MacB
Integrated Laboratories

Cyber Center of Excellence

San Antonio, Texas

Overview

We recognize that innovative ideas come from inspired people working in a creative environment. Our track record of innovation demonstrates our ability to identify areas where innovation can have major impact on operations. Working in concert with our Government counterparts, MacB's SMEs identify shortfalls in technology, processes, and personnel skills/experience and resolve them.

We developed the Cyber Center of Excellence in 2009 to provide training and certification solutions to our personnel, to provide hands-on laboratories to practice and improve their craft, and to develop cutting edge solutions to problems facing our clients in the information security arena. Our vision for the Cyber Center of Excellence includes partnering with government clients to identify specific operational or technical challenges, resulting in focused IR&D initiatives leading to innovative solutions to real-world problems.

MacB has a 20,000+ sq. ft. facility in San Antonio, Texas. Within this facility, we have a state-of-the-art reverse engineering and development lab housed inside of a 6,000+ sq. ft. SCIF which has been accredited by a Government customer. There is an additional 7,000 sq. ft. that has been constructed to DCID 6/3 and 6/9 standards allowing it to be easily accredited to meet emerging customer requirements. Finally, we have a 60-person, multi-purpose training/conference room with projection screens that can also be used as a Temporary Secure Working Area.

Wireless Cyber Network Operations

Computer & Network Forensics

Software Tool Development

Reverse Engineering

San Antonio, TX
4440 Piedras Dr. South, Ste. 300
San Antonio, TX 78228
210.732.7417

Corporate HQ
4021 Executive Drive
Dayton, OH 45430
937.426.3421

National Capital HQ
1953 Gallows Rd., Ste. 590
Vienna, VA 22182
703.761.0770

MacB POC
marketing-comms@macb.com

www.macb.com

Advanced Engineering Services and National Security Solutions

Mission Area/Technical Domain

System-Based Forensic Analysis

- ***FTK*** – a first responder's forensic toolkit with tools for live-approach system-based forensic analysis
- ***MemDump*** – a utility to forensically capture volatile memory without adversely impacting chain-of-custody during live-approach forensics
- ***KeyDump*** – a USB Key forensic analysis tool used to forensically examine USB file systems in a forensic sandbox
- ***USBCapture*** – a utility allowing analysts to seize control of the USB bus on a host without detection by Windows security logging
- ***Linux Virtual Memory Mapper*** – A utility to dump each running processes virtual memory

Reverse Engineering Embedded/Malwares

- ***RESynergy*** – a cross-platform collaboration tool allowing multiple reverse engineers to work on a single code base
- ***EMBERE*** – a tool that automates the comparison of multiple binaries for points of interest that may be in relation to malware hook points
- ***Splinter*** – a utility providing trusted debugger stubs for real time operating systems (RTOS)
- ***BlackMesa*** – custom debugger for an embedded operating system

System/Network Vulnerability Assessment

- ***NKC*** – A scriptable TCP/IP network packet scripting language used for network traffic analysis and vulnerability testing
- ***NAIL*** – An application that provides network fingerprinting capabilities
- ***Stingray*** – A visual pcap diffing utility
- ***Charibdis*** – A traffic injection capability designed to spoof source IP of traffic sequences to masquerade as legitimate traffic

Sensing and Exploitation

- ***Erebus*** – Customized android handset with mission intuitive interface providing enhanced sniffing/capture/and interrupt capabilities
- ***WiMax Sniffer*** – A software defined radio for WiMax frame capture and decoding, as well as traffic analysis and traffic injection
- ***Dolus*** – An android application implant prototype that enabled exfiltrating GPS fix, SMS, email, etc. (previous incarnations on Symbian OS9, BlackBerry, and Motorola platforms)
- ***Maelstrom*** – A real-time network forensics engine that provides clandestine collection of host-based data and network traffic

Training and Certification

- ***Reverse Engineering Fundamentals*** – a combination of CBT and hands-on instruction in reverse engineering tools and techniques
- ***MacB Standards*** – a combination of documents providing insight into our methodologies for Reverse Engineering and Security Testing
- ***MacDoodle*** – an online course management system containing training to provide an introduction to reverse engineering as well as an introduction to contract specific tasks