Boston Cybernetics Institute
Capability Briefing

Brief Outline

1. **Introduction**
2. **BCI Services**
   - A. Cyber Survivability Assessments
   - B. Cybersecurity Training
   - C. Tool Development
3. **Summary**

Boston Cybernetics Institute, PBC

- Founded November 2017 by former Lincoln Laboratory staff and military veterans
- Public benefit corporation (PBC)
- **Mission:** Promote and provide cybersecurity training and education in furtherance of the national defense of the United States of America
- Contract Vehicles:
  - GSA IT Schedule 70 High Adaptive Cybersecurity Services #47QTCA20D001G
  - Existing 8A partner (Joint Venture and Prime/Sub)
  - Sole Source Potential (Under FAR 6.302-1 "One responsible source"; FAR 6.30202 "Industrial Mobilization")
  - Acquisition method DFAR 212.7102: Pilot Program for Acquisition of Military-Purpose Non-Developmental Items

Team Expertise

- **Jeremy Blackthorne**
  - Cyber System Assessments Group, Lincoln Laboratory, **3 years**
  - MS in Computer Science, Rensselaer Polytechnic Institute
  - PhD candidate in Computer Science, Rensselaer Polytechnic Institute
- **Reed Porada**
  - Cyber Division, Lincoln Laboratory, **11 years**
  - Naval Research Laboratory, **5 years**
  - MS in Software Engineering, Carnegie Mellon University
- **Rodolfo Cuevas**
  - Cyber and Missile Divisions, Lincoln Laboratory, **9 years**
  - MS in Electrical Engineering, Cornell University
  - PhD candidate in Electrical Engineering, Cornell University
- **Evan Jensen**
  - Cyber System Assessments Group, Lincoln Laboratory, **2 years**
  - Facebook Red Team, **1 year**
  - BS in Computer Science, New York University
- **Clark Wood**
  - Cyber System Assessments Group, Lincoln Laboratory, **3 years**
  - MS in Computer Science, Florida State University
  - MS in Technology Policy, Massachusetts Institute of Technology
- **Benjamin Kaiser**
  - Secure Resilient Systems and Technology Group, Lincoln Laboratory, **3 years**
  - MS in Computer Science, Rensselaer Polytechnic Institute
  - PhD student at the Center for Information Technology Policy, Princeton University

- ➢ **40$^+$ years experience**
- ➢ **Published authors**
- ➢ **College instructors**
- ➢ **DEFCON CTF finalists**

BCI Services

1 Cyber Survivability Assessments

2 Cybersecurity Training

3 Tool Development

1 Cyber Survivability Assessment: Capability

Assessment Methodology

Mission Definition

1. Define Mission
2. Define Adversary Space
3. Define Metric Space

Experimentation

4. Model System Under Test
5. Model Specific Adversaries
6. Measure/Simulate Interactions

Analysis

7. Produce Metrics
8. Forecast security violations
9. Recommend Improvements

Monitoring

10. Iterate
11. Monitor Assumptions

Products

1. Time forecasts for unacceptable losses
2. Recommended improvements
3. Transparent and extendable analysis
    - System and adversary models
    - Measurements/simulations
    - Metrics
    - Attack demonstrations
    - Assumptions to monitor

1 Cyber Survivability Assessment: Experience

1. Found and demonstrated vulnerabilities in a Boeing 757 via external long range radio for the DHS Aircraft Cyber Evaluation (ACE) program [1]
2. Led a Data-driven cyber risk assessment for the FAA Aircraft Systems Information Security Protection (ASISP) program [2]
3. Support Col. William Young in creation of System-Theoretic Process Analysis for Security (STPA-Sec) [3], now taught at Air War College and Air Force Institute of Technology
4. Analyzed survivability of smartphone app for US Special Operations unit
5. Analyzed counter UAV/UAS for Massachusetts Department of Transportation Drone Pilot Program
6. Analyzed attack surface of Windows Event Logging for ARCYBER Cyber Protection Teams
7. Supported air vehicle survivability assessments for the Air Force Red Team

2 Cybersecurity Training: Capability

BOSTON CYBERNETICS INSTITUTE

Topics

- Reverse-Engineering
- Malware Analysis
- Vulnerability Assessment
- Exploit Development
- Secure Software Development
- Critical Thinking
- Systems Analysis
- Cybersecurity for Acquisitions

Services

- 1-hour brief to 24-week bootcamp
- Interactive, hands-on-keyboard training
- Custom curriculum development
- Follow-on coaching and mentorship

Location

- 40-person Boston classroom
- 16-person portable classroom
- All hardware/software provided

2 **Cybersecurity Training:** Experience

BOSTON CYBERNETICS INSTITUTE

- Government/Military
  - *Intro to Cybersecurity*, 1-day class, Air Force and SOCOM Acquisitions, 2016, 2017
  - *Reverse-Engineering*, 1-week class, Air Force 46th Test Squadron, 2017
  - *Vulnerability Assessment for Embedded Systems*, two 2-week classes, NAVAIR, 2017
  - *Vulnerability Research for Embedded Systems*, 1-week class, MITRE, 2018, 2019
  - *Vulnerability Research for Embedded Systems*, 2-week class, Air Force 90th COS, 2019
- Academia
  - *Penetration Testing and Vulnerability Analysis*, NYU-Tandon, 2012 – 2013 [6]
  - *Malware Analysis*, Rensselaer Polytechnic Institute, Spring 2013 [4]
  - *Modern Binary Exploitation*, Rensselaer Polytechnic Institute, Spring 2015 [5]
  - *Reverse-Engineering, multi-day* classes at MIT [8], RPI, BU, and West Point [9]
  - *Software Reverse-Engineering*, Tufts University, Spring 2019 [14]
- Conference Trainings
  - *Intro to Modern Binary Exploitation, Program Analysis with Binary Ninja,* REcon Montreal 2019
  - *Reverse Engineering with Ghidra*, RingZer0 2019
  - *Reverse Engineering with Ghidra*, Hack in the Box – Abu Dhabi 2019
  - Intro to Reverse-Engineering and Exploitation, AvengerCon 2019
- Capture-the-Flag Teams
  - Misc. topics, Lab RATs, Lincoln Laboratory, 2014 – 2016, DEFCON finalists 2017 [15]
  - Misc. topics, RPISEC [10], Rensselaer Polytechnic Institute , 2013 – 2015, DEFCON finalists 2018

3 Tool Development: Capability

1. Capability development for evading security products
2. Reverse-engineering closed systems
    a. to create interoperability layers
    b. to create open counterparts
    c. to create documentation
3. Extending closed systems
    a. through recombination of existing functionality
    b. through direct binary modification
4. Software implementation from standards documents

3 Tool Development: Experience

1. Developer on LARIAT: Cyber range simulation and management technology
2. AVLeak: anti-virus emulator artifact extractor [11]
3. Virtual machine side-channel communication tool [12]
4. Developed offensive tools for opposition force of Lincoln's Project C [13]
   a. Polymorphic memory-only implants
   b. Bespoke command and control protocols
   c. Evaded antivirus and intrusion detection
5. Developed low-level data transfer libraries/protocols for ARINC-429, SPI, USB, Ethernet, PCIe, and many others
6. Shellcode/assembly development for MIPS, SPARC, ARM, x86/x64, PowerPC, and MSP-430

Company Overview

The Boston Cybernetics Institute is a public benefit corporation, founded in 2017 by former cyber security researchers from MIT Lincoln Laboratory.

Its **mission** is to promote and provide cyber-security education and training in furtherance of the national defense of the United States of America.

Current Contracts

- Massachusetts Department of Transportation Drone Program cybersecurity consulting
- Cybersecurity executive protection services
- GSA IT Schedule 70 High Adaptive Cybersecurity Services #47QTCA20D001G

BOSTON CYBERNETICS INSTITUTE

Past Performance

- ARCYBER through Lincoln Laboratory, cybersecurity curriculum development, research, and consulting
- MITRE Embedded Systems Vulnerability Research Courses, 2018 and 2019
- 90th Cyber Operations Squadron 2-week Embedded Systems Vulnerability Research Course 2019

Certifications

- Secret and TS cleared Personnel
- Small Business
- Cage Code: 80CU5
- DUNS: 080984337

Jeremy Blackthorne
President
jblackthorne@bostoncybernetics.org
(248) 675-7577

CJ Lawson
Chief Operations Officer
cjlawson@bostoncybernetics.org
(540) 735-5013

Amber Forti
Senior Contracts Manager
aforti@bostoncybernetics.org
(540) 656-8037

References (1/2)

[1] “DHS FOIA Release (page 57): Aircraft Cyber Evaluation (ACE) ver. 8,” 2016. [Online]. Available: https://fortunascorner.com/wp-content/uploads/2018/06/DHS-Document-Release-on-Aviation-Cybersecurity.pdf.

[2] “DHS FOIA Release (page 7): Aircraft Systems Information Security Protection (ASISP) Research,” 2017. [Online]. Available: https://fortunascorner.com/wp-content/uploads/2018/06/DHS-Document-Release-on-Aviation-Cybersecurity.pdf. [Accessed: 09-Dec-2018].

[3] Young, W., & Porada, R. (2017). System-Theoretic Process Analysis for Security (STPA-SEC): Cyber Security and STPA. In *2017 Stamp Conference*. Retrieved from http://psas.scripts.mit.edu/home/wp-content/uploads/2017/04/STAMP_2017_STPA_SEC_TUTORIAL_as-presented.pdf

[4] J. Blackthorne and B. Yener, “CSCI 4972/6963 Malware Analysis,” 2013. [Online]. Available: http://security.cs.rpi.edu/courses/malware-spring2013/. [Accessed: 04-Mar-2018].

[5] P. Biernat *et al.*, “Modern Binary Exploitation - CSCI 4968,” 2015. [Online]. Available: https://github.com/RPISEC/MBE. [Accessed: 02-Apr-2018].

[6] E. Jensen and D. Guido, “CS 6573 Penetration Testing and Vulnerability Analysis.” [Online]. Available: http://bulletin.engineering.nyu.edu/preview_course_nopop.php?catoid=5&coid=14223. [Accessed: 04-Mar-2018].

[7] N. Daswani, “CS-GY 9163 Application Security,” 2014. [Online]. Available: http://bulletin.engineering.nyu.edu/preview_course_nopop.php?catoid=9&coid=23997. [Accessed: 04-Mar-2018].

[8] J. Blackthorne, P. Hulin, and T. Leek, “January 2016 MIT IAP Courses,” 2016. [Online]. Available: https://beaverworks.ll.mit.edu/CMS/bw/iap. [Accessed: 04-Mar-2018].

[9] “Deans Weekly Significant Activities Report: 16 September 2015,” 2015. [Online]. Available: https://www.usma.edu/centers/Deans Weekly Activity Report Past Issues/Dean’s Weekly Significant Activities Report 16 September 2015.pdf. [Accessed: 04-Mar-2018].

[10] “RPISEC.” [Online]. Available: https://rpis.ec/. [Accessed: 04-Mar-2018].

[11] J. Blackthorne, A. Bulazel, A. Fasano, P. Biernat, and B. Yener, “AVLeak: Fingerprinting Antivirus Emulators Through Black-box Testing,” in *Proceedings of the 10th USENIX Conference on Offensive Technologies*, 2016, pp. 91–105.

[12] S. d’Antoine, J. Blackthorne, and B. Yener, “Out-of-Order Execution as a Cross-VM Side Channel and Other Applications,” in *1st Reversing and Offensive-Oriented Trends Symposium*, 2017.

[13] M. L. Rossey, “Project C - Equipping the U.S. Cyber Protection Teams,” 2014. [Online]. Available: http://www.itea.org/images/pdf/conferences/2014_Tech_Review/Rossey_2014-11-05 ITEA MIT LL - email.pdf. [Accessed: 09-Dec-2018].

References (2/2)

[14] Tufts Course Schedule Spring 2019. Retrieved May 19, 2019, from https://www.cs.tufts.edu/t/courses/schedules/spring2019

[15] Dorothy, R. (2017). MIT Lincoln Laboratory team scores big at international hacking event | MIT News. Retrieved May 19, 2019, from http://news.mit.edu/2017/mit-team-lincoln-laboratory-scores-big-at-def-con-hacking-competition-0918

Appendix: Recorded Conference Presentations

Jeremy Blackthorne and Alexei Bulazel
Three Heads are Better Than One: Mastering NSA's Ghidra Reverse Engineering Tool
INFILTRATE 2019
https://vimeo.com/335158460

Evan Jensen and Rudy Cuevas
iPhone Surgery for the Practically Paranoid
Schmoocon 2019
https://www.youtube.com/watch?v=kJO43qvstCk&list=PL7-g2-mnZwSHh8eDi19IJkEiDxvj6iWIO&index=40