Could you begin with a brief description of your backgrounds and research interests?

MN: My background includes design techniques for mixed analogue, radio frequency and digital ‘very large-scale integration systems’ (VLSI), with respect to the integrity and security of the data being processed. I currently head up the Secafy Laboratory at Kobe University in Japan and am in the process of setting up a joint research laboratory with Professor Danger’s team.

NM: I work in the Secafy Laboratory and am particularly interested in integrated circuit-level security and safety technology, including physical attack countermeasures and permanent digital archives.

JLD: I am head of the digital electronic system research team at TELECOM ParisTech and a co-founder of Secure-IC. I undertake research in the field of the security and safety of embedded systems and the implementation of complex cryptographic algorithms.

Could you explain more about the work of the Secafy Laboratory at Kobe University?

MN: Secafy stands for hardware security and safety and we believe it is vital to design these principles into hardware from the very beginning. I see hardware as being the root of trust on which the security of networks can be built. We are focused on measuring the susceptibility of integrated circuits (ICs) to malicious attacks and environmental interference, and finding ways to detect and mitigate against these factors. Many students pass through our laboratory and leave with a practical understanding of the ways in which electronic systems can be compromised and design techniques for improving hardware reliability.

Why is it so important to research ways of making hardware more reliable and secure?

MN: Many more aspects of our lives are becoming reliant on the integrity of digitally-run and integrated systems. It is vitally important that these systems are not only robust and reliable in their performance, but also that they cannot be compromised by attackers. Critical applications include process controllers in cars, autonomous vehicles, banking and defence networks, and systems associated with vital infrastructure such as utilities.

NM: Modern technology relies on wireless broadband communication and non-stop connectivity. However, all practical hardware is exposed to unseen radio waves, which can sometimes affect the performance of a chip, particularly in VLSI. Therefore, it is important to ensure devices are robust and continue to perform well even in harsh environmental conditions.

JLD: Cyber attacks are increasingly common. One aspect of this are highly sophisticated attacks on hardware systems, which utilise expensive equipment and are run by skilled operators. Therefore, as scientists we need to be aware of how such attacks could be perpetrated and develop means to detect and prevent them.

What are the main objectives of your ongoing research?

MN: We are running multiple research streams that are linked by their common backgrounds in electromagnetics, the principles behind the operation of electronic devices and a mix of digital and analogue techniques. Every project is aimed at designing semiconductor integrated circuit chips and electronic systems to be secure and safe, and include a functional focus on computation, communication, sensing and actuation. We hope to enforce design techniques and standard simulation technologies that are system-wide, interdisciplinary and span all areas of physics.

Impact Objectives

- Measure the susceptibility of integrated circuits (ICs) to malicious attacks and environmental interference such as electromagnetic and electrostatic noise
- Further strengthen the design of ICs through the use of improved cryptographic engines, noise suppression technology and attack detection systems
- Stay one step ahead of malicious attackers by developing systems to improve the safety and security of future digital systems such as quantum information processing, autonomous transport and highly cognitive wireless communication, before issues arise
The SPACES projects and multiple related research streams being pursued by an international collaborative team, are all aimed at improving the security of the hardware that powers and regulates the networks linking the world’s critical systems.

At the Secafy Laboratory at Kobe University in Japan and the digital electronic system research team at TELECOM ParisTech in France, researchers are pursuing multiple research streams aimed at improving the reliability, robustness and security of integrated circuits and electronic systems. Professor Makoto Nagata, Head of the Secafy Laboratory, says: ‘Security and safety are in high demand in today’s digitally-connected society and we believe hardware should be the root of trust on which security can rely, since it is unmodifiable.”

Projects to date include the SPACES (Security Evaluation of Physically Attacked Cryptoprocessors in Embedded Systems) I and II projects, the development of detection and mitigation strategies against malicious interference and improvements to the robustness of integrated circuits (IC) to electromagnetic and electrostatic noise. Funding is provided by the Japanese Science and Technology Agency and the Japanese Society for the Promotion of Science and the projects are ongoing.

SIDE CHANNEL ATTACKS
Over a remarkably short time period, almost all aspects of our lives have become partially or wholly dependent on electronic processors and software. Engine control modules manage our cars, fly by wire systems control aircrafts, large distributed networks regulate our electrical and water supplies, and manufacturing depends on programmed robotic hardware. We all carry smartphones and rely on computers and expect our devices to be fully interconnected and information available on demand. Systems are reliant on high-speed internet access and non-stop connectivity. However, our increasingly digital world and the spread of the internet of things (IoT) creates vulnerabilities, which can be leveraged by ideologically or politically motivated attackers.

In addition, the push for miniaturisation and use of compact VLSI (very large-scale integration systems) electronic packaging exposes electronic systems and the integrated circuit chips that lay at their heart to noise caused by electromagnetic and electrostatic discharges. A further threat to the integrity of electronic systems comes from refurbished or improperly designed integrated circuits and even from the deliberate integration of hardware Trojans into chips, which can be used by an attacker to infiltrate networks.

All such threats have led to scientists developing increasingly sophisticated means to ensure the robustness of systems and to detect and prevent malicious attack. The approach of Professors Makoto Nagata and Jean-Luc Danger, and Associate Professor Noriyuki Miura’s teams is to strengthen the design of integrated circuits by incorporating improved cryptographic engines, noise suppression technology and attack detection systems.

Most of us are familiar with the concepts of hacking and cyber attack, but we rarely hear about ways in which data can be stolen or systems manipulated via remotely instigated physical attacks. Researchers have shown how unintended ‘side channels’ can be used to determine cryptographic keys or passwords, or to reduce the amount of detection work needed to decipher these codes. Side channels, which can be used to deduce information, include the timing of keystrokes, the timing of access to logs stored in cache, analysis of power usage and the tiny high frequency noises generated by the electronic crypto processors. In addition, faults can be deliberately introduced into cryptographic engines, which can lead skilled operators to derive information, which helps them hack a system.
ANALOGUE SENSORS

According to Miura: ‘Most side channel attacks (SCA) are by their nature minimally non-invasive and therefore difficult to protect against and detect.’ Local electromagnetic analysis (LEMA) probes can be used to detect the frequencies emitted by a chip when undertaking cryptographic processing. Critical ICs are these days protected by cryptoprocessors or engines, which use a secure key to encrypt input data, swiftly and efficiently. Indeed, the Secafy Laboratory has itself developed many of these cryptographic engines. However, a simple single wire coil inserted close to the chip can – through magnetic coupling – read these electromagnetic (EM) waves, which can be analysed for correlation to the cryptographic key.

Nagata’s team has developed a simple analogue solution to such SCAs. He says: ‘Our sensor operates on a physical golden rule – no one can observe anything without disturbing it.’ Two simple inductor capacitor coils are placed around the cryptographic elements on a chip, which oscillate differentially when a LEMA probe is inserted close to the die. The difference in oscillation resonance is detected by a frequency counter and the administrator is alerted of an attack. Nagata says: ‘The coils have different shapes and numbers of turns, allowing the sensor to detect the symmetrical placement of two probes even in the power-off state of the chip.’ The system is tolerant to voltage differences induced by environmental changes and works concurrently with any power current equalisation devices, which dampen the signals that might be detected by a LEMA probe.

To produce the SCA sensing device, a simulation environment was developed which recreated the minute power fluctuations generated by cryptographic processing. Miura explains: ‘The shape and number of turns of coils are tuned and optimised using the simulation, plus it can be used for exploration of detector performance against threat scenarios from micro EM probes in different shapes, materials and positions.’ Before developing the simulator, the team carefully measured side channel leakage from different chips fitted with encryption circuitry, to determine the weaknesses in each configuration. The solution developed incorporates the team’s trademark combination of simple analogue devices with sensitive digital information processing.

A related research stream has developed a sensor to detect anomalous electric currents in cryptographic engines, caused by faults naturally or intentionally introduced. This type of attack is termed a laser fault injection (LFI). Nagata says: ‘The attacker can inject a laser or otherwise use a high power EM wave focused on logic circuit elements on the chip. This can induce logical errors and erroneous output from a cryptographic engine.’ The errors can theoretically be correlated with the processing steps, enabling the cryptographic key to be deduced. Nagata adds: ‘Our analogue sensing technique, which detects disturbances in the electrical field in the chip substrate, is a strong countermeasure to these LFI attacks.’

ELECTROMAGNETIC NOISE

Many of the Secafy Laboratory’s advances are based upon the careful measurement of unintentional noise generated by the power delivery network within a device, which includes the integrated circuit chip. Noise is generated by circuits and propagated through the substrate of an integrated circuit, which can be measured by a probe conductively connected to the substrate, which is made from a semiconductor material such as silicon. By measuring the voltage variations generated through the substrate during cryptographic processing, the team demonstrated that correlations could be made between the waveforms produced and the logic functions, theoretically allowing an attacker to deduce the most probable keystrokes being used. However, as well as being a potential weakness, Nagata says: ‘We can use the substrate noise to our advantage. By careful characterisation and analysis of the noise profiles of different chips, we can identify non-authentic components which may be unreliable, or even those that have been fitted...’
The future will include artificial intelligence, truly autonomous transport and highly cognitive wireless communication. The research to maintain safety and security of such systems will never end.

With Trojan hardware, which could be used by an attacker to take control of a device.

As well as being a channel through which a system can be attacked, noise of an electromagnetic or electrostatic nature can also compromise the performance of a device. In particular, the Laboratory has studied the effect of noise levels generated by digital processing on wireless communication performance. This work was funded by the Japanese Ministry of Internal Affairs and Communications, which was concerned to ensure the continuing connectivity of vital networks in robotics, vehicles and aircraft, for instance. Miura says: ‘IC chips for wireless communication are susceptible to in-band interference propagating through side channels, such as the silicon substrate and power delivery network. These effects can degrade communication performance, or in the worst case, cause a loss of connection.’ He adds: ‘Some devices are also naturally exposed to incoming EM disturbance from nearby rotating motors and high voltage devices.’

To examine the effects of EM noise on wireless communication performance, the team created a hardware in the loop simulation (HILS), which is a test environment incorporating devices emulating some of the components of a complete electronic system. In this case, both the radio frequency communication system and side channel noises are simulated, the latter via an arbitrary noise generator. On-chip monitors measure the generated noise and its effect on the wireless communication function. The simulation enabled different methods of noise reduction to be tested and measured against the metric of observed improvement or degradation in wireless communication performance. Nagata explains: ‘Electromagnetic noise coupling is a known issue when analogue, radio frequency and digital components are combined on the same die or in the same package.’ A noise reduction system comprised of a thin magnetic film coated onto the IC chip was tested and shown to absorb some of the problematic EM frequencies.

INTERNATIONAL COLLABORATION
Looking ahead, the Japanese and French teams are developing a joint research laboratory for the further development of protection for embedded systems in electronic devices. Nagata explains: ‘The joint team will have all the necessary competences for such work, including expertise in micro-electronics, analogue design, digital processing, simulation techniques and signal processing, to name just a few.’ This productive relationship builds on Danger’s intimate insights into cryptographic algorithms and the underlying mechanisms for deducing cryptographic keys from information leakage channels. Nagata says: ‘Without this knowledge of side channel models, we could not build effective protections.’ He adds: ‘The joint development programme unifies deep scientific understanding with practical remedies that use both analogue circuits and digital information processing.’

Nagata’s team is also collaborating with many other industrial and research partners around the world, to continually improve detection and protection systems. He says: ‘We often hear about potential attack vulnerabilities from industry and work with companies involved in security, wireless communications, semiconductors, automotive electronics and many others. We have developed unique techniques in the field of hardware security and safety. We feel these principles are tightly entwined and should be built into the design of IC chips.’ Nagata feels it is vital that collaboration be pursued at an international level to try to keep one step ahead of malicious attackers and to ensure reliability of critical systems. He says: ‘The future will include artificial intelligence, truly autonomous transport and highly cognitive wireless communication. The research to maintain security and safety of such systems will never end. Our roles include developing standards for design and build, and making communities aware of potential vulnerabilities and the consequences of failure.’