CIDre

(**C**ONFIDENTIALITY $\wedge$ **I**NTEGRITY $\wedge$ **D**ISPONIBILITY) || **ré**PARTITION

L. Mé[1]
Ch. Bidan[1], G. Hiet[1], N. Prigent[1], G. Piolle[1], E. Totel[1], F. Tronel[1], V. Viet Triem Tong[1],
E. Anceaume[2], M. Hurfin[3], S. Gambs[3,4], and G. Guette[4]

[1]Supelec, France
[2]IRISA-CNRS, Campus de beaulieu, France
[3]INRIA Rennes Bretagne-Atlantique, France
[4]Université Rennes, France

Group Objectives

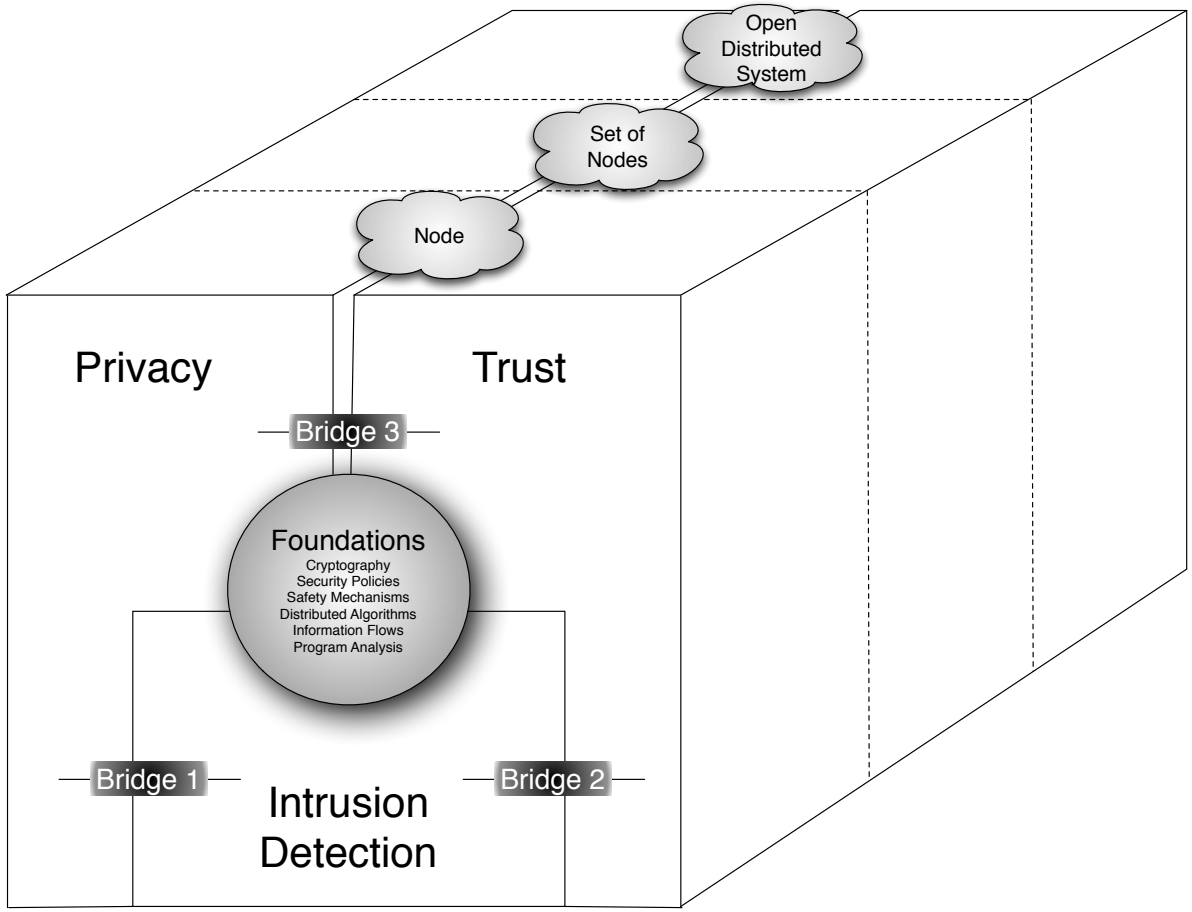
Security vs fault tolerance

- Security: a unique trusted computing base, ideally proved
- Fault tolerance: no single point of failure
- Two seemingly incompatible views:
  - A trusted computing base could become a single point of failure
  - Efficient fault tolerant replications protocols assume non-malicious failures

Our objective: complementarity

Study distributed systems that are trustworthy and respectful of privacy, even if some nodes in the system have been compromised by malicious attackers

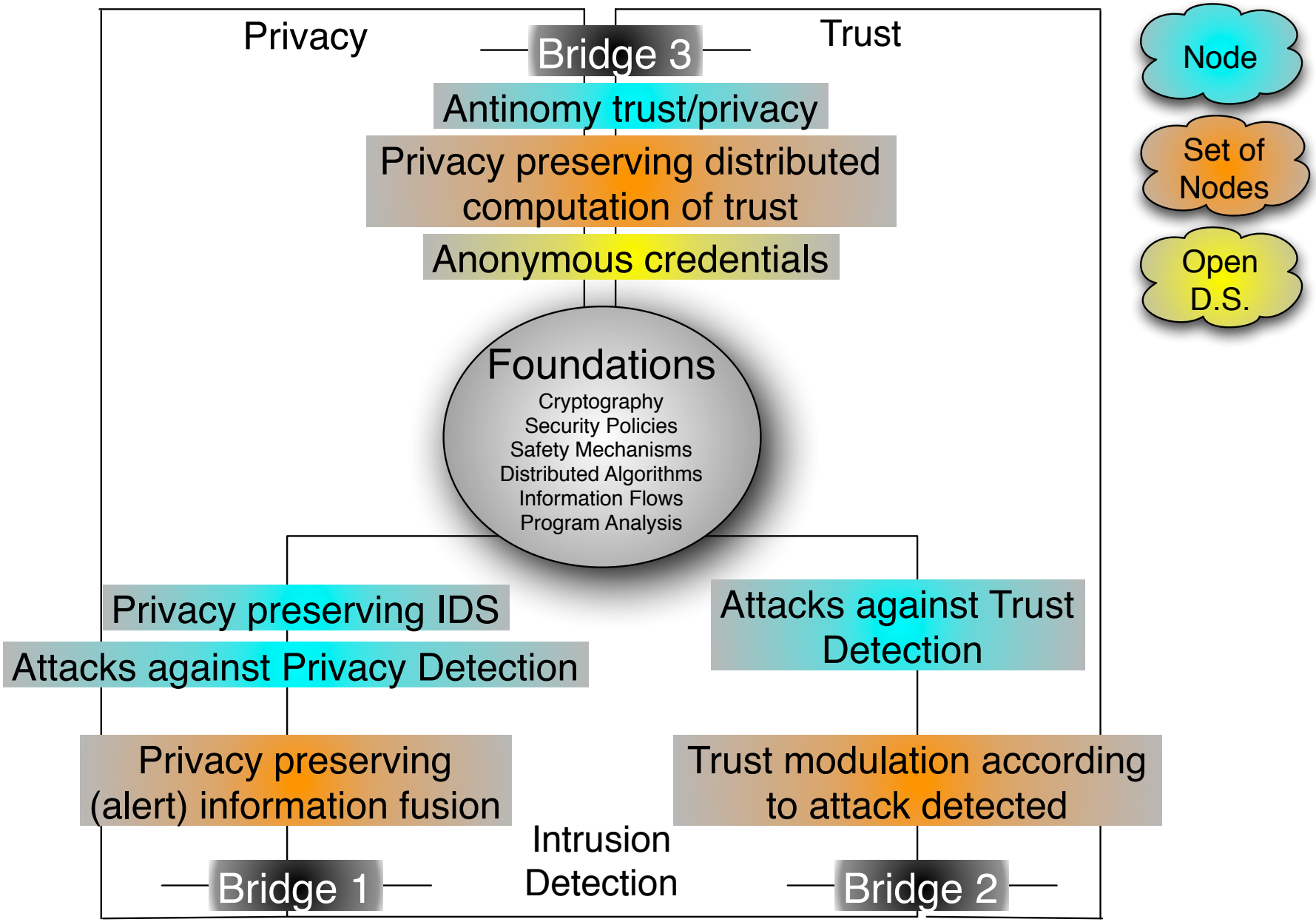
The big picture



(node, set of nodes, Open D.S.) X (privacy, trust, I.D.)

	Privacy	Trust	I.D
Node	privacy preserving identification scheme	1)protocols: from implicit to explicit trust 2)local eval. of trust, impact on the local security policy and its enforcement	1)data corruption detection (automatic defensive programming) 2)information flow I.D.: application to A/V and DBMS
Set of nodes	privacy properties (e.g., anonymity, unlikability, unobservability) for classical distributed algorithms	dynamicity of trust in a group, impact on the security policy of the group	1)distributed information flow detection model (web services) 2)normal distributed behavior (distributed correlation)
Open D.S	1)geoprivacy 2)privacy in social networks	reputation: storage in the overlay, protection against specific attacks, right to oblivion	$\emptyset$

Bridges


Privacy
Bridge 3
Trust
Antinomy trust/privacy
Privacy preserving distributed computation of trust
Anonymous credentials
Foundations
Cryptography
Security Policies
Safety Mechanisms
Distributed Algorithms
Information Flows
Program Analysis
Privacy preserving IDS
Attacks against Privacy Detection
Attacks against Trust Detection
Privacy preserving (alert) information fusion
Trust modulation according to attack detected
Intrusion Detection
Bridge 1
Bridge 2
Node
Set of Nodes
Open D.S.