Attribute Based Access Control
Jacoba Sieders - ABNAMRO
SLIDE FROM 2014: PREDICTIONS ON CONNECTIVITY

Connectivity across
ID federations
Datasets
Applications
Value chains
Companies
Continents
Jurisdictions
Platforms
Devices
Clouds
Things
Services
BaaS = Back-end as a Service

2017: API’s
API’s and de-perimeterization are daily business
SLIDE FROM 2014: PREDICTIONS ON BIG DATA

- Visual data discovery
- Automated decision-making
- 70% of large organizations purchase external data
- 100% by 2019. (Forbes)
- 180,000 data analysts US 2018

2017:
- Artificial intelligence
- Predictive analytics
- Machine learning
- Data driven everything
Purpose of digital data changed: information and operations & decisions
Population of digital users changed

Expert engineers..
Your grandma
Your toddler
Your malware
Your fridge
Roles of digital users

- My ID
- Customer
- Supplier
- Partner
- Private user
- Administrator
- Anonymous user
- Device
- Fraudster, mule
- Process
- Session
- IoT becoming "agent" on behalf of user
- Federated ID
Identity Lifecycle: more lifecycle states

from “JoMoLea”

Client

Contact date  Onboarding date  Date of death

Prospect  Client  Married  Children  Divorced  Retired  Heir

Contact date  Onboarding date  Date of marriage  Birthday(s)  Date of divorce  Retirement date  Date of death

ABN AMRO
Trends in IAM Relationship models; more relationship types

From identities to identity relationships

- **Entity**
  - **Prospect**
  - **Client**
    - **In good standing**
    - **Suspended**
  - **Refrigerator**

**Relationship type**

**Status Relationship type**

**Group/role**

**Other attributes**

- **IP-address**
- **Account number**
- **Geolocation**

**Personas**

- **Defaulter**
- **Shop owner**
- **Private client**
- **Delegate**

**Other attributes**

- **Defaulter**
- **Shop owner**
- **Private client**
- **Delegate**

**Group/role**

- **IP-address**
- **Account number**
- **Geolocation**

**Other attributes**

- **Defaulter**
- **Shop owner**
- **Private client**
- **Delegate**

**Group/role**

- **IP-address**
- **Account number**
- **Geolocation**

**Other attributes**

- **Defaulter**
- **Shop owner**
- **Private client**
- **Delegate**
Identity Analytics

Access requests should no longer be a la carte, **but user context aware** (ala Amazon or bol.com). Data mining patterns should **reveal similar users** with similar attributes and access, allowing for easy detection of access profiles, and suggested if not automated repair of anomalies.

Identity governance should respond to **user behaviour** (24x7), based on IAM data.

Need for:

- Data mining/clustering (the ability to detect identical users)
- Weighted search (access request should be filtered based on patterns of the previous requests)
- (semi) Automated repair (removal of anomalous access)
Digital Identity Links

- Chris Smith / 187654000000
- Clyde Noble / 528436000000

Data Types:
- Digital Identity
- authorizedFor
- authorizedFor-authorized DI
- authorizedFor-object DI
- ownsRelations
- ownsRelations-authorized DI
- ownsRelations-object DI

- Chris Smith / 187654000000
- parent2 / parent
- Billy Smith / 765432000000
- authorized / authorized
- authorized4 / authorized
- Noble Accountancy / 901685985208
- Clyde Noble / 528436000000
- Chris Smith / 187654000000
Conclusion “Seven any” all relevant for access decisions
ABAC building blocks

Trust level classification framework

- Attributes
- Trust Levels
- Devices Authentication means
- Principles
- Rules / Algorithms

Trust level classification model elements

Rule sets and policies

Interaction framework and governance on multiple rulesets with different owners:
- Rules should not clash

- Fine-grained, data-centric
- Context aware, rule based
- Real time access decisions
- Flex degrees of authentication
- Flex degrees of authorisation
- Trustlevel mapping
Fine-grained context aware access management - building blocks

- data classifier
- token management system
- session integrator
- connectors and interfaces

PDP - Policy Decision Points
PAP - Policy Administration Points
PIP - Policy Information Points
PEP - Policy Enforcement Points

XACML

Attributes:
- data quality
- data management
- Meta data

Rules:
- ownership in the business maintenance

- ABN-AMRO
Query-based Policy Enforcement Point
Format Preserving Encryption

1. Request Access
2. Request Access Decision
3. Retrieve Authorization Policies
4. Retrieve Attribute Values
5. Determine Access Decision
6. Provide Access Decision
7. Grant or Deny Access + Encrypt / Decrypt
8. Access Granted

PEP
PDP
PAP
PIP
Traditional preventative/detective/reactive controls + analytics

Security Operations Centre

Identity & Access Management

Fraud Detection

Business Continuity Management

Full situational awareness through merger of the control landscape

Instruction / Request

Transaction

(Payment settlement)

Wish

start

Infra: Device, network, etc.
ABAC features

- Context aware
- Rule based
- Fine-grained access decisions
- Step-up authentication (or step **down authorisation**)
- More flexible than Role Based Access Control (RBAC)
- Less rules hard-coded within applications
- Configuration within IAM tools: short time-to-market of new business rules
- Trustlevel on dataset or transaction
- Trustlevel on transaction request context
- Trustlevel framework enables immediate intervention if compromised
- Implementation: gradually evolve from RBAC to ABAC
- Most feasible: hybrid model serving both
  - (a role is also a rule and some access rules always remain fixed)
- Focus on **governance** and **business involvement** is crucial
### Summary

#### “Digitisation”:
- Data for information, operations, (automated) decisions
- Connectivity
- Deperimeterization
- Hybrid cloud
- Paas, Saas, laas, BaaS
- API’s
- Real time data retrieval
- Any device, time, network, user, transaction
- Micro services
- Automated decision making
- Artificial intelligence, machine learning,
- Predictive analytics

#### Identity & Access Management:
- Increasing importance of digital identity
- “Fine grained Identity”
- Rule based access decisions
- Flexible authentication
- Flexible authorisation
- Real time
- Context aware
- Data centric protection

→ For ABAC, focus on:
- (Meta)data quality
- Governance + ownership
- Business risk appetite
- Trust level models
- Hybrid set-up with RBAC?!
Time for questions!

jacoba.sieders@nl.abnamro.com  ABNAMRO Amsterdam +31634150150