INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 5 (2018) PAGES 3984 - 4002
RECEIVED : 09.09.2018 PUBLISHED : 01.10.2018

Oct 01, 2018

Acoustic Cryptanalysis With advance techniques

S.Seema, Assistant Professor, PG & Research Department Of Computer Science & Applications, K.M.G College Of Arts & Science, Gudiyattam.

Abstract

Many computers emit a high-pitched noise during operation, due to vibration in some of their electronic components. These acoustic emanations are more than a nuisance: They can convey information about the software running on the computer and, in particular, leak sensitive information about security-related computations. In a preliminary presentation (Eurocrypt'04 rump session), we have shown that different RSA keys induce different sound patterns, but it was not clear how to extract individual key bits. The main problem was the very low bandwidth of the acoustic side channel and several orders of magnitude below the GHz-scale clock rates of the attacked computers. In this paper, we describe a new acoustic cryptanalysis key extraction attack, applicable to GnuPG's implementation of RSA. The attack can extract full 4096-bit RSA decryption keys from laptop computers (of various models), within an hour, using the sound generated by the computer during the decryption of some chosen cipher texts. We experimentally demonstrate such attacks, using a plain mobile phone placed next to the computer, or a more sensitive microphone placed 10 meters away.

1. Introduction

One of the methods for extracting information from supposedly secure systems is side channel attacks: cryptanalytic techniques that rely on information unintentionally leaked by computing devices. Most side-channel attack research has focused on electromagnetic emanations (TEMPEST), power consumption and, recently, diffused visible light from CRT displays. The oldest eavesdropping channel, namely acoustic emanations, has received little attention. Our preliminary analysis of acoustic emanations from personal computers shows them to be a surprisingly rich source of information on CPU activity

Acoustic cryptanalysis is a side channel attack which exploits sounds, audible or not, produced during a computation or input-output operation by computer workstations, impact printers, or electromechanical cipher machines

2. History of cryptanalysis

2.1 Classical cryptanalysis

Cryptanalysis has coevolved together with cryptography ciphers being designed to replace old broken designs, and new cryptanalytic techniques invented to crack the improved schemes and to create secure cryptography.

Although the actual word "cryptanalysis" is relatively recent (it was coined by William Friedman in 1920), methods for breaking codes and ciphers are much older. The first known recorded explanation of cryptanalysis was given by 9th-century Arabian polymath, Al-Kindi (also known as "Alkindus" in Europe), in A Manuscript on Deciphering Cryptographic Messages. This treatise includes a description of the method of frequency analysis (Ibrahim Al-Kadi, 1992- ref-3).

Frequency analysis is the basic tool for breaking most classical ciphers. In natural languages, certain letters of the alphabet appear more frequently than others; in English, "E" is likely to be the most common letter in any sample of plaintext. In Europe during the 15th and 16th centuries, the idea of a polyalphabetic substitution cipher was developed. For some three centuries, the Vigenère cipher, which uses a repeating key to select different encryption alphabets in rotation, was considered to be completely secure (le chiffre indéchiffrable—"the indecipherable cipher"). Nevertheless, Charles Babbage (1791–1871) and later, independently, Friedrich Kasiski (1805–81) succeeded in breaking this cipher.

Moreover, automation was first applied to cryptanalysis in that era with the Polish Bomba device, the British Bombe development of it, the use of punched card equipment, and in the Colossus computers—the first electronic digital computers to be controlled by a program.

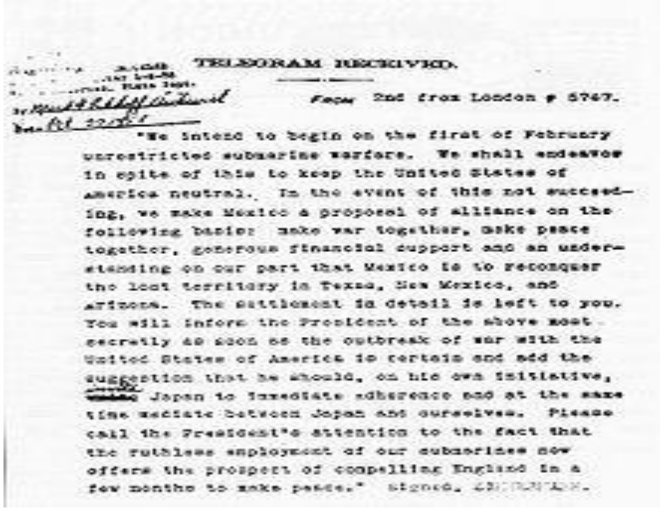
2.2 Modern cryptanalysis

Replica of a Bombe device

Modern cryptography has become much more impervious to cryptanalysis than the pen-and-paper systems of the past, and now seems to have the upper hand against pure cryptanalysis. In some systems even a chosen plaintext attack, in which a selected plaintext is matched against its ciphertext, cannot yield the key that unlock other messages. In a sense, then, cryptanalysis is dead. Kahn goes on to mention increased opportunities for interception, bugging, side channel attacks, and quantum computers as replacements for the traditional means of cryptanalysis.

Indeed, many important modern security vulnerabilities come from flaws in applications and protocols, not from problems with cryptographic primitives. Discovery of critical security flaws in operating systems, web browsers, plugins, web applications, and other trusted code is almost routine. And even where software and hardware functions as expected, phishing and social engineering attacks are key threats to information security today.However, any postmortems for cryptanalysis may be premature. Many serious attacks against both academic and practical cryptographic primitives have been published in the modern era of computer cryptography.

2.3 The results of cryptanalysis



TELEGRAM RECEIVED.

From 2nd from London # 5747.

"We intend to begin on the first of February
unrestricted submarine warfare. We shall endeavor
in spite of this to keep the United States of
America neutral. In the event of this not succeed-
ing, we make Mexico a proposal of alliance on the
following basis: make war together, make peace
together, generous financial support and an under-
standing on our part that Mexico is to reconquer
the lost territory in Texas, New Mexico, and
Arizona. The settlement in detail is left to you.
You will inform the President of the above most
secretly as soon as the outbreak of war with the
United States of America is certain and add the
suggestion that he should, on his own initiative,
~~[illegible]~~ Japan to immediate adherence and at the same
time mediate between Japan and ourselves. Please
call the President's attention to the fact that
the ruthless employment of our submarines now
offers the prospect of compelling England in a
few months to make peace." Signed, [illegible].

The Decrypted Zimmermann Telegram

.

Successful cryptanalysis has undoubtedly influenced history; the ability to read the presumed-secret thoughts and plans of others can be a decisive advantage, and never more so than during wartime. For example, in World War I, the breaking of the Zimmermann Telegram was instrumental in bringing the United States into the war. In World War II, the cryptanalysis of the German ciphers — including the Enigma machine and the Lorenz cipher — has been credited with everything between shortening the end of the European war by a few months to determining the eventual result (see ULTRA). The United States also benefited from the cryptanalysis of the

Japanese PURPLE code.Governments have long recognized the potential benefits of cryptanalysis for intelligence, both military and diplomatic, and established dedicated organizations devoted to breaking the codes and ciphers of other nations, for example, GCHQ and the NSA, organizations which are still very active today. In 2004, it was reported that the United States had broken Iranian ciphers. (It is unknown, however, whether this was pure cryptanalysis, or whether other factors were involved).

3. How Acoustic emanations shows them to be a rich source of Information on CPU activity :

Q1: What information is leaked?

This depends on the specific computer hardware. We have tested several desktop and laptop computers, and in all cases it was possible to distinguish an idle CPU (i.e., 80x86 "HLT" state) from a busy CPU. For some computers, it was also possible to distinguish various patterns of CPU operations and memory access.

This can be observed for artificial cases (e.g., loops of various CPU instructions), and also for real-life cases (e.g., RSA decryption).

The time resolution is usually on the order of milliseconds. In some context, such information can be used to reveal secret keys; see the next question.

Q2: How can a low-frequency (KHz) acoustic source yield information on a much faster (GHz) CPU?

In two ways. First, when the CPU is carrying out a long operation, it may create a characteristic acoustic spectral signature: for example, below we show how RSA signature/decryption sounds different for different secret keys. Second, we get temporal information about the length of each operation, and this can be used to mount timing attacks, especially when the attacker can affect the input to the operation (i.e., in chosen-ciphertext attack scenario).

Q3: Won't the attack be foiled by loud fan noise, or by multitasking, or by several computers in the same room?

Probably not. The interesting acoustic signals are mostly above 10 KHz, whereas typical computer fan noise and normal room noise are concentrated at lower frequencies and can thus be filtered out by suitable equipment.

In a task-switching systems, different tasks can be distinguished by their different acoustic spectral signatures.

When several computers are present, they can be told apart by their different acoustic signatures, since these vary with the hardware, the component temperatures, and other environmental conditions.

Q4: What countermeasures are available?

One obvious countermeasure is to use sound dampening equipment, such as "sound-proof" boxes, that is designed to sufficiently attenuate all relevant frequencies. Conversely, a sufficiently strong wide-band noise source can mask the informative signals, though ergonomic concerns may render this unattractive. Careful circuit design and high-quality electronic components can probably reduce the emanations. Alternatively, one can employ known algorithmic techniques to reduce the usefulness of the emanations to attacker. These techniques ensure the rough-scale behavior of the algorithm is independent of the inputs it receives; they usually carry some performance penalty, but are often already used to thwart other side-channel attacks.

Q5: What about other acoustic attacks?

Eavesdropping on keyboard keystrokes has been often discussed; keys can be distinguished by timing, or (as recently proposed by Asonov and Agrawal) by their different sounds.

While this attack is applicable to data that is entered manually (e.g., passwords), it is not applicable to larger secret data such as RSA keys.

Another acoustic source is hard disk head seeks; this source does not appear very useful in the presence of caching, delayed writes and multitasking. Preceding modern computers, one may recall MI5's "ENGULF" technique (recounted in Peter Wright's book Spycatcher), whereby a phone tap was used to eavesdrop on the operation of an Egyptian embassy's Hagelin cipher machine, thereby recovering its secret key.

Q6: Why bother with acoustic attacks, when TEMPEST and power-analysis attacks are available?

Side-channel attacks based on electromagnetic emanations are indeed very powerful and widely discussed. For precisely this reason, secure facilities take measures to protect against these, such as Faraday cages and isolated power supplies. However, these measures may be transparent to acoustic radiations -- consider a Faraday cage constructed of metallic mesh. Also, digital audio recording equipment is ubiquitous, and this creates new attack scenarios: for example, a compromised laptop carried into a secure computer room may record valuable acoustic information without its owner's knowledge. Another scenario is a program recording the computer on which it runs in order to learn information on other running programs, thereby breaching sandbox security boundaries or compromising NGSCB-like systems. Finally, known eavesdropping techniques, such as detecting window vibration by its effect on reflected laser beams, could allow additional attack scenarios.

Q7: What's so special about the "HLT" instruction, and why is it useful to detect it?

The CPU instruction that is easiest to detect acoustically, though by now means the only one detectable, is the 80x86 "HLT instruction. This instruction puts the CPU into a special low-power sleep state that lasts until the next hardware interrupt. On modern CPUs this temporarily shuts down many of the on-chip circuits, which dramatically lowers power consumption and alters acoustic emissions for relatively long time.

Experimentally, the difference between active computation (which normally never involves HLT instructions) and an idle CPU (where the kernel executes HLT instructions in its idle loop) is usually very prominent.

If the only program running is a cryptographic application, then this already suffices to detect when the program awakens to handle input and when it finishes its cryptographic tasks, and this information can be used to mount timing attacks as discussed above. Of course, additional subtler acoustic cues will yield further information.

Q8: What's so special about cryptographic operations?

Our experiments suggest that in most computers, each type of operation has an acoustic signature -- a characteristic sound. This applies to any operation, cryptographic or otherwise.

We focus on cryptographic operations because these are designed and trusted to protect information, and thus information leakgage from within them can be critical. For example, recovering a single decryption key can compromise the secrecy of all messages sent over the corresponding communication channel.

Q10: How do timing attacks work?

Timing attacks are one of the classes of attacks that take advantage of auxiliary side-channel information. They exploit the fact that many computational operations vary in time depending on the inputs to the operation, and thus by measuring the running time of the operation we learn something about its inputs. For example, consider the RSA cryptosystem. In this system, decryption of a ciphertext *c* is done by treating *c* as a large number and raising it to the *d*-th power, where *d* is the secret key.

The simplest (though inefficient) algorithm for computing this exponentiation is to multiply *c* by itself *d* times; this takes time proportional to *d,* so by measuring this time we get an estimate of *d*. The algorithms used in practice ("square and multiply" and its variants) are much more efficient, but exhibit similar properties unless carefully designed to thwart such attacks.

By combining many measurements that correspond to different properties of the key, the possibilities can be narrowed down until the key is fully recovered. This type of timing attacks was introduced by Kocher and demonstrated in practical settings by Boneh and Brumley.

4. Acoustical Intelligence:

Acoustical Intelligence (**ACOUSTINT**, sometimes **ACINT**) is an intelligence gathering discipline that collects and processes acoustic phenomena. It is a sub discipline of MASINT (Measurement and Signature Intelligence)

5. Acoustic Materials:

ABOUT CCM:

Our company is founded and based upon previous experience work related to well known Construction Companies all over the world. CCM(CONSTRUCTION MATERIALS SUPPLIERS) is a well established UAE based venture with a heavy expertise in providing construction solutions. As an Importer and Distributor of building materials we keep a track of fast revolving market and reflect its changes as well as innovations thereby adding to our list of building materials as well as various other products. CCM represents a number of leading manufacturers and suppliers of construction related materials. Our sales and distribution operations are being held all across UAE with the facilities headquartered in Ras Al Khaimah Free Zone.

Our materials improve comfort and safety as they increase quality and value in many diverse applications and industries including transportation, military, medical, marine, architectural, construction, heating and ventilation, agricultural, compressor, machine inclosure, home theater, audio/video component, domestic appliance, pipe wrap, Gen-Sets, and HVAC

Our Main Areas of Concentration & Expertise are:

- Sound Absorbent Materials for:

- Floors: Acoustic:
--Underlay/Membrane/Soundproofing/Sound Insulation barrier/Wood Floor - underlay (Polyethlene, Foam, Recycle rubber, Fiber Glass ... etc)
- Walls: Acoustic:
--Wall Panels/Wall Partion/Covering walls/Wall Soundproofing/Wall membrane (Polyethylene, Cork, Polyester fiber, Rockwool ... etc)
- Ceiling: Acoustic:
--Ceiling Panels (Natural wood fiber, Plaster board, Polyethlene…etc)

- Vibration Damping Materials:

--Anti-Vibration Sheets (Recycle Rubber, Cork...etc)

- Thermal Insulation Materials:

--Thermo-Acoustic insulating Panels (Natural wood fiber, Polyester...etc)

6. Acoustic Sources

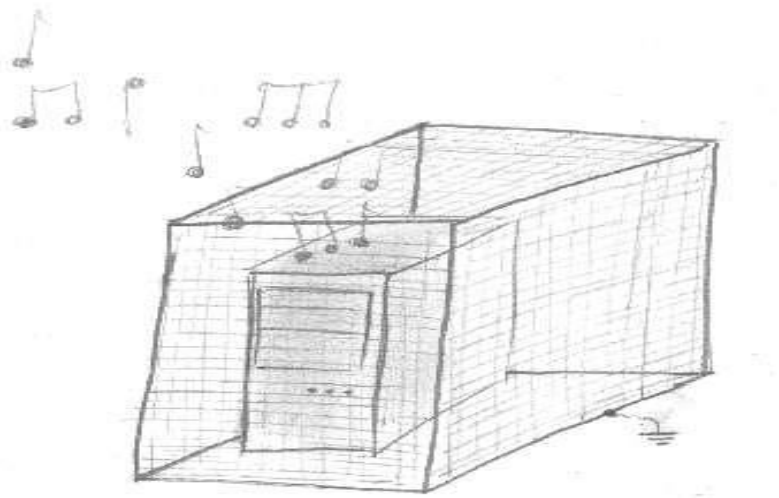
Precision Acoustics does not have a catalogue of transducers but prefers to work with clients to develop ultrasound transducers for their particular application.

Working with a standard range of casing options we can offer a low cost solution for customised transducers with frequencies above 500 kHz.

The PC Chips M754LMR motherboard has a bank of 1500µF capacitors near the CPU and power connector.

Here is the effect of applying a generous dose of Quik-Freeze spray (non-conductive, non-flammable, "will freeze small areas to -48°C") to these capacitors while the CPU is executing a loop of MUL instructions:

7. Experimental Setup



Below are several short samples, given in the form of a spectrogram and a WAV file. The spectrograms are snapshots from the Baudline signal analysis software running on GNU/Linux; horizontal axis is frequency (0Hz to 48KHz), vertical axis is time, and intensity is determined by power per frequency window (the greener the stronger).

All recordings were equalized (roughly -10dB below 1 KHz , +10dB above 10 KHz) using the mixer's rudimentary built-in equalizer.

The recordings below were made using low-end equipment: a Røde NT3 condenser microphone (US$170), an Alto S-6 mixer (US$55) serving as an amplifier and rudimentary equalizer, and a Creative Labs Audigy 2 sound card (US$70) for recording into a separate computer. The recordings below were made under nearly ideal conditions: the microphone was placed 20cm from the recorded computer, the PC case was opened and noisy fans were disconnected (where applicable).

Comparable results were achieved under more realistic conditions (i.e., the subject computer is intact and placed 1m to 2m from the microphone) using more expensive audio equipment.

For example, a high-quality analog equalizer can be used to attenuate strong low-frequency fan hums and background noise, allowing further amplification of interesting signals before analog-to-digital quantization.

Except where noted otherwise, the computer being recorded is a no-brand box using a PC Chips M754LMR motherboard, an Intel Celeron 666MHz CPU and an Astec ATX200-3516 power supply. This computer was chosen for its particularly striking acoustic emanations, but is by no means a special case: every computer we tested showed significant correlation between acoustic spectrum and CPU activities, and in about half the cases the effect could be heard by naked ear when using appropriate CPU activity patterns.

8. About Digital Signature Certificate

A Digital Signature Certificate, like hand written signature, establishes the identity of the sender filing the documents through internet which sender can not revoke or deny. Accordingly, Digital Signature Certificate is a digital equivalent of a hand written signature which has an extra data attached electronically to any message or a document. Digital Signature also ensures that no alterations are made to the data once the document has been digitally signed. A DSC is normally valid for 1 or 2 years, after which it can be renewed.

A Digital Signature is a method of verifying the authenticity of an electronic document. Digital signatures are going to play an important role in our lives with the gradual electronization of records and documents.

The IT Act has given legal recognition to digital signature meaning, thereby, that legally it has the same value as handwritten or signed signatures affixed to a document for its verification

The Information Technology Act, 2000 provides the required legal sanctity to the digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents.

8.1 What can I use digital certificates for?

Three uses are outlined here. Your digital certificate could be used to allow you to access membership-based web sites automatically without entering a user name and password. It can allow others to verify your "signed" e-mail or other electronic documents, assuring your intended reader(s) that you are the genuine author of the documents, and that the content has not been corrupted or tampered with in any way. Finally, digital certificates enable others to send private messages to you: anyone else who gets his/her hands on a message meant for you will not be able to read it.

Sending Digitally Signed Mail : You can use your Digital Certificate to digitally sign your emails sent through Outlook Express / MS-Outlook etc. Digitally signing the mail authenticates your identity and enables the receiver to ensure that the mail has come from you only. It also ensures that the content of the mail is not tampered in the transit and the mail received by the receiver is the same what you have sent.

8.2 WHO NEEDS A DIGITAL SIGNATURE CERTIFICATE

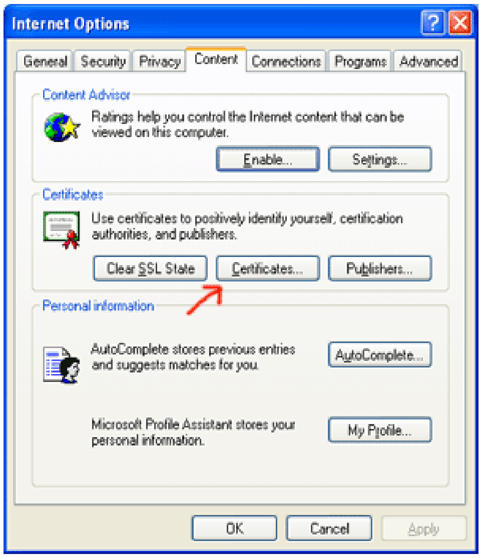
Accordingly following have to obtain Digital Signature Certificate:

1. Directors
2. Auditors
3. Company Secretary - Whether in practice or in job.
4. Bank Officials - for Registration and Satisfaction of Charges
5. Other Authorized Signatories.

8.3 TYPES OF DIGITAL SIGNATURE CERTIFICATE

There are 3 types of Digital Signature Certificates, having different security levels, namely : Class-1, Class-2 , Class-3.

For filing documents under MCA21, a Class-2 Digital Signature Certificate issued by a Licensed Registration Authority is required. We also offer Class 1 and 3 besides Class 2 certificates.

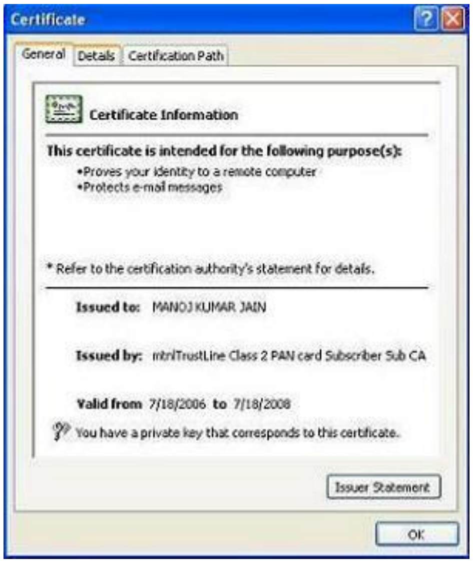


Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Protects e-mail messages

* Refer to the certification authority's statement for details.

Issued to: MANOJ KUMAR JAIN

Issued by: mtnlTrustLine Class 2 PAN card Subscriber Sub CA

Valid from 7/18/2006 to 7/18/2008

You have a private key that corresponds to this certificate.

9. Known attacks

In 2004, Dmitri Asonov and Rakesh Agrawal of the IBM Almaden Research Center announced that computer keyboards and keypads used on telephones and automated teller machines (ATMs) are vulnerable to attacks based on differentiating the sound produced by different keys. Their attack employed a neural network to recognize the key being pressed.

By analyzing recorded sounds, they were able to recover the text of data being entered. These techniques allow an attacker using covert listening devices to obtain passwords, passphrases, personal identification numbers (PINs) and other security information.

In 2005, a group of UC Berkeley researchers performed a number of practical experiments demonstrating the validity of this kind of threat.

Also in 2004, Adi Shamir and Eran Tromer demonstrated that it may be possible to conduct timing attacks against a CPU performing cryptographic operations by analysis of variations in its humming noise.

10. Types of cryptanalytic attack

Cryptanalytic attacks vary in potency and how much of a threat they pose to real-world cryptosystems. A certificational weakness is a theoretical attack that is unlikely to be applicable in any real-world situation; the majority of results found in modern cryptanalytic research are of this type.

Essentially, the practical importance of an attack is dependent on the answers to the following four questions:

1. What knowledge and capabilities does the attacker need?
2. How much additional secret information is deduced?
3. How much computation is required? (What is the computational complexity?)
4. Does the attack break the full cryptosystem, or only a weakened version?

10.1 Prerequisites of the attack

Cryptanalysis can be performed under a number of assumptions about how much access the attacker has to the system under attack. As a basic starting point it is normally assumed that, for the purposes of analysis, the general algorithm is known; this is Kerckhoffs' principle of "the enemy knows the system". This is a reasonable assumption in practice — throughout history, there are countless examples of secret algorithms falling into wider knowledge, variously through espionage, betrayal and reverse engineering. (On occasion, ciphers have been reconstructed through pure deduction; for example, the German Lorenz cipher and the Japanese Purple code, and a variety of classical schemes).

Other assumptions include:

- Ciphertext-only: the cryptanalyst has access only to a collection of ciphertexts or codetexts.
- Known-plaintext: the attacker has a set of ciphertexts to which he knows the corresponding plaintext.
- Chosen-plaintext (chosen-ciphertext): the attacker can obtain the ciphertexts (plaintexts) corresponding to an arbitrary set of plaintexts (ciphertexts) of his own choosing.
- Adaptive chosen-plaintext: like a chosen-plaintext attack, except the attacker can choose subsequent plaintexts based on information learned from previous encryptions. Similarly Adaptive chosen ciphertext attack.

Related-key attack: Like a chosen-plaintext attack, except the attacker can obtain ciphertexts encrypted under two different keys. The keys are unknown, but the relationship between them is known; for example, two keys that differ in the one bit.

These types of attack clearly differ in how plausible they would be to mount in practice. Although some are more likely than others, cryptographers will often take a conservative approach to security and assume the worst-case when designing algorithms, reasoning that if a scheme is secure even against unrealistic threats, then it should also resist real-world cryptanalysis as well.

The assumptions are often more realistic than they might seem upon first glance. For a known-plaintext attack, the cryptanalyst might well know or be able to guess at a likely part of the plaintext, such as an encrypted letter beginning with "Dear Sir", or a computer session starting with

"LOGIN:". A chosen-plaintext attack is less likely, but it is sometimes plausible: for example, you could convince someone to forward a message you have given them, but in encrypted form.

Related-key attacks are mostly theoretical, although they can be realistic in certain situations, for example, when constructing cryptographic hash functions using a block cipher.

10.2 Usefulness of attack results

The results of cryptanalysis can also vary in usefulness. For example, cryptographer Lars Knudsen (1998) classified various types of attack on block ciphers according to the amount and quality of secret information that was discovered:

- Total break — the attacker deduces the secret key.
- Global deduction — the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.
- Instance (local) deduction — the attacker discovers additional plaintexts (or ciphertexts) not previously known.
- Information deduction — the attacker gains some Shannon information about plaintexts (or ciphertexts) not previously known.
- Distinguishing algorithm — the attacker can distinguish the cipher from a random permutation.

Similar considerations apply to attacks on other types of cryptographic algorithm.

10.3 Computational resources required

Attacks can also be characterised by the resources they require. Those resources include:

- Time — the number of computation steps (like encryptions) which must be performed.
- Memory — the amount of storage required to perform the attack.
- Data — the quantity of plaintexts and ciphertexts required.

It's sometimes difficult to predict these quantities precisely, especially when the attack isn't practical to actually implement for testing.

Bruce Schneier notes that even computationally impractical attacks can be considered breaks: "Breaking a cipher simply means finding a weakness in the cipher that can be exploited with a complexity less than brute force.

Never mind that brute-force might require 2^{128} encryptions; an attack requiring 2^{110} encryptions would be considered a break...simply put, a break can just be a certificational weakness: evidence that the cipher does not perform as advertised." (Schneier, 2000).

10.4 Partial breaks

Academic attacks are often against weakened versions of a cryptosystem, such as a block cipher or hash function with some rounds removed. Many, but not all, attacks become exponentially more difficult to execute as rounds are added to a cryptosystem, so it's possible for the full cryptosystem to be strong even through reduced-round variants are weak. Nonetheless, partial breaks that come close to breaking the original cryptosystem may mean that a full break will follow; the successful attacks on DES, MD5, and SHA-1 were all preceded by attacks on weakened versions.

10.5 Academic weakness versus practical weakness

In academic cryptography, a weakness or a break in a scheme is usually defined quite conservatively: it might require impractical amounts of time, memory, or known plaintexts. It also might require the attacker be able to do things many real-world attackers can't: for example, the attacker may need to choose particular plaintexts to be encrypted or even to ask for plaintexts to be encrypted using several keys related to the secret key.

Furthermore, it might only reveal a small amount of information, enough to prove the cryptosystem imperfect but too little to be useful to real-world attackers. Finally, an attack might only apply to a weakened version of cryptographic tools, like a reduced-round block cipher, as a step towards breaking of the full system.

11. Methods of cryptanalysis

11.1 Classical cryptanalysis:

- Frequency analysis
- Index of coincidence
- Kasiki examination

11.2 Symmetric algorithms:

- Integral cryptanalysis
- Linear cryptanalysis
- Meet-in-the-middle attack
- Mod-n cryptanalysis
- Related-key attack
- Sandwich attack
- Slide attack

11.3 Hash functions:

- Birthday attack
- Rainbow table attack
- Chosen-cipher text attack
- Chosen-plaintext attack

12. Acoustic Output Measurements

Precision Acoustics is pleased to offer access to a full range of acoustic measurement services for medical and non medical ultrasound transducers .

The accurate characterisation of temporal and spatial parameters of a medical ultrasonic field is important for safety reasons. Using our fully automated test tanks, Precision Acoustics can measure the parameters required by international safety standards and regulatory organisations in the frequency range 0.5-20MHz.

Non medical products often require characterisation so that beam profiles and bandwidths can be quantified. Precision Acoustics can undertake measurements according to the relevant international standards to assess the beam profile and calculate the beam width for non-destructive testing transducers.

We also have the capability to characterise the acoustic properties of a wide range of materials in the frequency range 0.5-10MHz.

12.1 Measurements can be divided into three categories:

1. Calibrated Point Measurements

Hydrophone measurements of pressure, intensity and associated parameters. For medical transducers, MI (mechanical index), TI (thermal index) and tissue-attenuated pressure/intensity parameters can be calculated. Measurements of transmit and receive voltage responses are often also computed for underwater (sonar) transducers. Materials characterisation measurements are also included in the calibrated point measurement category.

2. Spatial Variation of Field Properties

These measurements are hydrophone-based and involve linear (1-D) and planar (2-D) mapping of pressure fields to a positional accuracy of 5um. This is particularly useful for determining transducer beam widths and radiating areas, but can also be used to determine position of transducer side lobes. Planar scanning can also be used to determine acoustic power when other methods are inappropriate.

3. Whole-field Characterization

Measurement of total acoustic power, power within an aperture and transducer efficiency can all be made with our Radiation Force Balance. For medical transducers, tissue-attenuated acoustic power can also be calculated.

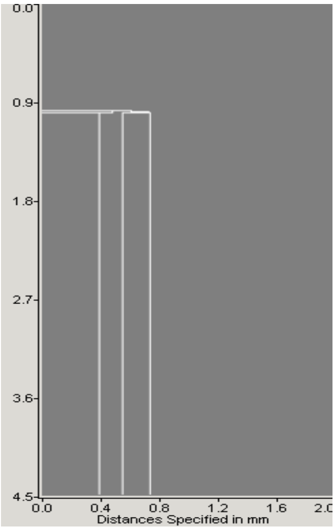
13. Acoustic Performance Modelling

A critical feature of many design processes is the ability to simulate the problems before undertaking the more costly stage of prototype fabrication. One of the principal modelling tools used within Precision Acoustics is a comprehensive finite difference simulation. It is capable of predicting the simulation full acoustic wave simulation through both solid and fluid media. This means that the propagation of longitudinal, shear, Love, Lamb, Rayleigh and Stoneley wave can all be simulated. Simulations can either be conducted in 2D Cartesian or 3D axi-symmetric cylindrical co-ordinates with either lossless and/or simple lossy materials.

Case Study 1: Needle Hydrophones Frequency Response

Application of the numerical model has been critical in the improvement of the frequency response of the Precision Acoustic needle hydrophone range. Historically, needle hydrophones had a very non-uniform frequency response at lower frequencies. A typical needle geometry was simulated and the radial interactions of waves diffracted from the edges of the needle tip could clearly be seen.

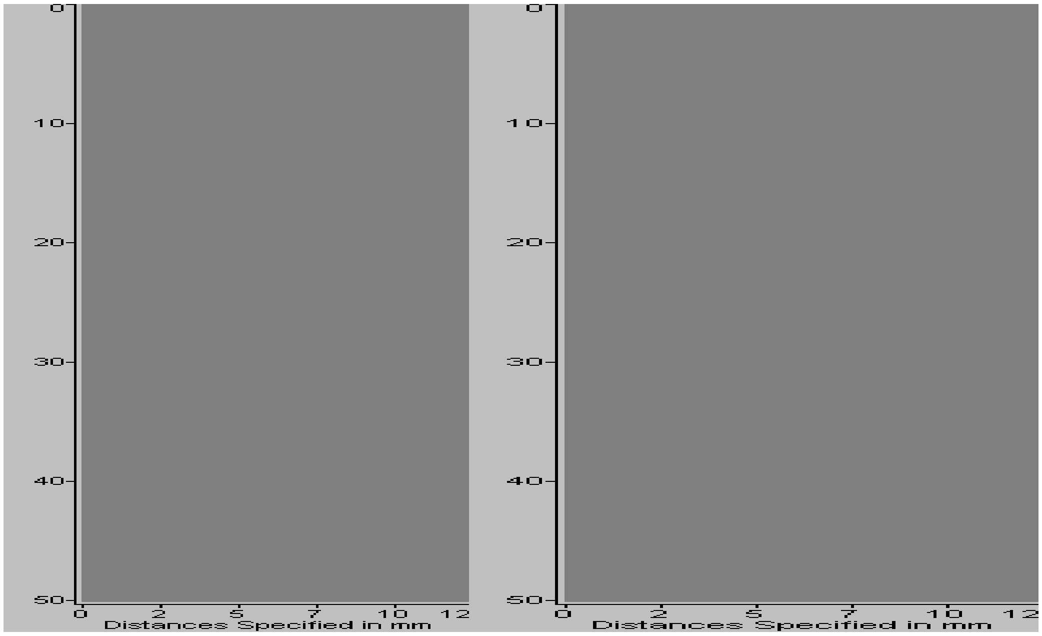
The geometry of the needle hydrophone tip was then modified in the simulation and when a satisfactory solution was obtained, this was then implemented on a revised design for the needle hydrophone. This process has been so successful that all Precision Acoustics needle hydrophones now incorporate the modifications suggested by the numerical simulations.



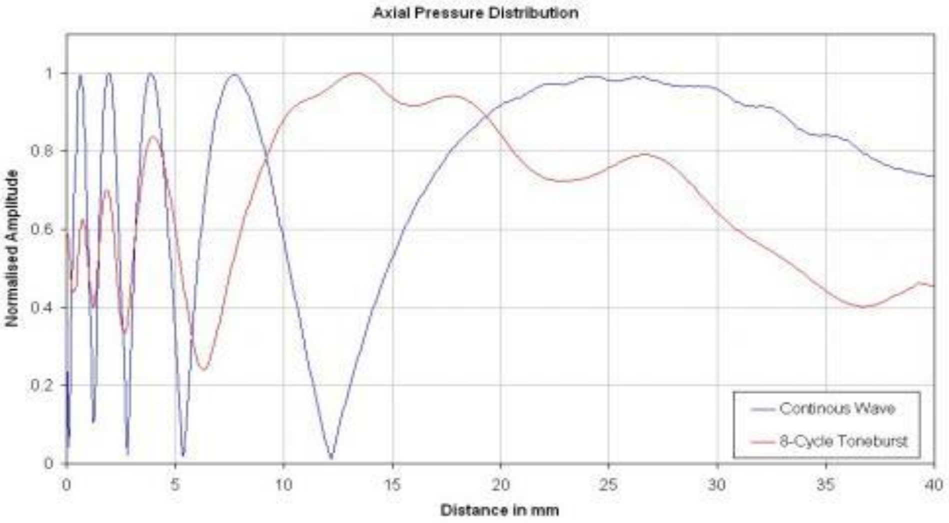
Case Study 1

Case Study 2: Pulse vs CW Transducer Fields

During one of our Hydrophone User Courses, Precision Acoustics were asked "Why does the last axial maxima of my transducer appear in a different position when I drive it with a toneburst?" Clearly this relates to the interaction of plate and edge waves from the transducer, but the explanation of this phenomenon was easiest explained with the assistance of some numerical simulations. The animations below display the same transducer drive with either CW or an 8-cycle toneburst whilst the graph displays the axial pressure maps derived from these simulations.



Case Study 2



This software, the AFiDS suite, has been developed by Dr. Andrew Hurrell over 10 years, and has been the subject of several conference presentations

14. CONCLUSION:

Adversaries can circumvent cryptography by monitoring plain text inputs and outputs of communication channels

- Key loggers capture and transmit all keyboard activity before what's being typed gets encrypted
- Adversary can install a key logging program on Alice/Bob's machine by:
  –CD/disk/download (with direct access to target machine)
  –Remotely connecting to and exploiting a flaw on target machine (to install key logger without Alice/Bob's knowledge)
  –Packaging key logger program as something benign and convincing target to Execute it.
- Alternatively, adversary can quietly install key logging hardware on Alice/Bob's machine
- Cryptography is a communications technology, with applications in computer security.
- Cryptography does not "solve" computer security.
- Most computer-security problems arise from unrelated issues
  –Programs are shipped with insecure default settings
  –Programs contain errors that attackers can exploit
  –Users execute malicious software because it seems benign

References:

1. Marchetti, Victor; Marks, John (1973), The CIA and the Craft of Intelligence
2. Wright, Peter (1987), Spycatcher: The candid autobiography of a senior intelligence officer, Viking
3. Yang, Sarah (14 September 2005), "Researchers recover typed text using audio recordingof keystrokes", UC Berkeley News,
4. http://www.berkeley.edu/news/media/releases/2005/09/14_key.shtml
5. Shamir, Adi; Tromer, Eran, Acoustic cryptanalysis:On nosy people and noisy machines], http://www.wisdom.weizmann.ac.il/~tromer/acoustic/
6. Asonov; Agrawal, Rakesh (2004) (PDF), Keyboard Acoustic Emanations