Media coverage of Acoustic Cryptanalysis paper

Website: http://www.cs.tau.ac.il/~tromer/acoustic/

Concise summary

Some popular articles:

Economist: ""Unsafe and sound"
Ars Technica: "New attack steals e-mail decryption keys by capturing computer sounds"

ExtremeTech:" Researchers crack the world's toughest encryption by listening to the tiny sounds made by your computer's CPU"

הארץ: וופורקימ מע RSA תנפצה תא וחנעיפ מילארשי מירקוח

Awarded Black Hat Pwnie Award for Most Innovative Research 2014

Additional articles in major venues:

NBC News, PCWorld, Forbes, כלכליסט, The Telegraph, The Register, Daily Mail (#1, #2), Channel 4 News, BoingBoing, Engadget, Habrahabr (site #22 in Russia), Gazeta.pl (site #8 site in Poland), Softpedia, Tom's Guide, Phys.org, Hack a Day

Social media, for example:

Reddit (top story of the week for all of Reddit, 1647 comments)

Slashdot

First 5 days: 431K page views (unique addresses).

Articles in major websites

(Filtered to sites wit Alexa global rank above 6000, or near-top rank for some country)

- The Economist (Peter Haynes)
  "Unsafe and sound"

http://www.economist.com/news/science-and-technology/21594240-ciphers-can-now-be-broken-listening-computers-use-them-unsafe-and

- Le Monde
  - Le Monde (David Larousserie)
    "Des ordinateurs sur écoute (au sens propre)"
    http://www.lemonde.fr/a-la-une/article/2014/01/13/des-ordinateurs-sur-ecoute-au-sens-propre_4347183_3208.html
  - Le Monde (Jacques Cheminat avec IDG NS)
    "Déchiffrer un message crypté en écoutant le son du processeur"
    http://www.lemondeinformatique.fr/actualites/lire-dechiffrer-un-message-crypte-en-ecoutant-le-son-du-processeur-56052.html

- NBC News (Devin Coldewey)
  "The sound of secrets: New hacking technique infiltrates by hearing — or touch"
  http://www.nbcnews.com/technology/sound-secrets-new-hacking-technique-infiltrates-hearing-or-touch-2D11777733
- ExtremeTech (Sebastian Anthony)
  "Researchers crack the world's toughest encryption by listening to the tiny sounds made by your computer's CPU"
  http://www.extremetech.com/extreme/173108-researchers-crack-the-worlds-toughest-encryption-by-listening-to-the-tiny-sounds-made-by-your-computers-cpu
  - Derivatives:
  - ByteOfNews article:
    "Researchers crack the world's toughest encryption by listening to the tiny sounds made by your computer's CPU"
    http://byteofnews.com/researchers-crack-the-worlds-toughest-encryption-by-listening-to-the-tiny-sounds-made-by-your-computers-cpu/
  - TECHNOLOGY article
    "Researchers crack the world's toughest encryption by listening to the tiny sounds made by your computer's CPU"
    http://technology.worldnewsviews.com/2013/12/18/researchers-crack-the-worlds-toughest-encryption-by-listening-to-the-tiny-sounds-made-by-your-computers-cpu
- PCWorld / Computerworld (Mark Hachman)
  "Listen up: RSA keys snatched by recording CPU sounds with a phone"
  http://www.pcworld.com/article/2082200/listen-up-rsa-keys-snatched-by-recording-cpu-sounds-with-a-phone.html
  http://news.idg.no/cw/art.cfm?id=909CF477-E8BE-B5A0-99DEF977E0C21389
- Ars Technica (Dan Goodin)
  "New attack steals e-mail decryption keys by capturing computer sounds"
  http://arstechnica.com/security/2013/12/new-attack-steals-e-mail-decryption-keys-by-capturing-computer-sounds/
  - Derivatives:
  - Aviation Record
    "New attack steals e-mail decryption keys by capturing computer sounds"
    http://aviationrecord.com/technology-22/new-attack-steals-e-mail-decryption-keys-by-capturing-computer-sounds-454.html

- Forbes (Tim Worstall)
  “Researchers Break RSA 4096 Encryption With Just A Microphone And A Couple Of Emails”
  http://www.forbes.com/sites/timworstall/2013/12/21/researchers-break-rsa-4096-encryption-with-just-a-microphone-and-a-couple-of-emails/
- כלכליסט (עומר כביר)
  “מיר פיתח שיטה לפריצת הצפנה על ידי האזנה למחשב”ש ידע 'פורפ"

http://www.calcalist.co.il/internet/articles/0,7340,L-3619940,00.html

- הארץ (עודד ירו)

“וופורקימ סע RSA תנפצה תא וחנעיפ סילארשי סירקוח”

http://www.haaretz.co.il/captain/software/.premium-1.2196283

- The Telegraph (Matthew Sparkes)
  “The sound of your PC could betray passwords”
  http://www.telegraph.co.uk/technology/internet-security/10527477/The-sound-of-your-PC-could-betray-passwords.html
- The Register (John Leyden)
  “Code-busters lift RSA keys simply by listening to the noises a computer makes”
  http://www.theregister.co.uk/2013/12/19/acoustic_cryptanalysis/
- Daily Mail (Damien Gayle)
  “How your computer's secrets could be cracked by a smartphone just LISTENING to it as it runs its encryption software”
  http://www.dailymail.co.uk/sciencetech/article-2526666/How-computers-secrets-cracked-smartphone-just-LISTENING-runs-encryption-software.html
- Daily Mail (Victoria Woollaston)
  “Hackers can steal your personal details by using a mobile phone to record the SOUND of your computer”
  http://www.dailymail.co.uk/sciencetech/article-2527166/Hackers-steal-personal-details-using-mobile-phone-record-SOUND-computer.html
- Channel 4 News - Geoff White on Technology (Geoff White)
  “The hacker’s latest weapon: a simple microphone”
  http://blogs.channel4.com/geoff-white-on-technology/hackers-latest-weapon-simple-microphone/585

- BoingBoing (Cory Doctorow)
  “ Deriving cryptographic keys by listening to CPUs' "coil whine" “
  http://boingboing.net/2013/12/20/deriving-cryptographic-keys-by.html
- Engadget (Michael Gorman)
  “Computers share their secrets if you listen”
  http://www.engadget.com/2013/12/20/encryption-cracked-by-computer-sounds/?ncid=rss_truncated
- Engadget (James Trew)
  “Alt-week 12.21.13 … the world's toughest encryption cracked by a microphone”
  http://www.engadget.com/2013/12/21/alt-week-12-21-13/

- Habrahabr - site #22 in Russia
  “Извлечение 4096-битных ключей RSA с помощью микрофона”
  http://habrahabr.ru/post/206572 [translated]
    - Derivatives:
    - Gigamir
      “Извлечение 4096-битных ключей RSA с помощью микрофона”
      http://gigamir.net/techno/pub467841 [translated]
- Gazeta.pl (Robert Kędzierski) - #8 site in Poland
  “Podsłuchali procesor i... odczytali szyfrowaną wiadomość. Zwykłą komórką!”
  http://technologie.gazeta.pl/internet/1,104530,15170951,Podsluchali_procesor_i____odczytali_szyfrowana_wiadomosc_.html [translated]
- Softpedia (Eduard Kovacs)

“Full 4096-Bit RSA Keys Extracted by Listening to the Sound Made by Computers”
http://news.softpedia.com/news/Full-4096-bit-RSA-Keys-Extracted-by-Listening-to-the-Sound-Made-by-Computers-410710.shtml

    - Derivative (or vice versa?):
    - Cyber Security Infotech’s blog
      “Full 4096-Bit RSA Keys Extracted by Listening to the Sound Made by Computers”
      http://csinfotechblog.wordpress.com/2013/12/20/full-4096-bit-rsa-keys-extracted-by-listening-to-the-sound-made-by-computers/
- Tom’s Guide (Jill Scharr)
  “Computer Sounds Give Up Secret Information”
  http://www.tomsguide.com/us/acoustic-cryptanalysis-rsa-algorithm,news-18011.html
  ZME Science (Mihai Andre)
  “Scientists hack a computer using just the sound of the CPU”
  http://www.zmescience.com/research/inventions/hack-cpu-sound-acoustic-19112013/
- Phys.org (Bob Yirka)
  “Research trio crack RSA encryption keys by listening to computer noise”
  http://phys.org/news/2013-12-trio-rsa-encryption-keys-noise.html
- Hack a Day (Adam Fabio)
  “Ambient Computer Noise Leaks Your Encryption Keys”
  http://hackaday.com/2013/12/20/ambient-computer-noise-leaks-your-encryption-keys/
- רשת ב’
  יצחק נוי- שבת עולמית- 25.1.2014
  Radio show
  http://www.magnetradio.com/noy/index.php?option=com_content&view=article&id=130&Itemid=128

Articles in smaller websites

- Naked Security (Paul Ducklin)
  “The sound made by your computer could give away your encryption keys”
  Ggreat article, they really read the paper!

http://nakedsecurity.sophos.com/2013/12/19/the-sound-made-by-your-computer-could-give-away-your-encryption-keys/

- Derivatives:
- Gizmodo
  "The Sounds Your Computer Makes Can Give Away Your Encryption Keys"
  http://gizmodo.com/the-sounds-your-computer-makes-can-give-away-your-encry-1486338511

- Tweakers.net (Dimitri Reijerman)
  "Rsa-sleutels gekraakt door te luisteren naar trillende condensators en spoelen"
  https://tweakers.net/nieuws/93259/rsa-sleutels-gekraakt-door-te-luisteren-naar-trillende-condensators-en-spoelen.html [translated]
- Motherboard (Ben Richmond)
  "Your Computer's Humming Can Give Away Encryption Keys"
  http://motherboard.vice.com/blog/your-computers-humming-can-give-away-encryption-keys
- The Hacker News (Mohit Kumar)
  "Acoustic Cryptanalysis: Extracting RSA Key From GnuPG by capturing Computer Sound"
  http://thehackernews.com/2013/12/acoustic-cryptanalysis-extracting-rsa.html
- Ubergizmo (Edwin Kee)
  "Researchers Listen To Computer CPU Sounds In Order To Crack Encryption Code" (from the article: "don't decrypt data unless you're in a really noisy room, like an auditorium during a heavy metal concert.")
  http://www.ubergizmo.com/2013/12/researchers-listen-to-computer-cpu-sounds-in-order-to-crack-encryption-code/
- DVICE (Robin Burks)
  "Researchers use CPU sounds to crack encryption"
  http://www.dvice.com/2013-12-19/researchers-use-cpu-sounds-crack-encryption
- SecurityWeek (Brian Prince)
  "Researchers Reveal How to Extract Decryption Keys With Sound"
  https://www.securityweek.com/researchers-reveal-how-extract-decryption-keys-sound
- Tripwire's The State of Security (Anthony M Freed)
  "Researchers Capture Computer Sounds to Decipher Cryptographic Keys"
  http://www.tripwire.com/state-of-security/top-security-stories/researchers-capture-computer-sounds-decipher-cryptographic-keys/
- Digi.no (Eirik Rossen)
  "Knekket kryptering med PC-støy"
  http://www.digi.no/925983/knekket-kryptering-med-pc-stoy [translated]
- iThome (文/陳曉莉)
  "研 究人員：「聽」CPU聲音就可破解4096位元的RSA密碼 "
  http://www.ithome.com.tw/itadm/article.php?c=84391 [translated]
- BASIC thinking (Von Tobias Gillen)
  "Was denn noch alles? Forscher entschlüsseln PGP durch Audiosignale"
  http://www.basicthinking.de/blog/2013/12/20/was-denn-noch-alles-forscher-entschluesseln-pgp-durch-audiosignale/ [translated]
- Audio Grains (Matt Gallagher)
  "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis"

http://audiograins.com/blog/2013/12/rsa-key-extraction-via-low-bandwidth-acoustic-cryptanalysis/

- Kaldata
  http://www.kaldata.com/IT-Новини/Извличане-на-4096-битови-RSA-ключове-с-помощта--85580.html [translated]
- Vocativ (Eric Markowitz)
  "How a Hacker Can Break Into Your Laptop With Just an iPhone"
  https://www.vocativ.com/12-2013/hacker-can-break-laptop-just-iphone/?ModPagespeed=noscript
- Geektime (וחדיא(
  "טושפ וופורקימ תרזעב 4096-bit RSA תא חצפל וחילצה מילארשי מירקוח"

http://www.geektime.co.il/rsa-4096-bit-cracked-by-israeli/

- Bit-tech
  Researchers grab encryption keys by listening
  http://www.bit-tech.net/news/bits/2013/12/19/encryption-listen/1
- Threat Pos
  "Researchers Find Way to Extract 4096-Bit RSA Key via Sound"
  http://threatpost.com/researchers-find-way-to-extract-4096-bit-rsa-key-via-sound/103234
- The Stringer (Gerry Georgatos)
  "Internet researchers crack RSA 4096-bit encryption"
  http://thestringer.com.au/internet-researchers-crack-rsa-4096-bit-encryption/
- Steven Gordon's Home (Steven Gordon)
  "Lecture on RSA Acoustic Cryptanalysis by Genkin, Shamir and Tomer"
  http://sandilands.info/sgordon/lecture-on-rsa-acoustic-cryptanalysis

Brief entries in major blogs

- Schneier on Security (Bruce Schneier)
  "Acoustic Cryptanalysis"
  https://www.schneier.com/blog/archives/2013/12/acoustic_crypta.html
- fefe.de entry (major German blog)
  "Bug des Tages: GPG-RSA-Schlüssel per Mikrofon extrahieren. Nein, wirklich! Money"
  http://blog.fefe.de/?ts=ac4f012c
- The Risk Digest Volume 27: Issue 64
  "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis (Genkin/Shamir/Tromer)"
  http://catless.ncl.ac.uk/Risks/27.64.html#subj6
- TG Daily
  "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis"
  http://hackers.tgdaily.com/rt_story/hackers_tech/rsa-key-extraction-via-lowbandwidth-acou/39654e32687670506a6b364d597237414576627 26a513d3d
- O'Reilly Radar
  "Audio Key Extraction"
  http://radar.oreilly.com/2013/12/four-short-links-19-december-2013.html

Social discussion sites

- Slashdot (+fascinating discussion):
  "Scientists Extract RSA Key From GnuPG Using Sound of CPU"
  http://slashdot.org/story/195775
- Reddit
  - Primary:
    "Scientists hack a computer using just the sound of the CPU. Researchers extract 4096-bit RSA decryption keys from laptop computers in under an hour using a mobile phone placed next to the computer."
    1602 comments in 1 day. Reached 4122 points, making it #1 item of the week.
    http://www.reddit.com/r/science/comments/1t8wtl/scientists_hack_a_computer_using_just_the_sound/
  - Weekly top stories:
  - Also:
    http://i.reddit.com/r/programming/comments/1t6k6i/rsa_key_extraction_via_lowbandwidth_acoustic
  -
  -
- YCombinator hacker news (+fascinating discussion):
  https://news.ycombinator.com/item?id=6927905
- Twitter
  https://twitter.com/search?q=acoustic%20rsa%20OR%20gnupg&f=realtime
- tehPARADOX.COM Online Sharing Community
  "Israeli scientists crack RSA-keys via Acoustic Cryptanalysis"
  http://tehparadox.com/forum/f28/israeli-scientists-crack-rsa-keys-6525597
- Bitcointalk
  "[WTF!] Toughest encryption cracked by listening to your CPU with a phone"
  https://bitcointalk.org/index.php?topic=376350.0
- opennet.ru discussion
  http://www.opennet.ru/openforum/vsluhforumID3/93142.html [translated]
- StackExchange
  "Can we ensure the security of a crypto-algorithm and -implementaton against acoustic cryptanalysis?"
  http://crypto.stackexchange.com/questions/12503/can-we-ensure-the-security-of-a-crypto-algorithm-and-implementaton-against-acou
- rotter (מיכרבא מורופ)
  http://rotter.name/kolot/prime/45146.php

Technical announcements/lists

- CVE-2013-4576
  https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4576
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4576

- GnuPG announcement and mailing list discussions:
  http://lists.gnupg.org/pipermail/gnupg-announce/2013q4/000337.html
  http://lists.gnupg.org/pipermail/gnupg-users/2013-December/thread.html#48500
- Ubuntu USN-2059-1: GnuPG vulnerability
  http://www.ubuntu.com/usn/usn-2059-1/
- Debian alert DSA-2821-1 and CVE tracker
  http://lwn.net/Articles/577512
  https://security-tracker.debian.org/tracker/CVE-2013-4576
- RedHat CVE tracker
  https://access.redhat.com/security/cve/CVE-2013-4576
  RedHat Bugzilla:
  Bug 1043327: CVE-2013-4576 gnupg: RSA secret key recovery via acoustic cryptanalysis
  https://bugzilla.redhat.com/show_bug.cgi?id=1043327
- oss-sec mailing list post:
  http://seclists.org/oss-sec/2013/q4/520
- SecurityTracker ID 1029513
  "GnuPG Acoustic Side-Channel Attack Lets Local Users Recover RSA Secret"
  http://www.securitytracker.com/id/1029513
- SecurityFocus Bugtraq ID 64424
  "GnuPG RSA Key Extraction Information Disclosure Vulnerability"
  http://www.securityfocus.com/bid/64424/info
- CISCO Vulnerability Alert IntelliShield ID 32229
  "GnuPG Acoustic Monitoring Key Disclosure Vulnerability"
  http://tools.cisco.com/security/center/viewAlert.x?alertId=32229

Media coverage of "Hands Off" paper

Website: http://www.cs.tau.ac.il/~tromer/handsoff/

Concise summary of major venues

MIT Technology Review - "How to Break Cryptography With Your Bare Hands"

Sky News - "Laptop Security Cracked 'Using Touch Of Hand'"

Heise Online - "Krypto-Schlüssel über das Erdungspotential ausspionierbar"

Ars Technica - "Stealing encryption keys through the power of touch"

30K pageviews as of September 2014

Detailed

- MIT Technology Review (David Talbot)
  "How to Break Cryptography With Your Bare Hands"
  http://www.technologyreview.com/news/530251/how-to-break-cryptography-with-your-bare-hands/
  - Derivate:
    Engadget (Jon Fingas)
    "You can steal data from a computer by touching it"
    http://www.engadget.com/2014/08/23/electrical-potential-data-theft/
- Gizmodo (Kelsey Campbell-Dollaghan)
  "Scientists Hack Cryptography Keys By Simply Touching a Laptop"
  http://gizmodo.com/scientists-hack-cryptography-keys-by-simply-touching-a-1624641299
- Sky News
  "Laptop Security Cracked 'Using Touch Of Hand'"
  http://news.sky.com/story/1322384/laptop-security-cracked-using-touch-of-hand
  - Derivative:
    orange news
    http://web.orange.co.uk/article/news/laptop_security_cracked_using_touch_of_hand
  - Derivate:
    SciTechPress.org
    "Laptop Security Cracked 'Using Touch Of Hand'"
    http://scitechpress.org/post/95365062407/laptop-security-cracked-using-touch-of-hand
- bit-tech (Gareth Halfacree)
  "Security keys leaked via touch, claim researchers"
  http://www.bit-tech.net/news/bits/2014/08/21/handsoff-attack/1
- technology.org
  Extracting secret crypto keys by human touch
  http://www.technology.org/2014/08/13/extracting-secret-crypto-keys-human-touch/
- Computerra (Компьютерра) (Андрей Васильков)
  "Перехват криптографических ключей в одно касание"
  http://www.computerra.ru/105438/physical-side-channel-key-extraction/
- Linux Weekly News
  "Security quotes of the week"
  http://lwn.net/Articles/607986/
- Spektrun.de (Jan Dönges)
  "Computer hacken durch Handauflegen"
  http://www.spektrum.de/news/computer-hacken-durch-handauflegen/1305588
- Heise online
  "Krypto-Schlüssel über das Erdungspotential ausspionierbar"
  http://www.heise.de/newsticker/meldung/Krypto-Schluessel-ueber-das-Erdungspotential-ausspionierbar-2294085.html
- Phys.org
  "Security event to learn about side-channel attacks on PCs"
  http://phys.org/news/2014-08-event-side-channel-pcs.html

- Ars Technica (Peter Bright)
  “Stealing encryption keys through the power of touch”
  http://arstechnica.com/security/2014/08/stealing-encryption-keys-through-the-power-of-touch/
- Tom’s Guide (Jill Scharr)
  “Just Touching a Laptop Can Reveal Secret Data”
  http://www.tomsguide.com/us/touch-electric-decryption,news-19373.html
- (עודד ירהארץ)ון
  “ותוא קרפ סג אוהש תויהל לוכי ?בשחמב דל עגנ והשימ”
  http://www.haaretz.co.il/captain/software/.premium-1.2414998
- Motherboard (Julia Alexander)
  “How to Steal an Encryption Key by Simply Touching a Laptop”
  http://motherboard.vice.com/read/how-to-steal-an-encryption-key-by-simply-touching-a-laptop
- VPN Creative (Dan Virgillito)
  “Researchers Show How to Steal Encryption Keys Through Touch”
  http://vpncreative.net/2014/08/26/researchers-encryption-keys-touch/
- גיק טיים (אבישי בסה)
  “הוא ליטוף סכלש בשחמל קורפל תנמ לע דירצש המ לכש רבתסמ
  http://www.geektime.co.il/mit-research-get-your-hands-off-my-laptop/
- The hacker news (Mohit Kumar)
  http://thehackernews.com/2014/08/stealing-encryption-keys-just-by.html
- Habrahabr - site #22 in Russia
  “ Потрогай, чтобы взломать”
  http://habrahabr.ru/post/234359/ [translated]
- Beartai (Dhanes Kaewmanee)
  “**เหนือ ชั้นเกินไปมั้ย?!**
  ทีมนักศึกษามหาวิทยาลัยเทลอาวีฟเผยว่าสามารถขโมยข้อมูลจากคอมพิวเตอร์ได้ ง่ายๆ เพียงแค่ใช้การสัมผัสเท่านั้น !!”
  http://www.beartai.com/news/30569 [translated]