Why Johnny can't afford Security Policies

Fabio Massacci

University of Trento

Work partly supported by

ANIKETOS

NESSOS

secure CHANGE

Seven Degrees of Separation

2002-
2009

1. Academic at University
2. Researcher in Industry
3. Member of Production Group
4. Marketing Salesman
5. Maintenance scapegoat
6. Customer's IT Technician
7. Responsible for Business Unit

- "The Customer" who shells the money

In 2002-2009 I was parachuted Deputy Rector for ICT Procurements. 3M€++ budget and 70+ people

What My “Customer” really wanted

DB - Chairman

I want a more flexible system: each member of staff should easily see and manage his funds

MT - CEO

I know what he said but this year…
there’s a budget cut of 3%.
You already spent 1.5M€ on the MAN.
Max 350K€ for ERP extra add-ons

GM - COO

Our staff is already committed to meet this year’s objectives.
I can only give you one person part-time to identify business requirements.

POLICY people says: All you need is …. Expressivity

"We make the point for the need of more expressive policy languages."

Samarati expressive OR flexible OR general OR extensible = 220

--ALL of them = 38

"The proposed language must be powerful enough to specify any relevant event of a security policy and cover several layers of abstraction."

Pretschner +OR= 34

--ALL = 11

"A more elegant and flexible approach is to express policies in logic that handles…"

Kephart +OR= 16

--ALL = 6

What does Expressivity Mean?

We need constraints about ROLE in the organization and the TIME of access.

You must consider Invoked SERVICES

Don't forget LOCATION

with TRUST level and CREDENTIALS.

and USAGE!

What about "best" moment to have sex?

SAMSUNG

US Patent 11/480858
from 07/06/2006

What Expressivity Actually Means

- Complex rules do define roles and complex criteria to dynamically assign users to them based on
  1. Role → too many citations
  2. Time of the day → 39.800 citations

     "The **time**-**based** constraint limits the **policy** to apply between 4:00pm and 6:00pm"
  3. Location → 27.300 citations
  4. Organization → 15.600 citations
  5. Task in the workflow → 12.200 citations
  6. Usage after access → 7.300 citations
  7. Credential submitted → 1.400 citations

  – …

  N Best moment to have sex… → 1 patent … for the moment…

How many people are needed to set up an “expressive” policy for a user?

- At least 6
  - Responsible for HR (sub)Unit costs 80€/h
    - Assistant who knows potential salary implications 54€/h
  - Responsible for Business (sub)Unit costs 80€/h
    - Assistant who knows how things really works 54€/h
  - IT Project Leader costs 70€/h
    - Assistant who knows what’s really possible 54€/h
- And they would need at least 30’ per user
  - (5’ x ROLE, SERVICE, TIME, CREDENTIAL, TRUST, LOCATION, USAGE, ETC)
- Minimum Policy Set-up Cost = 192€/user

The buck doesn't stop there yet…

- They (ADOBE, IBM, ORACLE, SAP, etc.) are going to bill you by the role…
  - The more complex the role, the more you pay
    - "Price is determined by what is managed rather than the number and type of product components installed […]
    - "Products may manage clients, client devices, agents, network nodes, **users**, or other items, and are licensed and priced accordingly."
  - 3.800€/role for powerful roles across ERP modules
  - 400€/user for "employee" (can do almost nothing)
  - 17-25% maintenance fee on licenses
- What this actually mean?
  - 13 Heads of Departments + 8 Head of Division
  - 1.500 Employees

The Problem is… POLICY Researchers have forgotten… Arithmetics!

Is this a joke? 80.000€ for licenses alone and just for access of Heads of Dept and between 600.000 € and 1.000.000 € for the rest? *Plus 250K Every year*?!? And software's aside!

MT Now DG at Ministry

GM Now CEO

What? Do you want 300.000€ in human resources and this just for setting up the draft of a security policy? *FIVE* people?!

I see: either I buy your expressive security policy or I hire 20 new associate professors…that's a new Department! But I see *a third option*… for you…

DB Still Chairman

FM Ex-Deputy

I understand everything but why couldn't you just give them a flexible system?