Electronic surveillance through the exploitation of compromising emanations

Emanations actively given off by target devices could lead to leakage of implementation-specific information, which could, in turn, be used to facilitate electronic surveillance. **Richard Frankland** and **Prof. Keith Martin** explain how these emanations work.

HOME

ELECTRO-MAGNETIC EMANATIONS

OPTICAL EMANATIONS

ACOUSTIC EMANATIONS

CURRENT AND FUTURE IMPACT ON SECURITY

Royal Holloway University of London

SearchSecurity.co.UK

summary

Surveillance can be defined as the observation of a target for the purpose of intelligence gathering, and electronic surveillance is the extension of this principle to the analysis of electronically collected signals. The exploitation of implementation-specific information leakage can be used to facilitate electronic surveillance. This leakage comes in the form of various types of emanations. These are actively given off by target devices as part of their typical operation, and can be a security risk; the source of the term "compromising emanations". When these compromising emanations come from devices that process sensitive data in plaintext, before or after it is encrypted, an attacker can use methods to exploit these compromising emanations and break the confidentiality of the data.

WHAT IS IT ALL ABOUT?

While the design of a system can make use of secure cryptographic primitives and promise complete overall security, the security of the actual implementation of that system is usually less of a sure thing.

As the use of cryptography continues to become more widespread, and as security-by-design becomes commonplace, attacks against weak-points are bound to increase. One such weak-point is often the actual implementation of the system.

Side-channel cryptanalysis is way of attacking a cryptographic system by making use of implementation-specific information, such as timing differences or differences in power consumption during operation. However, most of these attack methods call for an attacker either to have physical access to a target device, make alterations to the device, or be able to obtain more information about it than they would be expected to in a real world scenario.

Remote surveillance operations require a different focus, since the attack methods must be passive, feasible and, ideally, undetectable. The goal of attackers carrying out such operations is normally to obtain the desired information directly in its plaintext form without being detected.

HOME
ELECTRO-MAGNETIC EMANATIONS
OPTICAL EMANATIONS
ACOUSTIC EMANATIONS
CURRENT AND FUTURE IMPACT ON SECURITY

There is a significant weakness in human-computer interaction with sensitive plaintext input and data display. This weakness provides an attractive target for attackers. By focusing on human-computer interaction an attacker can exploit plaintext information leakage from a range of sources.

There is a significant weakness in human-computer interaction with sensitive plaintext input and data display.

These sources can leak the desired information itself or perhaps the data required to access it. This especially holds true for widely used weak forms of authentication, such as password or PIN input. For example, attackers already target user interaction with automated teller machines (ATMs) to obtain personal identification numbers (PINs) to commit fraud. Security-conscious users know to cover their hands when they enter their PIN at an ATM to avoid shoulder surfing – the act of directly observing restricted information from another person. This type of attack has been improved recently by the use of video feeds from covertly installed cameras.

By taking advantage of this type of plaintext leakage an attacker can passively, and, more importantly, undetectably break the confidentiality provided by certain types of cryptographic implementations. These include encryption of emails and typed documents, the snooping of login details, and virtually anything that is protected cryptographically for confidentiality but needs to be human-readable for usability.

The form that this leakage takes varies widely and is often specific to the devices that are being targeted, such as visual display units or data input peripherals. However, there are three main areas that have been identified and have had feasible attacks published in the scientific literature. These are:

- Electromagnetic emanations
- Optical emanations
- Acoustic emanations

In this article, each area will be introduced and summarised. Finally, the potential impact on the security landscape will be discussed.

HOME
ELECTRO-MAGNETIC EMANATIONS
OPTICAL EMANATIONS
ACOUSTIC EMANATIONS
CURRENT AND FUTURE IMPACT ON SECURITY

ELECTROMAGNETIC EMANATIONS

While compromising electromagnetic (EM) emanations have been studied confidentially in military and government circles as part of what is popularly referred to as TEMPEST, publicly available information on EM emanations is scarce.

However, growing academic research in information security is starting to bring knowledge concerning the potential security issues involving EM emanations into the open.

The history of openly published attack methods exploiting EM emanations stretches back to the mid-1980s, with work demonstrating the eavesdropping potential of passively picking up emanations as radio signals from cathode ray tube (CRT) monitors and reconstructing screen content. This technique is made possible by the mode of function of components in a CRT monitor, namely the amplification of the video signal for image display. This results in a large component of the radio emissions from a CRT being the video signal itself.

The next published attack dealing with EM emanations made use of compromising emanations from data cables connecting serial ports in home computers, allowing eavesdropping with a short wave radio. This work showed that EM emanations were both exploitable and capable of breaking confidentiality of displayed and transmitted plaintext data.

The methods used to perform these types of attacks made use of widely available radio receiver technology. The ease with which they could be perpetrated was even demonstrated long ago on the popular old BBC TV programme Tomorrow's World. This demonstrated that, from their inception, they were indeed functional and feasible attacks.

While the technology of modern day computing continues to evolve, the principles of the first EM eavesdropping attacks remain. Further developments in the field have resulted in similar techniques being applied to liquid crystal display (LCD) technology, with legible text being successfully retrieved from LCD desktop and laptop screens at distances of around 15 metres, using more specialised receivers to recover signals from the display video cables.

Attacks have also been developed that target plaintext data input in the form of keyboard use. Computer keyboards, of both older and modern construction, have been found to leak compromising EM emanations through device-specific methods of functionality, allowing remote and autonomous keystroke logging that can be

HOME
ELECTRO-MAGNETIC EMANATIONS
OPTICAL EMANATIONS
ACOUSTIC EMANATIONS
CURRENT AND FUTURE IMPACT ON SECURITY

achieved with the use of open source radio technology.

EM emanations are already taken into account by manufacturers of electronic devices due to the need to comply with emission standards for the reduction of EM interference, published by the International Electrotechnical Commission (IEC) through the Comité International Spécial des Perturbations Radioélectriques (CISPR) standards. However, these standards do not address the security issues that arise from EM emanations. While countermeasures have been suggested and implemented, such as software font design to reduce readable image reconstruction and physical shielding of devices, to our knowledge, there is no open, public standard specifically addressing the security issues brought about by compromising EM emanations.

OPTICAL EMANATIONS

Shoulder surfing is already a widely known optical attack method for compromising the confidentiality of secret data, such as a PIN or password. However, newer more novel methods of retrieving information from targets via optical techniques have recently appeared in the scientific literature.

These methods concern the retrieval of both sensitive displayed data (e.g. on a screen) and sensitive user input (e.g. keypad or keyboard input).

For example, it is possible to reconstruct screen content from low resolution CRT displays by measuring projected flickering light from the screen off a wall, or through opaque glass, using highly sensitive light sensors. This allows optical eavesdropping by just having visual access to the flickering light of a CRT monitor, projected onto a wall or some other suitable surface, without the need for direct line-of-sight access to the display.

Using similar equipment, it is also possible to reconstruct binary data from flashing status lights on various types of computer hardware, including those from a Federal Standard 1027 rated cryptographic module.

Using similar equipment, it is also possible to reconstruct binary data from flashing status lights on various types of computer hardware, including

HOME
ELECTRO-MAGNETIC EMANATIONS
OPTICAL EMANATIONS
ACOUSTIC EMANATIONS
CURRENT AND FUTURE IMPACT ON SECURITY

those from a Federal Standard 1027 rated cryptographic module. This standard is the predecessor of NIST's Federal Information Processing Standards for cryptographic modules; NIST FIPS 140-2. However, the successful capture of information relies as much on the design of the target device as it does on having line-of-sight access.

Another method of breaking the confidentiality of displayed data involves the capture of screen content through distance imaging of reflected images in common everyday objects. These include such items as spectacles, teapots, and even the human cornea, showing that in certain circumstances even blocking line-of-sight access to a display may not be enough to stop sensitive information leakage.

Optical eavesdropping of data input has also been demonstrated, using a consumer-grade webcam to relay video of keystrokes and then using image analysis techniques to determine key input autonomously, ultimately reconstructing the original data.

Defining countermeasures against these types of attacks can be problematic. The restriction of line-of-sight access to sensitive information remains the primary method of preventing an attacker from gaining access to sensitive information. Beyond this, countermeasures against attacks that do not require line-of-sight need to be tailored to specific attacks and the risks associated with them.

ACOUSTIC EMANATIONS

The use of sound to determine information leakage is focused towards capture and analysis of the clicks emitted by interaction with a keyboard or keypad.

The first attack method dealing with acoustic recognition of keystrokes was capable of differentiating between keystrokes through labelled acoustic signatures. It was found that telephone and ATM keypads, as well as computer keyboards, were vulnerable to attack. However, the manual labelling of specific keystrokes, and subsequent analysis by measuring for similarity, results in an attack with high specificity, requiring keystroke data related to the intended target user and device.

Further development of the idea of autonomous keystroke detection came with the application of complex statistical analysis of keystroke data in combination with other statistical processes based on English grammar to create an attack method capable of real-time keystroke detection after a short period of training. This attack also

HOME
ELECTRO-MAGNETIC EMANATIONS
OPTICAL EMANATIONS
ACOUSTIC EMANATIONS
CURRENT AND FUTURE IMPACT ON SECURITY

has the benefit of being able to determine typed characters regardless of word structure, such as would be found in a random character "strong" password, which could find application in remote attacks against data input for authentication, such as computer login passwords.

The latest methodology developed improves the reconstruction of plaintext data by using statistical analysis based on estimated distance between keys on a QWERTY keyboard and the assumption of the use of English words. This analysis of keystrokes results in the determination of the most likely words being typed in real time with no prior training or program preparation required. However, because this method presumes the typing of whole English words, it is not able to reconstruct random character sequences. Still, the ability to transcribe whole English text from sound can still be considered useful to an attacker, and can be used to compromise confidentiality of sensitive typed text.

What should be kept in mind here is that the above attacks were carried out with cheap, widely available audio recording technology. With the ready availability of audio "bugs" and long-distance audio recording tools such as parabolic microphones, which are sometimes even sold as hobby or toy consumer electronics, the implementation of these types of attacks does not require a significant financial investment.

One effective countermeasure against acoustic attacks against keyboards is the use of touch screens or virtual keyboards in place of regular, mechanical keyboards. This is due to the fact that mechanical keyboards emanate identifiable acoustic signatures from the keyboard backing plate, which acts like a drum, resonating differently depending on the location of the key being struck. Tapping keys on a uniform surface does not result in identifiable acoustic emanations.

One effective countermeasure against acoustic attacks against keyboards is the use of touch screens or virtual keyboards in place of regular, mechanical keyboards.

However, the use of touch screens or virtual keyboards does not preclude the viability of an optical attack and, depending on the specific implementation of such a countermeasure, may in fact facilitate them. Replacing the use of

HOME
ELECTRO-MAGNETIC EMANATIONS
OPTICAL EMANATIONS
ACOUSTIC EMANATIONS
CURRENT AND FUTURE IMPACT ON SECURITY

mechanical keyboards is unlikely to be popular among users, but there may be some potential for the modification of keyboard design to reduce the emanation of acoustic keystroke signatures, depending on whether acoustic keyboard attacks are seen as a great enough threat to warrant such an implementation.

CURRENT AND FUTURE IMPACT ON SECURITY

While generally still in proof-of-concept stages, these attacks demonstrate how powerful the successful recovery of plaintext can be, and how in some cases it can completely bypass common security measures.

Designing techniques to combat this form of leakage bridges the divide between information and physical security. Indeed, for the attacks mentioned here, it is unclear where official standardisation for implementing countermeasures, or even for quantifying vulnerability, may come from. Currently the only related standards that exist are the confidential TEMPEST standards for equipment with EM emanation countermeasures. While national governments do run endorsement and testing programs for private sector manufacturers of such equipment, there are no open, public standards that deal specifically with any of the forms of compromising emanations discussed in this article. Without the ability to accurately and consistently define threats and countermeasures across the security industry, those seeking to defend against attacks exploiting compromising emanations will be on the back foot.

Furthermore, the continued development of signal processing technology will be an important factor in the continuing development of attacks exploiting compromising emanations. For example, the acoustic attacks discussed can potentially be improved with the use of more advanced audio capture equipment, such as laser microphones. Improvements in the field of radio signal processing will not just improve the technical capability of EM-based attacks, but may also increase the potential for remote attacks from greater distances. This would result in increased potential for longer distance data collection, reducing the necessity for an attacker to be in close proximity to the target.

The growing power of consumer electronics may also lead to an increase in the feasibility of attacks. The increasing capabilities of smartphones, both in terms of computational power and in quality of integrated hardware, mean that in the future they may potentially be used by an attacker to carry out the types of attacks

HOME
ELECTRO-MAGNETIC EMANATIONS
OPTICAL EMANATIONS
ACOUSTIC EMANATIONS
CURRENT AND FUTURE IMPACT ON SECURITY

mentioned here; research and development into complex signal processing by handsets for commercial applications is already being carried out and implemented.

Finally, even more importantly, these processes can potentially be automated, allowing an attacker to set up a surveillance-style listening post, or even a sensor network, targeting emanations of interest. The attacker may then be able to manage the process remotely, or at most have to make an occasional visit in order to configure or collect data.

Although the attacks discussed here are likely to be considered beyond the capabilities of the everyday attacker, it is important not to rule any potential attack out, and it is definitely within the best interests of the security community to keep all forms of potential plaintext information leakage in mind.

These attacks are at an interesting stage in their development, somewhere between their initial discovery and demonstration of feasibility, and the development of any open standardisation or formalisation. With the increase of improved security and cryptographic implementations, plaintext information leakage will possibly become an attractive target for attackers, and so this field of security research is only likely to grow in importance in the coming years. ■

ABOUT THE AUTHORS

Richard Frankland originally obtained his bachelor's degree in Biomedical Science, but has had a long-standing interest in information security. Having recently completed his M.Sc. at RHUL, he is currently working towards a Ph.D. in Electronic Voting security at Technische Universität Darmstadt and CASED, Germany. His main research interests include security formalisation, standardisation and compliance.

Dr. Stephen Wolthusen is a lecturer in information security at Royal Holloway with research interests in information assurance and the use of formal methods in security. He teaches courses in Network Security and Digital Forensics.

HOME

ELECTRO-MAGNETIC EMANATIONS

OPTICAL EMANATIONS

ACOUSTIC EMANATIONS

CURRENT AND FUTURE IMPACT ON SECURITY