# Hacking 101

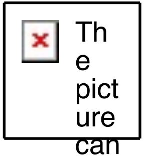
Jeremy Blackthorne

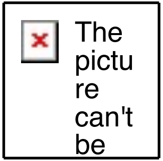
Boston Cybernetics Institute

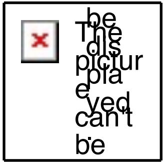
October 27th, 2021

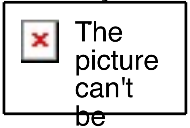
# Introduction: Jeremy Blackthorne

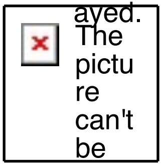
- **Boston Cybernetics Institute**
  - Co-founder and President
  - Research, consulting, and training
  - “Empowering people to control technology”
- **Former MIT Lincoln Laboratory**
  - Cyber System Assessments Group
  - “... gain and maintain unauthorized control over hardware/software systems.”
- **Education**
  - Bachelor in CS, University of Michigan - Dearborn
  - Master in CS, Rensselaer Polytechnic Institute
  - PhD candidate in CS, Rensselaer Polytechnic Institute
- **United States Marine Corps (2002 – 2006)**
  - 1st Battalion, 7th Marines, 1st Marine Division
  - Rifleman/scout sniper, three tours in Iraq
  - Currently a Cyber Auxiliarist


The picture can't be displayed.


The picture can't be displayed


The picture can't be displayed.


The picture can't be displayed.


The picture can't be displayed

# 1 Cyber Survivability Assessments: Experience

- Found and demonstrated vulnerabilities in a Boeing 757 via external long-range radio for the DHS Aircraft Cyber Evaluation (ACE) program [2]
- Led a Data-driven cyber risk assessment for the FAA Aircraft Systems Information Security Protection (ASISP) program [3]
- Support USAF Col. William Young in creation of System-Theoretic Process Analysis for Security (STPA-Sec), now taught at Air War College and Air Force Institute of Technology
- Analyzed survivability of smartphone app for US Special Operations unit
- Analyzed UAS / counter UAS for Massachusetts Department of Transportation Drone Pilot Program
- Analyzed attack surface of Windows Event Logging for ARCYBER Cyber Protection Teams
- Supported air vehicle survivability assessments on the Air Force Red Team
- Published Dec 2020 report with the Atlantic Council and Lincoln Laboratory, titled
  HOW DO YOU FIX A FLYING COMPUTER, Seeking Resilience in Software-Intensive Mission Systems: https://www.atlanticcouncil.org/wp-content/uploads/2020/12/How-do-you-fix-a-flying-computer.pdf

# 2 Cybersecurity Training: Capability

## Topics

- Linux / Windows
- Reverse-Engineering
- Malware Analysis
- Vulnerability Assessment
- Exploit Development
- Secure Software Development
- Systems Analysis
- Critical Thinking
- Data Science
- Machine Learning

## Services

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

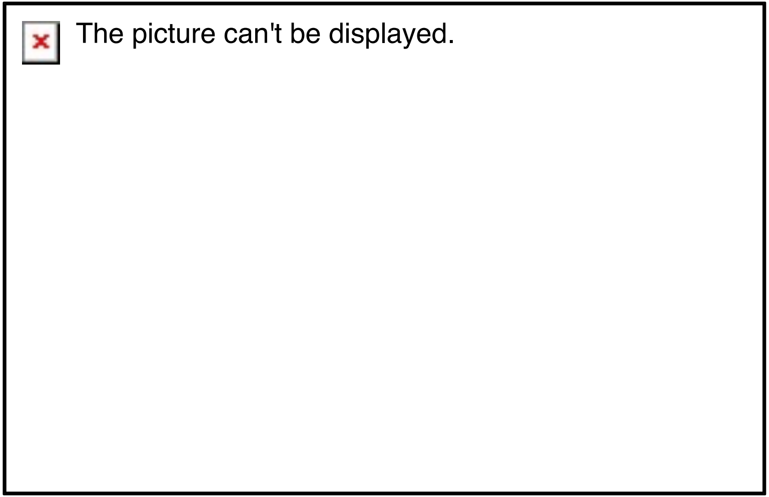
## Location

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

## Sample Lessons

https://www.youtube.com/channel/UCK1_Mwl_1FEH7z7MZPsAGvA

# 2 **Cybersecurity Training:** BCI Classroom

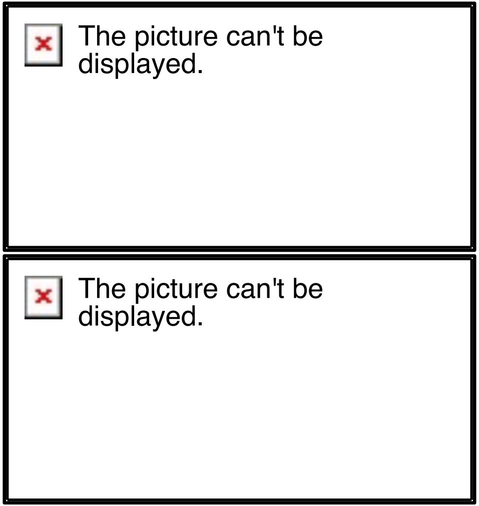


The picture can't be displayed.

BCI classroom in Fall 2019 arranged for a class of 20 students.

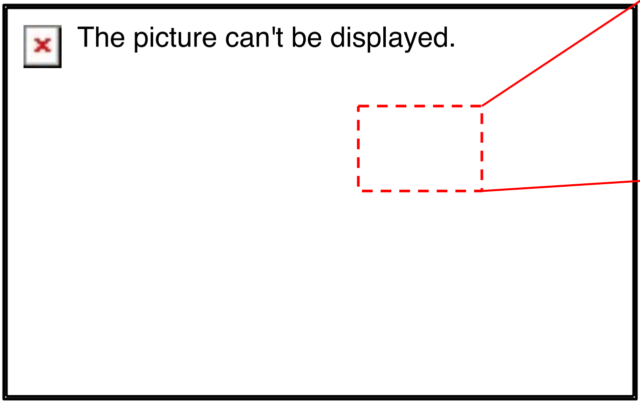
# 2 Cybersecurity Training: Remote Training Studios

- Quad-monitor setup
- 4k camera
- Quality microphone
- Drawing tablet
- Student test computer
- Studio lighting

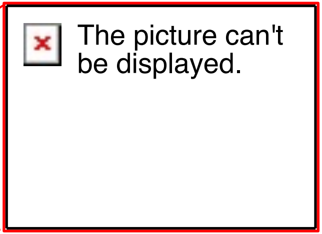

The picture can't be displayed.
The picture can't be displayed.

Broadcasting studios 1 and 2 (top and bottom).

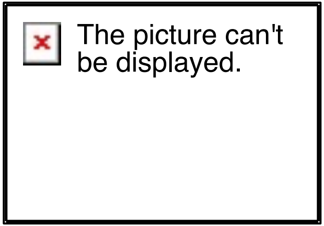
# 2 **Cybersecurity Training:** Embedded Systems Analysis



Instructor live broadcasts HD video to students of an embedded system under a microscope.



Live HD video of microscope.



System under microscope.

# 2 **Cybersecurity Training:** Recent Academic Experience

### Yale

- *Intro to Binary Reversing and Exploitation*, invited 1-day workshop, Dec. 2019
- https://seas.yale.edu/news-events/events/intro-binary-reversing-and-exploitation

### Harvard

- *Intro to Reversing and Exploitation*, invited 1-day workshop, Nov. 2019
- Student review: https://www.linkedin.com/feed/update/urn:li:activity:6604189668877623296/
- Director of Cyber Project at Harvard Belfer Center: https://twitter.com/LZXDC/status/1198962703521525760

### MIT

- *Reverse Engineering Software*, invited 1-week IAP Course, Jan. 2016
- http://web.mit.edu/iap/www/iap16/searchiap/iap-9289af8f51340f9501513cc17d7f0154.html

### West Point

- *Software Reversing and Exploitation*, invited 2-day workshop, 2015
- https://drive.google.com/open?id=1rVpbITRE90590DFK25X1ukoq8PJskqvG
- https://www.facebook.com/141834871911/photos/the-cadet-competitive-cyber-team-c3t-competed-in-the-annual-cyberstakes-live-cap/10153971978366912/

### Tufts

- *Software Reverse Engineering*, Spring semester 2019: https://www.cs.tufts.edu/t/courses/schedules/spring2019
- *Into to Binary Reversing,* 1-day workshop for WiCS 2019: https://www.linkedin.com/feed/update/urn:li:activity:6632037758808449024/

### RPI

- *Modern Binary Exploitation*, Spring semester 2015: https://github.com/RPISEC/MBE
- *Malware Analysis*, Spring semester 2013: http://security.cs.rpi.edu/courses/malware-spring2013/

# 2 Cybersecurity Training: Recent Industry Experience

## AvengerCon 2020, 2019

- *Intro to Binary Reversing and Exploitation* (1-day)
- https://www.avengercon.com

## INFILTRATE 2020

- *Reverse Engineering with Ghidra* (4-day)
- https://infiltratecon.com/conference/training/reverse-engineering-with-ghidra.html
- Review: https://systemoverlord.com/2020/10/17/course-review-reverse-engineering-with-ghidra.html

## RingZer0 2021, 2020, 2019

- *Reversing with Ghidra* (4-day)
- https://ringzer0.training/reverse-engineering-with-ghidra.html

## REcon 2019

- *Intro to Modern Binary Exploitation* (4-day)
- https://recon.cx/2019/montreal/training/trainingmodern.html
- Review: https://twitter.com/DarthMaulware/status/1144381376910643200
- *Program Analysis with Binary Ninja* (4-day)
- http://recon.cx/2019/montreal/training/traininganalysis.html

## Hack in the Box, Abu Dhabi 2019

- *Reversing with Ghidra* (4-day)
- https://conference.hitb.org/

# 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 (now licensed to SimSpace and Circadence)
2. AVLeak: anti-virus emulator artifact extractor [4]
3. Virtual machine side-channel communication tool [5]
4. Developed offensive tools for opposition force of Lincoln’s Project C [6]
    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

# 3 **Tool Development:** Recent Conferences

## REcon 2019

- *The Backdoor Foundry: A Toolchain for Building Application Specific Implants*, Evan Jensen
- https://www.youtube.com/watch?v=796gFJKFFHc

## SchmooCon 2019

- *iPhone Surgery for the Practically Paranoid* by Evan Jensen, Rudy Cuevas
- https://www.youtube.com/watch?v=kJO43qvstCk

## INFILTRATE 2019

- *Three Heads are Better Than One: Mastering Ghidra* by Alexei Bulazel, Jeremy Blackthorne
- https://vimeo.com/335158460

## CounterMeasure 2019

- *Reverse-Engineering with NSA's Ghidra* by Jeremy Blackthorne
- https://youtu.be/ciS61BTzpN0

## UAS Summit 2019 – AUVSI New England

- *Commonwealth CUAS Program* by Rodolfo Cuevas
- *Drone Data: Security and Privacy Implications* by Reed Porada
- http://auvsinewengland.org/events-3/robotica-series-events/uas-summit-2019/uas-summit-2019-agenda.html

# References

[1] "TITLE 8 - CHAPTER 1. GENERAL CORPORATION LAW - Subchapter XV. Public Benefit Corporations," 2019. [Online]. Available: http://delcode.delaware.gov/title8/c001/sc15/. [Accessed: 11-Apr-2019].

[2] "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.

[3] "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].

[4] 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.

[5] 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*, 2017.

[6] 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].

[7] "iPhone Surgery for the Practically Paranoid - Evan Jensen & Rudy Cuevas - YouTube." [Online]. Available: https://www.youtube.com/watch?v=kJO43qvstCk. [Accessed: 09-Dec-2019].