Optical TEMPEST

Joe Loughry
University of Denver
Denver, Colorado 80208 USA
Email: joe.loughry@cs.du.edu

***Abstract*—Research on optical TEMPEST has moved forward since 2002 when the first pair of papers on the subject emerged independently and from widely separated locations in the world within a week of each other. Since that time, vulnerabilities have evolved along with systems, and several new threat vectors have consequently appeared. Although the supply chain ecosystem of Ethernet has reduced the vulnerability of billions of devices through use of standardised PHY solutions, other recent trends including the Internet of Things (IoT) in both industrial settings and the general population, High Frequency Trading (HFT) in the financial sector, the European General Data Protection Regulation (GDPR), and inexpensive drones have made it relevant again for consideration in the design of new products for privacy. One of the general principles of security is that vulnerabilities, once fixed, sometimes do not stay that way.**

I. Introduction

Since the publication sixteen years ago of the first two papers on optical TEMPEST, open source information on security of compromising emanations—and side channels in general—has exploded. Before the late 1990s, only a handful of papers had been published in the open literature on the subject of TEMPEST[1] and the topic was mostly relegated to the folklore of infosec; the only two scientific studies of unintentional compromising emanations remained van Eck [2] and Smulders [3] although Wright's book around the same time [4] described anecdotal reports dating back to the first world war. But following Kocher's seminal 1996 paper on side channel attacks [5] and Kuhn & Anderson [6] having shown—essentially by adding forward error correction to EMC—that covert channels were not limited by the system boundary, two papers appeared within a week of each other on complementary aspects of optical emanations [7], [8]. Since then, the two papers, between them, have been cited more than 300 times.

A. Organisation

The first part of this paper is a critique of mistakes that were made by one of the first investigators of optical TEMPEST, in the methodology, model building, writing, and follow-up of the earliest research. This is followed by a survey of ways that later authors have repaired the damage. A cautionary tale of forgetting lessons learnt in security is rounded out by a description of some aspects of the the design of a new information security product with these principles in mind.

II. The story I never told you before

Optical TEMPEST was discovered working at a bank. In the raised-floor computer room on the sixth level of a glass high-rise building in downtown Seattle, surrounded by other glass high-rises with their own computer rooms visible at night by the reddish glow of Light Emitting Diode (LED) indicators, I was working very late. Dial-up modems had not yet gone completely extinct, $10\,\mathrm{Mbit\,s^{-1}}$ Ethernet was increasingly common on PCs, and leased lines ran everywhere from the computer room to branch offices, thousands of them. This was the environment where optical TEMPEST was discovered in 1992. I told my postgraduate professor at Seattle U. about it. Cautious experiments were performed. A literature survey was quietly done to see if anyone had ever noticed it before, and the National Computer Security Center (NCSC) was asked if they knew of it. All inquiries ran into a classified information roadblock; just about the only thing that was known for sure at the time, in the open literature, was that nearly everything about TEMPEST was classified (but the name was probably not an acronym).

A. Missed opportunities

Around this time, I made a serious mistake. Unbeknown to me, Markus Kuhn, a postgraduate student at Cambridge, was working along similar lines. I had thought of optical emanations from video display screens but dismissed the idea as physically impossible, without ever testing it. I was wrong. I thought the decay time of Cathode Ray Tube (CRT) phosphors was too slow to carry information about the video signal[2] in the diffuse light available to non-line-of-sight interception, and consequently, I never looked for it.

Markus Kuhn found and successfully exploited a tiny ripple near the peak of the response curve of CRT phosphors. The gross shape of the curve belies the fact that that tiny ripple is detectable in the time domain optical signal, if your detector is fast enough.

[1]TEMPEST, here, is the U.S. National Security Agency (NSA) code name for 'the problem of compromising radiation'—radio frequency (RF) *or* acoustic, according to the original reference, which was only declassified in 2007—including both exploitation and control [1]. Beyond the 1972 definition of TEMPEST, military and academic researchers have since expanded the spectrum of interest to include DC, optical, thermal, magnetic, and acceleration side channels.

[2]Speaking of video signals, laser printers intensity-modulate an infrared laser with a video signal, and some plastics are transparent to infrared light. It might be worthwhile to measure laser printers for information-bearing optical emanations outside visible wavelengths, as Kubiak has done for RF [9]–[12], Ulaş *et al.* have done for conducted powerline emanations [13], and Enev *et al.* have done for conducted powerline emanations from video displays [14].

978-1-4673-9698-1/18/$31.00

Kuhn's detector—a photomultiplier tube—was better than mine; the gain–bandwidth product is superior to that of the large-area photodiode/transimpedance amplifier combination I used, but we were looking for different things: Kuhn for diffuse emanations from an entire screen, and I for line-of-sight photons from a particular LED on an isolated piece of equipment (although we did eventually figure out how to separate multiple superimposed signals from diffuse optical emanations collected by non-line-of-sight means). The difference is that Markus Kuhn actually looked, and he found an effect that I missed.

B. Delay of first publication

Why didn't we publish in 1994? Part of the reason was perfectionism; I wanted to be able to explain the phenomenon and make predictions, not only describe it. In addition, by that time I had left the bank and was working for a defence contractor on a classified project. I had a security clearance now, and a greatly expanded awareness of counterintelligence sources and methods.

And so, following procedures, we submitted the paper to NSA for approval to publish. It took a year and a half to approve.[3] Eventually, NSA wrote back and said, 'approved for public release'. I wonder what they spent all that time doing.

C. Roads not taken

Universal Serial Bus (USB) devices hadn't happened yet, but today they're ubiquitous. Later and informal investigation of some light-up USB cables—a fad that didn't last—turned up evidence of Class II optical emanations related to data passing through the USB cable, but evidence for Class III optical emanations remains inconclusive.

Considered narrowly outside the scope of optical TEMPEST, for the purpose of this paper, are line-of-sight attacks that essentially reduce to direct or indirect imaging of the display [15]–[20]. This is somewhat unfair, as the original attack by Loughry & Umphress required, for the most part, line-of-sight access—except, as previously mentioned, in §8.2—but in the time domain, not space. Optical TEMPEST is a time domain effect. Other remote attacks employing optical means, such as visual or interferometric measurement of keyboard or printer acoustic emanations [21]–[24], or a highly novel reverse covert channel using a document scanner [25], are outside the scope of this paper. Screen burn-in, for example, is data remanence, not optical TEMPEST [26]. Finally, induced optical emanations [27]–[34] and [8, Appendix A] are properly considered out-of-band covert channels [35]–[37], despite being compromising optical emanations in the time domain, because they are purposely induced by a nefarious software or hardware agent, or by activity controllable by a third party, introduced into the target system by the attacker.

[3] Actually, it didn't quite happen that way. Our paper was approved for publication very quickly, in only a few weeks; we submitted it to the 10th USENIX Security Symposium where it was immediately accepted. A few days later, NSA called us back, and in a panic, insisted that we withdraw the paper from the conference. I had to apologise to the programme chair; it was awfully embarrassing, and the delay in publishing was almost two years.

III. MAC and PHY

Of the potential optical signal sources available in a standard office computer (power light, hard disk activity indicator, keyboard LEDs, network interface link indicators, charging indicators on laptops, optical disc read head and activity indicators, optical mouse, and, of course, the screen), we looked hard, at the time, at the other two large populations of blinking LEDs in the world: disk activity lights[4] and Network Interface Cards (NICs). Neither source proved fruitful; we were unable to find any evidence of Class III optical emanations from storage devices or link activity indicators on Ethernet cards. The one exception—and it was a bad one—was WAN interfaces on the back panel of enterprise routers, devices which live in racks that sometimes back up to windows; see [8, §4.3.1]. Aside from those, the complete absence of compromising optical emanations from Ethernet link activity LEDs is believed to be a consequence of the fact that the Ethernet protocol is well divided into two layers: MAC and PHY.

In the Ethernet protocol, the Media Access Control layer (MAC) marshals bits into frames and hands them off to the Physical layer (PHY), which deals exclusively with voltages and waveforms and wires, or radio, or fibre optics. The MAC talks to the PHY using a protocol called Media Independent Interface (MII)—GMII for gigabit Ethernet—over a pair of 4-bit-wide parallel channels (send and receive) clocked at 25 MHz [39].

In the case of twisted pair wire, only a few suppliers make PHY chips and generally they do it right, providing dedicated pins on the PHY chip for connecting LEDs for status indication and internally stretching pulses to the LEDs to make high-speed activity visible to human eyes. In most PHYs, the minimum duration of pulse stretching is programmable, and in some PHYs it can even be turned off [40, Table 39]. The contrast here with the situation we found regarding relatively low-speed serial interfaces is stark; there, the temptation was seemingly overwhelming for circuit designers to drive LEDs directly from generously high voltage and high current serial communication signals—arguably providing reliable indication of signal quality and perhaps of marginal signal levels at very low cost. Garden variety LEDs are plenty fast enough to reproduce amplitude-modulated signals well into the nanosecond range without any special driver circuits required.

A. High Frequency Trading (HFT)

Sometimes, security problems that you thought you had fixed already, come back to bite you.

In the early years of this century, a new style of automatic financial trading appeared, facilitated by the convergence of gigabit per second networks, computers with 64-bit address spaces, and deregulation [41]. Their trading advantage came from the finite speed of light; by physically locating their trading algorithms as close as possible to the exchange,

[4] Guri *et al.* finally made it work in 2017 by hovering a drone in the air outside the building [29]; unlike data exfiltration using keyboard LEDs [38, Chapter 90], the hard disk LED channel is covert, not clandestine.

they could eke out a response time advantage measured in milliseconds. With the margin between success and failure so narrow, and backers willing to spend money on bespoke hardware in return for larger profits, HFT traders pursued ever-smaller improvements in latency and responsiveness to changes in market conditions and requirements, culminating in Field Programmable Gate Array (FPGA) or Application Specific Integrated Circuit (ASIC) implementation of a minimal gigabit Ethernet MAC, as fast as physics would allow and additionally capable of three things that conventional Ethernet hardware could not do:

1) ultra-low latency (μs),
2) ability to read data transmitted near the beginning of an Ethernet packet before the entire packet had been received, and
3) ability to cancel a speculative trade—if needed—after the Ethernet packet had begun transmitting, but before it had finished.[5]

Their systems did not have to be universally interoperable, only compatible enough to talk to the exchange, and that only for the few months the hardware was typically used before being replaced by something even faster [42].

The risk in this kind of cowboy engineering is that of Chesterton's fence; non-obvious safeguards may be dropped, leaving the implementation vulnerable to exploitation. While not described there (*ibid.*) it is not unreasonable to speculate that HFT engineers—there were many HFT groups besides the one in Korea—may have looked critically at the PHY in their search for another few microseconds to harvest. And developmental hardware, especially, sometimes needs monitoring or diagnostic LEDs for debugging. It is purely speculation, but there might be a 'window' of opportunity for rival HFT firms with a telescope and very high speed photodetector to exploit any incautiously situated LED indicators connected directly to high-speed registers.

IV. Design of a new product with optical TEMPEST principles in mind

Optical TEMPEST began in a bank, took a holiday in the Intelligence Community (IC), and now has circled back to fintech. The remaining frontier is privacy.

Under the General Data Protection Regulation (GDPR) in Europe, and to a lesser extent the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States, the privacy of individuals and their personal information is protected by law. In the U.S. at least, this makes health care providers more risk-sensitive than they are cost-sensitive. One particular problem—amongst many—that needs to be solved in the U.S. arises from a quirk of the U.S. Food and Drug Administration (FDA), the main regulator of medical diagnostic and therapeutic devices. The cost of gaining FDA approval for use of a medical device is high, necessitating sometimes years of clinical trials, and extensive design and development documentation.[6] As a result, perhaps millions of vulnerable medical devices—only a few years old—exist that never have got the required security patches for their embedded computers' operating system (OS) as recommended by the OS manufacturer. The reason for the shortfall in software maintenance is the excessive cost of FDA recertification in the event any diagnostic- or therapeutic-relevant changes are made to the configuration of a medical device [43]. In fact, the analogous situation happens in classified military and intelligence community networks as well. Commercial aviation experiences the problem less than either classified networks or healthcare for two reasons: firstly, being mobile, aviation control systems tend to be more isolated and special-purpose embedded computers than the Commercial Off-the-Shelf (COTS) hardware favoured by medical device and intelligence community developers; and secondly, DO-178 [44].

In this section I describe some of the design considerations for new development informed by experience with optical TEMPEST vulnerabilities and countermeasures. The notional infosec product described is intended to isolate vulnerable medical devices with the aim of protecting individuals' privacy by eliminating one mode of entry of hackers to the hospital's internal computer networks.

In a parallel universe to the HFT hardware designers in the previous section, we use similar techniques to different ends; the MAC here is a state machine implemented in hardware, not for low-latency but for high-security; the PHY returns, for security reasons—in the interest of complete transparency of implementation—to its roots in the magnetics of IEEE 802.3i, where the number of turns in a toroidal transformer can be counted. The design and development methodology is that of the intelligence community, but the anticipated buyer does not reside in the U.S., and is not expected particularly to trust the U.S. government. The only reasonable defence against this level of mistrust is believed to be complete openness and transparency of design, development, and implementation.

A. Simplicity and transparency of implementation

Part of the design is essentially an optoisolator for the purpose of domain separation between the 'private' and 'public' sides of the privacy problem. Integrated circuit optoisolators can be bought but they are designed for galvanic isolation, not infosec.

The receiver side of the circuit is shown in Figure 1. The photodiode operates in reverse bias (photoconductive) mode for two reasons: speed, and simplicity of implementation. The same photodiode operated in photovoltaic mode would be more sensitive to very low level signals and have a lower dark current, but would require a transimpedance amplifier for current-to-voltage conversion, which would make the design more complicated and thereby more difficult to evaluate for

[5]The trick was accomplished by purposely corrupting the checksum at the end of a packet, relying upon correct behaviour of the exchange's Ethernet interface to discard the packet instead of processing it.

[6]The situation is little different in either commercial aviation or military and intelligence community systems for classified information: process maturity, formal or semi-formal design, and exhaustive testing before certification and approval for use.

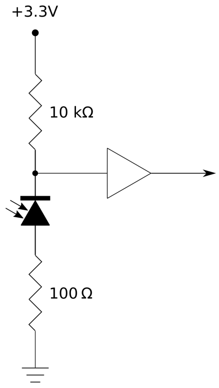

Figure 1. The photodiode circuit is purposely made as simple as possible for transparency of implementation; the $10\,\mathrm{k}\Omega$ pull-up resistor for reliability together with a $100\,\Omega$ series resistor to protect a bidirectional driver (here represented by a generic buffer) from being shorted to ground in case it were accidentally set to output a HIGH logic level at the same time the photodiode is illuminated.

security. The rest of the design is equally unconventional (Figure 2). Rather than using available 'IP' blocks (Intellectual Property—pre-designed software modules delivering standard functionality such as ARM cores or Ethernet MAC), we prefer a clean-room design approach built from IEEE 802.3 standards, avoiding closed-source IP. The result, we believe, in combination with open tests, will be considered trustworthy by everyone in the world.

B. *Design discussion*

Simplicity of implementation is paramount. There are no amplifiers, no MAC or PHY chips, no process nodes that cannot be de-capped and have a representative sample to be examined under a microscope. The development tool chain must be open source and international.

It must be acknowledged that optical TEMPEST, ironically, is a vulnerability that can be exacerbated by extreme reliance on simplicity of implementation. But experience with optical TEMPEST and side channels has inspired so many other researchers to find and exploit diverse vulnerabilities, that the only remaining avenue of approach is to strike as many components as possible from the system, in the belief that a component that is not there cannot fail, has no vulnerabilities, and lasts forever.

V. CONCLUSION

Since the publication in 2002 of the first peer-reviewed research on compromising optical emanations, other researchers have carried it further. But technological progress has shifted the boundaries of what was possible, necessitating re-visit of the same vulnerabilities from time to time. This is a general principle of security; vulnerabilities, once fixed, sometimes do not stay fixed.

ACKNOWLEDGEMENTS

Thanks to many anonymous and pseudonymous commenters on Hacker News ⟨news.ycombinator.com⟩ for helping develop the ideas in this paper.

REFERENCES

[1] National Security Agency, "TEMPEST: A signal problem," *Cryptologic Spectrum*, 1972.

[2] W. van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computer Security*, vol. 4, no. 4, pp. 269–286, December 1985.

[3] P. Smulders, "The threat of information theft by reception of electromagnetic radiation from RS-232 cables," *Computer Security*, vol. 9, no. 1, pp. 53–58, February 1990.

[4] P. Wright, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. New York: Viking Press, 1987.

[5] P. Kocher, "Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems," in *Advances in Cryptology—Crypto 96*. Springer, 1996, pp. 104–113, lNCS 1109.

[6] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations," in *Second International Workshop on Information Hiding (IH'98)*, Portland, Oregon, USA, 15–17 April 1998, pp. 124–142.

[7] M. G. Kuhn, "Optical time-domain eavesdropping risks of CRT displays," in *Proceedings of the 2002 IEEE Symposium on Security and Privacy*. Berkeley, California: IEEE Computer Society, 12–15 May 2002, pp. 3–18.

[8] J. Loughry and D. A. Umphress, "Information leakage from optical emanations," *ACM Transactions on Information and System Security*, vol. 5, no. 3, pp. 262–289, 2002.

[9] I. Kubiak, "The unwanted emission signals in the context of the reconstruct possibility of data graphics," *IEE Proceedings—Vision, Image and Signal Processing*, vol. 6, no. 11, October 2014.

[10] ——, "LED printers and safe fonts as an effective protection against the formation of unwanted emission," Military Communication Institute, 22A Warszawska St., 05-130 Zegrze, Poland, Tech. Rep., 2017.

[11] ——, "The structure of useful signal and the efficacy of sensitive emission of laser printers," Military Communication Institute, Zegrze, Poland, Tech. Rep., 2017.

[12] ——, "LED printers and valuable data," Military Communication Institute, Warsaw, Poland, Tech. Rep., June 2017.

[13] C. Ulaş, U. Aşık, and C. Karadeniz, "Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines," *Computers & Security*, vol. 58, pp. 250–267, May 2016.

[14] M. Enev, S. Gupta, T. Kohno, and S. N. Patel, "Televisions, video privacy, and powerline electromagnetic interference," in *CCS'11*, Chicago, Illinois, USA, 17–21 October 2011, pp. 537–550.

[15] M. Backes, M. Duermuth, and D. Unruh, "Compromising reflections—or—how to read LCD monitors around the corner," in *Proceedings of 29th IEEE Symposium on Security and Privacy*, May 2008.

[16] D. Balzarotti, M. Cova, and G. Vigna, "ClearShot: Eavesdropping on keyboard input from video," in *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, Oakland, California, May 18–21 2008.

[17] M. Backes, T. Chen, M. Duermuth, H. P. Lensch, and M. Welk, "Tempest in a teapot: Compromising reflections revisited," in *Proceedings of the 2009 IEEE Symposium on Security and Privacy*, Oakland, California, May 17–20 2009.

[18] R. Raguram, A. M. White, D. Goswami, F. Monrose, and J.-M. Frahm, "iSpy: Automatic reconstruction of typed input from compromising reflections," in *CCS'11*, Chicago, Illinois, USA, 17–21 October 2011.

[19] Y. Xu, J. Heinly, A. M. White, F. Monrose, and J.-M. Frahm, "Seeing double: Reconstructing obscured typed input from repeated compromising reflections," in *CCS'13*, Berlin, Germany, 4–8 November 2013, pp. 1063–1074.

[20] R. Jenkins and C. Kerr, "Identifiable images of bystanders extracted from corneal reflections," *PLoS One*, vol. 8, no. 12, p. e83325, December 2013.

[21] D. Asonov and R. Agrawal, "Keyboard acoustic emanations," in *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, Oakland, California, May 9–12, 2004, pp. 3–11.

[22] L. Zhuang, F. Zhou, and J. Tygar, "Keyboard acoustic emanations revisited," in *Proceedings of the 12th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, November 7–11, 2005, pp. 373–382.

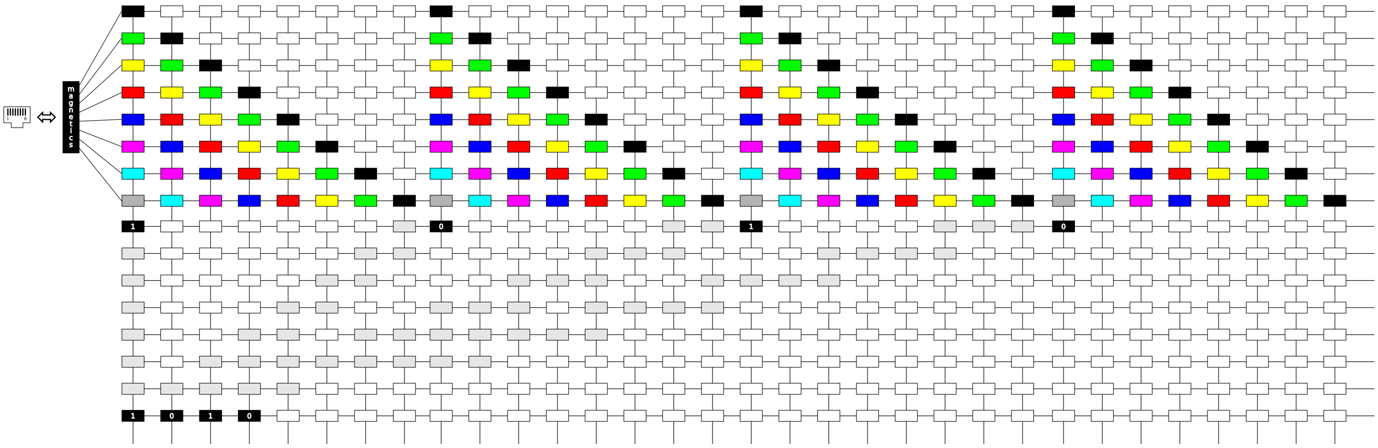

Figure 2. Deep pipeline implementation of an Ethernet MAC; only a small portion of the pipeline is shown. The MII is clocked asynchronously by the state machine as bits are de-marshalled efficiently into one slot each. Profligate expenditure of resources trades off for very favourable parallelism and equally transparent computation of sizes, offsets, padding, checksum, and digital signature application and validation.

[23] Y. Berger, A. Wool, and A. Yeredor, "Dictionary attacks using keyboard acoustic emanations," in *CCS'06*, Alexandria, Virginia, October 30–November 3, 2006, pp. 245–254.

[24] M. Backes, M. Dürmuth, S. Gerling, M. Pinkal, and C. Sporleder, "Acoustic side-channel attacks on printers," in *Proceedings of the 19th USENIX Security Symposium*, Washington, D.C., August 11–13, 2010.

[25] B. Nassi, A. Shamir, and Y. Elovici, "Oops!…I think I scanned a malware," arXiv:1703.07751v1 [cs.CR], 22nd March 2017.

[26] *Protocol for the Disposition of MDH Computer Equipment, Associated Magnetic and Other Data Storage Media, and Data Remanence*, Maryland Department of Health, December 1998.

[27] V. Sepetnitsky, M. Guri, and Y. Elovici, "Exfiltration of information from air-gapped machines using monitor's led indicator," in *2014 IEEE Joint Intelligence and Security Informatics Conference*, 2014, pp. 264–7.

[28] M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "VisiSploit: An optical covert-channel to leak data through an air-gap," https://arxiv.org/abs/1607.03946, 13 July 2016.

[29] M. Guri, B. Zadov, E. Arias, and Y. Elovici, "LED-it-GO: Leaking (a lot of) data from air-gapped computers via the (small) hard drive LED," http://cyber.bgu.ac.il/advanced-cyber/system/files/LED-it-GO_0.pdf, 2017.

[30] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xLED: Covert data exfiltration from air-gapped networks via router LEDs," arXiv preprint 1706.01140 [cs.CR], 4th June 2017.

[31] A. C. Lopes and D. F. Aranha, "Platform-agnostic low-intrusion optical data exfiltration," in *3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)*, Porto, Portugal, 19–21 February 2017.

[32] M. Guri, D. Bykhovsky, and Y. Elovici, "aIR-Jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (IR)," arXiv preprint arXiv:1709.05742 [cs.CR], 18th September 2017.

[33] Z. Zhou, W. Zhang, Z. Yang, and N. Yu, "Exfiltration of data from air-gapped networks via unmodulated LED status indicators," University of Science and Technology of China, Key Laboratory of Electromagnetic Space Information, of Chinese Academy of Sciences, arXiv preprint 1711.03235v1, 10th November 2017.

[34] Z. Zhou, W. Zhang, and N. Yu, "IREXF: Data exfiltration from air-gapped networks by infrared remote control signals," University of Science and Technology of China, arXiv preprint 1801.03218v1 [cs.CR], 10th January 2018.

[35] B. W. Lampson, "A note on the confinement problem," *Comm. ACM*, vol. 16, no. 10, pp. 613–615, October 1973.

[36] M. Hanspach and J. Keller, "On the implications, the identification and the mitigation of covert physical channels," in *9th Future Security Conference*, Berlin, 16–18 September 2014, pp. 563–570.

[37] B. Carrara and C. Adams, "Out-of-band covert channels—a survey," *ACM Computing Surveys*, vol. 49, no. 2, November 2016.

[38] N. Stephenson, *Cryptonomicon*. Avon Books, 1999.

[39] *TLK100 Industrial Temp, Single Port 10/100 Mb/s Ethernet Physical Layer Transceiver*, Texas Instruments, August 2009.

[40] *Intel® 82579 Gigabit Ethernet PHY, Datasheet v2.1*, Intel Corporation, 2011.

[41] M. Lewis, *Flash Boys*. New York: W. W. Norton & Company, 2014.

[42] M. Hurd, "The accidental HFT firm," In the *Meanderful* blog ⟨https://meanderful.blogspot.com/2018/01/the-accidental-hft-firm.html?m=1⟩, 24th January 2018.

[43] D. Talbot, "Computer viruses are "rampant" on medical devices in hospitals," *Technology Review*, 17th October 2012.

[44] RTCA, Incorporated, *DO-178C Software Considerations in Airborne Systems and Equipment Certification*, December 2011.