

Project Milestone Presentation

Instructor: Khaled Diab

Milestone Presentation

- Each group presents project progress
 - Presentation time shouldn't exceed 8 minutes
 - QA period is 1—2 minutes long
- First presentation starts at 9:30 am (sharp)
- To reduce switching overhead:
 - Each group needs to submit their slides through CourSys by 8 am
 - The file name should include your <group_id>
 - Acceptable formats: PDF, PPT, PPTX

Slides

- Motivation (1—2 min)
- Problem (1 min)
- Challenges (1 min)
- (Preliminary) Solution (2—3 mins)
- (Preliminary) Results (1—2 mins)
- Learned Lessons (Optional)

Current Projects

1. Tool/Attack: Implementing ROP gadget hunter
2. Attack/Defense: Controlling IoT devices through light commands
3. Defense: Detecting and repairing control-flow hijacking attacks
4. Attack: DNS rebinding attack for IoT devices
5. Detection: Automatic detection of malicious IoT behavior
6. Detection: Intrusion detection and concealment using GANs
7. Attack: HTTP desync attacks
8. Attack: Clickjacking attacks by exploiting XSS vulnerabilities
9. Tool/Defense: Implementing Virtual Private Network
10. Detection/Defense: Lightweight detection of DDoS attacks on SDN

Schedule

Time	Group
9:30—9:40	Implementing ROP gadget hunter
9:40—9:50	Controlling IoT devices through light commands
9:50—10:00	Detecting and repairing control-flow hijacking attacks
10:00—10:10	DNS rebinding attack for IoT devices
10:10—10:20	Automatic detection of malicious IoT behavior
10:20—10:25	Break
10:25—10:35	Intrusion detection and concealment using GANs
10:35—10:45	HTTP desync attacks
10:45—10:55	Clickjacking attacks by exploiting XSS vulnerabilities
10:55—11:05	Implementing Virtual Private Network
11:05—11:15	Lightweight detection of DDoS attacks on SDN
