Sirius

INFORMATION BASED SECURITY

CSIIS

Presented by Nexor

The vision is to provide a more flexible approach to information sharing that will, in the future, match more closely operational imperatives of flexibility and dynamism.

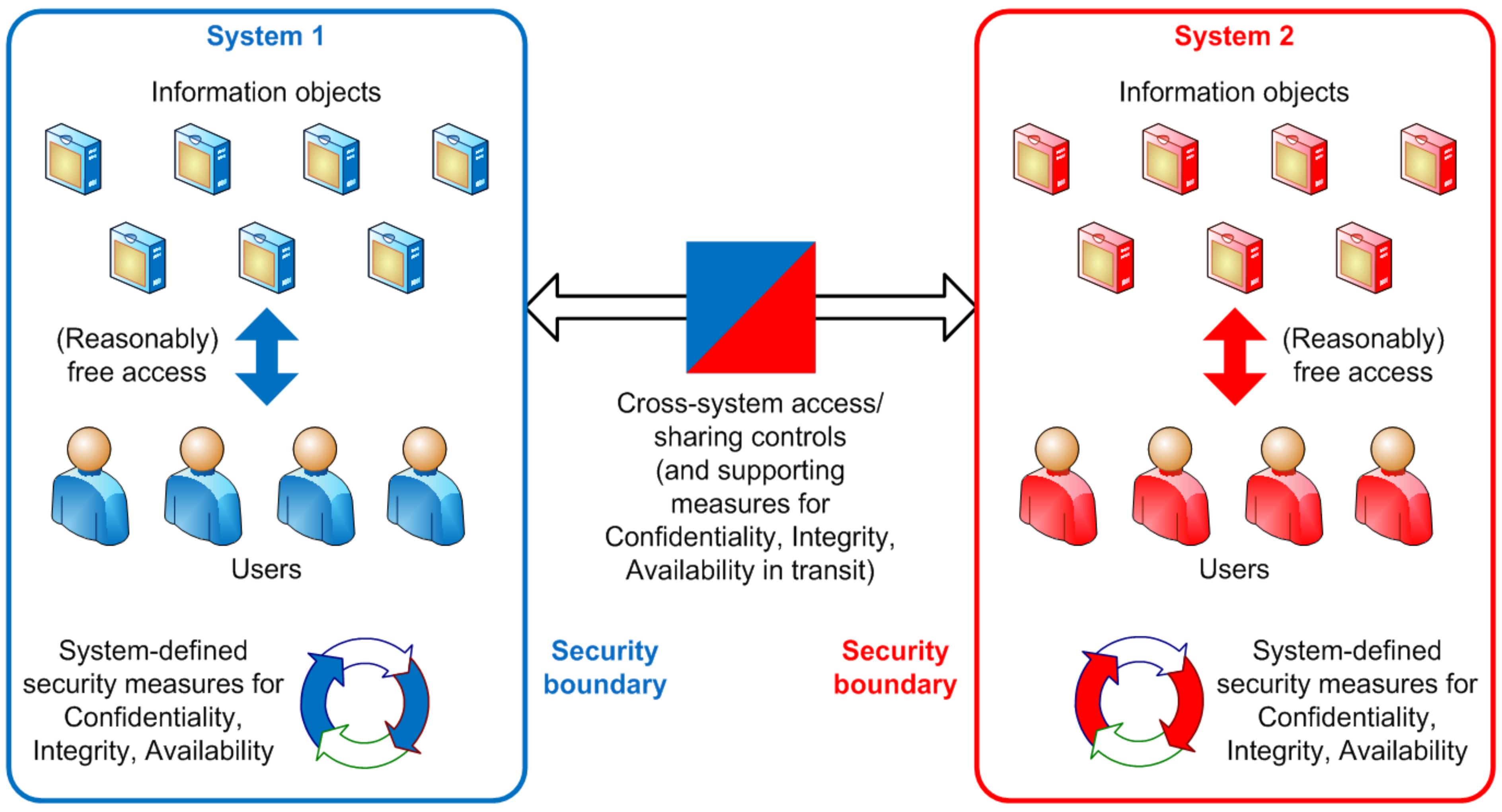
RESEARCH CHALLENGE

Current high assurance security systems are stove piped, with security defined by system boundaries:

- Users cannot share information, reducing effectiveness
- Users find less secure workarounds.

Issues:

- Security properties are managed at the system level, not the individual object level
- Boundary devices too rigid and hard to assure
- Lack of modelling tools for fine-grained trust.



System 1

Information objects

(Reasonably) free access

Users

System-defined security measures for Confidentiality, Integrity, Availability

Cross-system access/ sharing controls (and supporting measures for Confidentiality, Integrity, Availability in transit)

Security boundary

Security boundary

System 2

Information objects

(Reasonably) free access

Users

System-defined security measures for Confidentiality, Integrity, Availability

> "In 2020, enterprise IT departments will not own the device, and in the case of cloud-based services, they may or may not control the network, server, OS or application the end user is consuming.
> In 2020, what is left that IT actually still can directly control? The answer is the information itself."
>
> **Gartner 2013**

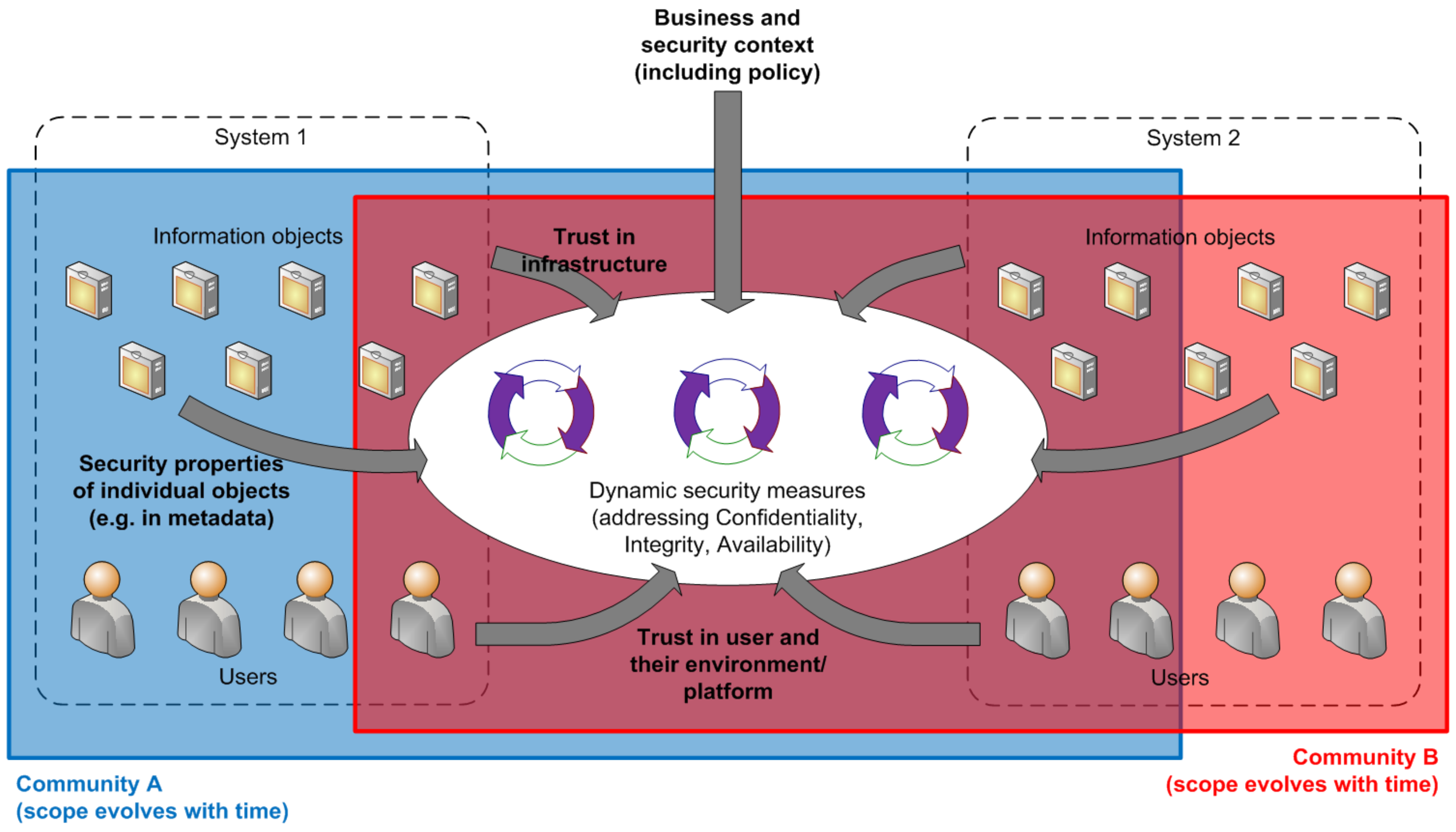
LONG TERM GOAL

Business communities that are not constrained to system boundaries:

- Security measures at rest / in transit / in processing
- Security measures determined and enforced dynamically, based on multiple inputs.

Challenges to address:

- Understanding trust relationships
- Assurance
- Maintaining association between information and security properties.



Business and security context (including policy)

System 1

Information objects

Trust in infrastructure

Security properties of individual objects (e.g. in metadata)

Dynamic security measures (addressing Confidentiality, Integrity, Availability)

Users

Trust in user and their environment/ platform

System 2

Information objects

Users

Community A (scope evolves with time)

Community B (scope evolves with time)

PROJECT OUTCOMES

Scoping study to determine how an Information Based Security paradigm could be applied and recommend future activities to enable realisation.

- Analysis of a set of real-life scenario
- New trust and modelling techniques
- Information and engineering perspectives
- Recommendation to move to a capability demonstration.

This project was funded by MoD(Dstl) via the QinetiQ-led CSIIS industry team (Sirius) and delivered by Airbus Defence and Space, BAES, HW Comms, Nexor, QinetiQ and Thales.

http://nxr.co/csiis

The approach will support intelligent and fine-grained protection for information at rest; information being processed; and information in transit.

IAAC Sponsors

Registered Number 04326237