# Poster: Unified Access Control for Surgical Robotics

Ryan Shah
ryan.shah@strath.ac.uk
University of Strathclyde

Shishir Nagaraja
shishir.nagaraja@strath.ac.uk
University of Strathclyde

**ACM Reference Format:**
Ryan Shah and Shishir Nagaraja. 2019. Poster: Unified Access Control for Surgical Robotics. In *The 24th ACM Symposium on Access Control Models and Technologies (SACMAT '19), June 3–6, 2019, Toronto, ON, Canada.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3322431.3326450

## 1 INTRODUCTION

Modern teleoperated surgical robot systems, such as the da Vinci [7] and RAVEN II [1], incorporate the use of sensors to aid with increasing safety and accuracy. However, the majority of these robots are now Internet-connected. Thus robotic safety is a security objective — an attack on a robot can cause its actuators to jump, causing significant injury to a patient, or worse. Prior art has focused on the cyber- and physical-domains [2, 3] of such robots, however, there has been minimal focus towards securing the accuracy of these robots. To ensure accuracy, secure calibration and measurement traceability are important prerequisites that must be satisfied. These goals can be achieved by the collaboration between multiple parties namely, the robot operator, the manufacturer, calibration agencies, and measurement-standards agencies such as the NIST (USA) and NPL (UK) which operate high-integrity reference devices. This collaborative approach to safety in the face of cyber attacks, motivates a new multi-level mandatory access control model. In this position paper, we discuss security requirements of calibration and traceability in connected robots, and provide arguments in support for a unified, hybrid access control model for multi-level integrity, confidentiality, and conflict management.

## 2 THE CALIBRATION-SAFETY ACCESS CONTROL PROBLEM

To provide a high degree of accuracy, we must maintain the calibration of all components in a robot. If we consider a temperature sensor mounted on the needle driver of a surgical robot, where the operation range is between 10 and 60 degrees Celsius, we should expect accurate measurements with low measurement uncertainty when operating within this range. As an output of calibration, a calibration certificate is produced, outlining essential information about the instrument's condition, traceability statement, standards of calibration used, contact information for certificate inquiries, etc. One key aspect of this is the traceability statement. Traceability involves the verification of a component's calibration, to ensure that it can be traced to some finite number of antecedent calibration units.

To ensure traceability, in the face of cyber attacks on a robot, it is essential that the robot's measurements are traceable to highest-integrity reference measurements (national standards). Attacks can directly target the calibration status of the robot or even secondary impacts of an attack can affect calibration (such as inducing drift in accuracy). If we consider a robot in surgery to become the victim of a cyber attack, it is vital to ensure the calibration is valid so that the highest degree of accuracy is preserved throughout the surgery. Thus, to do this we need to continuously check the calibration status of the component is valid. Furthermore, we also need to ensure that the calibration status of parent units is also valid. Invalid calibration will affect all subsequent units further down the traceability chain, as each level is calibrated by its first-hop parent.

Upon exploring the calibration problem space, we note three fundamental access control requirements.

**Multi-Level Integrity:** We must maintain the integrity of calibration for all components in a robot system, and the corresponding calibration certificates. As well as this, we must also maintain the integrity of calibration and certificates for parent units at each level in a component's traceability chain. The highest level of integrity would be the national measurement institutes because each unit is calibrated by its first-hop parent and thus having invalid calibration at the top level NMIs would mean that all units up to the robot at the hospital are incorrectly calibrated. Similarly, the lowest level of integrity is at the hospital.

**Multi-level Confidentiality:** We must ensure that the calibration process undertaken, and traceability lookup operations, do not leak sensitive information. Under the continuous calibration regime, if calibration traffic is subject to statistical analysis, it could reveal confidential business and patient information. From this, we can deduce that the hospitals have the highest level of confidentiality, whilst the NMIs which have public (unclassified information) will have the lowest level of confidentiality.

**Conflict of Interests:** We must avoid conflicts of interests between calibration facilities and OEMs, for example, if a calibration operator was calibrating several robots for a hospital, they should not be able to calibrate robots from any other hospital.

## 3 ACCESS CONTROL MODEL

While managing confidentiality and integrity requirements, we need to further protect against hospitals and intermediaries who are in direct competition with each other. This motivates the need for a hybrid access control model, that builds on the BLP, BIBA and Chinese Wall models [4]. The multiple levels of integrity and confidentiality are inherently transferred from the calibration hierarchy. The NMIs provide the highest level of accuracy and lowest uncertainty of measurements for calibration, and thus all subsequent


*SACMAT '19, June 3–6, 2019, Toronto, ON, Canada*

ACM ISBN 978-1-4503-6753-0/19/06.
https://doi.org/10.1145/3322431.3326450

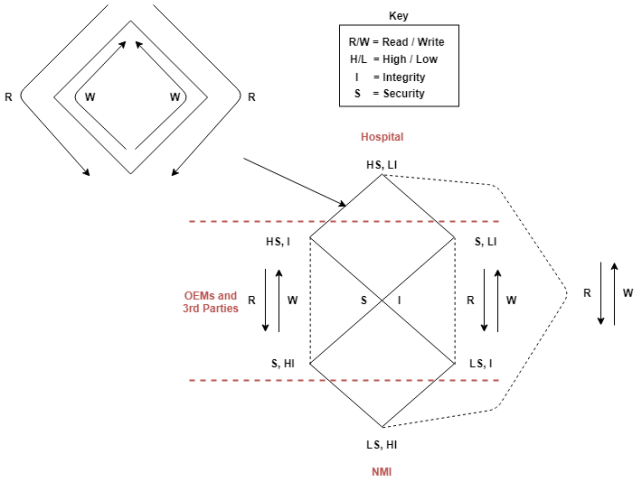


**Figure 1: Access Control Model**

units in a traceability chain depend on the validity of calibration of the root unit at the NMIs. Notably, the integrity requirement decreases as we progress further down the hierarchy towards the component level (at the hospital). Likewise, the confidentiality requirements are the reverse, where the hospitals at the lowest level have the highest confidentiality whilst NMIs have the lowest confidentiality requirement.

Furthermore, we note that the information flow in the calibration hierarchy is an instance of Sandhu's observation [4] that BIBA and BLP are the same model. The linear ordering on the security levels of calibration is defined such that each step of the traceability chain is assigned a specific security level (BLP). The organisations are assigned an integrity level, which indicates the degree of accuracy and assurance pertaining to that organisation, for example, NMIs will be issued the highest integrity level (BIBA). Since the access control rules are essentially the reverse of BLP, to enable a combination of BLP and BIBA in our calibration hierarchy, we must reverse BIBA. This enables lower levels to read from higher levels but not write, and vice-versa. For example, the hospitals with surgical robots at the lowest levels can read calibration certificates from higher levels (OEMs, NMIs, etc.) but cannot calibrate. Similarly, OEMs and NMIs can calibrate lower levels, but not read from them. Therefore, the rules for information flow as they apply to the hybrid model, shown in Figure 1, are as follows:

(1) Simple property: A principal (S) may read a calibration certificate (O), only if $L(S) \geq L(O)$.
(2) Confinement within Chinese walls: A calibration service provider (S) can only calibrate a device (O), if the security label of the device dominates that of the service provider i.e if $L(O) \geq L(S)$.

We now further define terms of our information flow model, described in the above discussion and information flow rules. The notation style we use is primarily based on the work of Sandhu [4].

**(Definition) Integrity Label Set:** A set of integrity labels is denoted as $\Omega = \{\omega_1, \omega_2, \ldots, \omega_q\}$, where each label corresponds to a unique integrity level.

**(Definition) Conflict of Interest Set:** A Conflict of Interest (COI) set is defined as the set of subsets, where each subset corresponds to calibration service providers that are in direct conflict with one another. Follow standard notation, the set of $n$ COI sets is denoted by $\{COI_1, COI_2, \ldots, COI_n\}$. Each set $COI_i = \{1, 2, 3, \ldots, m_i\}$ contains the set of $m_i$ providers, that are in conflict.

**(Definition) Security Label:** A security label is defined as a set of two $n$-sized vectors $\{[i_i, i_2, \ldots, i_n], [p_i, p_2, \ldots, p_n]\}$, where $i_j \in \{COI_j \cup \perp \cup T\}$, $p_j \in \Omega$ and $1 \leq j \leq n$. When $i_j = \perp$, the calibration traceability chain does not contain information from any provider in $COI_j$. When $i_j = T$, the calibration traffic contains information from at least two providers, who are in a COI set $COI_j$. Where $i_j \in COI_j$, the calibration traffic contains information from the corresponding service provider in $COI_j$. Finally, $p_j \in \Omega$ denotes the integrity component of the security label.

## 4 CALIBRATION LIFECYCLE AND ACCESS CONTROL

Upon exploration, we note that for components in a robotics suite, there are three phases for the calibration life cycle of a component: (1) initial calibration, (2) recalibration upon certificate expiration, and (3) other factors pertaining to recalibration.

### 4.1 Initial Calibration

A component's initial calibration is the first step in its lifecycle, which outputs a calibration certificate and establishes the final link in the traceability chain. The initial calibration is primarily performed at the manufacturing stage, using the manufacturer's calibration facility or some third party (TP) facility, or by NMIs.

**Component Birth:** From the notion of establishing the final link to the traceability chain, we refer to initial calibration as the *birth* of the component. This process implements secure initialisation of the component, by imprinting it with a key pair, which is performed at one of the intermediate levels $\{[\perp, \perp, \ldots, OEM_i, \ldots, \perp][\omega_j]\}$ of confidentiality and integrity, corresponding to $OEM_i$. An operator can only calibrate a component, when there is no conflict of interest with the component OEM, i.e. $L(OEM_i) \geq L(TP_j)$, where $i$ is the index of the OEM and $j$ is the index of the third-party calibration service provider. The output certificate will be associated with a security label $\{[\perp, \perp, \ldots, OEM_i, \ldots, TP_j, \ldots, \perp][\omega_i]\}$. The security label assigned to the certificate also lists the company names in the respective conflict of interest classes, as the certificate contains information about the OEM which manufactured the component, as well as the TP operator that carried out its calibration.

### 4.2 Recalibration

The recalibration process, due to either continuous calibration or if a certificate has expired, is a process that is carried out for all units and components in the calibration hierarchy at some stage of their life. In accordance with our access control model, a calibration operator can write upwards to the certificate, if there are no conflicts of interest and the security label of the operator dominates that of the certificate. Similar to the *birth* of a component, recalibration also outputs a calibration certificate which replaces the existing one, and the previous certificate will be archived. Notably, both

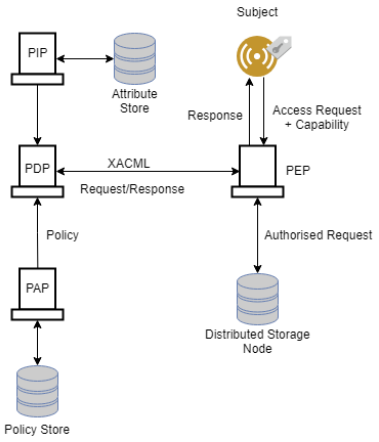


**Figure 2: XACML Architecture with Capabilities**

the certificates will have the same level as the existing calibration certificate. For example, if a different calibration facility (different operator) was to calibrate the component, then it must have the same security level as the certificate (or higher) and there must be no conflicts of interest. Using a different calibration facility may also inherently involve a different traceability chain, and this must be maintained. Thus replacing the certificate and archiving the previous one (at the same security level) allows for maintaining proper traceability and providing evidence in the event that unauthorised recalibration has taken place (a malicious calibration operator has purposely given a recalibration to provide an invalid/broken traceability chain). To provide a concise example of recalibration, consider a component from some OEM, $OEM_i$, who's calibration was performed by an operator at a third party calibration facility, $TP_j$, at the level $\{[\bot, \bot, \ldots, OEM_i, \ldots, TP_j, \ldots, \bot][\omega_i]\}$. To recalibrate this component, the recalibration would have to be performed by a calibration operator at the same level as $TP_j$. Furthermore, in the case of recalibration due to certificate expiry, we assume that parent units from upper levels (i.e. $\{[\bot, \bot, \ldots, OEM_i, \ldots, TP_j, \ldots, TP_k, \bot][\omega_i]\}$) have a valid calibration status.

### 4.3 Access Control Mechanism

In terms of a mechanism to implement our hybrid access control model, we must first discuss whether or not a conjunction of the three models can be expressed in XACML (eXtensible Access Control Markup Language) [6], which can be extended to incorporate capabilities for capability-based access control [5].

Seitz et al. [5] describe using JSON to implement capabilities, which are then parsed using the standard XACML architecture (Figure 2). To avoid using JSON, which incurs additional overhead (even with the benefit of smaller assertion size), we propose embedding security labels within capabilities and attached to objects in storage, which are directly embedded into XACML requests. XACML requests are written in XML, where the type of data fields can be specified by an XML schema, and so we can use an XML schema to define the structure of a capability with a security label:

- **Capability ID (cid)**. A unique UUID type to represent the capability token.
- **Issue Time (itime)**. The time the capability was issued.
- **Security Label (label)**. The security label which signifies the integrity labels and dominance relations.

The capability can be extended further to directly incorporate access rights and conditions within the capability itself, which can be issued to those wanting to read certificates or calibrate (write). Embedded capabilities are interpreted by the XACML access control architecture (Figure 2). The request and embedded capability is initially sent to the Policy Enforcement Point (PEP) which is then directed to the Policy Decision Point (PDP). Using the request and a policy, a response is made and given to the PEP to allow/deny access to the requester.

## 5 CONCLUSION

In this work, we have presented a real-world case to highlight the calibration-safety access problem, described in Section 2. From this, we propose three requirements of multi-level integrity, preventing information leakage and managing conflicts of interest. These requirements make the basis for proposing a conjunction of three access control models: BLP, BIBA and Chinese Wall, into a unified hybrid model. We show this hybrid model fulfils our confidentiality and integrity requirements across a multi-level hierarchy, whilst compartmentalising hierarchical components to avoid conflicts of interest. Finally, we describe a mechanism to implement our model using XACML and capabilities.

## 6 FUTURE WORK

For future work, we will provide a working mechanism using XACML using embedded capabilities, to incorporate security labels that determine the resulting access permission. Furthermore, using machine learning to detect invalid calibration of components could provide a new approach to access control. For example, if components in a robot system, which are grouped together logically, detect that another component has an invalid calibration, they can decide based on a quorate threshold of agreement whether or not access to recalibrate that device can be done. The decision for access would be determined by numerous factors, such as: component behaviour, comparing output values to expected performance determined by calibration, etc.

## REFERENCES

[1] Blake Hannaford, Jacob Rosen, Diana W Friedman, Hawkeye King, Phillip Roan, Lei Cheng, Daniel Glozman, Ji Ma, Sina Nia Kosari, and Lee White. 2013. Raven-II: an open platform for surgical robotics research. *IEEE Transactions on Biomedical Engineering* 60, 4 (2013), 954–959.

[2] Daniel Kruse, John T Wen, and Richard J Radke. 2015. A sensor-based dual-arm tele-robotic system. *IEEE Transactions on Automation Science and Engineering* 12, 1 (2015), 4–18.

[3] Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, and Stefano Zanero. 2017. An Experimental Security Analysis of an Industrial Robot Controller. In *Proceedings of the 38th IEEE Symposium on Security and Privacy*. San Jose, CA.

[4] Ravi S Sandhu. 1993. Lattice-based access control models. *Computer* 11 (1993), 9–19.

[5] Ludwig Seitz, Göran Selander, and Christian Gehrmann. 2013. Authorization framework for the internet-of-things. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops*. IEEE, 1–6.

[6] OASIS Standard. 2005. extensible access control markup language (xacml) version 2.0.

[7] Gyung Tak Sung and Inderbir S Gill. 2001. Robotic laparoscopic surgery: a comparison of the da Vinci and Zeus systems. *Urology* 58, 6 (2001), 893–898.