# Unified Access Control for Surgical Robotics

Ryan Shah and Shishir Nagaraja

University of Strathclyde Science

## Abstract

Ensuring the accuracy of output of surgical robotics is vital, as an incision (during surgery) that is too deep could result in the death of the patient. A large contribution to the level of accuracy of components comes from its calibration. Calibration ensures the output is of high accuracy and is traceable to antecedent calibration units up to national standards. However, each of the levels in the calibration hierarchy have different security requirements (confidentiality and integrity), who may also be in conflict with each other. We propose a hybrid access control model for surgical robotics that maintains integrity and confidentiality requirements across a lattice structure and manages conflicts of interests.

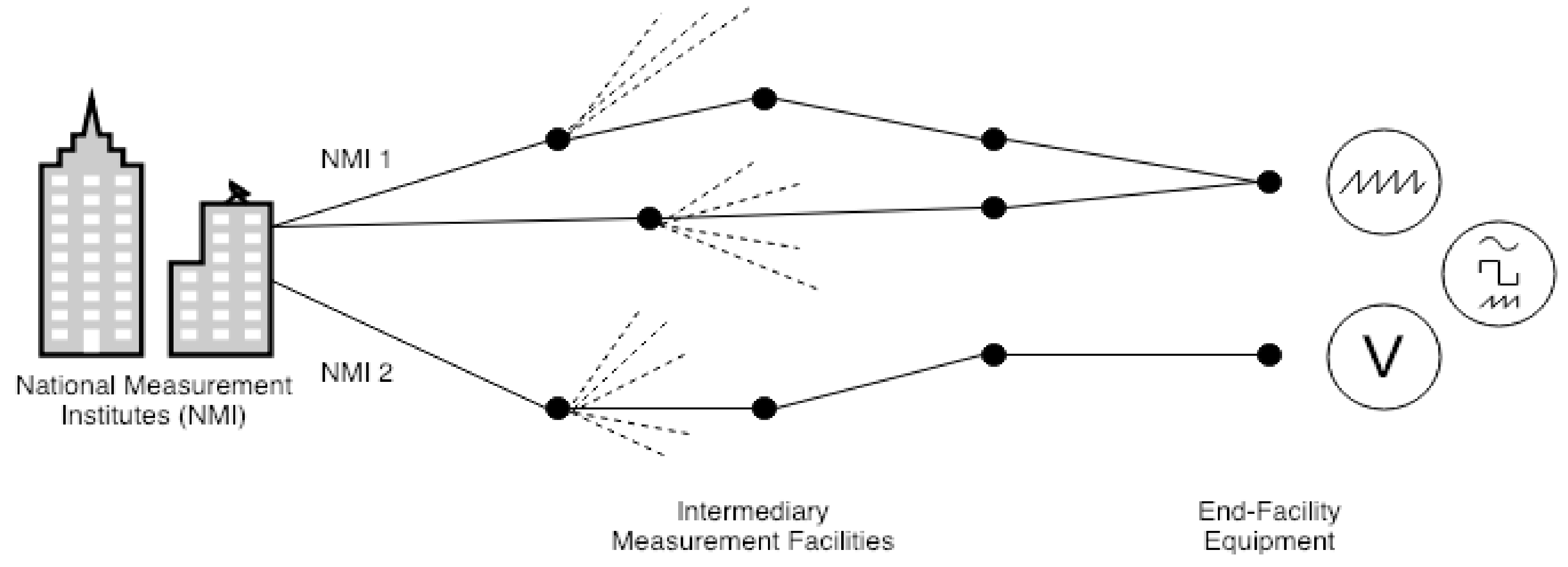
NMI 1
NMI 2
National Measurement Institutes (NMI)
Intermediary Measurement Facilities
End-Facility Equipment
V

Figure 1 – Calibration Hierarchy

## 1. Introduction

Modern surgical robot systems provide higher accuracy and increased patient safety for surgical procedures compared to human surgery.

When Internet-connected, attacks on a surgical robot can affect its calibration status – impacting its accuracy. During a surgery, we must ensure surgical robots remain robust in the event of an attack, or other factors that result in invalid calibration.

To maintain a high accuracy we must have secure and reliable calibration. Reliable calibration is achieved through an unbroken chain of traceable calibration, involving multiple parties (Figure 1):

- Robot Operators (i.e. Surgeons)
- Manufacturers (OEMs)
- Calibration Service Providers (CSPs)
- National Measurement Institutes (NMIs) (i.e. NPL in UK and NIST in USA)

The collaboration of multiple parties that request certificates and perform calibration, particularly during on-the-fly calibration, motivates the need for a new multi-level mandatory, hybrid access control model for multi-level integrity, confidentiality, and conflict management.

https://arxiv.org/abs/1902.09587

## 2. The Calibration-Safety Access Control Problem

To maintain high accuracy for surgical robots we must **maintain valid calibration**. A calibration certificate is output, outlining information such as operating ranges and parent units.

Cyber attacks and invalid calibration (from parent units) can tamper with calibration status of robots.

- We must perform calibration **on-the-fly** to ensure robust operation and high level of accuracy.

To perform calibration on-the-fly, we must regulate access for calibrating components/units and requesting calibration certificates.

- Gaining access to calibration and certificates can **leak information**.

**Multi-Level Integrity**

- Integrity must be maintained for all robot components and corresponding calibration certificates – as well as parental units.

**Multi-Level Confidentiality**

- The calibration process and lookup operations (i.e. traceability) must not leak sensitive information.

**Conflicts of Interest**

- Conflicts of interest between calibration service providers and OEMs must be avoided.

## 3. Access Control Model

NMIs at the top level have the lowest confidentiality and highest integrity, while components at the hospital have highest confidentiality and lowest integrity requirements.

Information flow in the hierarchy is an instance of Sandhu's observation [1] that BLP and BIBA are the same model.

- To enable the combination of BLP and BIBA, we must reverse BIBA.
- Lower levels can read from higher levels but not write and vice-versa.

**Set of Integrity Labels**

- A set of integrity labels is defined as $\Omega = \{\omega_1, \omega_2, \dots, \omega_q\}$, where each label corresponds to a unique integrity level.

**Conflict of Interest Set**

- A conflict of interest (COI) set is the set of subsets, where each corresponds to $m_i$ CSPs in conflict - $COI_i = m_1, m_2, \dots, m_i$

**Security Label**

- A security label is defined as a set of two n-sized vectors
$$S = \{[i_i, i_2, \dots i_n], [p_i, p_2, \dots, p_n]\},$$
where $i_j \in COI_j \cup \perp \cup T,\ p_j \in \Omega,\ 1 \leq j \leq n.$

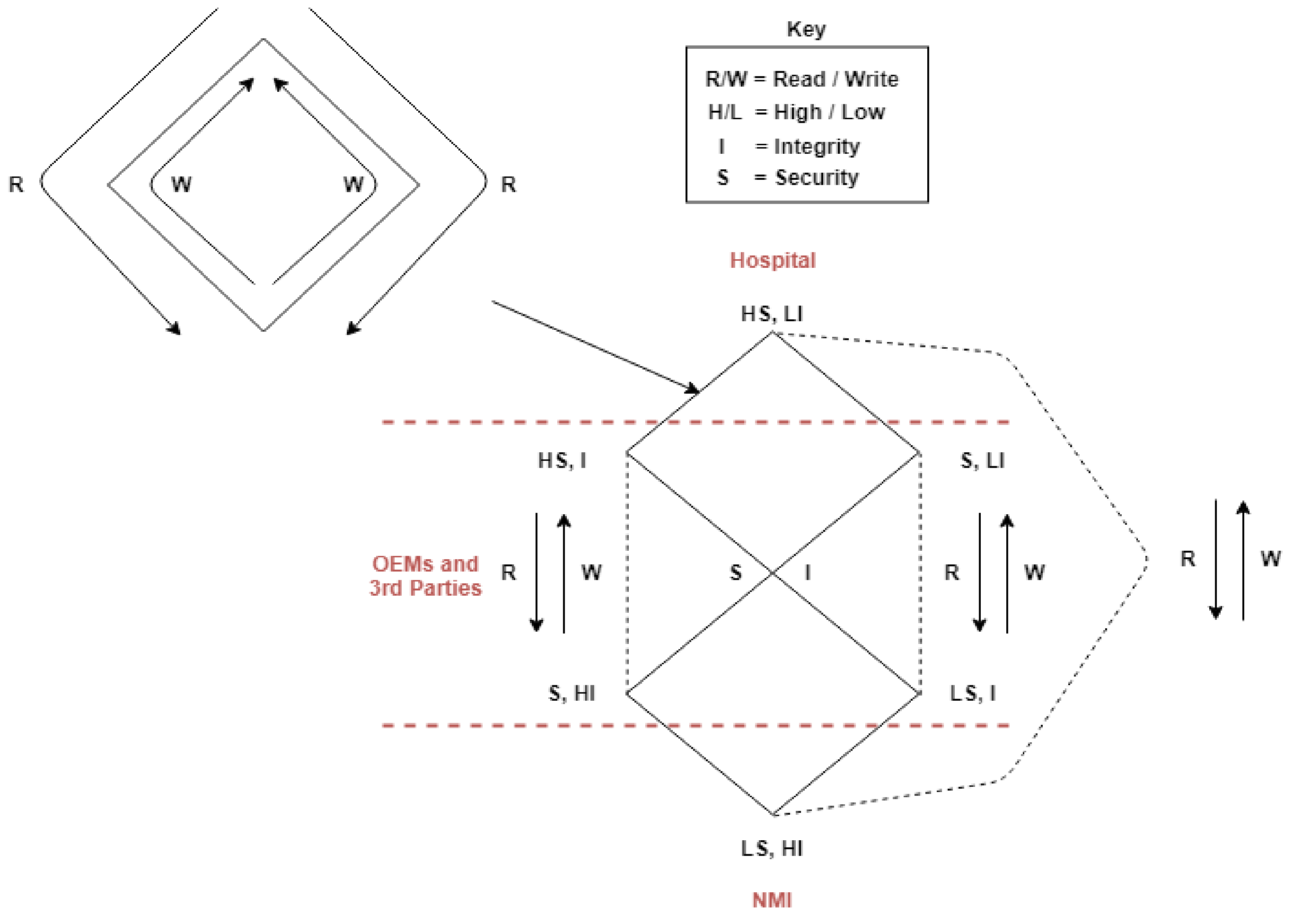

Figure 2 – Access Control Model

## 4. Calibration Lifecycle

**Initial Calibration (component *birth*)**

- Imprint component with key pair at intermediate level
$$[\perp, \perp, \dots, OEM_i, \dots, \perp], [\omega_j]$$
- Operator at $TP_j$ can calibrate if no conflict with component $OEM_i$ and outputs certificate with label
$$[\perp, \perp, \dots, OEM_i, \dots, TP_j, \dots, \perp], [\omega_i]$$

**Recalibration upon expiry**

- Operator can calibrate if no COI and label dominates certificate

**Other factors pertaining to calibration**

- Parent units have invalid calibration or accuracy of component drifts within valid calibration period – parent units must be calibrated first

## 5. Future Work

- XACML requests directly embedded with capabilities and label evaluation within policies
- Calibration status of components (and their parents) can be learned over time, for consensus among other components in a robot to formulate access decisions

[1] Ravi S Sandhu. "Lattice-based access control models". In: Computer 11 (1993). pp. 9–19.