DATA SHEET

System Evaluation, Exploitation, and Research (SEER)

The Problem

How well do you actually know your application or device?
Whether explicitly required or not, it is vital to understand the risks related to their use, including how well designed, protected, and resilient they are to attack. That means understanding the potential threats and how they might infiltrate, exploit, or disable your systems and how to appropriately design, configure, and architect your systems to mitigate those threats while meeting the needs of your environment.

Are you intrigued by a particular technology or system?
The decision to adopt a new technology must be made with appropriate prudence and thoughtfulness. Whenever a new integrated system or application is proposed, you must first verify and validate the premise, purported functionality, and alleged security. Once assessed, there are often mitigations and improvements that must be implemented to meet the needs of your environment and security standards.

The Owl Solution

Created in 2010, the Owl **System Evaluation, Exploitation, and Research (SEER)** laboratory (previously DIAL) is designed to perform custom security assessments of integrated systems and applications to inform actionable decisions.

SEER is the cost-effective, state-of-the-art resource for independent security inspection and testing of products, systems, and applications, including systems composed of multiple hardware and software elements. For our analyses, the SEER lab employs an experienced team of subject matter experts in a variety of technologies. The primary output from SEER analyses is an evaluation report detailing the security strengths and weaknesses identified during testing.

SEER experts find what you don't know – the "unknown unknowns" – through a thorough dissection of your products and systems, analyzing them for vulnerabilities against your security objectives.

The Owl SEER Lab Helps You:

+ Maintain a holistic defense against rapidly evolving threats
+ Gain an unbiased understanding of potential vulnerabilities
+ Assess your threat model and mitigate security liabilities
+ Ensure compliance with best practices, regulations, and standards
+ Reinforce public and user acceptance and deploy with confidence

OUR EXPERIENCE

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

+ Secure mobile operating systems
+ System and architectural security
+ Operating system internals
+ Network security
+ Authentication and authorization technology
+ Forensics inspection and analysis
+ Exploit development and fuzzing
+ Wireless and Bluetooth inspection
+ DoD Security Technical Implementation Guide (STIG) and NIST / RMF validation
+ Black-box, Gray-box, White-box testing
+ Reverse engineering
  + Computers
  + Mobile devices
  + Infrastructure hardware
  + Applications
+ System analysis
  + Web and Cloud
  + Single-Board Computer
  + Tablet
  + Virtual Machine
  + Containerized
+ Security Enhanced Linux (SELinux) policy coverage and enforcement analysis

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

SEER Process

SEER generalizes methodologies from industry standard guidelines. Your needs drive every aspect of our security evaluations and research.

- **Objectives:** requirements gathering and scoping
- **Technical Plan:** functional decomposition of target, overview of intended approach, mapping to objectives
- **Evaluation:** analysis based on proven security guidance – Open Source Security Testing Methodology Manual (OSSTMM), Penetration Testing Execution Standard (PTES), Open Web Application Security Project (OWASP), NIST/RMF, MITRE ATT&CK, and DoD STIGs
- **Interim Updates:** advisories of any critical or high findings
- **Report:** executive summary, target of evaluation overview, approach, results, and recommendations
- **Debrief:** review all findings and recommendations

SEER Tools

SEER puts the top commercially available, open source, 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:

- **Cellular base stations:** 2G, 3G, 4G, and 5G
- **Mobile Forensics tools:** MSAB XRY and Cellebrite UFED
- **Reverse engineering tools:** Ghidra, jadx, and more
- **Dynamic analysis tools:** Objection/Frida, MobSF, Android Studio, and more
- **Network analysis tools:** Burp Professional, nmap, Aircrack-ng, Wireshark, and more
- **Our in-house Device Analysis Regression Test Harness (DARTH):** Simulates user device input and automates mobile device analysis.

Why SEER?

An independent security evaluation provides you, and any associated certification or approving authority, a high degree of confidence that your 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 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 our System Evaluation, Exploitation, and Research laboratory and how it can help you?

Contact us today at **info@owlcyberdefense.com** or visit **owlcyberdefense.com**

SECURED BY OWL

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