EMBEDDED SECURITY FOR THE IoT

ABIresearch® TRUSTED INTELLIGENCE SINCE 1990

NAGRA KUDELSKI GROUP | IOT SECURE BY DESIGN

TABLE OF CONTENTS

INTRODUCTION

The Internet of Things is now entering a phase of mass deployment across many industries, accelerated by the COVID-19 crisis in order to enable the automation and remote control of industrial systems as well as the more efficient production and management of critical supply chain assets like medical supplies and basic consumer goods. At the same time, these IoT deployments have come under increasing attack from hackers and the threat environment is shifting quickly.

But in Microsoft's IoT Signals study, nearly all companies surveyed (97 percent) have security concerns when adopting IoT. A key conclusion of the survey was that security must be addressed from the beginning for both devices and networks. Internet connectivity is a two-way street. It's more important than ever to address security because IoT devices provide digital access to home and work networks – and the sensitive data stored there.

Kudelski IoT – part of the Kudelski Group, a global leader in digital security solutions – is one of the companies driving R&D and technology advancement in security for the Internet of Things. Kudelski IoT is sponsoring this ABI Research report in order to help companies across the IoT ecosystem make informed decisions about how to secure their IoT devices and ecosystems. The report therefore references Kudelski IoT keySTREAM and other Kudelski IoT security services and technologies as examples where relevant. For more information about Kudelski IoT, please visit www.kudelski-iot.com.

RISK AND SECURITY IN THE IOT

Security for the IoT is increasingly being recognized as a critical requirement; not only due to the logical and physical security aspects that are so closely entwined with digital security, but also because of the need to effectively manage deployments. This requires perfunctory identification for the purposes of authentication, attestation, and access control, at a minimum. The challenge with the IoT is that the devices and their applications are broad and varied, meaning that more traditional and standardized cybersecurity technologies are not so easily applied in many scenarios; often, they need to be significantly adapted.

With the expansion of the connected ecosystem comes the expansion of the threat landscape. As such, the risks are not only multiplied, but they are also new and unknown. For this reason, thinking about security at product inception is key; by integrating security at the development phase, trust can be built into the hardware and the software. Beyond that, it is also critical that security be effectively maintained post-market. New threats can emerge after a product has been commercialized, so an essential functionality is to ensure that the risk can be quickly identified and mitigated in the field. Consequently, secure device lifecycle management is as important as embedding security into product hardware. In fact, much of the management capabilities are best trusted when anchored in secure hardware. The benefits of end-to-end security cannot be overstated for the long-term viability, and value, of connected products.

EMBEDDING SECURITY AND ANCHORING TRUST

Secure hardware provides the ideal trust anchor from which secure software and services can be leveraged. Existing secure hardware can sometimes be used in the IoT, but in most instances, they need to be adapted or new solutions devised to fit the new contexts. Due to the great variation in IoT form factors, resource requirements, component choice, firmware and software applications, among others, the use of one over-arching secure hardware form factor is simply not possible.

Today, a range of solutions are available for the IoT including secure elements, secure ICs, eSIM, trusted platform modules, trusted execution environments, secure microcontrollers and application processors, hardware security modules, among others, all targeting different use cases and device types. IoT-specific versions have emerged from pre-existing standards to cater to new demands and requirements, with many focusing on embedding and integrating themselves into the very core of the hardware integrated into devices that have limited capabilities. Key is ensuring that the secure hardware is compatible with the device at hand and its intended use.

For example, lightweight/energy efficient devices (such as sensors and other devices that need long battery life) will require a low-power CPU. Embedded security in this scenario is ideal; it does not require high CPU due to reduced dependency on OS resources or other third-party software.

Even on a high-end device, critical security functions running as part of a large software stack create a large attack surface (*i.e.* on a Linux kernel). The key is determining where to put critical security functionality to reduce the attack surface. TEE can be one option, but a physical secure element can also be implemented separately from the rich CPU environment. This would further minimize the risk of existing CPU threats (such as Meltdown and Spectre) that could negatively impact security.

In general, implementing security separately makes it easier to upgrade and manage the lifecycle in a secure way. This is a key part of the security by design principle.

Central to creating secure embedded hardware are the IP cores at the heart of the silicon. IP cores are modular functional designs that can be integrated into chips and MCUs. Microelectronic advances, driven by mobile and IoT demand, has created sophisticated System-on-Chip (SoC) solutions, resulting in MCUs with diverse functionalities in a single package. Multi- function MCUs are available in mono-core or multi-core architectures in order to handle the extra functionalities.

The business model is based on licensing the IP core designs to semiconductors and SoC manufacturers. There are also open-source alternatives that have emerged recently, such as RISC-V. The MIPS Open initiative has also made an open source version of the MIPS 32- and 64-bit Instruction Set Architectures (ISAs).

From a security perspective, it is possible to embed security features into chip hardware, such as with Arm's TrustZone, a TEE technology which has been particularly popular. Alternatively, security-specific IP cores have also hit the market. They can work with varied processor architectures and ISAs. The goal is to provide authentication, confidentiality, integrity, and protection across a wide variety of applications.

Underlying these use cases, a diverse number of functions are typically offered with security IP cores:

- **Root of Trust**: A hardware, firmware, or software component that is inherently trusted to perform security services on a device.
- **Secure Boot**: A secure or trusted boot scheme adds a number of cryptographic checks to the process in order to verify the integrity of the different components, drivers, applications, and initialization sequences, so that an effective chain of trust can be formed from the start of the process.
- **Cryptographic/Security Protocol Accelerators**: Cipher (symmetric), public key (asymmetric), hash and Hash-Based Message Authentication Code (HMAC) integrity algorithms, and post-quantum.
- **True Random Number Generator (TRNG)**: Based in hardware, they are used to generate cryptographic keys, initialization vectors, and nonces.
- **Physically Unclonable Function (PUF)**: Created from the variable physical and electrical properties of an IC, generating a unique fingerprint for the associated IC. They essentially leverage the entropy of the manufacturing process. This fingerprint can then be used as a unique key in algorithms for authentication, identification, encryption/decryption, *etc.*

- **One-Time Programmable (OTP) Memory**: Non-volatile memory where data can only be written to the memory once, remaining unchanged and permanent (it is maintained after power-off). It is generally used to store keys, certificates, credentials, and other secure information.
- **Isolated Execution Environment / Secure Enclave**: An isolated execution space where code can be run outside the influence of the standard OS,. Making use of hardware-enforced barriers, the execution space can be partitioned into a non- secure and secure world.
- **Memory Protection Unit**: A programmable unit that allows privileged software to define memory access permissions.
- **Tamper Resistance**: Resistance to physical tampering of the hardware through various sensors voltage, temperature, and clock sensors.
- **Side Channel Attack (SCA) Resistance**: Resist against Differential Power Analysis (DPA) and Electro Magnetic Analysis (DEMA) attacks.

Most IP core vendors include ISAs, which provide the basic operations that a processor must support (*i.e.*, type of instructions, maximum length, format, *etc.*) in order to facilitate development of hardware and associated applications. More recently, they are accompanied by broader software development toolkits, with many focusing on how best to aid secure application development, such as leveraging a TEE or enabling secure communications.

These efforts are aimed at facilitating product development, not just for the creation of a new device, but also to offer support post-market (*i.e.*, for provisioning, onboarding to cloud, and life cycle management). Many silicon IP and semiconductors offer various accompanying products, from basic development toolkits, SDKs, and APIs for third-party integration, to firmware and embedded OSs, to full-blown life cycle management platforms and existing plug-ins available to the most popular cloud providers (*e.g.*, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud).

As such, in terms of security, the embedded hardware forms the foundation from which a host of trusted functionalities can be enabled, serving a wide range of secure applications.

AN IMPLEMENTER'S PERSPECTIVE

At the heart of adopting and implementing a secure IoT solution that is fit for purpose is the underlying prerequisite to understand the use case. Implementers need to evaluate the value of specific IoT security features against the actual in-field deployment of the device. This requires weighing various factors: threat landscape, risk appetite, device capabilities (power, compute, connectivity), production costs (BOM), regulatory requirements, future proofing (updatability, expansion), *etc*. As such, it is important to IoT device development to understand different embedded security options and choose the one that:

- Meets security needs (mitigates the threats and supports the use cases envisioned);
- Works within the constraints of the hardware;
- Works within the power consumption constraints of the hardware;
- Provides a foundation for future use cases that might be later implemented.

For example, an eSIM can be as secure as a Secure Element (SE) provided the SIM vendor and Telco have put in place the infrastructure to update it in the field. Being able to patch a device is part of robust security, and so an eSIM might be a preferable choice. Alternatively, an SE can support updates by default using the device manufacturers FOTA mechanism. GSMA provisioning processes are very robust with only trusted actors in the provisioning chain. However, they can be cumbersome and are only adapted to GSMA environments. Solution providers need to develop compliant products and subscription management services, with testing and accreditation required for the use of GSMA digital certificates to authenticate with other M2M remote provisioning system elements. As such, an SE could be the alternative.

Another example is with choosing TEE, which sometimes is not as robust depending on the provisioning processes. Implementers will have to determine who will manage the TEE app, how will it be handled, at what stage in the production process is it "locked"/personalized, among other questions.

As a final example, software hardening is less robust, but it also does have less impact on the device hardware and BOM. However, it is more applicable for devices with greater power resources. The tradeoff on the hardware cost is an impact on the development processes and processing power.

Implementers will have to weigh their requirements vis a vis the benefits and limitations offered by the various technologies. Companies like Kudelski IoT offer a full range of design and assessment services that support companies in creating the most effective IoT security architecture for their specific product and ecosystem. These services range from design sprints to threat assessments, security architectures, security evaluations and even full device and ecosystem design. Kudelski then offers a range of different technology solutions and services that can be used to mitigate the threats identified and to implement a wide variety of different IoT security use cases.

CHOOSING THE RIGHT HARDWARE

The IoT security space is still relatively nascent, but continually and dynamically evolving. For implementers, there is a range of choice in terms of secure hardware form factors that can serve a variety of purposes. Beyond design guidance, Kudelski can also provide support for most of the technologies highlighted above with its IoT keySTREAM system. Partnerships with semiconductor manufacturers, OEMs and service providers are key to building comprehensive, end-to-end solutions and catering to the wide variety of security form factors required by today's device manufacturers.

Kudelski offers the possibility of integrating various secure hardware technologies leveraged in embedded contexts, including secure elements, eSIM, TPMs, TEEs, and secure MCUs.

SECURE ELEMENTS

Secure Elements are probably the most lightweight secure form factor available for the IoT and are available for various applications (smartcards, SIM, smart microSDs and USB tokens). While NFC embedded SE (eSE) have been popular in smartphones and tablets for years, more recent developments around integrated and discrete SE have emerged. They are not necessarily coupled with an NFC controller, and are typically targeted at consumer and industrial IoT devices. Most products on the market are certified CC EAL 5+ for authentication services during connectivity (including within LPWA usage). The focus here is to enable high-level security for edge nodes (such as LTE-M and NB-IOT modules for example) as well as secure onboarding onto cloud services.

Kudelski's own Pico SE-800 Secure Element has a unique identity, provisioned at production, eliminating the need for OEMs to securely personalize devices. Underpinned by the keySTREAM Secure Client Library (SCL, which provides an API layer to the device firmware) and Kudelski's cloud-based keySTREAM Security Server on the backend, the solution enables zero-touch provisioning of devices to AWS IoT and Azure IoT.

Features enabled by the solution include end-to-end encryption of data from chip to cloud, authentication mechanisms for communication and commands, secure boot, remote attestation, secure Firmware Over The Air (FOTA), fine-grained access control to data, chip-to-chip security, remote feature enablement and support for Datagram Transport Layer Security (DTLS) stacks, among others. The pre-shared key scheme used by the solution is highly optimized for Low-Power Wide-Area (LPWA) use cases, helping to conserve bandwidth and battery life. Further, the Pico SE chip itself is certified CC EAL 5+. The solution provides security lifecycle management for any IoT device, regardless of the customer's choice of silicon or cloud platforms.

Beyond the stand-alone SE is a parallel movement for integrated SE (iSE/inSE), with the aim to integrate the SE directly into the SoC. Global Platform is supporting the movement and published two open specifications in 2019 to facilitate the standardization of iSE: Open Firmware Loader (OFL) which standardizes how firmware can be loaded and managed in the tamper-resistant hardware platform; and Virtual Primary Platform (VPP) which defines the security services running on the tamper-resistant platform, called a Virtual Primary Platform (VPP). The potential for iSE beyond smartphones is for usage in 5G and NB-IoT devices.

Kudelski offers an IP sub-system for an iSE that can be integrated into third party chipsets, providing security functions to the SoC itself (such as secure boot and runtime integrity checking) and can also be used for security applications such as SIM card (UICC), DRM, biometric identification, blockchain and many other applications. The design includes a number of key features:

- Cryptographic hardware that is robust and designed to resist side-channel attacks;
- A dual-core, redundant CPU based on RISC-V that is designed to resist physical glitching and invasive attacks;
- The ability to secure applications and data stored in external NVM by implementing a Secure Flash Access (SFA) block to provide protection and integrity for program and data access;
- The inclusion of a hardware key management block to provide a Root of Trust with hardware protected keys;

Kudelski has a long history of licensing, implementing and certifying its security IP blocks in 3rd party silicon, having done so for more than 10 years in the set-top box industry with dozens of chip vendors and hundreds of different models.

eSIM

eSIMs (also known as eUICC, *i.e.*, a soldered-on UICC) is a SIM card with a remote provisioning function. It is able to store multiple communication profiles that authenticate a device for use on a provider's network, one of which is enabled (recognized by the device and used for communication). The network of the MNO in the enabled profile is used for communication. Profiles other than the enabled profile are disabled (they are not recognized by the device). More to the point, eSIMs have a bootstrap profile to allow out of the box connectivity. The profiles can then be changed OTA. This provides a platform to enable borderless connectivity and flexibility as it relates to service agreements and avoids operator lock-in.

eSIM is fast becoming a mainstream technology in the M2M market, especially in the automotive/connected cars industry. New reprogrammable eSIMs based on the GSMA's second version of its global specification have hit the consumer market. They enable remote SIM provisioning, but do not have the fleet management capability of M2M eSIMs. The main difference between the two specifications is ownership, if some form of authentication is required and if the message sent has to be pushed or pulled.

An emerging alternative to eSIM is the iSIM (iUICC), a parallel endeavor to GSMA's iSE. It is not a standard yet but is enjoying important industry interest. The main difference is that the iSIM moves SIM functionality onto a device's permanent hardware array, enabling OEMs to design the functionality directly with an SoC. The iSIM is located in a secure enclave within the SoC or MCU, rather than being a separate SE. It is an interesting and potentially displacive technology, as it will allow for secure functionality even in devices that lack separate, albeit discrete security modules. This means the BOM can be significantly reduced from a hardware-security perspective.

Kudelski has partnered with a number of smartcard and hardware vendors on SIM projects. In partnership with STMicroelectronics, Kudelski integrated ST4SIM eSIM solutions into the Kudelski IoT Security Platform, targeting automotive and industrial use cases.

With Idemia, Kudelski has integrated IDEMIA's DAKOTA IoT (eUICC) and TSM (Trusted Service Management) solutions into the Kudelski IoT Security Platform. The solution allows the remote download of mobile operator subscriptions to connected objects deployed in the field and authorizes them to use the network.

A number of other movements are leveraging SIM functionality as the best alternative to an SE. The GSMA's IoT SAFE (IoT SIM Applet For Secure End-2-End Communication) aims to provide a common mechanism to secure IoT data communications using a highly trusted SIM for the provision of security services including TLS and DTLS authentication, and lifecycle management for example.

Deutsche Telekom on the other hand is spearheading the development nuSIM, an integrated SIM for the IoT. The telco offers the open specification for the secure provisioning of operator credentials during module or device production. DT already has numerous partners, with Qualcomm being one of the first to incorporate the nuSIM in its 9205 LTE modem. Kudelski joined the ecosystem in 2019 and working with DT to incorporate security into nuSIM implementations.

TRUSTED PLATFORM MODULES

The TPM is an international specification developed and published by the TCG and is an MCU that can securely store artifacts used to authenticate the platform (PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy, as a Root if Trust in obfuscated software, for white box cryptography, among other use cases.

Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments. TPMs can be used in computing devices other than PCs, such as mobile phones or network equipment, and today, with version TPM 2.0, in other IoT and edge devices.

Top TPM vendors for the IoT space are Infineon and STMicroelectronics, under their popular OPTIGA and STSAFE lines, respectively. Microchip is also a popular vendor, perhaps with less clout globally, but well established in the space. Nuvoton is another company offering traditional TPMs for the PC space.

TPM adoption continues to see a steady growth rate overall in terms of shipments, with 268 million units expected to ship in 2020 globally. The technology is already well established in the traditional PC devices market, with near ubiquitous integration across the board. The connected car segment, and in utilities and IIoT are two growing markets beyond PC for TPM integration. For automotive, this is driven by usage of TPM to secure V2X/Vehicle-to-Vehicle (V2V) communications, and similarly in the industrial space, for secure communication and authentication between industrial gateways and backend services.

In large part, TPMs are a standardized technology, widely accepted as a secure hardware enclave that can effectively store secure artifacts. These artifacts, and notably certificates and encryption keys, form the basis of identity, authentication, and access management that is essential to secure device life cycle management in the IoT space. The appeal of TPMs is significant in spaces where functional safety is key, where regulation requires the implementation of secure technology, and especially in critical infrastructure settings.

However, it must be stressed that TPMs more easily serve larger devices with higher computing and power capabilities, and are not quite suited to low-power, low-resource devices, such as sensors and other edge devices. TPMs are popular on routers and gateways, and other middle-of-the-chain devices, as well as on the backend. They are well suited in situations where there is a requirement for higher levels of trust (equivalent to FIPS 140-2, level 3) in the device identity process.

Kudelski is integrating its keySTREAM technology with TPMs for use primarily in edge security applications. Because many edge gateways contain significant computing power and contain TPM capabilities, they offer reasonable protection of key material and crypto algorithms, and can be safely used, especially when physical security measures are also taken.

TRUSTED EXECUTION ENVIRONMENT

The TEE is a secure state of the main processor in a smartphone (or any connected device). It ensures that sensitive data are stored, processed, and protected in an isolated, trusted environment. The TEE offers isolated safe execution of authorized security software, known as "trusted applications". These trusted apps enable the provision of end-to-end security by enforcing protected execution of authenticated code, confidentiality, authenticity, privacy, system integrity, and data access rights. Compared to other security environments on the device, the TEE also offers high processing speeds and a large amount of accessible memory.

The most well-known implementation is GlobalPlatform's API for smartphones. In September 2019, GlobalPlatform published four technical documents to bring TEE to a wider range of IoT devices, including automotive, consumer, and industrial. The organization has standardized trusted application deployment and management, optimized for IoT devices.

Arm TrustZone technology is the most popular embodiment of TEE. It enables the development of a separate Rich OS and TEE by creating additional operating modes to the normal domain, known as the secure domain and the monitor mode.

TEEs can be used in conjunction with other hardware security form factors, such as eSEs, TPMs, and MCUs, with the TEE used to securely execute the code and the eSE to store the token. Overall, TEE is more suited to application security, especially where an OS is being run (including a Real-Time OS (RTOS)), so it is a popular security technology for automotive applications, for example (notably, infotainment systems).

While Arm is the clear leader of TEE technologies with its TrustZone IP, other TEEs are available in the market, including from vendors like Trustonic (Trustonic Secure Platform) and Hex Five Security (MultiZone Security). Beyond the embedded space, SGX from Intel are available for CPUs.

TEE shipments are forecasts to hit 698 million globally in 2020, with the vast a majority destined for the smartphone market (95%). Going forward however, TEE technologies like TrustZone are expected to make a significant impact in the secure IoT hardware space, notably in markets including automotive, industrial, smart cities and buildings, smart homes, and wearables. Driven by Arm's new ARMv-8-M architectures for Cortex-M, it is clear that TrustZone is set to become a key security technology for IoT deployments.

SECURE MICROCONTROLLERS

A secure MCU is a type of authentication IC, but with fuller processing capabilities and the possibility of programming the software to preform different tasks (able to be provisioned for a hardware-based root of trust, for example), as opposed to a simpler IC that reads data from input and performs actions based on instructions written in the memory (and so, generally performs that one task).

A secure MCU is essentially a tamper resistant MCU (ranging from 8 bit to 64 bit) with dedicated encryption engines, libraries, and TRNGs, secure Non-Volatile Memory (NVM) storage, and allowing for secure communication and key/certificate protection, in addition to hash functions for authentication purposes and IP protection.

This class of MCU is a less resource-intensive, or discrete, version of a TEE, designed specifically for low-end IoT devices (for example, those using ARM Cortex M family). Starting at the end of 2019, however, the latest Arm Cortex-M23/33/35P cores means that TrustZone TEE technology will effectively be available for secure MCUs.

There are general-purpose secure MCUs and application-specific secure MCUs (*e.g.*, automotive- grade MCUs requiring Automotive Safety Integrity Level (ASIL) compliance). Primary use cases of general-purpose secure MCUs include IoT embedded systems (industrial utilities, healthcare, smart city), consumer electronic devices, and other scenarios that require a strong security infrastructure.

The secure MCU is often tied to a device life cycle management platform and associated software tools (including drivers, APIs, and middleware), enabling the remote management, update, and patching of the secure MCU and related platform (notably *via* OTA management).

Secure MCU vendors include all the top semiconductor companies today. Leading the space are STMicroelectronics, with its STM32 line of Microcontroller Units (MCUs), NXP, with its Kinetis platform, and Renesas with its Synergy line. Cypress (in the process of being acquired by Infineon), Microchip, and Nuvoton also provide highly competitive MCU solutions.

Renesas, NXP, and STMicroelectronics have announced new offerings leveraging the Arm Cortex M-33 (respectively, Renesas RA, NXP LPC5500, and NXP-ST STM32L5), while Microchip and Nuvoton will be offering MCUs based on the Cortex M-23 (SAM L11 and NuMicro M2351, respectively).

Global secure MCUs (without TEE) are set to hit 108 million shipments by end of 2020. While TEEs will increasingly feature in secure MCUs going forward for application isolation, technologies like TrustZone are still relatively costly (especially in terms of license fees and royalties). Alternative technologies used in secure MCUs include basic hardware firewalls, and the creation of multiple domains through micro-virtualization. Fully-fledged TEEs will not be necessary in all cases, and IoT vendors can easily settle for simple SEs for key/token storage for low-power devices, while outsourcing anything more complex to gateways that include TEEs.

CONCLUSIONS

The ecosystem for secure technologies targeting embedded systems is in full expansion, and vendors, including Kudelski, are providing offerings for an increasingly broad range of devices, including low-power devices with limited computing resources. It is a testament to the fast pace of security development that technologies like SEs, ICs, eSIMs, TPMs, and TEEs are increasingly available for such devices, at costs that are becoming more affordable to reach a wider audience.

This is further aided by the trend pushing semiconductor and IP companies to provide software development tools that facilitate go-to-market. Certainly, the interest of large cloud providers to allow connectivity to their platforms and storage of the resulting collected data has been a significant catalyst to enabling favorable conditions for rapid development and prototyping.

These elements are key drivers in promoting security at the core of IoT. Certainly, the availability of technologies and vendor offerings is increasingly wide and varied, and the choice can be overwhelming. Key to choosing the right implementer is ensuring that they can facilitate the deployment of a secure IoT solution. This starts with the planning and decision-making process, to secure design and testing, to in-field deployment and management. One thing is clear: IoT security as a whole requires an end-to-end perspective and the right implementer is a partner that can securely accompany an IoT deployment from start to finish, regardless of the technologies involved.

Published October 2020

249 South Street

Oyster Bay, New York 11771 USA

Tel: +1 516-624-2500

www.abiresearch.com

About ABI Research

ABI Research provides strategic guidance for visionaries needing market foresight on the most compelling transformative technologies, which reshape workforces, identify holes in a market, create new business models and drive new revenue streams. ABI's own research visionaries take stances early on those technologies, publishing groundbreaking studies often years ahead of other technology advisory firms. ABI analysts deliver their conclusions and recommendations in easily and quickly absorbed formats to ensure proper context. Our analysts strategically guide visionaries to take action now and inspire their business to realize a bigger picture. For more information about subscribing to ABI's Research Services as well as Industrial and Custom Solutions, visionaries can contact us at +1.516.624.2500 in the Americas, +44.203.326.0140 in Europe, +65.6592.0290 in Asia-Pacific or visit www.abiresearch.com.