DATA SHEET

OWL Cyber Defense

Device Vulnerability Assessment

The Problem

Do you know what your device really does? Whether explicit or not, you have security goals for every computing device and application you use. You have to make sure you understand how well protected, and how resilient your systems are to attack. That means understanding the threats you face and configuring systems appropriately for your environment.

We can help you assess your threat model, and evaluate your application or device against that model. We approach your device like an attacker would, finding things a defender might not see. We can ensure that your solution complies with best practices, standards, and regulations, and can shorten time to market and accreditation, while helping to reinforce public and user acceptance. We keep up with both the good guys and the bad guys, so we're aware of the latest threats and mitigations.

Our time-proven systems and processes help our customers maintain a holistic defense against numerous fast-changing problem areas. We provide independent validation, providing an unbiased assessment of risk and security posture. Our experts find what you don't know – the "unknown unknowns" related to security posture, risk and liability, and regulatory compliance. We dissect your product and analyze it for vulnerabilities against agreed-upon security objectives. Our approach is platform agnostic, with cross-technology awareness of hidden issues.

What We Do For You

Owl created the Device Inspection Analysis Laboratory (DIAL) to perform custom security inspections of wired, wireless, computer processing equipment, network devices and mobile hardware and associated software products, infrastructure and communications equipment, end-user devices, application software, and stand-alone devices.

> *We test what you can't – with our extensive state-of-the-art lab and resources*

OUR EXPERIENCE

For DIAL analyses, Owl applies an experienced team of subject matter experts in multiple technologies, including:

- Secure mobile operating system development
- System and architectural security
- Operating system internals
- Network security
- Authentication and authorization technology
- Forensics inspection and analysis
- Exploit development and fuzzing
- Wireless, Bluetooth, and Near Field Communications (NFC) inspection
- DoD Security Technical Implementation Guide (STIG) development and validation
- Black-box, Gray-box, White-box testing
- Reverse engineering
  - Computers (servers, laptops, workstations, etc.)
  - Mobile devices (phones, tablets, NFC endpoints, Bluetooth, WiFi, etc.)
  - Infrastructure hardware (routers, switches, firewalls, IDS/IPS, etc.)
- Security Enhanced Linux (SELinux) and SELinux for Android™
  - Policy development
  - Coverage and enforcement analysis
  - Extensibility and code enhancement of your design gives you the confidence that your solution won't become their problem.

What We Do For You (Continued)

DIAL is a cost-effective state-of-the-art resource for independent verification and validation (IV&V) of products and systems, including systems composed of multiple hardware and software elements. The primary output from Owl DIAL team analyses is a vulnerability assessment detailing all observable security strengths and weaknesses identified during testing and analysis. Understanding the potential vulnerabilities enables our customers to mitigate security liabilities and deploy with the confidence that their system is appropriately protected.

SECURED BY OWL

Our Tools

The Owl DIAL puts commercially available and in-house developed tools in the hands of some of the top subject matter experts in the industry to analyze the deepest aspects of system security. Our primary resources include:

- Cybersecurity professionals with experience in penetration testing, device rooting, exploit development; SELinux policy analysis & development; Android hardening
- Device Inspection Analysis Lab
  - 2G cellular base station
  - Electronics test & measurement equipment, microscopes
  - IDA Pro
- Mobile Forensics tools that can extract data from 1000's types of devices, including: MSAB XRY and Cellebrite UFED
- Device Analysis Regression Test Harness (DARTH). Simulates touchscreen input, takes snapshots of screen via micro-HDMI interface, and compares to expected output

Why Owl?

Our security specialists have a broad foundation for understanding the peculiarities of device, software, and protocol inspection from both a defensive and offensive posture. An Owl independent security evaluation provides our customers, and any associated certification or approving authority, a high degree of confidence that their security objectives are being met. Owl's reputation within the U.S. Government security community provides additional confidence to approving officials in providing justification to authorize operation. Our DIAL evaluations aid in shortening the approval process and provide a level of confidence that, as future threats evolve, every reasonable precaution has been and will be taken to avoid compromise.

Want to learn more about the our Device Vulnerability Assessment and how it can help you?

Please contact the Owl team at info@owlcyberdefense.com

OWL Cyber Defense

Owl Cyber Defense Solutions, LLC leads the world in data diode and cross domain network cybersecurity. With a constant focus on customers in the military, government, critical infrastructure, and commercial communities, Owl develops market-first, one-way data transfer products to meet a variety of operational needs, from entry level to enterprise.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com