MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

ACADÉMIE
MILITAIRE
SAINT-CYR COËTQUIDAN

IRISA

Vers la sécurité dans un environnement opérationnel collaboratif dynamique

Didier Alquié, Nicolas Belloir,
Jérémy Buisson, Lionel Touseau

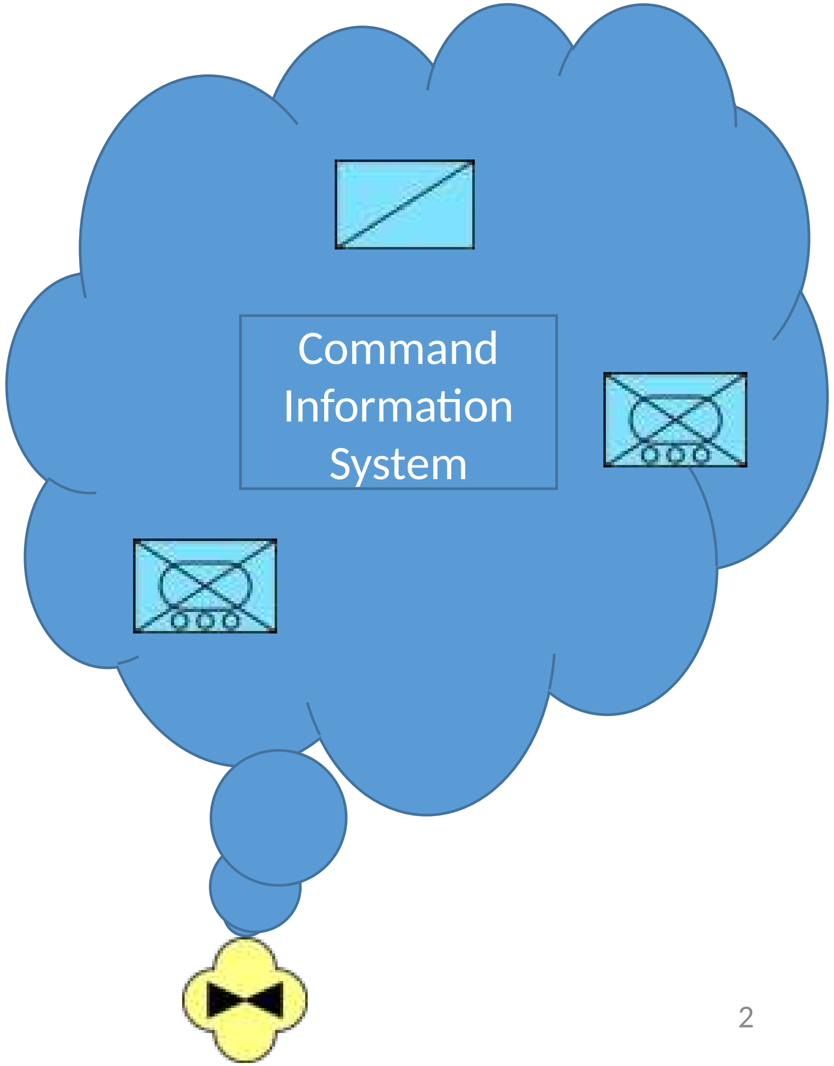
15 novembre 2022

Collaborative systems, collaborative combat

- Field units collectively fulfill a mission

- From network-centric to collaborative
  - Telecommunications for situation awareness
  - Shared tactical picture
  - Distributed network of sensors and effectors

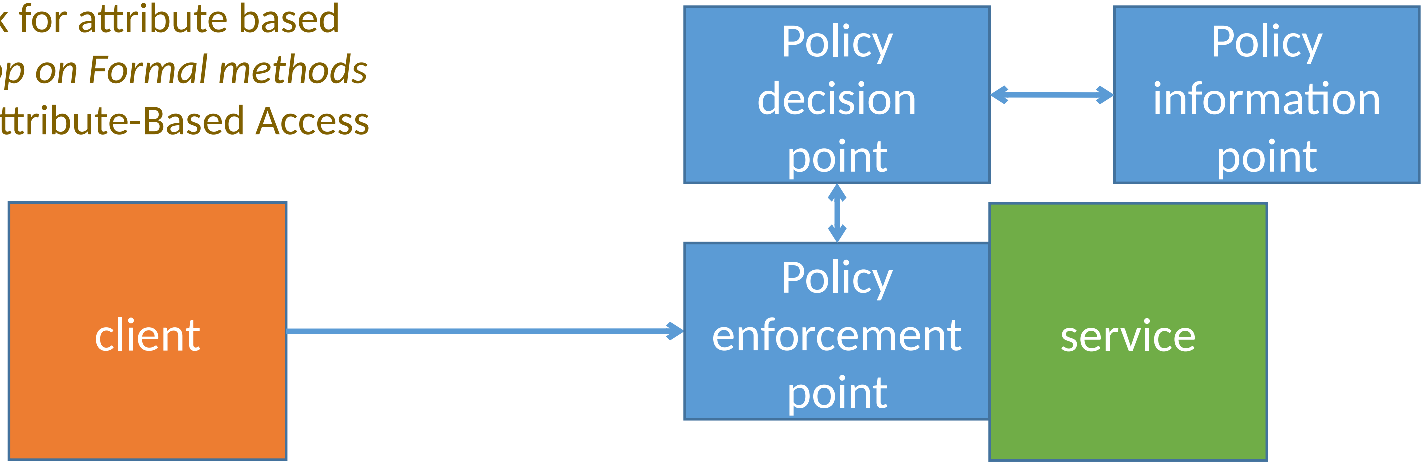
- **Opportunistic** collaboration



Attribute-based access control

- Attributes characterize the subjects and his request's context beyond identity
- A policy computes whether access is granted
  - function of the attributes, evaluated by a policy decision point

Wang, Wijesekera, and Jajodia, “A logic-based framework for attribute based access control,” in *Proceedings of the 2004 ACM workshop on Formal methods in security engineering*. Hu, Kuhn, Ferraiolo, and Voas, “Attribute-Based Access Control,” *Computer*, vol. 48, no. 2, Feb. 2015



Attribute-based encryption

- Asymmetric encryption
  - One public key used to encrypt
  - Several private keys

- Attributes characterizes the context, beyond identity
- A policy matches what subsets of attributes are allowed to decrypt
  - Immune to pooling several private keys

- May be used to control reading access, similarly to ABAC

Attribute-based encryption

Key Policy ABE

- Attributes are embedded in the ciphertext, encrypted using the public key
- Private keys embed the policy
  - Only private keys whose policy accepts the set of attributes embedded in the ciphertext can decrypt
- A key issuer holds a secret master key, used to derive the public key and private keys
  - Enforces the decryption policies

Goyal, Pandey, Sahai, and Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in *13th ACM conference on Computer and communications security*.

Ciphertext Policy ABE

- The policy is embedded in the ciphertext, encrypted using the public key
- Private keys encode sets of attributes
  - Only private keys whose set matches the policy embedded in the ciphertext can decrypt
- A key issuer holds a secret master key, used to derive the public key and private keys
  - Certifies the possession of attributes

Bethencourt, Sahai, and Waters, “Ciphertext-Policy Attribute-Based Encryption,” in *2007 IEEE Symposium on Security and Privacy (SP ’07)*.

Additional features with (CP) ABE

- Proxy re-encryption
  - ✉ Revocation

Yu, Wang, Ren, and Lou, "Attribute based data sharing with attribute revocation," in 5th ACM Symposium on Information, Computer and Communications Security.

- Valued attributes

Li, Yu, Liu, Feng, Qin, and Srivastava, "An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things," IEEE Journal of Biomedical and Health Informatics, 2021.

- And other features
  - Large attribute universe, traceability, policy update, multi-authority, etc.

Zhang, Deng, Xu, Sun, Li, and Zheng, "Attribute-based Encryption for Cloud Computing Access Control: A Survey," ACM Computing Survey, vol. 53, no. 4.

Forthcoming research questions

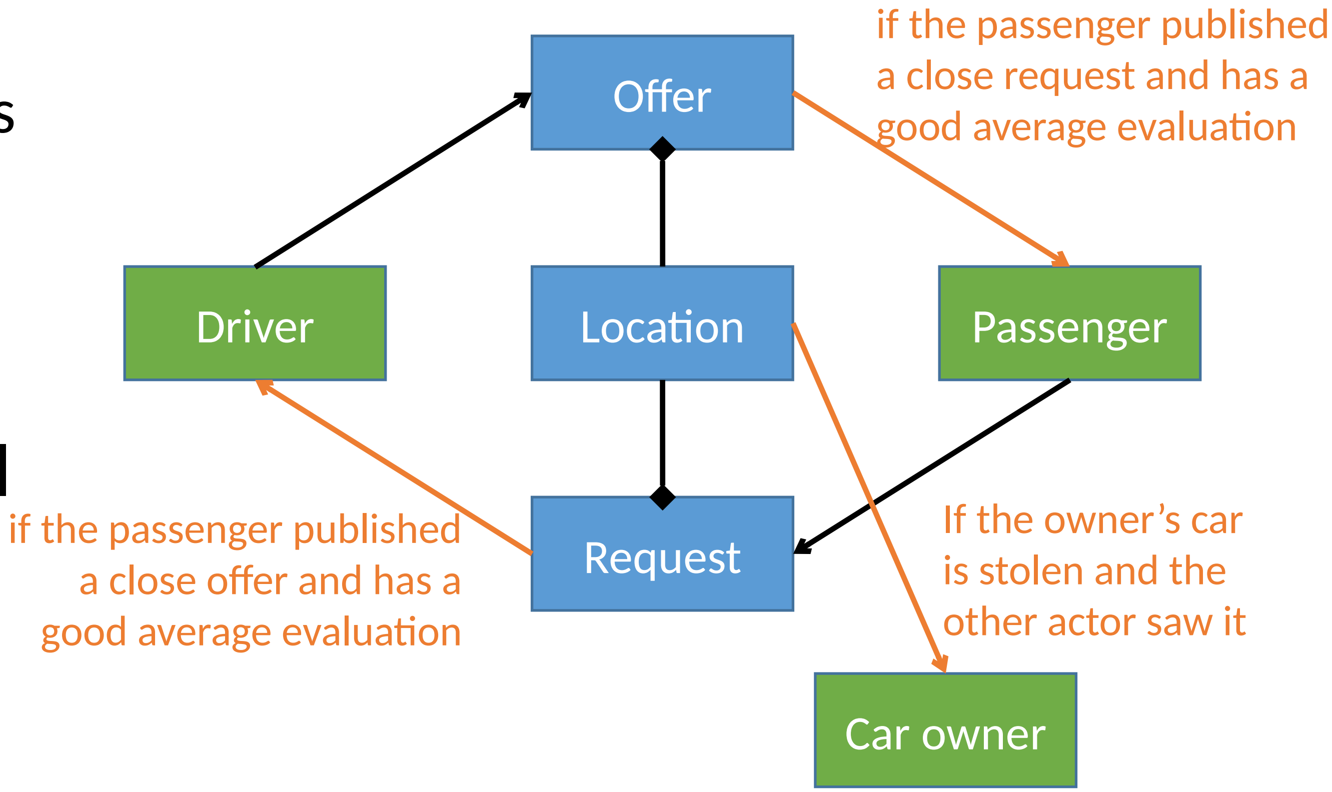
- Is it feasible to use ABE in order to operationally secure collaborative combat?
- How do we model a system architecture secured thanks to ABE?
- How can ABE support dynamic, decentralized, opportunistic collaborations?

Simplified, synthetic scenario

- Data centric architecture
  - Focus on data artifacts
  - Express relations between systems and artifacts
  - Express the attribute-based policy

- Attributes model the operational context

- Urban carpooling system


Offer
if the passenger published a close request and has a good average evaluation
Driver
Location
Passenger
if the passenger published a close offer and has a good average evaluation
Request
If the owner's car is stolen and the other actor saw it
Car owner

Conclusion

- Foundations of the AMSCC-Thales Chair of Cyberdefense's scientific program
  - **Security and data access in collaborative combat**
    - Using of appropriate cryptographic algorithms (stating 2023)
    - Defining security architectures aimed at integrating behavioral aspects into the management of access rights (stating 2024)

    - Dynamic consideration of unplanned entities in the action

- Formal launch of the AMSCC-Thales Chair of Cyberdefense
    - Tomorrow, Wednesday 16 at 3pm, AMSCC booth