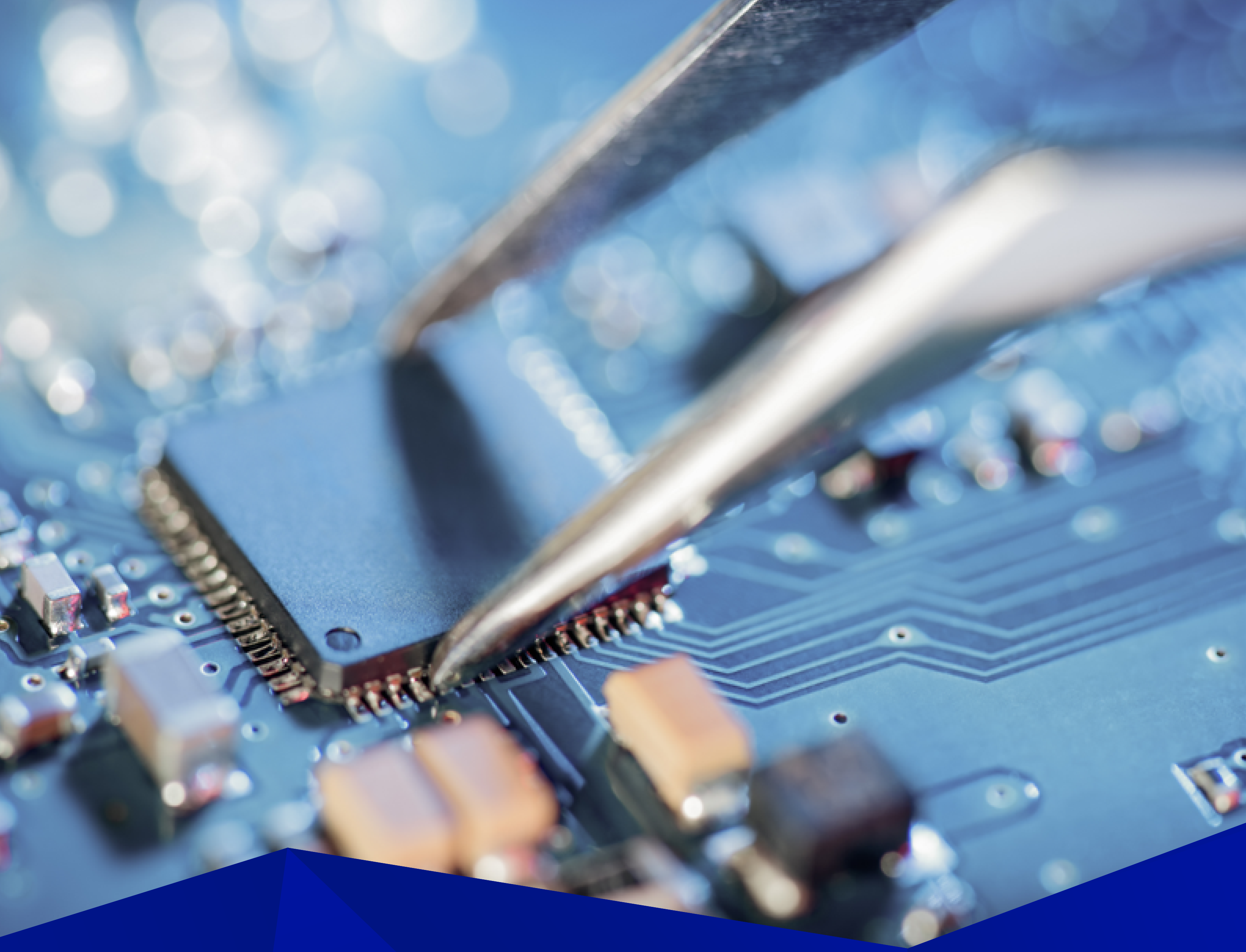


HARDWARE SECURITY SERVICES

F-Secure Consulting

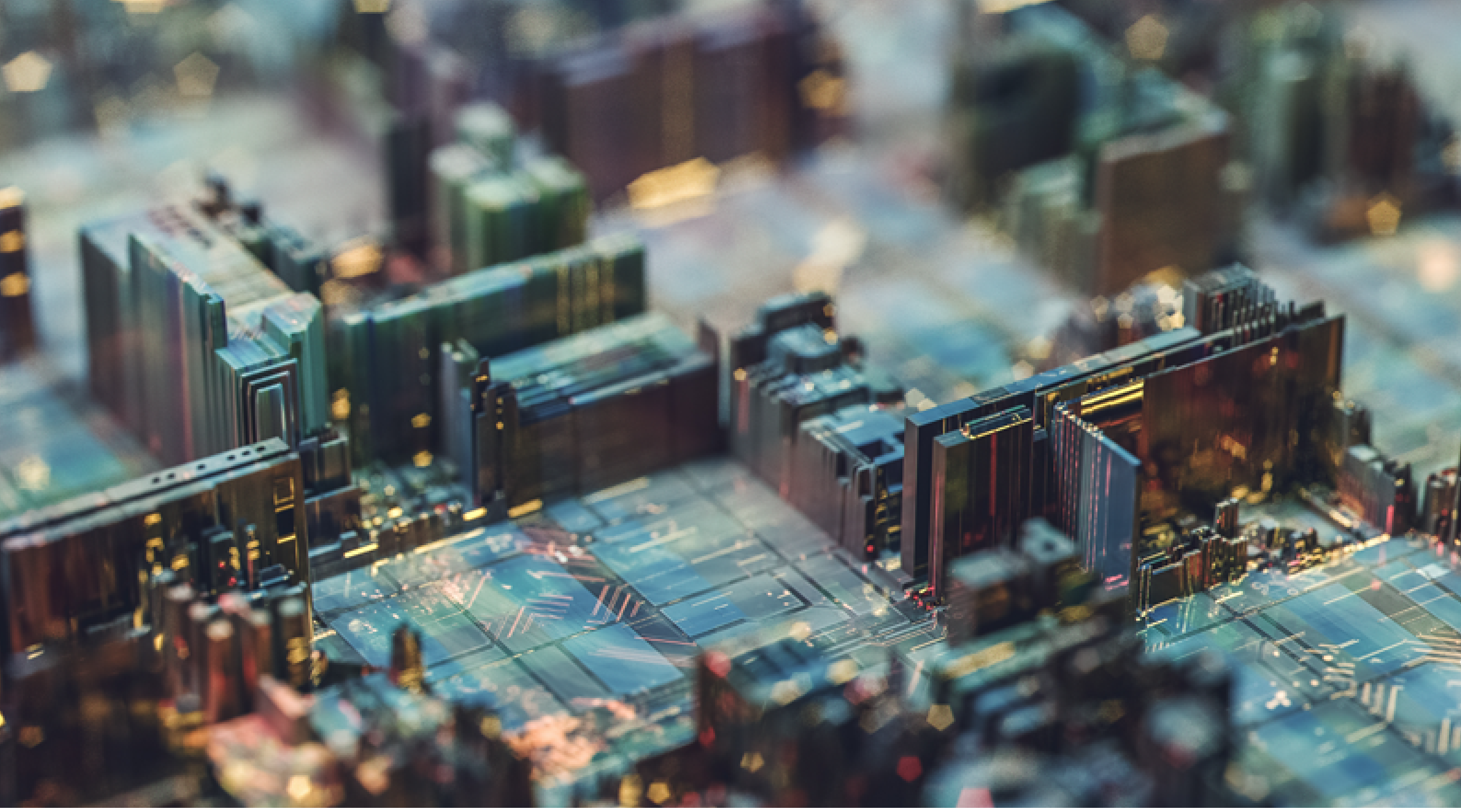
F-Secure

CONTENTS

INTRODUCTION

Man and machine. It takes a combination of the latest human expertise and continuously improving technology to comprehensively predict, prevent, detect and respond to threats. F-Secure's holistic approach to security involves not only smart software and cutting edge AI technology, but extensive human knowledge and insight. Our Hardware Security team is a prime example of the human expertise that sets us apart.

F-Secure's Hardware Security team, founded as Inverse Path in 2005, provides information security consulting to the most unique, challenging and critical industries in the world. We provide industry-leading services to secure hardware, safety-critical embedded systems, software applications and IT infrastructure. With a vast breadth of experience in hardware and software design and engineering, we are trusted by companies across the globe to assess and test their products and processes. Our work safeguards products from malicious compromise, and in doing so protects the safety of passengers, ensures the resilience of critical infrastructure, and secures company trade secrets and intellectual property.



HARDWARE SECURITY: IT'S ABOUT CONVERGENCE

A thorough understanding of the interaction between hardware and software is essential for ensuring the security of integrated products. F-Secure's Hardware Security team distinguishes itself not only with extensive experience in hardware security engineering as well as conventional software security consulting, but also by a deep understanding of hardware's convergence with software. We deliver detailed and comprehensible security analysis of software and hardware systems, along with practical and effective mitigation and protection strategies.

The line between hardware and software is blurry when it comes to integrated products, and the physical nature of hardware brings about special considerations that must be appreciated when working to secure a product. The most prominent of these are as follows:

Unlike software, oversights in hardware decisions cannot be easily patched.

When secure network update procedures are in place, patching software is a feasible and understood task. Fixing hardware, however, is usually much more complicated and expensive. The omission or inclusion of specific components, the presence or absence of specific board interconnections, and the interoperation with non-upgradable firmware or ROMs all pose challenges that may require a physical product recall to address vulnerabilities and other security concerns. Costly mistakes can be avoided by making the right design choices and selecting the proper components from the very beginning of the design process.

Hardware attacks cannot be throttled or filtered.

Traditional server-based software services allow for control of their visibility, availability, rate of access, patching, monitoring and overall exposure. The exposure of hardware products to adversaries, however, is radically different. Malicious parties have physical access to your product, which means unlimited opportunity to attempt various attacks. Evaluating the exposed attack surface is vital, not only in terms of the functional interfaces exposed by the product software/firmware, but also in relation to anything that is physically exposed to a potential attacker (e.g. debugging ports, exposed memories, all PCB traces).

You are not always in control of your own product.

Components supplied by a third party may have dependencies or restrictions. It's not uncommon for customers, even those who fully control their core intellectual property, to find that critical parts of their infrastructure, product or hardware components are opaque. When maximum security or safety must be guaranteed, it is vital to scope and focus penetration testing and reverse engineering where it matters. With proper analysis, we will ensure that none of your hardware subcomponents or firmware can be used against your own product.

When it comes to safety, failure is not an option.

Our extensive experience with the automotive and avionics industries results in a deep understanding of the interaction between safety and security, software and hardware. To ensure that safety is never jeopardized, it is critical to determine the actions compromised firmware code could potentially take in relation to accessible hardware. This requires assessing all circuit paths from firmware-controlled I/O and ensuring role separation and isolation of all safety-critical components. A mastery of hardware and software convergence is essential when auditing each and every layer, thereby ensuring product safety resilience and avoiding liability in worst-case scenarios.

An engineering perspective produces solutions that are meaningful and manageable.

To maximize the chances of security recommendations being implemented within the customer processes, a successful security assessment must identify mitigations and solutions that are realistic, manageable and effective. Years of helping companies around the world building software and hardware products from the ground up has instilled in our team an engineering perspective that enables us to produce solutions that are not only effective, but practical to implement.

SERVICES

Our wide-ranging skill set allows us to offer security auditing services ranging from traditional software to lower level firmware and hardware designs. We place particular emphasis on the exploration of unconventional attack vectors.

Design review

The capacity to analyze higher level specifications, whether concerning a cryptographic protocol, API design or overall application layout, is essential in tackling potential vulnerabilities from the very inception of a product. We routinely analyze early stage development plans for software and hardware products, identifying and reviewing the critical steps that can deeply affect long term security goals. A detailed architecture security review early in the process is key to maximize any customer's security budget and to preventing expensive mitigation strategies later.

Example design reviews we perform include, but are not limited to:

- Cryptographic APIs design and usage
- Over-the-air (OTA) programming systems
- Short-range and long-range RF communication
- CPU isolation and virtualization frameworks
- Cross-domain hardware isolation and unidirectional data diodes
- Cross-domain data multiplexing
- Internet-of-Things (IoT) devices and infrastructures
- Tamper proofing systems
- Side channel protection

Code review

We analyze codebases of all sizes to evaluate exposed attack surface, identify relevant entry points and pinpoint security vulnerabilities. A deep understanding of hardware enables our experts to evaluate specific low-level execution context characteristics of any architecture running firmware code, an advantage in spotting potential hardware integration issues.

Example code reviews we perform include, but are not limited to:

- VHDL code for FPGA logic synthesis
- Secure Boot schemes
- Microcontroller and SoC bootloader, firmware
- ARM® TrustZone® Secure world firmware
- Hardware security module firmware and applets
- Smartcards applets
- IoT applications
- Custom server-side backend implementations
- Mobile applications

Penetration testing

We have extensive experience in grey box and black box penetration testing, with particular focus on reverse engineering hardware layouts and firmware code, as well as traditional software.

Example penetration tests we perform include, but are not limited to:

- Hardware data diodes
- Microcontroller and SoC bootloader, firmware
- Hardware security modules
- Smartcards
- Point-of-sale devices
- Access control systems
- Industrial control systems
- Automotive and avionics systems
- IoT devices
- Bluetooth / NFC tags
- Short-range and long-range RF communication

F-Secure Foundry

Our well-rounded perspective of product development, whether related to engineering, development, or defensive or offensive aspects, makes our team an efficient and enabling partner in creating hardware and software solutions. Our background in both conventional and exotic security research combined with our experience in system administration, open source, mission-critical software development and hardware engineering provides a uniquely wide range of skill sets ready to tackle research and development of production-grade secure solutions.

We have helped many customers bring secure products from the drawing table to deployment of manufacturing – products that have been created with a built-in security mindset from the very beginning.

Our hardware security services have been awarded with IEC 62443 certification.

Example production-grade development projects include, but are not limited to:

- Long-range vehicle information systems
- Remote sensor networks for industrial applications
- Testing hardware and software suites for security products
- Secure hardware devices for consumer or industrial applications

F-Secure Foundry: foundry.f-secure.com

INDUSTRIES

We focus on the most unique, challenging and critical sectors. Our customers range from small businesses to public and government organizations to Fortune 500 companies.

Automotive

Modern vehicles include connected features for entertainment, telemetry and safety reasons.

We work with car makers and automotive component manufacturers to ensure that exposed entry points (e.g. Wi-Fi, cellular) are secure against compromise, ensuring vehicle safety. We perform security assessments, evaluating threats originating from remote data connections down to the inner separation and communication flow between vehicle bus-facing internal components and the main application processor.

We also work with vehicle add-ons such as car sharing and "black box" telematics equipment. The added connectivity of these devices, with their NFC, cellular, Wi-Fi or Bluetooth capabilities, expand the vehicle attack surface. We audit these devices for security compliance and to avoid liability for their integrators.

Avionics

Modern aircraft can be considered the biggest "things" in the Internet of Things arena, given their ever-increasing connectivity ranging from simple in-flight Internet connections to remote telemetry and diagnostic channels. We help aircraft and avionics manufacturers ensure safety-critical systems are protected from hardware and software security issues.

Our primary expertise consists of ensuring that interconnected systems operate according to the most restrictive security standards, working as intended between the aircraft controls, airline, passenger and infotainment and passenger devices domains. Whether evaluating in-flight entertainment interfaces, maintenance ports or the inner electronics isolation and separation of hardware data diodes and signal switches protecting aircraft controls, we evaluate all attack surfaces and implementation layers, from low-level electronics to pure applications.

Consumer

The protection of intellectual property on devices disseminated around the world cannot solely rely on software means, and requires low-level hardware support. We implement effective security and intellectual property protection for various types of consumer electronics. Our team routinely evaluates consumer products, with analysis of all "jailbreaking" paths that can potentially be used to subvert their intended operation or expose security-sensitive IP, assets or personal identifiable information.

Enterprise

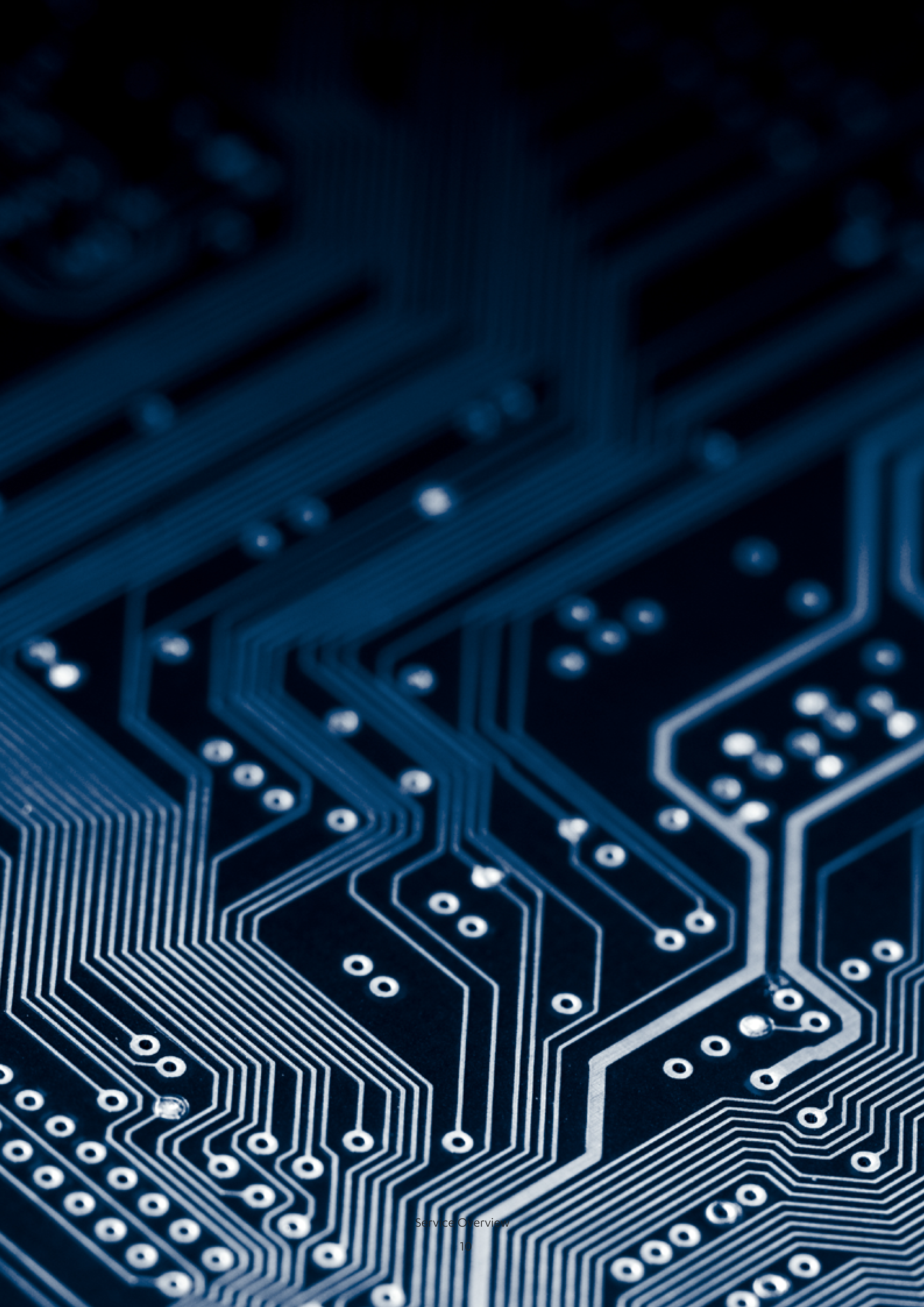
Our team audits the IT infrastructures of the largest enterprise environments, uncovering vulnerabilities on mission-critical servers and applications before malicious parties can exploit them. We work with infrastructures of all sizes to evaluate, implement and audit integration of access control systems, authentication tokens, hardware security modules and in general, interactions that go beyond generic software.

Financial

As recognized leaders in credit card security and having uncovered flaws in Chip and PIN systems, our team secures entire banking infrastructures, from consumer cards to backend systems. We assess transaction protocol design and smartcard implementation of cardholder payment cards; we routinely evaluate Point-of-sale devices and ATMs for their resilience against hardware attacks; and we assess backend services responsible for fraud management, as well as the web and mobile applications responsible for presenting services to the user.

Industrial

We specialize in securing safety-critical infrastructure from the ground up. We have vast experience in auditing proprietary control systems, whether operating on land or in air, sea or space. Industrial Control Systems (ICS) are represented by an overwhelming variety of classes of devices that can include exotic custom-made embedded systems, RF bridges, "smart" tools, robots and more. Our extensive low level experience with hardware, firmware and wireless equipment enables us to provide services for the full spectrum of devices that fall under the ICS domain.



CASE STUDIES

The following anonymized case studies provide a glimpse into the types of projects our team has had the privilege of working on.

Hardware diodes

Main industries: Automotive, Avionics, Consumer, Industrial

Proper segregation of safety-sensitive domains (e.g. aircraft controls) from insecure ones (e.g. in-flight entertainment) relies on deep layers of separation. Some level of interconnection is inevitable and for protection, data diodes are often employed to ensure a unidirectional flow that forbids communication from less secure domains towards more privileged ones.

We audited the design and implementation of data diodes in several projects. In aviation, our work helps manufacturers address deficiencies in their applications before certification.

In automotive, we help customers implement the same strict principles that drive avionics systems, but for segregating vehicle buses from “rich” embedded systems exposed to the Internet.

Vehicle infotainment

Main industries: Automotive

The connectivity of modern in-car entertainment systems or vehicle telematic units potentially exposes cross-domain systems that can interact with intimate vehicle control buses and the Internet at the same time.

We have worked with automotive manufacturers on several projects to verify the resilience of such systems to local and remote attacks, often resulting in total compromise allowing remote access to the vehicle CAN bus. Our understanding of all involved layers allowed us to propose sensible mitigations as well as long-term design changes to ensure the adequate level of separation between inner components and prevent a worst-case scenario, even on a fully compromised infotainment unit.

Car sharing

Main industries: Automotive, Consumer

The popularity of keyless car sharing systems using NFC cards or customer mobile phones with Bluetooth results in a greatly expanded vehicle attack surface, sometimes even with third party add-ons which were not anticipated by the original car manufacturer.

We helped several customers secure entire fleets of vehicles against NFC-based, Internet-based or physical attacks that would have potentially resulted in the compromise of individual vehicles or, in the worst case, every vehicle in the fleet.

Vehicle black boxes

Main industries: Automotive

Many insurance companies promote the installation of add-on vehicle telematic units (e.g. “black boxes”) to lower premium prices by keeping GPS and acceleration logs for each customer. The proper operation of a vehicle black box is important for passenger safety, vendor reputation and to avoid liability issues that could arise from tampering or misuse. These devices, however, are often extremely insecure.

We helped several customers identify inadequate products at the beginning of their selection process. We also performed extensive assessments of deployed units to mitigate and address critical security vulnerabilities.

Traffic Message Channel

Main industries: Automotive

We successfully deployed a Traffic Message Channel infrastructure for an entire country, allowing law enforcement and traffic managers to publish real-time information concerning accidents and queues.

Our team’s wide range of skills resulted in vertical development of the infrastructure from the web application, allowing easy input of events, up to the RDS encoder and FM transmitter responsible for broadcasting signals to the satellite navigation systems of an entire country.

Photovoltaic sensor networks

Main industries: Industrial

We developed machine-2-machine (M2M) networks consisting of remotely deployed sensors (e.g. temperature, irradiance) all securely connected to embedded cellular gateways and centrally managed with data presentation on the final web or mobile application.

Such networks normally exhibit a poor or non-existent level of security, however leveraging our R&D resources, the customer was able to not only receive a state-of-the-art functional infrastructure, but also a fully secure one.

Counterfeit protection

Main industries: Consumer, Industrial

Consumer and industrial appliances or equipment are often victims of “pirate clones” on foreign markets. While little can be done to prevent such counterfeits in emulating hardware, often the quality of the product and its performance efficiency rely on secret algorithms included in the device firmware.

Our services allowed customers the competitive advantage of locking down trade secrets and intellectual property included in device firmware, making the introduction of a cost-effective clone more difficult.

Smart tools

Main industries: Industrial

The competitive advantage afforded by enabling smart equipment is reaching assembly lines, even on manufacturing tools once completely analogue (e.g. welding machines).

Such integrations, however, are often applied on top of insecure legacy systems and by companies with little security knowledge.

We helped manufacturing customers secure their production lines against insecure smart products, which can be potentially tampered with to severely compromise final product quality, or even line safety.

Access control

Main industries: Avionics, Consumer, Industrial

Modern access control systems almost universally rely on cryptographic algorithms implemented on RFID/NFC or contact based smartcards. In several cases such access tokens also perform complex interactions with mobile clients to support advanced features.

We fully assessed the security of entire access control implementations for customers, and ensured their resilience against cloning, tampering, emulation and even simple/moderate side channel attack resistance.

POS analysis

Main industries: Financial

The role of point-of-sale devices in securing financial transactions, protecting cardholder PINs and card data, providing tamper-proof and tamper-evidence behaviour in case of compromise, is obvious even to cardholders.

Our expertise in the financial sector allowed us to help customers assess the security of PoS devices as well as perform forensic analysis on units believed to have taken part in cardholder fraud.

Credit card fraud

Main industries: Financial

Our team is a world leading expert in the EMV (also known as Chip and PIN) protocol and all aspects of its implementation, having uncovered novel attacks in this area. Our deep knowledge of the EMV protocol and low level implementation on PoS devices and ATMs allowed us to aid customers in implementing early fraud detection against the most common and refined attacks known to exist. We almost universally find that financial institutions of any size are simply not aware nor advanced enough to protect against highly advanced, but highly detectable, fraud conditions.

Network routers

Main industries: Consumer

The conventional home DSL network router represents a class of devices widely used in every Internet-connected home. Security concerns for such routers include protecting operator/vendor intellectual property against hardware attacks, protecting connected clients' network traffic, and ensuring resilience against Internet-facing and local network compromise attempts.

Our team helped several customers with securing their existing devices, supporting product choices with preliminary security evaluations, and developing smart routers with advanced security features.

Hardware Security Modules

Main industries: Automotive, Enterprise

The use of HSM devices is common amongst competent service providers who want to avoid handling cryptographic secrets on conventional servers. This is good practice in taking the customer out of the equation when it comes to liability issues in the case of compromise of customer data, and it is the first step in achieving full encryption for all sensitive assets.

Working with HSM customers we ensured correctly implemented integration, avoiding mistakes that would allow exposure of data or secrets outside the HSM. We also helped customers choose the right HSM implementation to meet operational needs and ensure resilience against advanced attacks. Working with HSM manufacturers, we helped assure the correct operation of the product against abuse and hardware attacks before they reached the market.

ARM® TrustZone®

Main industries: Automotive, Consumer

The support for ARM® TrustZone® (TZ) technology allows developers to engineer custom trusted platform modules by enforcing domain separation of “secure” and “normal” worlds.

The use of this technology, commonly employed on mobile phones for DRM protection, is now emerging in the automotive sector to allow reuse of a single CPU in mixing safety-critical tasks with potentially untrusted applications.

Our team has been responsible for evaluating, designing and training for effective and secure TZ implementations, tasks that require a deep understanding of inner hardware layout. Early consulting in this area is important to avoid costly mistakes with TZ. When handled with the proper expertise, TZ technology can result in massive production savings due to a reduced part number count.

USB armory

Example of a hardware product that we have developed

USB armory is a Linux-based computer for security applications with an extremely compact USB stick form factor. It is 100% open hardware and software, and entirely made in Italy.

The device is a testament to our capabilities in developing hardware products from the ground up, as no third party was consulted and its design, electronic schematics, PCB layout and software development have all been accomplished in-house.

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com | twitter.com/fsecure | linkedin.com/f-secure

F-Secure®