Computer Standards & Interfaces 34 (2012) 225–229

Contents lists available at SciVerse ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Cyberphysical systems security applied to telesurgical robotics

Gregory S. Lee [a,*], Bhavani Thuraisingham [b]

[a] Mechanical Engineering, The University of Texas at Dallas, Richardson, TX 75080, USA
[b] Computer Science, The University of Texas at Dallas, Richardson, TX 75080, USA

ARTICLE INFO

Article history:
Received 9 February 2010
Received in revised form 13 June 2011
Accepted 19 September 2011
Available online 24 September 2011

Keywords:
Cyberphysical systems
Security
Telesurgical robotics
Telesurgery

ABSTRACT

Researchers in telesurgical robotics and security collaborated to develop the Secure ITP, a security enhancement to the Interoperable Telesurgery Protocol (ITP). The ITP defines the structure for communication between telesurgery robots and controllers and has been adopted and tested by fourteen research groups in telesurgical robotics. The Secure ITP uses open source software tools and follows guidelines in Federal Information Processing Standards (FIPS) documents published by the National Institute of Standards and Technology (NIST) to create asecurity enhancement prototype for demonstration purposes and tofacilitate the development of new security technologies which addressthe stringent requirements of telesurgery.

© 2011 Elsevier B.V. All rights reserved.

1. Introduction

Next generation surgical robots under development at the University of Washington BioRobotics Laboratory (BRL) and at SRI International will allow surgeons to perform robotic based Minimally Invasive Surgery (MIS) remotely [1,2,3]. Teleoperated surgical robots, or telesurgical robots, will allow highly trained medical personnel to provide skilled care from distant locations [1,3]. This capability may be used in civilian settings to allow surgeons to care for patients in underserved remote locations or in disaster areas. Ultimately, telesurgical robots will be deployed into the battlefield to provide nearly immediate medical assistance to wounded soldiers [1,2].

These possibilities cannot be realized without developing telesurgical robots specifically to function securely. The University of Texas at Dallas (UTD) collaborated with the BRL to develop a security enhancement to the Interoperable Telesurgery Protocol (ITP). The ITP standardizes communication between telesurgical robot hardware (slaves) and telesurgical robot controllers (masters) so that slaves may interchangeably operate different masters [4,5]. Fourteen telesurgery research groups have adopted the standard and participated in a successful test of interoperability conducted by the BRL [6]. The Secure ITP addresses security issues for ITP based telesurgical robots allowing security to be deeply implemented in these complex cyberphysical systems. It addresses four security elements: communication, authentication, authorization, and security policy development and enforcement.

The project uses software to simulate the hardware and unmodified control code from the BRL's RAVEN telesurgical robot [7] (see Fig. 1). OpenSSL provides several security tools for used to begin the development the Secure ITP.

2. Background

Surgical robots, such as the daVinci® by Intuitive Surgical Incorporated of Sunnyvale, CA, are being used for a growing number of surgeries. These robots allow surgeons to perform Minimally Invasive Surgery (MIS) by indirectly controlling MIS instruments using robotic manipulators. Non-robotic MIS sometimes requires surgeons to place the surgical instruments in difficult and uncomfortable orientations in order to access the surgical site. The arms of a surgical robot may be placed in any configuration to reach the surgical environment.

Surgeons manipulate the surgical environment from a control console by using a controller and by viewing the surgical environment on a monitor. This abstracts surgery to the exchange of information between the surgeon and robot through the controller station and renders the physical location of the surgeon virtually irrelevant [3].

Federal Food and Drug Administration approved surgical robots are not designed for teleoperation, but have been modified to allow surgeons to teleoperate the robot. One telesurgery has been well documented, but far from common [8]. Next generation surgical robotics research seeks to develop surgical robots specifically for telesurgery.

The BioRobotics Laboratory at the University of Washington has developed the RAVEN, a next generation telesurgical robot prototype [9]. SRI International has also developed a next generation telesurgical robot, called the M7. Both the RAVEN and M7 prototypes have been teleoperated in functionality experiments over dedicated

* Corresponding author at: Case Western Reserve University, Electrical Engineering & Computer Science Department, 10900 Euclid Ave., Cleveland, OH 44106, USA.
E-mail addresses: leegs@case.edu (G.S. Lee), bhavani.thuraisingham@utdallas.edu (B. Thuraisingham).

0920-5489/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2011.09.001

Fig. 1. The monitor on the left displays a graphical representation of the simulated RAVEN surgical robot pose in the upper screen and ITP communication information for the slave in the lower screen. The laptop on the right displays the ITP communication console for the telesurgery master which transmits position data from the two Falcon® haptic displays.

communications networks and the public Internet by surgeons using master controllers located thousands of miles away [1,10].

The Army Telemedicine and Advance Technology Research Center (TATRC) and the DARPA Trauma Pod programs seek to develop telesurgical robots for military applications, including deployment to the theater of battle [1,2]. Telesurgical robots will also benefit civilian medicine by allowing highly specialized surgeons to intervene where typically they could not; or by allowing groups of surgeons to provide care in disaster areas where their physical presence would place greater strain on scarce local resources. The feasibility and usability of telesurgery in these scenarios, however, depends not only on the design of the robot mechanism and timely communications, but also the ability for telesurgical robots to function securely in unknown and possibly adversarial environments.

The BRL and SRI research groups are collaboratively developing a communications standard for telesurgery called the Interoperable Telesurgery Protocol (ITP). The standard specifies how the master and slave components communicate. It allows master and slave devices to operate interchangeably and it also allows independent development of master and slave devices. The protocol is still under development, however, fourteen telesurgical robot projects have adopted the protocol and participated in a successful test of interoperability [6].

Cyberphysical systems, such as telesurgical robots, have been identified by the Department of Homeland Security (DHS) as a class of devices which must develop hardware, software and security concurrently [11]. The decision by developers to transmit unencrypted live video data from the Predator drone exemplifies the need for the independent but concurrent development of security commensurate with the task and environment [12]. Knowing that seemingly safe systems assumed to be beyond the reach of adversaries still fall victim to attack; that telesurgical robots are specifically designed to be deployed to diverse and uncontrolled environments, and that security is best developed by security experts concurrently with hardware development indicates the need for developing security for telesurgery now.

3. Project description

The Secure ITP draws on established security guidelines to provide a proof of concept prototype and security framework for security in telesurgical robotics. The security measures and secure communication links for ITP based communications work in concert with the unmodified ITP communication. The Secure ITP established a framework which allows new security technology for telesurgical robotics to be developed concurrently with, but independent of the robotic hardware.

Leveraging the existing ITP standard to build the security solution without external dependencies facilitates the adoption of the Secure ITP by many projects already using the ITP. The open source software package, OpenSSL, provides tools for creating secure communication links and to provide other types of security for the telesurgical robots.

The Secure ITP applies authorization levels to the telesurgical master and slave hardware through the use of certificates used to authenticate the devices for secure communications. These same types of certificates also provide authentication and authorization for the surgeon and patient. The authorization levels allow security policies to be defined to demonstrate the need for thoughtful and complete security solutions to meet the specific needs of telesurgery.

As more advanced security techniques and tools are created to meet the requirements of telesurgery, they will replace the existing implementations in a manner nearly invisible to the telesurgical robots researchers. Regardless of future innovations, all security measures will be provided by the Secure ITP instead of external tools. New and specifically designed security technology will be provided by the Secure ITP which meet the technical requirements of telesurgery that current standards and technology cannot meet. Providing the security for telesurgery in a single software package simplifies its implementation and minimizes the possibility of misconfiguration.

3.1. Communications

The ITP protocol specifies two communications channels between the surgical robot master and slave [5]. One is a Transmission Control Protocol (TCP) based supervisory channel which requires all communications reach the destination, but is tolerant to moderate delay. The second channel carries the commanded inputs from the master to the slave and information from the slave back to the master.[1] This channel transmits data every millisecond.[2] The data on this channel must experience minimal delay, but is resilient to small amounts of intermittent packet loss and therefore uses the User Datagram Protocol (UDP).

Transport Layer Security (TLS) is the protocol suggested by the National Institute of Standards and Technology (NIST) for secure communication over TCP [13]. This is the TCP based protocol used for secure web transactions. Datagram TLS (DTLS) is a form of TLS adapted for use with UDP communication. The Secure ITP uses TLS and DTLS to Secure ITP communication on the corresponding channels (see Fig. 2).

TLS and DTLS communication may use any of a number cipher algorithms, however, the Secure ITP only uses of the Advanced Encryption Standard (AES) to encipher communication between the master and slave. The National Security Agency has published a policy that all key lengths specified in the published AES standard (128, 192, and 256 bits) may be used to protect information classified up to and including the level of SECRET and key lengths of 192 and 256 bits are adequate to protect information classified up to and including TOP SECRET [14]. Enciphering the communications between the telesurgical robot master and slave using AES protects the privacy and integrity of the transmitted data to a level commensurate with both operational military and civil environments and can be accomplished using currently available computing hardware.

New secure communication technology specifically for telesurgery is becoming available [15]. This technology attempts to provide the same level of privacy and integrity as AES based TLS and DTLS while using less computational resources and increasing redundancy and

[1] Video is currently handled outside the ITP.

[2] The PlugFest 2009 event to test the interoperability of ITP communication was conducted at 100 Hz.

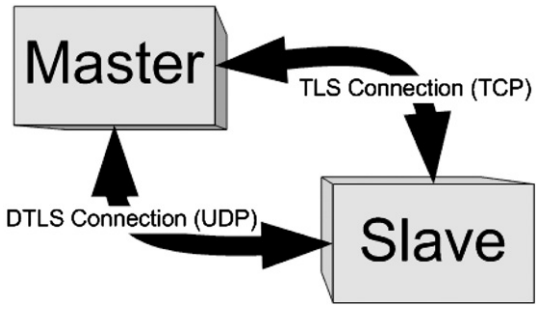

Fig. 2. Communication between the telesurgical robot master and slave requires two channels. One channel uses TCP and TLS, while the other channel uses UDP and DTLS.

robustness. Because of the modularity for the Secure ITP framework, this technology could be used replace TLS and DTLS communication in the Secure ITP when functionality is verified. Any ITP based project using the Secure ITP will then be able to take advantage of this new communication technology by updating the Secure ITP framework in their project with minimal disruption.

3.2. Authentication

The TLS and DTLS protocols use X.509 certificates for authentication. These certificates contain identity information about the certificate holder. A Certificate Authority (CA) digitally signs a certificate to verify the authenticity and to prevent any alteration of the certificate. In the Secure ITP specification, all parties exchange certificates to allow each to verify the authenticity of the others[3] (see Fig. 3). All parties to a telesurgery are provided with the root certificate from the CA which contains information used to verify the signatures.

Besides the master and slave devices, the surgeon and patient are authenticated using certificates. Other surgical resources will soon be authenticated using this X.509 certificates (e.g. medical support staff, medical instrumentation, surgical instruments, medications, *etc.*). The need to authenticate resources formally increases for telesurgery and certificate based authentication addresses this need.

3.3. Authorization

Version three of the X.509 certificate specification (X.509V3) defines certificate extensions. Extensions expand x.509 certificates to include custom information. The Secure ITP defines a custom field to assert an authorization level for the certificate holder. For instance, the certificate presented by a master to the slave may indicate that the surgical robot is intended for non-human surgery only. Security policies will dictate how to use this information for security (see Section 3.4). Preliminary authorization levels which exist at this time include MAINTENANCE, NON-SURGICAL, NON-HUMAN, HUMAN, and OVERRIDE to indicate the acceptable uses for master and slave devices (see Table 1).

Authorization for other devices can be included in the X.509 certificates assigned to them. For instance, an authorization level for a surgeon could indicate the surgical procedures the surgeon may perform or the maximum time delay the surgeon may tolerate in telesurgery. A certificate for a patient can include specific procedure to be performed, allergies, and even the authorized surgeons. Assumptions like these acceptable for local surgery require formal, standard and systematic protocols in telesurgery.

[3] Typical implementations, as in secure web servers, authenticate the server with a certificate and the client with a username and password pair.

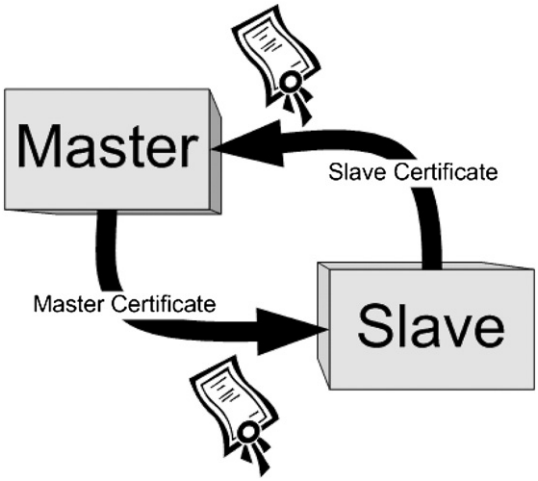

Fig. 3. The telesurgical robot master and slave devices exchange certificates for each device to authenticate the other.

3.4. Security policies and enforcement

Authentication, authorization levels and policy enforcement are critical for secure operation of telesurgical robots. Security policies and enforcement mechanisms exist currently only as proofs of concept in the Secure ITP. Preliminary authorization levels for the master and slave devices form the basis of preliminary security policies. For instance, the authorization levels of the master and slave must be compatible for the surgical robot to be used (see Tables 1 and 2). Other information may also be included in an X.509V3 certificate to facilitate security policy development.

The Secure ITP project provides a Certificate Authority tool to generate certificates with the custom fields for telesurgery used to authenticate and determine authorization levels of the entity bearing the certificate. It also generates the root certificate which must be distributed to all devices participating in Secure ITP operation to allow them to verify certificates.

Future methods for creating a secure telesurgical robot are expected to grow beyond this preliminary development. Software attestation techniques developed for the demanding telesurgery environment will become part of the Secure ITP once functionality is verified [16].

4. Discussion

The Secure ITP draws upon established security techniques and leverages the existence of a commonly used robotic telesurgery specific communication protocol to begin development of security of telesurgery. The result illustrates the need to develop security specifically for telesurgery and the need to develop that security concurrently with the development of the robotic telesurgery cyberphysical systems.

While the Secure ITP uses well known standards for secure communication, these protocols only ensure privacy and information integrity on individual communication channels. The communication between a telesurgical master and slave will require a highly robust, redundant

Table 1
Authorization levels and corresponding acceptable uses currently defined for master and slave devices by the Secure ITP.

Authorization level	Acceptable uses
MAINTENANCE	Maintenance only
NON-SURGICAL	Testing and maintenance
NON-HUMAN	Non-human medical
HUMAN	Human medical
OVERRIDE	No restrictions

Table 2
The table shows preliminary security policies concerning the combinations of authorization levels for master and slave devices. M = MAINTENANCE, N S = NON-SURGICAL, N H = NON-HUMAN, H = HUMAN, O = OVERRIDE, ✓ = Compatible, ✗ = Not Compatible.

		Master				
		M	N S	N H	H	O
Slave	M	✓	✗	✗	✗	✓
	N S	✓	✓	✗	✗	✓
	N H	✓	✓	✗	✗	✓
	H	✗	✗	✗	✓	✓
	O	✓	✓	✓	✓	✓

and secure communication link. A protocol to meet these requirements does not yet exist. A new communication protocol which begins to address requirements specific to telesurgery is currently under development [15]. The Secure ITP also functions as a framework to allow new technology protocols, such as this one, to be developed independently and implemented once mature. Telesurgical robotics researchers may immediately benefit from the new security technology.

Authentication and authorization measures provided for the Secure ITP by the X.509 standard also requires further development to address telesurgery. Time stamping or similar method will be added to the Secure ITP protocol to address the time based security needs of telesurgery. Also, a means to track the number of uses of surgical instruments which may only be used a fixed number of times will need to be developed. An infrastructure to accommodate these security measures must be created to accompany these tools. It is possible that new technology may be developed that does not resemble X.509V3 and it could be adopted without impacting development of the robotic systems.

Security policies for telesurgery must be developed which are not only sound from a security perspective, but they must also be compatible with surgical and operating room practices and not impact the technical performance of a complex telesurgical cyberphysical system. The described policies illustrate the need for development to begin now. Policies must establish how many aspects of a telesurgical robot, and telesurgery will function. It must accommodate future aspects of telesurgery, such as telementoring, and respond to compromise and failure and policy enforcement must adapt to the situation and be understandable by surgeons with limited security training. All this must be accomplished without distracting the surgeon from the primary task of surgery.

Software and hardware attestation and verification are aspects of security in telesurgery which recent development of the Secure ITP has only begun to address using OpenSSL tools. Current development further demonstrates the need for these tools and provides the framework for future development. Research applicable to telesurgery for advanced software integrity verification has begun [16]. Methods of hardware verification and attestation, however, remain unaddressed. An initial framework for these tools being developed for the Secure TIP will allow robotics researchers to accommodate the architecture such methods and measures may require during hardware development as well as for use in security policy development.

5. Conclusion

The University of Texas at Dallas collaborated with the University of Washington to implement a security enhancement to the Interoperable Telesurgery Protocol. The Secure ITP provides a proof of concept and a framework for the future development of advanced and dedicated security to meet the stringent requirements of the telesurgery environment. It currently implements secure communication, authentication, authorization and preliminary security policies and enforcement based on published standards. This preliminary solution may be implemented by ITP based projects without the need for secondary configurations.

The Secure ITP enciphers communications between the master and slave using techniques and protocols specified by Federal Information Processing Standards (FIPS) documents published by NIST. The communications use the TLS and DTLS protocols and the AES cipher. Certificates based on the X.509 standard provide authentication for the telesurgical master and slave devices, as well as for the surgeon and patient. Authorization levels are also included in extended fields of the certificates. Preliminary security policies use authorization levels to further secure the telesurgical robot master and slave devices.

As a proof of concept, the Secure ITP illustrates the possible scope and the need for the development of technology to specifically address the requirements of secure telesurgery. It also provides a framework for the development of future technology. New technology for security in the delicate environment of telesurgery can replace existing functionality provided by the Secure ITP with a minimal disruption to the telesurgery cyberphysical system research projects.

The development of the Secure ITP in concert with the design of the Interoperable Telesurgery Protocol and telesurgical robot directly addresses the DHS assertion that security should be developed concurrently with hardware and that it be designed by security experts. Separating the development of security from the development of telesurgical robotics allows all researchers involved to focus on core competencies, thus, resulting in better solutions developed concurrently and preventing the problems caused by non-expert developed and/or retrofitted security measures.

The research conducted at the BRL and at SRI has the stated purpose of developing telesurgical robots capable of being deployed to the battlefield and disaster areas. Telesurgical robots may be deployed in the most adversarial and uncontrolled of situations, or in the most secure of settings, however, attacks and security compromises must be anticipated. Regardless, secure operation must be maintained in every environment. Robotics engineers, security experts, and surgeons must collaborate to develop solutions which meet the requirements of the complex telesurgery cyberphysical system. By establishing the Secure ITP as a framework early in the development process, the design of the robotic hardware and security will be simultaneously address to provide a solution which meets the needs of every element. Whereas system architecture developed independently of security may lead to incompatibility between security and hardware, the concurrent development of security and hardware will provide a comprehensive and well integrated solution which addresses the technical needs of the robotic hardware, the functional and medical needs of surgeons, the structure indicated by security experts and the level of sophistication which results from long term, focused development. Telesurgery will not be viable without it.

Acknowledgments

Support for this research was provided by The University of Texas at Dallas Erik Jonsson School of Engineering in Richardson, TX.

The authors wish to thank Professor Blake Hannaford and the members of the BioRobotics Laboratory at the University of Washington in Seattle, WA for their support and collaboration.

References

[1] J. Rosen, B. Hannaford, Doc at a distance, IEEE Spectrum 43 (2006) 34–39.
[2] P. Garcia, J. Rosen, C. Kapoor, M. Noakes, G. Elber, M. Treat, M. Hanson, J. Manak, C. Hasser, D. Rohler, R. Satava, Trauma Pod: a semi-automated telerobotic surgical system, International Journal of Medical Robotics and Computer Assisted Surgery 5 (2009) 136–146.
[3] R.M. Satava, How the Future of Surgery is Changing: Robotics, Telesurgery, Surgical Simulators and Other Advanced Technologies, Technical Report, University of Washington Medical Center, 2006.

[4] H. King, B. Hannaford, Breaking the Interoperability Barrier through Emerging Standards in Teleoperation, Technical Report, University of Washington, 2009.
[5] B. Hannaford, T. Low, Interoperable Telesurgery Protocol (ITP) version 0.44, http://brl.ee.washington.edu/Research_Active/Interoperability/index.php/Draft_Specification, 2009.
[6] H. King, B. Hannaford, K.-W. Kwok, G.-Z. Yang, P. Griffiths, A. Okamura, I. Farkhatdinov, J.-H. Ryu, G. Sankaranarayanan, V. Arikatla, K. Tadano, K. Kawashima, A. Peer, T. Schauss, M. Buss, L. Miller, D. Glozman, J. Rosen, T. Low, Plugfest 2009: global interoperability in telerobotics and telemedicine, IEEE International Conference on Robotics and Automation, 2010, pp. 1733–1738, (ICRA 2010).
[7] G.S. Lee, B. Thuraisingham, Secure Surgical Haptics and Robotics: The Raven Test Platform, Technical Report, The University of Texas at Dallas, 2008.
[8] J. Marescaux, J. Leroy, M. Gagner, F. Rubino, D. Mutter, M. Vix, S.E. Butner, M.K. Smith, Transatlantic robot-assisted telesurgery, Nature 413 (2001) 379–380.
[9] M. Lum, D. Friedman, J. Rosen, G. Sankaranarayanan, H. King, K. Fodero, R. Leuschke, M. Sinanan, B. Hannaford, The RAVEN — design and validation of a telesurgery system, International Journal of Robotics Research 28 (2009) 1183–1197.
[10] C.R. Doarn, M. Anvari, T. Low, T.J. Broderick, Evaluation of teleoperated surgical robots in an enclosed undersea environment, Telemedicine and e-Health 15 (2009) 325–335.
[11] N. Adam (Ed.), Workshop on Future Directions in Cyber-physical Systems Security, Department of Homeland Security, Newark, NJ, 2009.
[12] S. Gorman, Y.J. Dreazen, A. COLE, Insurgents hack U.S. drones: $26 software is used to breach key weapons in Iraq; Iranian backing suspected, Wall Street Journal A1 (2009).
[13] C. Chernick, C. Edington, M. Fanto, R. Rosenthal, NIST Special Publication 800-52: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf, 2005.
[14] National Security Agency, National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf, 2003.
[15] M. Tozal, Y. Wang, E. Al-Shaer, K. Sarac, B. Thuraisingham, B. Chu, On secure and resilient telesurgery communications over unreliable networks, in: The 30th IEEE International Conference on Computer Communications (INFOCOM 2011).
[16] K. Coble, W. Wang, B. Chu, L. Zhiwei, Secure software attestation for military telesurgical robot systems, Military Communications Conference, 2010, pp. 965–970, (MILCOM 2010).

Gregory S. Lee, Ph.D. received his Doctoral and Master of Science degrees in Electrical Engineering from the University of Washington in Seattle, WA and his Bachelor of Arts degree in Physics from Whitman College in Walla Walla, WA. He has conducted research inforce feedback haptics, computer vision and robotics.

Bhavani Thuraisingham, Ph.D. received her Bachelor of Science degree in Mathematics and Physics with first class at the University of Ceylon, her Master of Science degree in Mathematical Logic at the University of Bristol, UK and her Doctoral degree in Theory of Computation at the University of Wales, UK. She worked at MITRE in Bedford, as a department head in Data and Information Management as well as Chief Scientist in Data Management in the Intelligence and Air Force centers. At the National Science Foundation (NSF), she established the Data and Applications Security Program and co-founded the Cyber Trust theme and was involved in interagency activities in data mining for counter-terrorism. Dr. Bhavani Thuraisingham is the Director of the Cyber Security Research Center and the Louis A. Beecherl, Jr. I Distinguished Professor in the Erik Jonsson School of Engineering and Computer Science at the University of Texas at Dallas (UTD) since September 2010.