NSF Grant 1329751

CPS: Breakthrough: Secure Telerobotics

Howard Jay Chizeck (PI)
chizeck@uw.edu

Tadayoshi Kohno (Co-PI)
yoshi@cs.washington.edu

University of Washington
Seattle

Introduction

This project – developing methods and tools to enhance **security, privacy and safety** of telerobotic systems

Results:

- Tools for monitoring and detection of unexpected and malicious activities in telerobotic systems [1-4]
- Mechanisms to prevent security threats against telerobotic systems [6]
- Methods to correct for errors caused by random failures and malicious actions
- Movement-based [5] or force and signature-based "Haptic Passwords" [7,8] for authentication

Telerobotic Systems

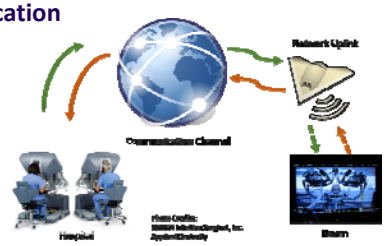
Systems where human operators interact with remote robots — *anywhere where it is too dangerous, too far away, too large or too small to be done by humans*

- Underwater, space, mining, firefighting
- Military operations
- Search and rescue robotics
- Telerobotic surgery

Telerobotic systems – sometimes must use existing, publicly available networks, combined with ad-hoc wireless and satellite networks

Telerobotic Security Challenges

Open and uncontrollable communication channels → **malicious entities (attackers) can disrupt or take over operator-robot communication**



Or with false identity

Work to Date

Threats Identification and Evaluation

*** Attack classification, based on the impact on human operators:**

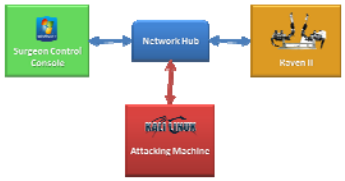
- Intention modification
- Intention manipulation
- Hijacking

*** Attacker's position in the network:**

- Network observer
- Network intermediary

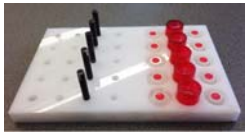
*** Experimental Analysis**

- Impact of attacks evaluated through a series of experiments involving human subjects



- **Considered telerobotic tasks:**

Fundamentals of Laparoscopic Surgery task



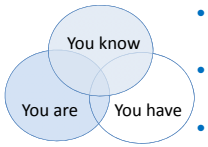
Fitt's law task

- **Attacks:**
  - Denial-of-service
  - Operator's intent reordering
  - Operator's intent loss
  - Operator's intent delay
  - Operator's intent modification
- **Metrics:**
  - Overall procedure time
  - Fitt's index of difficulty
  - Subjective assessment of task difficulty

*** Results**

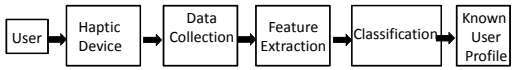
- Telerobotic systems currently vulnerable to a variety of efficient attacks *(single packet attacks!)*
- Some attacks easily preventable using well-established and readily available security mechanisms (encryption and authentication methods currently under evaluation)
- ***Tensions between cyber security, safety and usability requirements of teleoperated systems render many existing security solutions infeasible*** → teleopration security a unique challenge!

Haptic Passwords

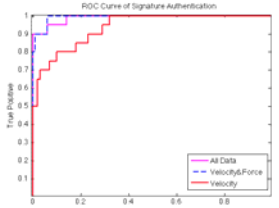


- Combines 'what you know' and 'who you are'
- Uses motion and force information to authenticate user
- Significantly increases the password space

- How a person writes (i.e. pen tip velocity, force, orientation, etc.) is unique.
- How a person uses stylus haptic device or pen/finger on touch screen to write contains user dependent information



- **Preliminary Experimental Results**
  - 9 subjects to date
  - 100% correct identification (using signature; (less than ~85%) using simple mark (letter L)
  - Very small chance of forgery (false positive) if tolerate having to re-enter signature 1 time in 10



References

[1] T. Yusuf, T. Bonaci, T. Kohno, H.J. Chizeck, *"Dr. Hacker, I Presume? An Experimentally-based Discussion about Security of Teleoperated Surgical Systems"*, **2014 USENIX Summit on Health Information Technologies**, San Diego, CA, August 2014.
[2] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, H. J. Chizeck, **"To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics," arXiv:** 1504.04339, April 2015.
[3] T. Bonaci, A.Alva, J. Herron, R. Calo, H. J. Chizeck. **"I Did It My Way: On Law and Operator Signatures for Teleoperated Robots, 4th Annual Conference on Robotics, Law and Policy (WeRobot 2015)**, Seattle, April 10-11, 2015.
[4] T. Bonaci, J. Yan, J.Herron, T. Kohno, H. J. Chizeck. "Experimental Analysis of Denial-of-Service Attacks on Teleoperated Robotic Systems." **ICCPS: 6th ACM/IEEE International Conference on Cyber-Physical Systems.** Seattle, April 14-16, 2015.
[5] H. J. Chizeck, Tamara Bonaci, Thomas Lendvay. "Enhanced Security and Safety in Telerobotic Systems." US Patent Number: 9,148,443, Sept. 29, 2015.
[6] Howard Jay Chizeck, Tamara Bonaci. "Using Supplemental Encrypted Signals to Mitigate Man-In-The Middle Attacks on Teleoperated Systems." International Patent Application Number: PCT/US13/67528; filed 10/30/2013.
[7] Howard Jay Chizeck, Junjie Yan, Tamara Bonaci, Jeffrey Herron, Kevin Huang, Aaron Alva. "Haptic Passwords." Provisional Patent 62/134,435; filed 3/17/2015.
[8] J. Yan, K. Huang, T. Bonaci, and H. J. Chizeck. "Haptic Passwords." **2015 IEEE International Conference on Intelligent Robots and Systems (IROS)**, Hamburg, Germany, Sept. 28-Oct, 2, 2015.

Graduate Students

Tamara Bonaci (PhD UWEE 2014), Junjie Yan, Kevin Huang (NSF GRF), Jeffrey Herron

Undergraduates

T. Yusuf