

Wojskowy Instytut Łączności - Państwowy Instytut Badawczy

<https://www.wil.waw.pl/wil/oferta/laboratorium/laboratorium-analiz-ata/18155,Laboratorium-Analiz-Atakow-Cybernetycznych.html>
2021-11-28, 23:54

Laboratorium Analiz Ataków Cybernetycznych

Unikatowa komórka rozwijająca narodowe kompetencje w zakresie przeciwdziałania atakom cybernetycznym, posiadająca jeden z największych w Polsce superkomputerów (195 TFLOPS). W przeciwieństwie do innych jednostek naukowych, sprzęt ten wykorzystywany jest wyłącznie w obszarze cyberbezpieczeństwa i kryptologii.

LAAC dysponuje nowoczesną infrastrukturą teleinformatyczną wykorzystującą technologie wirtualizacji, chmury oraz sieci definiowanych programowo. Może być wykorzystana do badań nad metodami zapewniania bezpieczeństwa cyberprzestrzeni, w tym rozpoznania cyberzagrożeń, ich analizy oraz ochrony przed nimi poprzez:

prorowadzenie badań naukowych i prac rozwojowych nad wykrywaniem działań nieuprawnionych w sieciach teleinformatycznych:

- badań złośliwego oprogramowania (tworzenie algorytmów detekcji i modelowanie ataków),
- identyfikowanie anomalii w ruchu sieciowym (tworzenie wzorców ataków, wzorców ruchu „prawidłowego” i złośliwego, tworzenie ścieżek ataków, wyznaczanie najbardziej skutecznych miejsc i metod przeciwdziałania),
- detekcja ataków i anomalii na urządzenia końcowe (hosty, stacje robocze),

ciągłą analizę podatności systemów wykorzystywanych przez SZ RP na nowe generacje ataków cybernetycznych:

- tworzenie środowisk do modelowania i testowania podatności urządzeń i sieci na zamodelowane zagrożenia (w oparciu o infrastrukturę sieciową i moc obliczeniową LAAC - możliwość emulacji ponad 5.000 węzłów),

opracowywanie mechanizmów tworzenia świadomości sytuacyjnej dla zdarzeń w cyberprzestrzeni:

- modelowanie metod prowadzenia pasywnych i aktywnych operacji obronnych w cyberprzestrzeni z uwzględnieniem rozwoju systemów wizualizacji i planowania działań oraz budowy narzędzi defensywnych i ofensywnych,
- rozwój metod rozpoznania środowiska cyberprzestrzeni przeciwnika, w zakresie topologii sieci, podatności i możliwości ich eksploracji,
- rozwój metod zarządzania ryzykiem, w tym oceny wpływu zdarzeń w cyberprzestrzeni na działania w innych domenach prowadzenia działań militarnych, uwzględniając zasoby fizyczne i konieczność zapewniania ciągłości działań operacyjnych,

prowadzenie na potrzeby MON szkoleń w zakresie bezpieczeństwa cyberprzestrzeni na różnych poziomach zaawansowania,

utrzymanie i rozwój Laboratorium Analiz Ataków Cybernetycznych.

Infrastruktura LAAC pozwoli również na prowadzenie badań w dziedzinie funkcjonowania systemów dowodzenia i łączności, w tym tworzenia bezpiecznej infrastruktury teleinformatycznej, poprzez:

badania możliwości wdrażania w SZ RP standardów sieci FMN (ang. *Federated Mission Networking*) i bezpiecznej współpracy w środowisku federacyjnym,

badania mechanizmów zapewnienia niezawodności i odtwarzalności systemów dowodzenia i łączności,

badania możliwości zastosowania metod uczenia maszynowego i sztucznej inteligencji do budowy zaawansowanych funkcji rozpoznania.

Superkomputer (195 TFLOPS) działa pod kontrolą systemów:

OpenStack – system chmury obliczeniowej umożliwiający tworzenie wyodrębnionych środowisk komputerowych i sieci;

HPC – system zarządzania środowiskiem obliczeń wysokowydajnych (ang. *High Performance Computing*);



logo LAAC