Defend encryption systems against side-channel attacks

Pankaj Rohatgi, Technical Director, Cryptography Research Division, Rambus - March 16, 2015

From its ancient origin as a tool for protecting sensitive wartime or espionage-related messages, cryptography has become a foundational building-block for securing the systems, protocols, and infrastructure that underpin our modern interconnected world. But the physical mechanisms used in performing encryption and decryption can leak information, making it possible to bypass this security. Protecting designs against such side-channel attacks starts with understanding how such attacks operate.

At its very essence, cryptography is a branch of mathematics dealing with efficiently computable transforms that convert inputs to outputs using additional data known as a cryptographic key. These transforms have the property that, despite observing many input/output pairs, it remains infeasible to compute or invert the transform without the knowledge of the key.

An example of a cryptographic transformation is the *symmetric-key* based Advanced Encryption Standard (AES-256). An AES-256 encryption device that has access to a 256-bit secret cryptographic key, can transform any sensitive message - known as plaintext - into an unintelligible form known as the ciphertext. Anyone observing the ciphertext, without knowing the plaintext or the key, cannot recover the plaintext or the key. Further, even an observer who knows or can choose the plaintext and can observe the corresponding ciphertext can still not recover the secret key being using within the encryption device. However, any AES decryption device that has access to the same 256-bit secret key as the encrypting device, can readily recover the plaintext from the ciphertext.

Another example of a cryptographic transformation is a *public-key* based RSA (Rivest-Shami--Adelman) digital signature algorithm. This algorithm uses pairs of cryptographic keys consisting of a non-secret public key and a secret private key. A signing device that has access to a secret private key can attach a "tag" or digital signature to any message. This RSA signature has the property that without knowledge of the private key, it is infeasible to calculate the digital signature to a message. Anyone who receives a message with a digital signature on that message can use the corresponding public key to establish the authenticity of the message by verifying that the digital signature corresponds to that message.

Strong mathematical guarantees make cryptographic primitives (established, low-level cryptographic algorithms) highly popular as building blocks for securing systems and infrastructure. Encryption is widely deployed to protect confidential data during storage or transmission over insecure networks. Digital signatures are widely used for validating the authenticity and integrity of software, software updates and the data that systems rely upon. Other cryptographic primitives such as message authentication codes, key agreement protocols, and hash functions are also widely deployed for protecting information and systems from attacks.

However, successful attacks on fielded cryptographic systems have also highlighted the pitfalls of relying on purely mathematical guarantees for securing physical systems. It may be infeasible to extract keys mathematically from message traffic, but monitoring message traffic is only one of many possible approaches to breaking encryption.

One common attack vector is exploiting deficiencies in protecting secret cryptographic keying material. Real world systems need to be carefully designed so that secret keys cannot be easily recovered by malicious software or via a simple hardware attack. Unfortunately, incidents where systems get compromised due to poorly protected secret keys are still common.

Another source of problems has been poor communication between the cryptographers, who are mostly mathematicians, and the engineering community that actually develops these systems. If cryptographers do not properly convey all the requirements needed for the mathematical proofs of security - such as the non-reuse of certain parameters or the quality of certain random inputs – to the system designers, the resulting implementations may be vulnerable to a mathematical attack. For example, hackers were able to recover the digital signature key used for signing code for the Sony PlayStation 3 because designers reused a once-per-signature parameter across multiple signatures.

Side-channel attacks

Even if a system protects keying material and meets all the mathematical requirements of the security proofs, there is a class of attacks on all cryptographic implementations that can easily and non-invasively recover secret keys from a system. These attacks, known as side-channel attacks, rely on the fact that any physical realization of cryptography in hardware or software cannot be an atomic black-box transform as assumed by the mathematical proofs of security. A physical system must necessarily leak information about the process of computing the transform into the environment.

Examples of this "side-channel" information include the time taken by the cryptographic operation, the power consumption, EM and heat emissions of the cryptographic device while computing the transform, and the like, all of which depend on the physical details of the implementation. Depending on proximity, an attacker could gather some of this side-channel information and use it to recover the secret cryptographic key. While remote attackers may only be able to get low-bandwidth information such as the approximate time taken by the cryptographic calculations, attackers in closer proximity may be able to collect much higher bandwidth channels, such as the power consumption profile or the EM emissions profile of the device.

Once an attacker has collected side-channel data for a cryptographic computation, there are two classes of attacks that can be mounted using the collected data to recover the key. The first class of attacks, known as *simple side-channel analysis,* recovers the secret key from the side-channel data collected during a single cryptographic transaction. Simple side-channel attacks are more commonly applicable to public-key cryptography-based systems such as RSA.

In this case, the cryptographic calculation consists of a key-dependent sequence of operations. Because each type of operation is likely to have a unique power or EM profile, examining a device's power consumption or EM emission profile while it is performing the RSA operation typically reveals the sequence of operations the device performed. The secret key can then be easily reconstructed from this operation sequence.

Attacks of the second class, known as *differential side-channel analysis,* are typically applicable to symmetric key based algorithms such as AES as well as in situations where the collected side-

channel data is very noisy or of otherwise poor quality. This style of attack uses statistical hypothesis testing on side-channel data across multiple cryptographic transactions to recover the secret key, piece-by-piece.

The basic concept behind differential side-channel analysis is that side-channel leakage from power, EM, or timing correlates to the cryptographic activity occurring within the device. It even correlates to individual subactivities occurring in the device that depend only on small portions of the key and known data such as inputs or outputs. But other subactivities occurring within the device as well as the noise from the measurement process are all uncorrelated to the targeted subactivity.

This correlation means that an attacker can guess the value for a portion of the key and predict the resulting target subactivity for each transaction. The attacker can then use a correlation calculation between predicted subactivity and side-channel data to verify whether the key guess is correct. Incorrect key portion guesses will show no correlation between predicted subactivity and the side-channel traces, whereas the correct key guess will show a statistically significant correlation. These statistical techniques are so powerful that, with sufficient data, subactivity corresponding to a single transistor switching could be utilized for an attack.

History of side-channel attacks

Smart-cards and the history of side-channel attacks

Side-channel analysis was discovered in the mid-1990s, starting with timing analysis followed by analysis involving measuring instantaneous power consumption from smart-card based systems. At that time, smart-card based payment, metering, access control, and conditional access systems were the most prominent cryptographic devices operating in hostile environments where they could be readily accessed and subject to attacks by external attackers or even by their own users.

Smart cards being fairly limited devices, the power supply and clock to the smart-card were completely under the control of the attacker. Further, much of the smart-card silicon and software was devoted to cryptographic processing. As a result, even with very crude and low-cost measurement apparatus it was possible to get a clean power consumption signals from smart cards and that information was available at the individual clock cycle level.

With such clean signals, all smart-cards-based systems at that time could be easily attacked. This catastrophic security failure nearly brought down the entire smart-card industry, and in the late 1990s and early 2000s, researchers and smart-card vendors expended substantial R&D effort to implement countermeasures against these attacks. In parallel, the banking and conditional-access industry that relied upon smart-card security instituted standards and product testing regimes to ensure that these countermeasures were effective.

As a result of this tremendous investment, today’s smart-cards undergo some of the most stringent testing being performed for resistance against side-channel and other physical attacks. This testing is part of mature standards, such as the Common Criterion Security IC Platform Protection Profile, and most smart-card vendors have experience fielding several generations of secure products.

The intense focus by the security community to mitigate this catastrophic threat to the smart-card industry also meant that little attention or resources were spent to analyze side-channel vulnerabilities in larger devices. At that time, there was ample justification for ignoring larger devices. In most cases, larger devices performing cryptography, such as servers or desktops or other large systems, were typically kept in physically secure locations where attackers could not collect high-bandwidth side-channels such as power consumption without being detected.

Because these large systems consisted of many components, they had their own power supplies and regulators to supply different voltages to different components. As a result it was assumed that any power signal collected from the outside the secure location would be too noisy to be practical threat – a fact that was easy to observe and verify. In addition, these complex systems suffered from a variety of remotely exploitable software vulnerabilities, so addressing the remote vulnerabilities was prioritized over exploring physical attacks. Side-channel countermeasures in these larger systems, if any existed, were limited to protections against remotely exploitable timing attacks. Over time, a myth developed that side-channel attacks were just a smart-card problem and large systems were largely immune to these attacks.

Evolution of the threat to large systems

The ubiquitous deployment of cryptography in mobile, embedded, IoT, vehicular, smart-grid, and hosted/cloud-based systems, however, has meant that many systems performing sensitive cryptographic operations are no longer in physically secure locations. Over the last few years, then, attention has once again returned to the side-channel vulnerabilities of large systems.

In looking at these vulnerabilities, researchers and attackers had to confront the obvious challenge that measuring and isolating power consumption related to cryptographic operations on large, complex system with many components is not easy, nor is dealing with the large amount of noise generated by unrelated activity. However, as it has turned out, just a bit more sophistication on the side-channel acquisition side has resulted in tremendous improvements in the quality of side-channel signals available from larger devices. As a result, these larger devices are now subject to the same simple and differential side-channel attacks that were applicable to smart-cards a decade ago! In fact, even the most basic, low-cost smart-cards available today offer substantially more resistance to side-channel attacks than even FIPS certified, large, tamper resistant systems that don’t implement side-channel countermeasures.

Two key improvements have greatly extended the reach of side-channel attacks on large systems. One is the use of cheap near-field and far-field probes to capture EM emissions from large devices rather than focusing on the power line. The other is the use of elementary signal processing techniques - such as filtering and demodulation - to isolate and enhance the leakage information-bearing signal from the noise.

The use of near-field emissions arose because while some large systems produce strong cryptography-related emissions that can be captured from several feet away using a standard, far-field RF antenna tuned to the emission frequency, most large systems produce weaker emissions that are only available from shorter distances or in the near-field. For example, when operating with a typical M-field probe (which is essentially a loop of wire) in close proximity to the device, it becomes possible to isolate different EM emission sources by moving the probe across different parts of the device. Signal processing can then substantially increase the signal-to-noise ratio of the captured signal because cryptography-related emissions may be prominent in only certain parts of the spectrum.

The first step in a side-channel attack against a large device family, therefore, is to identify the best probe position and the spectral bands where the best leakage can be found. This task can be greatly simplified if it is possible to operate the device in a mode where it performs the cryptographic operation intermittently and observe the probe signal's spectrogram. Figure 1 shows such a spectrogram from a 1cm M-field probe placed behind a modern smart-phone while it is performing the RSA operation intermittently.

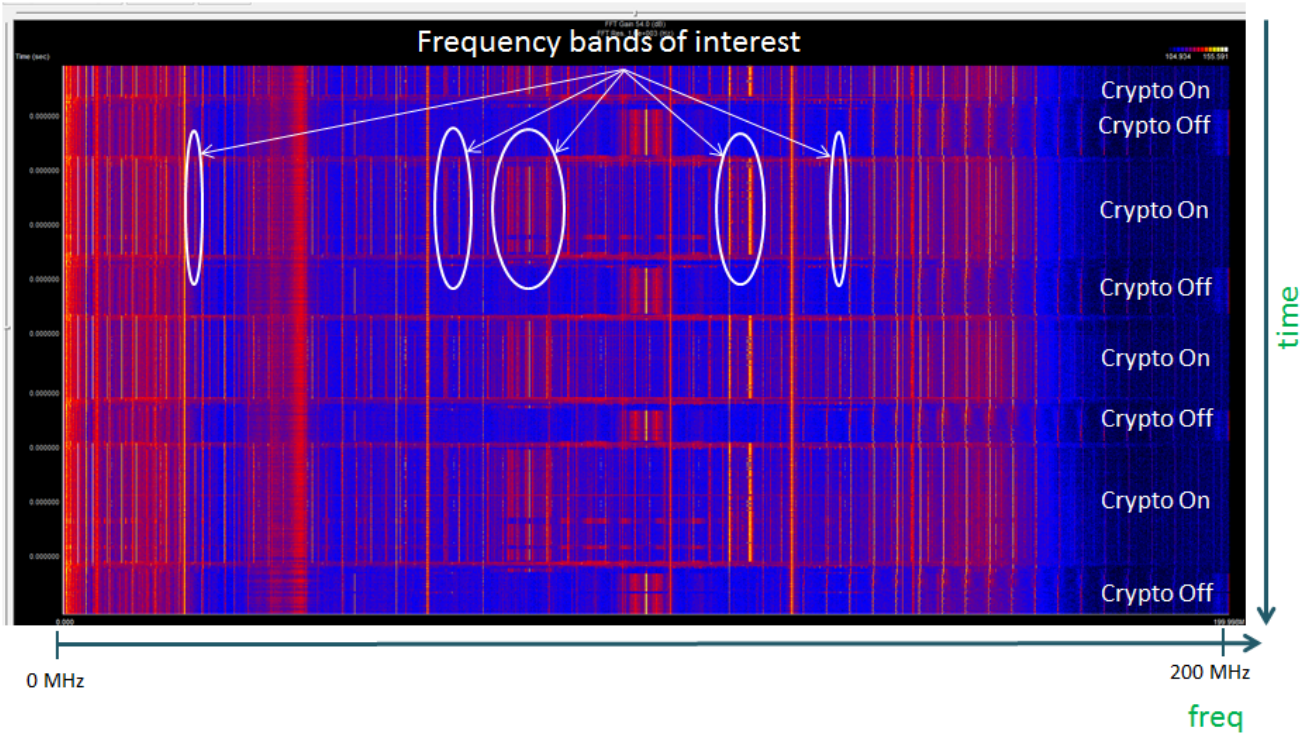

Figure 1: Spectrogram of EM signal collected by M-field probe placed behind a modern mobile phone that is intermittently performing the RSA cryptographic algorithm in software. Bands of energy that appear only during the cryptographic operation identify the frequency bands where information about the RSA operation leaks into the EM side-channel.

The spectrogram clearly shows energy bands that appear only during the RSA operation and indicates that the probe in its current position is picking up emissions related to the RSA operation. The spectrogram further identifies the frequency bands where this information is being leaked. With this information the attacker can then further adjust the probe position to maximize the RSA leakage energy pickup and set analog and digital filters, and other signal processing parameters for the bands identified in the spectrogram, to further isolate the RSA related signal from other unrelated signals and noise.

After signal processing, the resulting RSA EM leakage signal in this example was clear enough for an attack using simple side-channel analysis. In fact, our lab has analyzed more than 30 modern 4G smartphones, with different operating systems and manufacturers, and has successfully extracted the secret keys used by RSA software running within them using simple EM analysis. In addition, we found symmetric algorithms such as AES running in software on these devices to be attackable using differential EM analysis.

Other researchers have used similar techniques to extract secret keys from PCs using ground potential leakage (signal obtained by grounding the chassis) using low-cost, custom acquisition hardware. These attacks seriously call into question the security of server machines that use RSA to set up secure HTTPS or SSL connections with customer browsers, yet are kept not in secure corporate data centers but rather in co-located server hosting facilities with server cages for physical protection.

More threats

More threats

In addition to exploring threats to large systems, recent research activity has focused on attacks on cryptographic operations occurring within a small hardware core embedded within in a large SoC (system on chip), such as an FPGA, set-top box chip, or a mobile application processor. In this setting, the positioning of the EM probe on either the chip surface or on a bypass capacitor on the system board to localize the leakage signal is critical. But other than that, these SoCs can fall prey to the same differential power analysis attacks in as the smart-cards from the 1990s.

For example, the University of Bochum in Ruhr has for a long list of attacks on various FPGAs targeting their bitstream decryption engine. Figure 2 shows a probe placed on a bypass capacitor on the motherboard of an Intel server chip as the best location to for attacking the AES-NI hardware contained within this processor. {Image 2}

Figure 2: Probe location on the motherboard for capturing the EM signal from AES-NI hardware engine on an Intel server chip

The trustworthiness of a large number of systems, and indeed of the entire computer and networking infrastructure today, is dependent on the secrecy of a small number of critical keys. These "root" keys are used to directly or indirectly sign and validate the software and updates to the commonly used operating systems and the billions of systems and devices worldwide. These root keys are instrumental in preventing someone from surreptitiously taking over people's machines. Some "root" keys are used to securely identify servers and public keys belonging to different companies, so that users are not fooled into interacting with the websites and services set up by imposters.

Such critical keys are typically kept within Hardware Security Modules (HSMs), which are systems designed specifically to provide the maximum protection to cryptographic keys from physical attacks. HSMs deploy an active shield and a variety of sensors designed to detect any attempts to tamper with the device to extract its internal, secret keys. Any tamper event device causes the device to erase its keys.

But while many critical HSMs today are kept in physically secure and monitored locations, there is

increasing pressure to deploy HSMs in less controlled spaces. Many such deployments have already occurred. Yet, the current generation of HSMs has poor to non-existent protections against side-channel attacks. In fact, some modern HSMs emit EM signals that can be observed from outside the server in which they are installed, and are vulnerable to RSA key recovery from emissions from a *single* signature operation. Figure 3 shows how an M-field probe placed outside a server containing a PCI-based HSM can capture a signal that can be used to extract the secret RSA private key otherwise kept securely within the HSM.

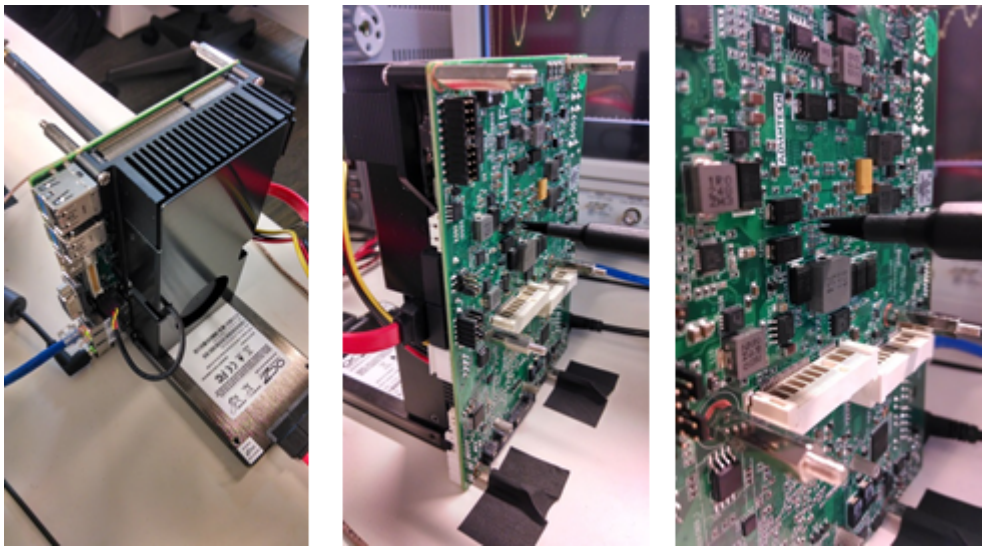

Figure 3: Photograph showing how a 3cm M-field probe placed outside a server chassis containing a modern PCI express based HSM could be used to capture the EM side-channel signal related to the RSA operation occurring with the HSM

Emerging standards and requirements

Fortunately, solutions are available for these large-system, SOC, and HSM threats. The common criterion protection profiles for smart-cards that require side-channel protections are already well established, as are EMVCo's standards for payment cards and national and international standards for electronic passports and national ID cards. They can be applied to these other systems.

The recent onslaught of side-channel research and attacks on large systems has already prompted many other industry associations and standards bodies to add side-channel countermeasure and testing requirements into emerging standards. For example, the Payment Card Industry (PCI) standard for Point of Sale terminals (PCI PTS POI Standard), Version 4.0, now requires all point of sale terminals to be physically tested for side-channel vulnerabilities. Over the past few years, all defense systems subject to anti-tamper requirements have needed to demonstrate protections against side-channel attacks. MovieLabs, a highly influential research and development venture started by the six major motion picture studios, has issued a specification for enhanced content protection that requires DRM systems to be side-channel resistant. As a result, many upcoming content protection standards for high-definition video players (e.g., 4K content) will be requiring vendors to defend and test against side-channel attacks.

Other such standards revisions are taking place. The popular FIPS 140-2 standard for cryptographic modules is in the process of being updated and the proposed FIPS 140-3 or the ISO/IEC 19790 standard that would replace it, both specify protection against and testing for side-channel vulnerabilities. Many upcoming security standards, such as those for secure grid and the like, point

towards the upcoming FIPS/ISO standards for achieving physical security. In addition, there are several companies and conditional access vendors that are placing side-channel requirements on their vendors.

The discovery of side-channel attacks in the mid-1990s with the initial focus on smart-cards led to a myth that these attacks are applicable only to smart-cards and other limited devices. However, over the past few years, this myth is being debunked as side-channel attacks have been demonstrated on a wide variety of large devices. Emerging standards from the DRM, payment, content protection, mobile, defense, and automotive industries are requiring devices to demonstrate resistance to such attacks. The time is now, therefore, for vendors to begin the process of designing and testing to protect their systems against side-channel attacks.