🤩 Main

CRAFT: Cybersecure Robotics And Future Talent

CRAFT is an interdisciplinary education and training project focused on robotics cybersecurity. It brings together robotics, cybersecurity, and applied learning to help students understand security challenges in robotic systems and develop practical skills relevant to real-world environments.

CRAFT combines theoretical foundations with applied learning. The project supports student learning through: 3 hours theoretical modules; Offensive and defensive approaches; Hands-on activities in automotive, hardware security, and robotic labs; Tabletop exercises.

Authors: Yue Hu yue.hu@uwaterloo.ca, Sebastian Fischmeister sebastian.fischmeister@uwaterloo.ca

Course list

1. **Module 1: Analysis and Fingerprinting of Robot Traffic, Yue hu & Diogo Barradas**

   Course summary: Analyzes robotic network traffic to infer robot behaviour.

   Attack module: Uses eavesdropping, traffic analysis, feature extraction, and ML to infer robot actions.

   Defense module: Uses authentication, obfuscation, and traffic regularization to reduce inference risks.

   Hands-on Activity: Collect traffic from a robotic teleoperation system or simulation; Analyze traffic using protocol identification and summary statistics; Build an action classifier or an obfuscation-based defense

2. **Module 2: Teleoperation and Remote Presence Security in Robotics, Brandon DeHart**

   Course summary: Introduces teleoperation and its network security risks.

   Attack module: Intercepts, modifies, and takes over robot communication signals.

   Defense module: Secures communication using network protection and redundancy.

   Hands-on Activity: Interact with a remotely operated robot over a network; Perform signal interception and modification attacks; Implement and evaluate secure communication methods.

3. **Module 3: Vision-Based SLAM Security and Adversarial Attack on Mobile Robots, William Melek**

   Course summary: Introduces vision-based SLAM and its sensor security risks.

   Attack module: Covers data poisoning and sensor corruption attacks on vision inputs.

   Defense module: Uses ML models to detect corrupted and adversarial sensor data.

   Hands-on Activity: Corrupt image datasets used for SLAM localization; Train a classifier to detect and filter corrupted images; Evaluate navigation failures caused by unfiltered corrupted data.

4. **Module 4: Security in Robot Learning and Demonstrations, Yash Vardhan Pant**

   Course summary: Introduces robot learning from demonstrations and its security risks

   Attack module: Uses adversarial demonstrations to alter learned robot behavior.

   Defense module: Uses robust learning to detect and filter malicious demonstrations.

   Hands-on Activity: Implement RL and IRL in a simulated environment; Generate adversarial demonstrations to influence policies; Evaluate impact on behavior and system robustness.

5. **Module 5: Robots as AI Agents: Offensive and Defensive Privacy in Motion Planning, Stephen L. Smith**

   Course summary: Introduces privacy risks in robot motion planning.

   Attack module: Manipulates cost functions to gather data from sensitive regions.

   Defense module: Uses penalization and multi-objective planning for privacy.

   Hands-on Activity: Modify motion planning costmaps in simulation or on a TurtleBot; Implement offensive and defensive planner strategies; Analyze effects on robot paths.

6. **Module 6: Bug Finding by Fuzzing Robot Simulation, Meng Xu**

   Course summary: Introduces fuzz testing in robotic systems.

   Attack module: Uses fuzzing to discover bugs and vulnerabilities.

   Defense module: Examines software testing as a method to improve system robustness.

   Hands-on Activity: Perform fuzz testing on robotic software and simulations; Develop input corpora and identify unexpected behaviors; Evaluate robustness and identify vulnerabilities.

7. **Module 7: CAN Bus security and attacks in the automotive field, Sebastian Fischmeister**

   Course summary: Introduces CAN bus communication and its security vulnerabilities.

   Attack module: Covers ECU impersonation, message flooding, and protocol state attacks.

   Defense module: Uses rule-based and learning-based intrusion detection for CAN security.

   Hands-on Activity: Interact with a PCB set simulating CAN network of ECUs; Perform message sniffing, replay, or spoofing attacks; Analyse CAN frames to extract information and alter system behavior.

8. **Module 8: Secure Control Design for Automotive Systems, Mohammad Pirani**

   Course summary: Introduces control-layer security in automotive systems.

   Attack module: Covers stealthy and replay attacks on vehicle dynamics.

   Defense module: Uses detection and mitigation algorithms for vehicle control attacks.

   Hands-on Activity: Explore zero-dynamics, spoofing, and interference attacks; Simulate attacks using MATLAB; Develop and test defense mechanisms.

9. **Module 9: Hardware Manipulation and Electronics Packaging Security, Michael Mayer**

   Course summary: Introduces electronics packaging and physical-layer hardware vulnerabilities.

Attack module: Covers thermal manipulation and hardware tampering to alter chip behavior.

Defense module: Uses signal-based validation and device fingerprinting to verify hardware integrity.

Hands-on Activity: Manipulate hardware conditions (e.g., temperature) to alter system behavior; Observe and analyze effects of physical tampering; Evaluate detection and prevention of hardware-level attacks.

10. **Module 10: Radio Frequency Interference, George Shaker**

Course summary: Introduces wireless jamming and its impact on communication systems.

Attack module: Covers jamming techniques in comparison with spoofing.

Defense module: Uses beamforming and antenna design to mitigate jamming.

Hands-on Activity: Perform jamming experiments in controlled environments; Analyze device behavior under jamming; Compare responses across different setups.

11. **Module 11: Secure Processor Design, Hiren Patel**

Course summary: Introduces secure processor design and hardware vulnerabilities.

Attack module: Covers Spectre and cache side-channel attacks.

Defense module: Uses mitigation for speculative execution and cache leakage.

Hands-on Activity: Implement and analyze microarchitectural attacks; Measure timing to exploit side-channel information; Test mitigations against data leakage and memory faults.

12. **Module 12: Privacy and Security in Physical Interactive Technology, Oliver Schneider**

Course summary: Introduces privacy risks in wearables and haptic systems.

Attack module: Uses deceptive design to exploit user behavior and consent.

Defense module: Uses design techniques to ensure privacy, awareness, and safety.

Hands-on Activity: Explore offensive and defensive scenarios with physical or wearable tech; Design and prototype interactions using brainstorming and haptic sketching; Evaluate privacy and consent implications.

13. Module 13: Social Robots and Cybersecurity, Yue Hu & Leah Zhang-Kennedy

Course summary: Introduces social robotics and its cybersecurity risks.

Attack module: Uses robots for phishing, deception, and behavior manipulation.

Defense module: Detects and mitigates manipulative robot behavior.

Hands-on Activity: Interact with a social robot or simulation to elicit information; Identify manipulative questioning and interaction patterns; Design technical or human-centered defenses.