IOActive®

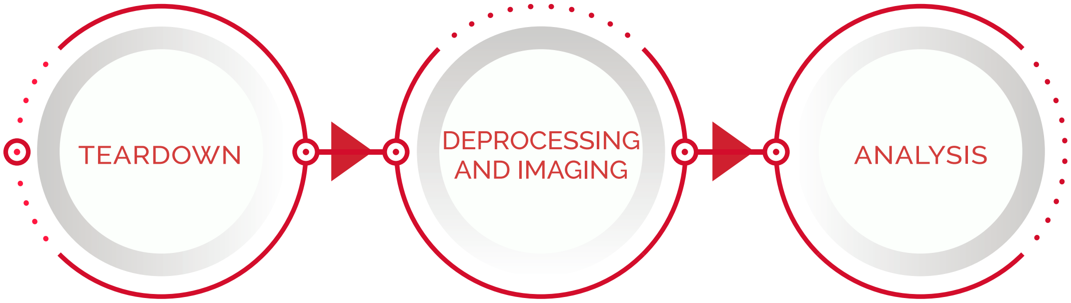
Research-fueled Security Services

Silicon Security Services

IOActive has spent over two decades at the forefront of cybersecurity, using a research-fueled approach intended to identify novel attack paths before they can be discovered and exploited by malicious threat actors. As the security of systems (and systems of systems) increasingly depends upon proper hardware security design and implementation, IOActive has invested in honing silicon-level attack techniques that complement the advanced embedded-device, side-channel, and fault-injection attacks we've perfected.

> *IOActive's silicon security team helps risk managers, product owners, designers, and cybersecurity professionals understand and manage the emerging risks of silicon-level and hardware-based supply chain attacks.*

Our silicon security practice has added black-box and gray-box attacks to our commercial white-box work, which includes development of threat models at the microprocessor and SOC level, supporting clients in defining security design requirements, and performing register transfer level (RTL) and GDS partial layout reviews.


TEARDOWN

DEPROCESSING AND IMAGING

ANALYSIS

Key business services generated from IOActive's refined black-box techniques include the following:

Research and Analysis

An understanding of the basic floorplan and node technology of a microchip supports a wide variety of functions, including initial assessments around security architecture, feature sets, and custom optimizations. This understanding can be critical in determining whether to use a particular model and supplier for a product, or whether a more thorough analysis of an IP infringement incident is warranted.

Security Feature Confirmation and Assessment

The choice of hardware supplier and implementation can have a highly consequential impact on the overall security of a product or ecosystem. This consequence is often more impactful with hardware than with software, since many hardware vulnerabilities cannot be fixed with shipping a patch, necessitating costly physical replacement of the device or component. It's critical to know that a key supplier is delivering on the promised security features of their product.

Netlist Extraction

The extraction of a netlist—the high-level logical design of a microchip—is a key step in developing a detailed understanding of a microchip. IOActive can use a netlist to develop a detailed, chip-specific attack, our clients may employ it to gain an understanding of the critical operation details necessary for making informed security risk assessments.

Data Extraction NVMs

The extraction of key information stored in ROM, Fuse, EEPROM or Flash, such as firmware or cryptographic material from a secure element, processor, or system-on-chip (SOC), can have impactful consequences for the security of the device and ecosystem. Additional analysis of the extracted data using traditional software reverse-engineering techniques may lead to the development of useful remote-code execution attacks on an otherwise secure device. Also, the loss of cryptographic material may enable a malicious company to create unlicensed product clones, or allow an attacker to compromise an entire fleet of devices.

Supply Chain Risk Sampling

There have been numerous recent examples of counterfeit chips on the market, sold knowingly or unknowingly by distributors and resellers. Using a risk-appropriate level of technical and sampling assessment, we can provide a desired statistical level of assurance that the pool of components are not counterfeits.

Hardware Backdoor Detection

A hardware backdoor exploit can occur when the attacker has access to the design of the chip. The design of the chip is altered by the attacker, either by changing or adding circuitry to the original design. This can expose the device so that activity can be monitored, or data stolen from the system without being noticed. IOActive has the technology and expertise to compare a known good chip against the current supply. Transistor-level analysis can detect the presence of any changes in the hardware.

IP Infringement Support

It's not unusual for competitors to infringe on particular intellectual property (IP), either intentionally or unintentionally. IOActive can provide technical support through our optical and scanning electron microscope imagery to support internal IP infringement assessments.

IOActive understands the value of these services to both legitimate and malicious entities, and will not provide them to organizations without a legitimate purpose for assessing the chips, devices, or systems. These services are intended to support counterfeit interdiction efforts, help clients to improve their resistance to silicon-level attacks, reduce the risk of IP theft, and mitigate other consequential impacts.

ABOUT IOACTIVE

IOActive is a trusted partner for Global 1000 enterprises, providing research-fueled security services across all industries. Our cutting-edge security teams provide highly specialized technical and programmatic services including full stack penetration testing, program efficacy assessments and hardware hacking. IOActive brings a unique attacker's perspective to every client engagement to maximize security investments and improve clients' overall security posture and business resiliency.