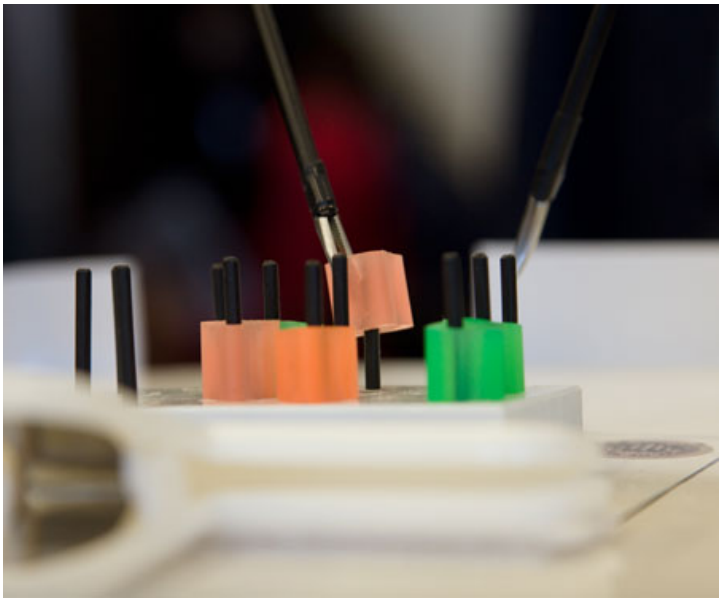
Cyberatak na roboty naukowe

Aby poprawić bezpieczeństwo samochodów przeprowadza się testy wypadkowe celem określenia ich słabych punktów z maksymalną dokładnością oraz celem zapewnienia bezpiecznych warunków jazdy.

Jest to idea, która przyświeca zespołowi prowadzącemu serię eksperymentów na University of Washington. Aby sprawdzić łatwość przeprowadzenia złośliwego ataku na zdalnie sterowane operacje oraz aby położyć nacisk na bezpieczeństwo tego systemu, dokonano tam włamania do systemu operacyjnego robota nowej generacji, stosowanego wyłącznie do celów naukowych.



Badacze UW przeprowadzili cyberatak w czasie, gdy uczestnicy studiów wykorzystywali zdalnie sterowanego robota operacyjnego do usuwania bloków z tablicy.

Ze względu na rozwój technologii należy położyć nacisk na rozpowszechnienie zdalnych robotów sterowanych w warunkach codziennej eksploatacji z innej lokalizacji. Są to rozwiązania idealnie dopasowane do zastosowania w sytuacjach stwarzających zagrożenie dla życia ludzkiego, takich jak gaszenie pożarów w zakładach chemicznych, rozpraszanie materiałów wybuchowych lub uwalnianie ofiar trzęsień ziemi spod zawalonych budynków.

Poza nielicznymi eksperymentalnymi operacjami przeprowadzanymi zdalnie, lekarze zazwyczaj wykorzystują roboty operacyjne do przeprowadzania zabiegów na pacjentach znajdujących się na tej samej sali z wykorzystaniem bezpiecznego połączenia komputerowego. Jednakże pewnego dnia, teleroboty zapewne będą wykorzystywane rutynowo do przeprowadzania operacji chirurgicznych, np. na wiejskich terenach słaborozwiniętych, na polach walki, na oddziałach z pacjentami zarażonymi wirusem Ebola lub w przypadku katastrof na drugim końcu świata.

W treści dwóch najnowszych opracowań UW BioRobotics pracownicy laboratoryjni udowodnili, że pracę telerobotów nowej generacji wykorzystujących sieci publiczne, (będące jedyną opcją w przypadku katastrof lub w oddalonych lokalizacjach) można z łatwością sparaliżować lub utrudnić poprzez typowe formy cyberataków. Zastosowanie środków bezpieczeństwa w celu powstrzymania tego typu ataków będzie stanowiło zagadnienie krytyczne dla ich bezpiecznego zastosowania oraz wykorzystania.

"Chcemy, by teleroboty kolejnej generacji zachowały odporność na większość wykrywanych zagrożeń w taki sposób, by nie narażać na fizyczne zagrożenia operatora, pacjenta lub innych osób," powiedziała Tamara Bonaci, doktorant UW na wydziale elektrycznym.

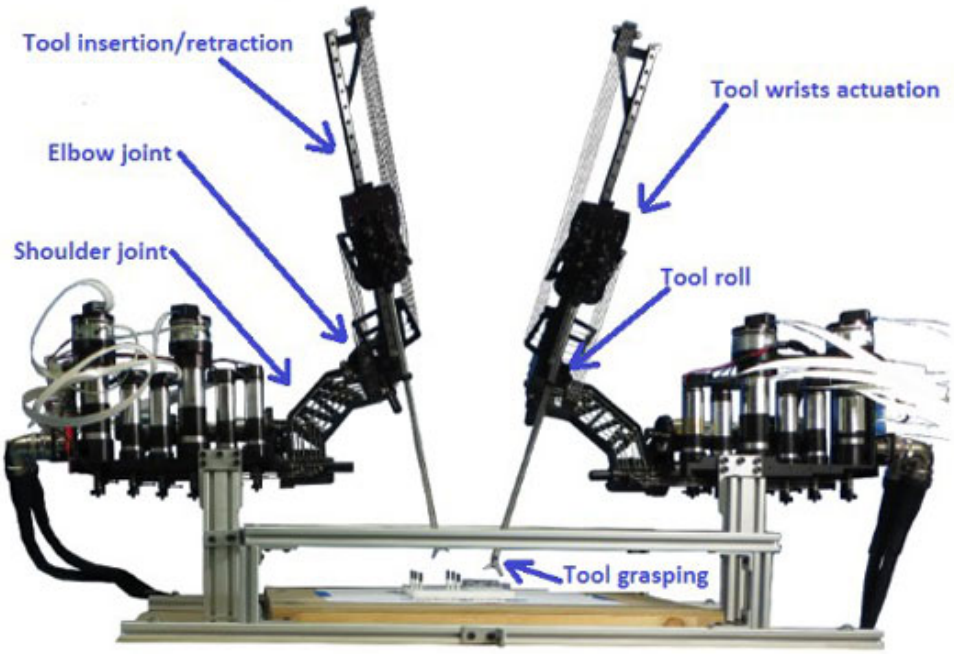
Aby obnażyć słabe punkty, zespół UW rozplanował zastosowanie typowych cyberataków, podczas stosowania przez uczestników studiów sterowanego zdalnie robota operacyjnego skonstruowanego w UW (dla celów naukowych) do usuwania bloków gumowych zlokalizowanych pomiędzy kołkami na tablicy.

Poprzez wywołanie ataków "od środka" wprowadzających zmiany poleceń przepływających pomiędzy operatorem a robotem, zespół mógł dokonać złośliwego uszkodzenia dużej ilości funkcji robota. Z tego powodu trudno było, m.in., chwytać dowolne obiekty ramieniem robota. Poza tym, całkowicie

uniemożliwione zostało przechodzenie do sterowania w trybie ręcznym. Podczas ataków prowadzących do awarii, w których sprzęt powodujący uszkodzenia zalewał system bezużytecznymi danymi, roboty stawały się nieprzydatne lub operowanie nimi pozostawało utrudnione.

W niektórych przypadkach, operatorzy byli w stanie zrównoważyć opisane zakłócenia na podstawie opracowania względnie prostego zadania obejmującego pracę z ruchomymi bloczkami. Naukowcy uważają, że w sytuacjach, gdzie precyzyjne ruchy mogą decydować o życiu lub śmierci, np. w przypadkach operacji chirurgicznej lub akcji poszukiwawczo – ratunkowej, tego typu cyberataki mogą nieść za sobą dużo bardziej skomplikowane konsekwencje.

Za pomocą niewielkiego zestawu niewłaściwych danych, zespół był zdolny przeprowadzić złośliwy atak aktywacji mechanizmu zatrzymania robota w sytuacjach awaryjnych czyniąc go w ten sposób bezużytecznym.



Raven II został opracowany przez naukowców UW w celu określenia możliwości przeprowadzania operacji z wykorzystaniem robotów sterowanych zdalnie.

Próby zostały przeprowadzone z wykorzystaniem zdalnie sterowanego robota Raven II z otwartym kodem źródłowym opracowanego przez profesora Blake Hannaforda z UW oraz byłego profesora UW Jacoba Rosena wspólnie z ich studentami. Raven II jest obecnie produkowany i sprzedawany przez firmę Applied Dexterity Inc. z siedzibą w Seattle. Jest to sterowany zdalnie robot nowej generacji stworzony do wspomagania badań nad zaawansowanymi technologiami dla potrzeb prowadzenia operacji chirurgicznych z wykorzystaniem robotów. System, o którym mowa, nie został jeszcze wdrożony do zastosowania klinicznego. Nie został on jeszcze zatwierdzony przez FDA.

Roboty operacyjne, które uzyskały już zatwierdzenie FDA do zastosowania klinicznego i które zazwyczaj umożliwiają chirurgom usuwanie guzów, naprawę zastawek serca lub przeprowadzać inne czynności metodami nieinwazyjnymi, wykorzystują zastosowanie odmiennych kanałów komunikacyjnych i zazwyczaj nie opierają one swojego działania na ogólnodostępnych sieciach publicznych, co mogłoby prowadzić do ułatwionego występowania cyberataków, nad którymi pracował zespół UW.

Źródło: http://www.nanowerk.com/news2/robotics/newsid=40010.php
http://laboratoria.net/technologie/23675.html
Informacje dnia: Jak otworzyć laboratorium? Dziękujemy za odwiedziny na targach Labs Expo W przyszłości będziemy jedli mięso z drukarki Ruszył nabór na wspólne projekty przedsiębiorców i naukowców; w puli 66 mln zł Błonica - choroba groźna także dla dorosłych 87% internautów uważa hejt za poważny problem społeczny Jak otworzyć laboratorium? Dziękujemy za odwiedziny na targach Labs Expo W przyszłości będziemy jedli mięso z drukarki Ruszył nabór na wspólne projekty przedsiębiorców i naukowców; w puli 66 mln zł Błonica - choroba groźna także dla dorosłych 87% internautów uważa hejt za poważny problem społeczny Jak otworzyć laboratorium? Dziękujemy za odwiedziny na targach Labs Expo W przyszłości będziemy jedli mięso z drukarki Ruszył nabór na wspólne projekty przedsiębiorców i naukowców; w puli 66 mln zł Błonica - choroba groźna także dla dorosłych 87% internautów uważa hejt za poważny problem społeczny

Partnerzy