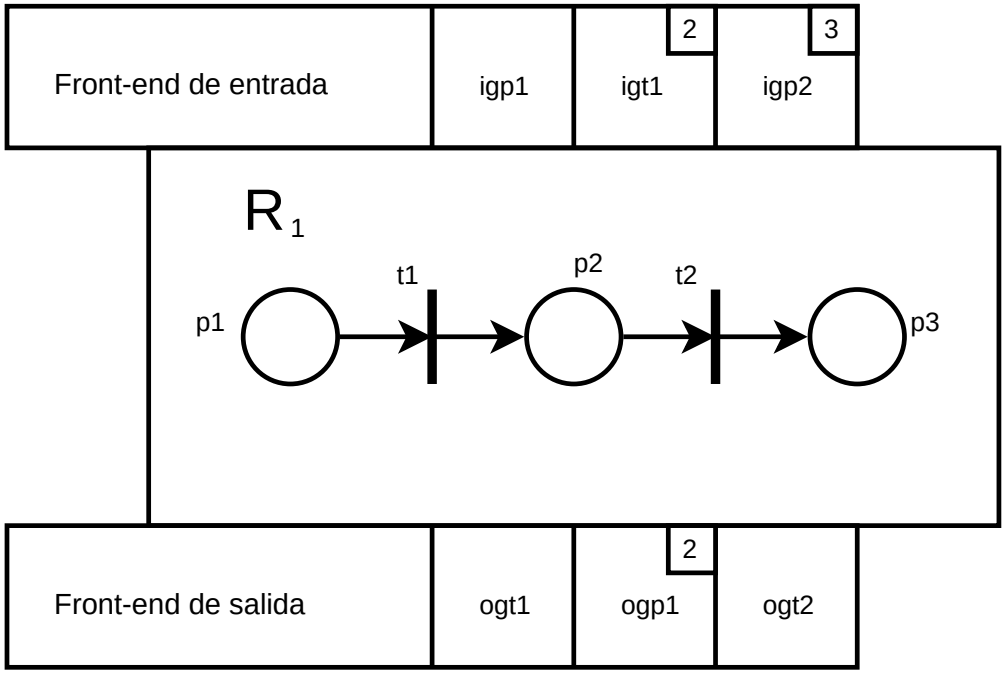
- $\left\{ \begin{array}{l} \text{Input} \\ \text{Output} \end{array} \right\}$ gate $\left\{ \begin{array}{l} \text{Place} \\ \text{Transition} \end{array} \right\}$ (igp, igt, ogp, ogt)





Front-end

- { Input, Output } front-end



Front-end

Retomando la matriz de la red de Petri del ejemplo

$$PIM_{12} = \begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \end{array} \begin{array}{c} \begin{array}{cccc} t_3 & t_4 & t_5 & t_6 \end{array} \\ \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 \end{bmatrix} \end{array} \qquad TIM_{12} = \begin{array}{c} \\ p_4 \\ p_5 \\ p_6 \\ p_7 \end{array} \begin{array}{c} \begin{array}{cc} t_1 & t_2 \end{array} \\ \begin{bmatrix} -1 & 0 \\ 2 & 0 \\ 0 & 0 \\ 0 & -3 \end{bmatrix} \end{array}$$

De PIM_{12} obtenemos $\begin{cases} \text{igt por cada elemento} > 0 \\ \text{ogt por cada elemento} < 0 \end{cases}$

De TIM_{12} obtenemos $\begin{cases} \text{igp por cada elemento} < 0 \\ \text{ogp por cada elemento} > 0 \end{cases}$

Así, de la representación matricial podemos sacar el front-end sin necesidad de dibujar nada

Red acoplable

Una red acoplable es una cuádrupla $R_a = \langle R, F, f_i, f_o \rangle$.

Red acoplable

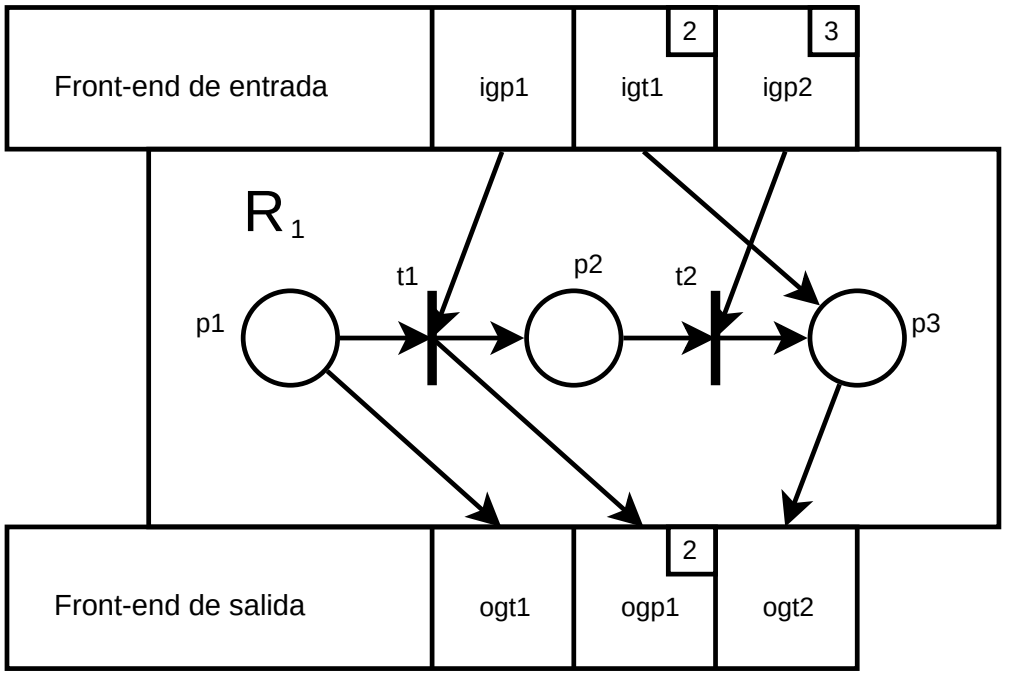
Una red acoplable es una cuádrupla $R_a = \langle R, F, f_i, f_o \rangle$.

- Parte pública: F
- Parte privada: R, f_i y f_o, siendo
  - $f_i : IG \to R_i$ la función de entrada
  - $f_o : R_i \to OG$ la función de salida

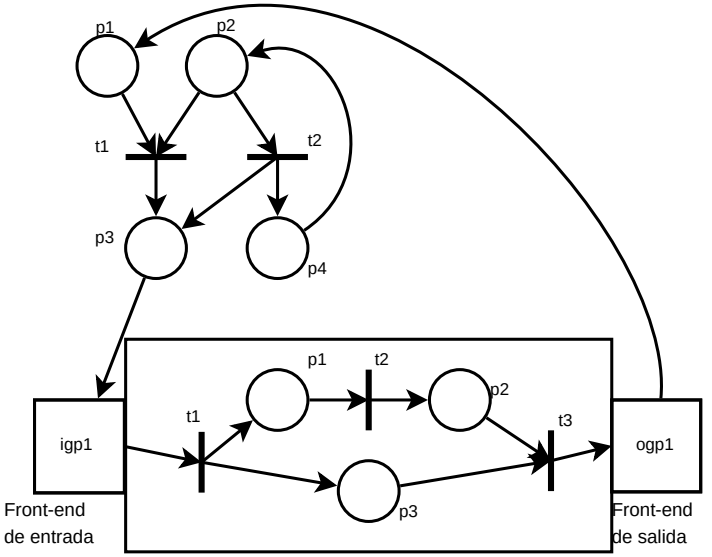
Red acoplable

Una red acoplable es una cuádrupla $R_a = \langle R, F, f_i, f_o \rangle$.

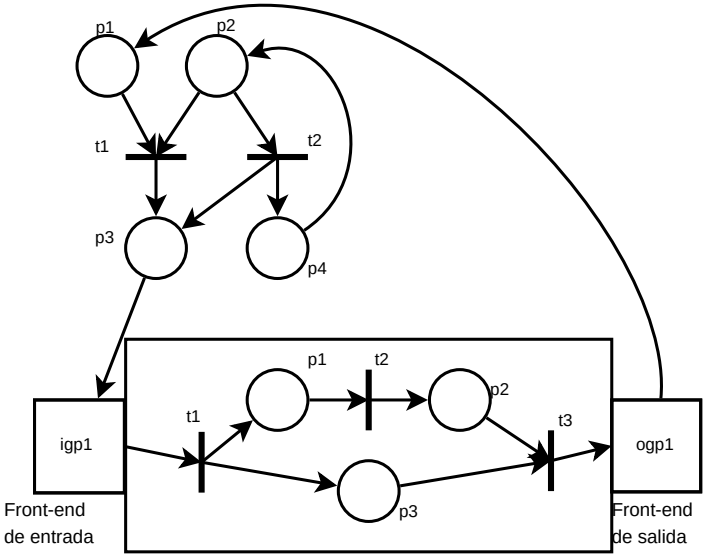
- Parte pública: F
- Parte privada: R, f_i y f_o, siendo
  - $f_i : IG \to R_i$ la función de entrada
  - $f_o : R_i \to OG$ la función de salida

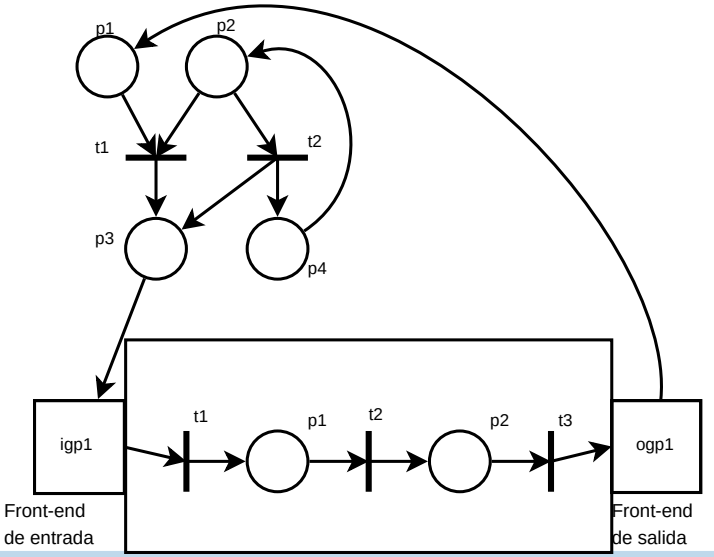


Red acoplable



Red acoplable





PNML

Revisión general de PNML

Objetivo:

1. Representar subredes de una red de Petri
2. Incluir interfaces de entrada y salida para cada subred

Revisión general de PNML

Objetivo:

1. Representar subredes de una red de Petri
2. Incluir interfaces de entrada y salida para cada subred

Usarremos PNML, pero:

- Es un lenguaje XML para representar redes de Petri
- No tiene capacidad para representar subredes

Revisión general de PNML

Objetivo:

1. Representar subredes de una red de Petri
2. Incluir interfaces de entrada y salida para cada subred

Usarremos PNML, pero:

- Es un lenguaje XML para representar redes de Petri
- No tiene capacidad para representar subredes

Por tanto necesitamos modificar/ampliar la gramática de PNML para conseguir los objetivos

Revisión general de PNML

PNML está basado en XML. Por tanto:

1. Comienza con una línea con información del fichero

```
<?xml version="1.0" encoding="utf-8"?>
```

2. Cada elemento tiene un id único dentro del fichero
3. La estructura general es la siguiente:

```
<?xml version="1.0" encoding="utf-8"?>
<pnml>
  <net id="myNet" type="http://www.pnml.org/version-2009/grammar/
     ptnet">
    <name>
      <text> My new net </text>
    </name>
    <page id="page1">
      .......
    </page>
  </net>
</pnml>
```

Revisión general de PNML

Los principales elementos son:

- Lugar: con un id

```
<place id="p1">
  <name>
    <text>Lugar 1</text>
  </name>
  <initialMarking>
    <text> 2 </text>
  </initialMarking>
</place>
```

Revisión general de PNML

Los principales elementos son:

- Lugar: con un id

```
<place id="p1">
  <name>
    <text>Lugar 1</text>
  </name>
  <initialMarking>
    <text> 2 </text>
  </initialMarking>
</place>
```

- Transicion: con otro id

```
<transition id="t2">
  <name>
   <text>Transicion 2</text>
  </name>
</transition>
```

Revisión general de PNML

Los principales elementos son:

- Lugar: con un id

```
<place id="p1">
  <name>
    <text>Lugar 1</text>
  </name>
  <initialMarking>
    <text> 2 </text>
  </initialMarking>
</place>
```

- Transicion: con otro id

```
<transition id="t2">
  <name>
   <text>Transicion 2</text>
  </name>
</transition>
```

- Arco: con un id, un origen y un destino

```
<arc id="a1" source="p1"
     target="t2">
  <name>
    <text>Arco 1</text>
  </name>
  <inscription>
    3
  </inscription>
</arc>
```

Revisión general de PNML

Por claridad, obviaremos algunas etiquetas.

- Lugar

```
<place id="p1">
  <initialMarking>
    <text> 2 </text>
  </initialMarking>
</place>
```

- Transicion

```
<transition id="t2"/>
```

- Arco

```
<arc id="a1" source="p1" target="t2">
  <inscription> 3 </inscription>
</arc>
```

Elementos extendidos PNML: Subnet

Elementos extendidos en PNML:

- Subnet

```
<subnet id="sn1">
  <interface id="sn1-interface">
    ...
  </interface>
  <content id="sn1-content">
    ...
  </content>
</subnet>
```

Elementos extendidos PNML: Interface

Interface

```
<interface id="sn1-interface">
  <gate id="igp1" action="input" type="place"/>
  <gate id="igp2" action="input" type="place"/>
  <gate id="ogt1" action="output"
        type="transition">
    <inscription>
      <text> 2 </text>
    </inscription>
  </gate>
</interface>
```

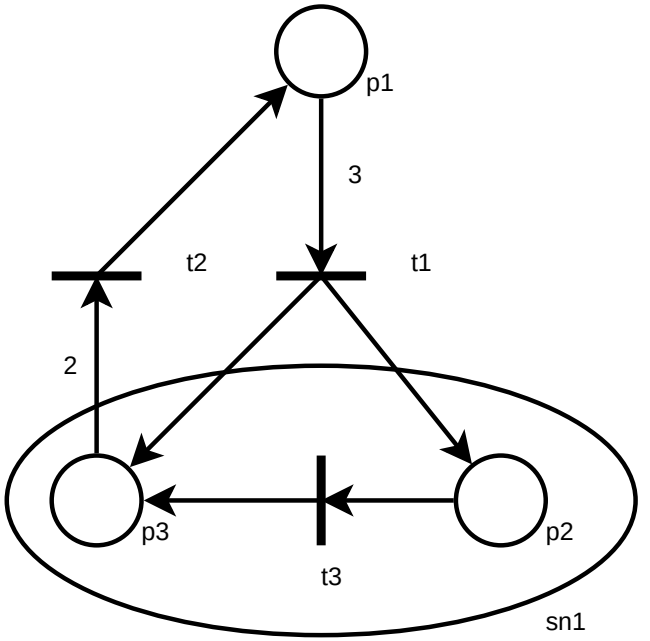
Elementos extendidos PNML: Content

Content

```
<content id="sn1-content">
  <place id="p2"/>
  <place id="p3"/>
  <transition id="t3"/>
  <arc id="sn1-a2" source="igp2" target="p2"/>
  <arc id="sn1-a3" source="igp1" target="p3"/>
  <arc id="sn1-a4" source="p3" target="ogt1">
    <inscription>
      <text> 2 </text>
    </inscription>
  </arc>
  <arc id="a5" source="t3" target="p3"/>
  <arc id="a6" source="p2" target="t3"/>
</content>
```

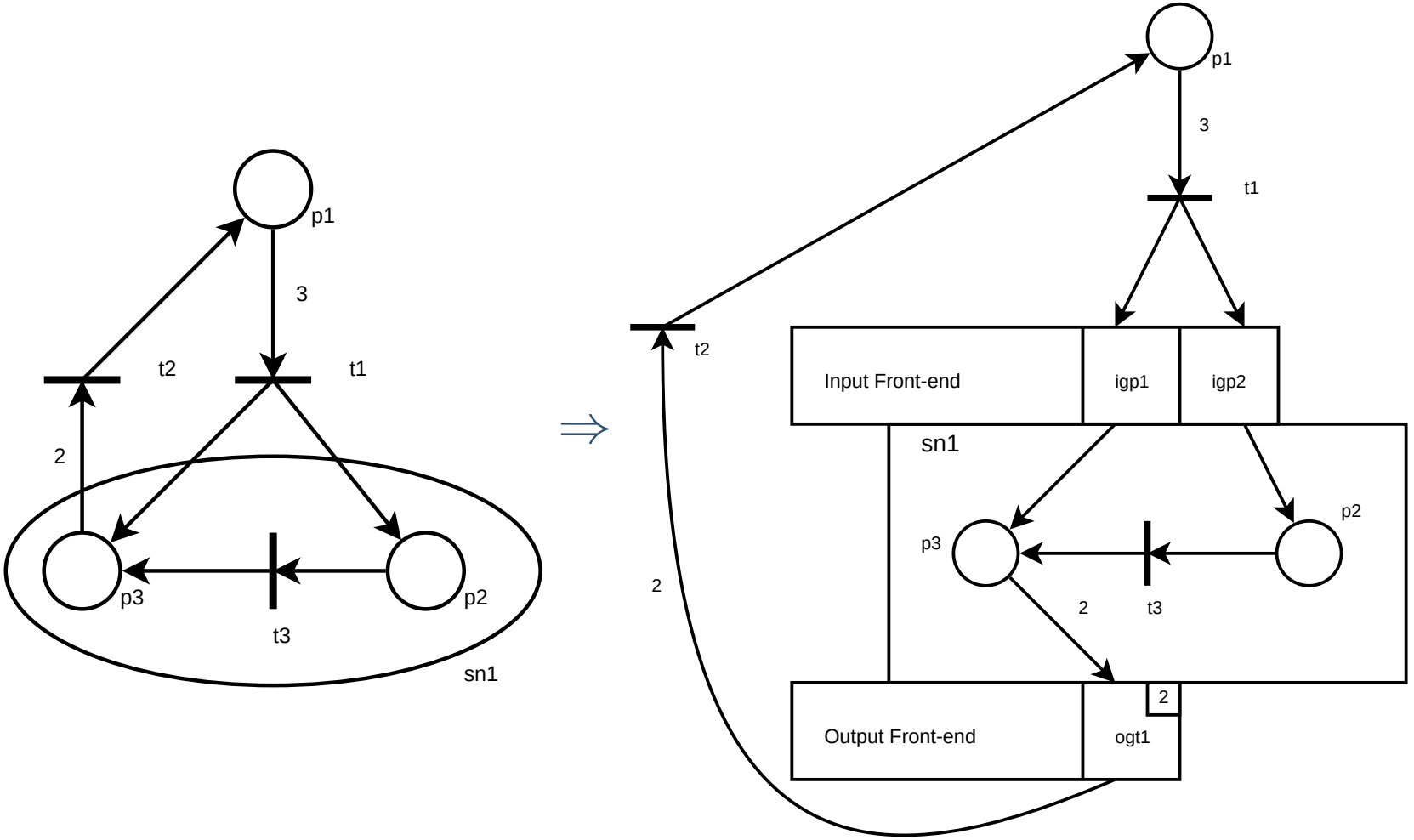
Ejemplo extensión PNML

Ejemplo:



Ejemplo extensión PNML

Ejemplo:



Ejemplo extensión PNML


```
<subnet id="sn1">
  <interface id="sn1-interface">
    <gate id="igp1" action="input" type="place
          "/>
    <gate id="igp2" action="input" type="place
          "/>
    <gate id="ogt1" action="output" type="
          transition">
      <inscription>
        <text> 2 </text>
      </inscription>
    </gate>
  </interface>
  <content id="sn1-content">
    <place id="p2"/>
    <place id="p3"/>
    <transition id="t3"/>
    <arc id="sn1-a2" source="igp2" target="p2"
          />
    <arc id="sn1-a3" source="igp1" target="p3"
          />
    <arc id="sn1-a4" source="p3" target="ogt1"
          >
      <inscription>
        <text> 2 </text>
      </inscription>
    </arc>
    <arc id="a5" source="t3" target="p3"/>
    <arc id="a6" source="p2" target="t3"/>
  </content>
</subnet>
<place id="p1"/>
<transition id="t1"/>
<transition id="t2"/>
<arc id="a1" source="p1" target="t1">
  <inscription>
    <text> 3 </text>
  </inscription>
</arc>
<arc id="a2" source="t1" target="igp2"/>
<arc id="a3" source="t1" target="igp1"/>
<arc id="a4" source="ogt1" target="t2">
  <inscription>
    <text> 2 </text>
  </inscription>
</arc>
<arc id="a7" source="t2" target="p1"/>
```

Seguridad en redes de Petri

Seguridad

- **Privacidad**. Determinadas partes de la red deben ser ocultadas: el contenido es secreto, por lo que no todo el mundo debería poder conocerlo.

Seguridad

- **Privacidad**. Determinadas partes de la red deben ser ocultadas: el contenido es secreto, por lo que no todo el mundo debería poder conocerlo.
- **Integridad**. Cualquier cambio en las partes securizadas debe ser detectado. Si cualquiera de estas partes sufre cualquier tipo de modificación, la información puede haberse visto comprometida y quizá no sea válida o correcta. Pero no podemos saber lo que se ha cambiado: sólo podemos detectar que el original ha sido alterado.

Seguridad

- **Privacidad**. Determinadas partes de la red deben ser ocultadas: el contenido es secreto, por lo que no todo el mundo debería poder conocerlo.
- **Integridad**. Cualquier cambio en las partes securizadas debe ser detectado. Si cualquiera de estas partes sufre cualquier tipo de modificación, la información puede haberse visto comprometida y quizá no sea válida o correcta. Pero no podemos saber lo que se ha cambiado: sólo podemos detectar que el original ha sido alterado.
- **Autenticación**. Puedo autenticar el origen de la red/subred (firmador, autor o validador).

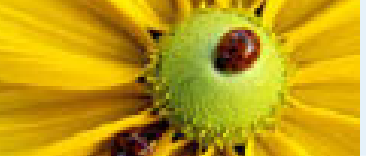
Seguridad

- **Privacidad**. Determinadas partes de la red deben ser ocultadas: el contenido es secreto, por lo que no todo el mundo debería poder conocerlo.
- **Integridad**. Cualquier cambio en las partes securizadas debe ser detectado. Si cualquiera de estas partes sufre cualquier tipo de modificación, la información puede haberse visto comprometida y quizá no sea válida o correcta. Pero no podemos saber lo que se ha cambiado: sólo podemos detectar que el original ha sido alterado.
- **Autenticación**. Puedo autenticar el origen de la red/subred (firmador, autor o validador).
- **No repudio**. Con esta característica, se evita la posibilidad de suplantar a otra persona es evitada. Por tanto, aquel que firma una parte no puede decir que no lo ha hecho: el firmante no puede negar que lo es.

Selección de subredes: XPath

Podemos aplicar seguridad a:

- La red de Petri entera
- Sólo a determinadas partes de ella



Selección de subredes: XPath

Podemos aplicar seguridad a:

- La red de Petri entera
- Sólo a determinadas partes de ella

La manera estándar es el uso de expresiones XPath, que devuelve el conjunto de nodos xml que tienen que ser procesados (cifrados o firmados). Por ejemplo:

- '/' - Indica la red completa, el nodo raíz
- '`/pnml/net/page/subnet[@id="sn1"]`' - Indica que sólo debe procesarse la subred con id=”sn1”
- '`/pnml/net/page/subnet`' - Indica que deben procesarse todas las subredes

XMLEncryption

XMLEncryption asegura la privacidad:

```
<content id="sn1-content">
  <place id="p2"/>
  <place id="p3"/>
  <transition id="t3"/>
  <arc id="sn1-a2" source="igp2" target="p2"/>
  <arc id="sn1-a3" source="igp1" target="p3"/>
  <arc id="sn1-a4" source="p3" target="ogt1">
    <inscription>
      <text> 2 </text>
    </inscription>
  </arc>
  <arc id="a5" source="t3" target="p3"/>
  <arc id="a6" source="p2" target="t3"/>
</content>
```

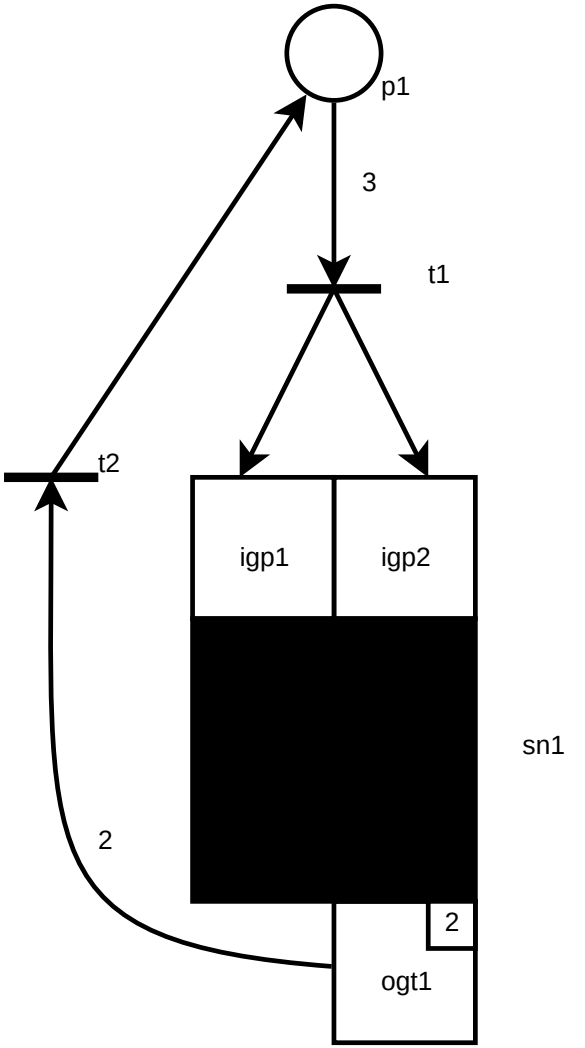
XMLEncryption


```
<content id="sn1-content">
 <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
   Type="http://www.w3.org/2001/04/xmlenc#Element">
  <xenc:EncryptionMethod
     Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"
     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" />
  <xenc:CipherData
     xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
   <xenc:CipherValue
      xmlns:xenc="http://www.w3.org/2001/04/xmlenc#">
       Wr1njyJlYYOM9lAYqcwGCWkw2L4pUjQD2GGVoU9lVZOwKqHY8y3lGY8FY4i5K
       AGY8FY4i5K3G8grIe1HRFqe7RtkFiXZgGMeYnQp6oB6ckKp3KFKHVqtucc9rA
       VzOgC7XAwe61HRFqe6RRVzXjNM9hlVZOwKqHY8y3l3GY8FY4i5K3G8grIe2xN
       xfw17hoYCUdwkzM12iiBJaKQcZcAALcLX2RTF9McAJOElonRrNdUgi9SCBz5Z
       kPdQCFJaGFAoKYmDZF9OjTBQ4qf9FVf8OsUXSxqRnXUeUZEB7rhgVY68gyCp4
       TGPZOWz/Yb7Sbq1pNiG6wqNbsepKWG9EV6n9rjSfiOocvy9wL8m1I0HmAp2l4
       RRVzXjNMLU5ZgGMeYny8NVPQmUSDX7NRtnR6YnQp6oB6GY8F=
   </xenc:CipherValue>
  </xenc:CipherData>
 </xenc:EncryptedData>
</content>
```

XMLEncryption

Se permite la sustitución de una red cifrada por otra:

- Quitar la subred a eliminar del código fuente xml
- Insertar la nueva red cifrada en el código xml
- Modificar los id de los arcos que entran o salan para hacerlos coincidir con el nuevo nombre de las puertas



XMLSignature

- XMLSignature provee los servicios de **integridad, autenticación y no repudio**.

XMLSignature

- XMLSignature provee los servicios de **integridad, autenticación y no repudio**.
- La firma digital se anexa en el documento con datos para la correcta verificación de la misma

XMLSignature


```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#
              WithComments"/>
        <ds:Transform Algorithm="http://www.w3.org/2002/06/xmldsig-filter2">
          <dsig-xpath:XPath xmlns:dsig-xpath="http://www.w3.org/2002/06/xmldsig-filter2"
                Filter="intersect">
            /pnml/net/page/subnet[@id="sn1"]
          </dsig-xpath:XPath>
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>prCzhLgTCZ1ck6MjQnFy6cASCZw=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    QoO7mQmGBFTg2UxgiZnzlsnKi8V477JC0v12JPItL53zIOCpjhOwLoyxENl6v8lCLoJ9WwFHlBKk
    r3GdqrgZimNXMUjwR4zkd9FVNcIrn85DuRjHAazDwSuPMq9w0N5A07c0xJ24uvn9zzpbQxfblYTb
    kiy08+S0pqczUfbv52g=
  </ds:SignatureValue>

  ..........
```

XMLSignature


```
.....
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509Certificate>
      MIICgTCCAeqgAwIBAgIETfh4CTANBgkqhkiG9w0BAQUFADCBhDELMAkGA1UEBhMCRVMxETAPBgNV
      BAgTCExBIFJJT0pBMREwDwYDVQQHDAhMT0dST8KlTzEgMB4GA1UEChMXVU5JVkVSU0lEQUQgREUg
      TEEgUklPSkExDDAKBgNVBAsTA1BGQzEfMB0GA1UEAwwWScKlSUdPIExFw6BOIFNBTUFOSUVHTzAe
      Fw0xMTA2MTUwOTE0NDlaFw0xMTA5MTMwOTE0NDlaMIGEMQswCQYDVQQGEwJFUzERMA8GA1UECBMI
      TEEgUklPSkExETAPBgNVBAcMCExPR1JPwqVPMSAwHgYDVQQKExdVTklWRVJTSURBRCBERSBMQSBS
      SU9KQTEMMAoGA1UECxMDUEZDMR8wHQYDVQQDDBZJwqVJRO8gTEXDoE4gUOFNQU5JRUdPMIGfMA0G
      CSqGSIb3DQEBAQUAA4GNADCBiQKBgQChePFNVCIfphFlyXQ9BysiR5BfXIuv3AnAK8OFuw4tTFwC
      nVUjJeGnkUYQO32oUuffEBK8WsEqjeH8A7zrHTRQjfYZWyuGWrM8gJXOa5POMROPm7c3H8b5a6Nx
      Fc2zLwR0tYkqLI2xqDOFII2RwK5L2yGeV4T4y8i3h1UOOFTSEwIDAQABMA0GCSqGSIb3DQEBBQUA
      A4GBAIDOvAAdOCaTpya83bGB2KmngMJrNxxWDpAi5LGFrN8iCShmbTpIeIbYBUAaBpZtdhOnhq4n
      wD5QOENSFipQcdH5GEpPM9Rquy6xMwfda9EU5UfOSEmbk4fK2vaIOVjynpQsJ9P99enO2smQlyvw
      DhBa7Xacz6qDut8ghUeuV5Js
    </ds:X509Certificate>
  </ds:X509Data>
  <ds:KeyValue>
    <ds:RSAKeyValue>
      <ds:Modulus>
        oXjxTVQiH6YRZcl0PQcrIkeQX1yLr9wJwCvNBbsOLUxcAp1VIyXhp5FGEDt9qFLvnxASvFrBKo3h
        sAO86x00UI32GVsrhlqzPICVzmvz9DETj5v3Px4GdWujcdfasy8EdLWJKiyNsagzhSCNkcCuS9sh
        nleE8MvIt4dVNDhU0hM=
      </ds:Modulus>
      <ds:Exponent>AQAB</ds:Exponent>
    </ds:RSAKeyValue>
  </ds:KeyValue>
</ds:KeyInfo>
</ds:Signature>
```

Seguridad integral

Aspectos a tener en cuenta

- XMLEncryption **sustituía** el contenido en claro por el contenido cifrado. Sin embargo, XMLSignature **adjunta** información adicional con datos de la firma. Esto permite tener varias firmas sobre el mismo contenido.

Seguridad integral

Aspectos a tener en cuenta

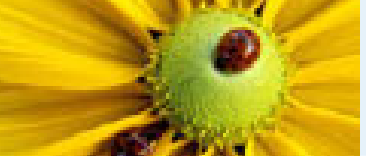
- XMLEncryption **sustituía** el contenido en claro por el contenido cifrado. Sin embargo, XMLSignature **adjunta** información adicional con datos de la firma. Esto permite tener varias firmas sobre el mismo contenido.
- En XMLEncryption se puede sustituir una subred por otra con el mismo front-end. Sin embargo, esto no es posible si la subred está firmada con XMLSignature ya que detectaría cambios

Seguridad integral

Aspectos a tener en cuenta

- XMLEncryption **sustituía** el contenido en claro por el contenido cifrado. Sin embargo, XMLSignature **adjunta** información adicional con datos de la firma. Esto permite tener varias firmas sobre el mismo contenido.
- En XMLEncryption se puede sustituir una subred por otra con el mismo front-end. Sin embargo, esto no es posible si la subred está firmada con XMLSignature ya que detectaría cambios
- En el caso de subredes firmadas y cifradas, el orden en el que se aplican estas técnicas es importante y depende de lo que quiera el gestor.

Conclusiones



Conclusiones

He desarrollado un método exhaustivo para definir subredes con interfaces. La interacción entre estas subredes y el resto de la red se realiza siempre a través de sus front-ends. El método de representación elegido ha sido PNML. Una vez realizado esto, la conclusión de este trabajo es mostrar que es posible aplicar medidas de seguridad a redes de Petri para ampliar en 4 características adicionales a estas redes (o subredes):

- Privacidad: no todos pueden acceder a algunos datos
- Integridad: se detectan cambios no permitidos
- Autenticacion: asegura la autoría de alguna información
- No repudio: una persona no puede suplantar a otra

Con XMLEncryption conseguimos privacidad. Integridad, autenticación y no repudio se obtienen con XMLSignature

Publicaciones

Artículos en Congresos Internacionales

- EMSS Roma 2011. Security and Protection in Petri Nets sending and storage. Signing and Encryption.
- EMSS Atenas 2013. Analysis of information partial encryption options for exchanging Petri Nets systems
- EMSS Burdeos 2014. Petri net representation with ciphered subnets: definition of PNML extensions for subnets representation and use of XMLEncryption for ciphering.
- EMSS Bergeggi 2015. Validation and approval of Petri Net ciphered subnets: security in Petri Nets sharing and storage using PNML, XMLSecurity and XMLSignature

Premios

- Premio al mejor estudiante de doctorado en el EMSS Burdeos 2014

Artículos enviados a revistas

- Journal of Computation Science. Security and Protection in Petri Nets sending and storage. Signing and Encryption
- Simulation, modelling practice and theory. Validation and approval of Petri Net ciphered subnets: security in Petri Nets sharing and storage using PNML, XMLSecurity and XMLSignature

Gracias por su atención