Cyber-Attacks on the Network.

(March 10 2022)

L Velec, IEEE, Faculty of Arts and Science.

University of Wisconsin Rivers Falls.

Department of Art Science,

Engineering Department of University of Wisconsin Rivers Falls.

Professor: Jacob Hendricks

Author: Lissette I, Velec. (Lissette.velec@my.uwrf.edu).

ABSTRACT: **—**In the recent decades, cyber threats have increased. In the era of covid and wars, many companies are not highly prepared to combat such attacks.

This make Cyber Threat intelligence with Figures (CIF) need to optimize resources and focus on this great conflict that affect us all. Globally we find ourselves in an environment where cybersecurity attacks have increased by more than 20 percent. This makes us have a risk of cyber threats, cybercrimes that take risks from our data. Internet architecture and infrastructure of Things (IoT) it has had many technological advances, providing technologically advanced solutions that have allowed different innovations and implementations in different systems. Besides, he manages many advances but he is also a threat.

INTRODUCTION:

I

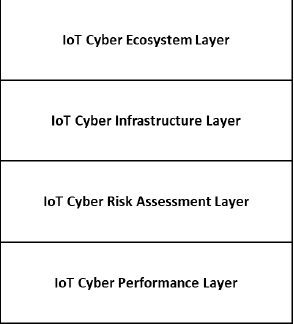
N IoT Cyber-security-attacks an IoT system consists of several sections: The first would be the perception applications, the second network, and finally the application. These systems that are composed in layers have threats in the network. These layers are used to write the architecture of the IoT system as it collects all the information on devices. The IoT network layer transmits information privately wirelessly or by wires. Consequently the application is providing services for people who want to customize them. **[[1]](#footnote-1)‘**Things’’ through internet embedded with an electronic chip, sensors, and other forms of hardware. Each device is uniquely identified globally by Radio Frequency Identifier (RFID) tags.

There is a lack of monitoring and wireless devices that would be mobiles and the contradiction and incompatibility that the network systems exist. There are currently different types of attacks on IoT networks. Based on the declines, that exists in cybersecurity and shortcomings. There is a lack of monitoring and wireless devices that would be mobiles and the contradiction and incompatibility that the network systems exist. There are also individual cyber warriors who with their knowledge can infiltrate or copy filtering software systems, and can infiltrate entities or organizations. Many of these programs that are manipulated by anonymous netizen groups that do not belong to any affiliation can have page flows from even an entire city or country. The problems that challenge the enormous security of applications, devices, and users, could be the context of any of the internet is somewhat complicated. This is due to being something to reach and popularity of the cloud this serves as intermediate management of business systems. on the cloud. Segmented security solutions Examples, firewall applications at the perimeter of a variable network do not actually protect data is now on the move across devices, clouds, networks. We also add the data centers that exist that they are the ones that house our confidential information of the companies they also address security challenges that generate the visualization in the cloud that rethinks the security states. [[2]](#footnote-2) “Currently, malicious attacks are more easily abrupt due to the growing number of IoT networks”. The malware attacks are usually planned to infect the privacy of IoT nodes, computer systems, and smartphones over the internet” How to prevent attacks? They are different types of attacks. There are these advances that have not yet had a real impact on user protection, if block chain technology is used to cover these IoT problems; they intend to close this gap. It sounds contradictory but based on the decentralization of transactions. These DoS deny attacks are an attacker attacking or attempts to prevent the legitimacy of users accessing information or services. These DoS attacks happen when an attacker floods a network with information when searching for a URL. But in reality they only have one amount at a time since an attacker overloads the server with applications and these requests cannot be processed quickly. Then the denial of service appears as the site cannot be accessed. Internet networks are subject to countless attacks, since they have a variety of direct and indirect attacks. It is actually a concern as it represents a great threat to multiple services. The development of an exchange system has become global. There are several contexts in the social, economic and cultural aspects, since these are the basis for the regulatory systems to give in to the unification that favors trade. The economic, social and cultural contexts that underlie the regulation systems give in to the unification that favors international trade.

1. Prevention of Cyber – Attacks.

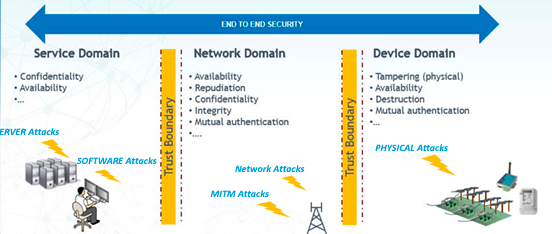
In reality there is no consensus that is global in relation to illicit conduct. Many people think that everything can be solved using technology on many occasions if it is true, but this is not completely true since there are many failures. The data traffic in the networks of users and passwords could be obtained illicitly to commit computer fraud, they can also be used to distort and alter machinery and there are also specialized teams in capturing and intercepting information. There is no type of solution that can actually protect a company or individual users from cyber-attacks, even large corporations have suffered from these vulnerabilities over the years. But we must ask ourselves why this happens? The question is something unknown in security systems. Of course risks can be reduced and these vulnerabilities are considered difficult to attack a company or different entities. However, also an easy and effective method to know if you are part of a bot is to see if the inputs connections of your computer are open and check if those loop holes are open. You could only windows + r to open the run window, in that console type cmd and hit enter, you will get the command prompt console in which you will place netstat -ano, It will show you a list of established external connections and show the port it uses, left-click on the taskbar and go to task manager, also then go to the task manager details tab and compare and stop all the tasks you are not doing or disconnect the strange connections. This is not a guarantee but it helps to stop or prevent cyber-attacks. However **[[3]](#footnote-3)“**A simple example of Network Denial is characterized by an attacker that logs into a router at the border of an organization’s network and stops it from transferring data. Example of the results in the blocking of all traffic on a network and isolates the target organization, temporarily preventing it from transmitting any information in or out using computer networks**”**.

There are many updates that solve bugs, including cybersecurity ones, you have to find an antivirus or malware that protects computers in a certain way so that our files are protected from any type of malicious attack. Passwords must also be set or generated. There are effective tools for generating passwords. Every time you want to enter the networks, it is recommended to write the address directly. This is a defense method that identifies the page that will be visited. Also the downloads made could be threats and we must know the nature of where it comes from and if it is effective.



1. Example of an Abstract Model Cyber Risk model.

Firewalls are a system that protects and prevents networks. This control system between the networks. The firewall can classify depending on the type of use. This traffic going in and out of the computer. Here we can observe the entities and relationships between their related attributes. These relationships are between many IoT administrations in reality they do not have the experience to develop different IoT situations. In reality, the network market will never stop. People who develop different types of technologies are always providing their IoT team with their new innovations for the security of different transfers. Today there are new developments such as 5G which actually has no server and foggy IoT systems. Also, AI will also show protection and potential for prevention in case of detection and recovery in real-time and take action for IoT systems with improvements than other platforms that are already traditional. IoT platforms must offer comprehensive solutions that unify wired devices and applications from multiple vendors.



2. Example Figure IoT Threats.

1. General Category of Cyber Security Threats.

Threats are acts that are made by people who want to extort or harm. These groups or individuals who have experience in data theft want to disrupt information systems. These cyber threats include a number of malwares and denial of services, there is also no doubt that there are injection attacks that we have described above. These cyber threats also have no doubt that they originate from a variety of sources and internal connections could be terrorists and hackers. There are also employees, contractors, groups or an independent individual who abuse to do malicious acts.[[4]](#footnote-4) “Malware refers to software programs designed to damage or perform other unwanted actions on a computer system”.

lll Vulnerabilities.

Deep learning is something automatically that a model can perform tasks in different ways directly, such as images, text, sounds, among others. This is implemented through the architecture of neural networks, it would be more like network layers, and if there are more layers, the network will be more extensive. Also the demand for service of various applications between the cloud has grown immensely, as there is a growth of these vulnerabilities. There are organizations that direct how to encourage the proper use of cloud services. Cloud Security Alliance is a type of non-profit organization that promotes best practices on how to use the cloud. [[5]](#footnote-5)**“**This paper discusses the vulnerabilities of the API in cloud management software. Based on these vulnerabilities, this paper will demonstrate how eavesdropping on cloud API authentication services

and API exhaustion attack can be initiated. To address the threat due to the vulnerabilities of the API, we need to detect on-going attack which exploits the vulnerabilities**”**

Organizations that are vigilant in surveillance have fallen victim to vulnerabilities in the cloud, network, etc. There are countless services but without any I exist since it does not really guarantee not to have an attack. There are companies with figures that encrypt their authentications to provide better security. Let's say that there is software that is monitoring the packets that are in traffic movements between users, which could be public or independent institutions, this service could easily steal the names of users and much more information. These hacking attacks redirect network traffic to your computer instead of being the destination server. Example if a student opens a remote session let's say with a server the computer you want to attack act as a ghost an invisible driver and all kinds of information between the remote service and the innocent user is captive. We explain that in this way the hacker gathers the passwords etc without the server or user being aware of this situation. There is also a category of services that claim to be good but are insecure, such as NFS or NIS, these are developed in LAN Local area network but have been extended to be used in Wide Area Network WAN. NFS Network file system has no authenticity that can prevent a hacker.

1. Evaluation of Vulnerabilities.

We must think about how to know how to protect ourselves to fight the enemy. We have to protect and carry out currently available technology procedures that, in reality, sometimes do not provide or guarantee that the system is secure. It should also be noted that routers can to a large extent secure the gateways that are in the networks, firewalls also in a certain way ensure some type of glitch in the networks. There is a wide range of encrypted streams. Actually, the system implementing the routers configures them correctly and the firewalls can prevent us from an attack and warn us of harmful activity. To achieve this, we have to know how to configure it. There are also companies that are responsible for constant surveillance on the networks. There are dynamic resources, but it is somewhat complex since many do not have the necessary experience for these changes. An example must be protected if the applications of servers, networks, etc., which we wish to deliberate, stay updated. It is something extensively complex since there are virus worms in the software that are constant if we are not aware of what happens technologically. We must continue to review vulnerabilities and prevent evaluating nearby and future problems. These simple practices will make security systems deliver results and indicate the confidence of our networks. Example if you would have to make a vulnerability in your personal home, you would check it to see if the windows are closed or the door if there is a gas leak. Likewise, it would verify if you had vulnerability in the networks, assuring you of your identity as that of your family.

How to secure our net against Cyber-Attacks.

Secure topologies The LAN base is a network architecture, it provides physical and logical and that is between distance with transmission medium nodes. In reality, every case is different since there are several options. to implement it. The physical topology that pertains to the number of IEEE electrical and electronic engineers these topologies are for LAN connections. The ring. Connect the knots in two connections. They are known as token rings. There are no Ethernet connections using this ring topology. In reality, these rings are not used as they would be commonly used, there are configurations for example in libraries or universities. The bus topology, nodes connected in a cable backbone, does not require as much cabling and is effective. But the backbone cable makes it somewhat of a fault if you have to go offline it's actually somewhat controversial because they are used in end-to-end LANs using coaxial cables. the star topology the nodes are connected through where the communication that the hub would be passes. there is a single point of failure in the central hardware connecting these nodes.

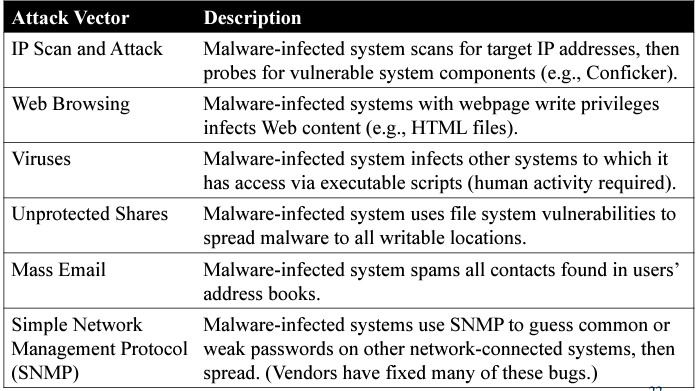


Figure Types Malwares Damage the Red.

How much are

TABLE I

When preparing your graphics IEEE suggests that you use of one of the following Open Type fonts: Times New Roman, Helvetica, Arial, Cambria, and Symbol. If you are supplying EPS, PS, or PDF files all fonts must be embedded. Some fonts may only be native to your operating system; without the fonts embedded, parts of the graphic may be distorted or missing.

A safe option when finalizing your figures is to strip out the fonts before you save the files, creating “outline” type. This converts fonts to artwork what will appear uniformly on any screen.

Figure axis labels are often a source of confusion. Use words rather than symbols. As an example, write the quantity “Magnetization,” or “Magnetization M,” not just “M.” Put units in parentheses. Do not label axes only with units. As in Fig. 1, for example, write “Magnetization (A/m)” or “Magnetization (Am−1),” not just “A/m.” Do not label axes with a ratio of quantities and units. For example, write “Temperature (K),” not “Temperature/K.”

Multipliers can be especially confusing. Write “Magnetization (kA/m)” or “Magnetization (103 A/m).” Do not write “Magnetization (A/m) × 1000” because the reader would not know whether the top axis label in Fig. 1 meant 16000 A/m or 0.016 A/m. Figure labels should be legible, approximately 8 to 10 point type.

1. Subfigure Labels in Multipart Figures and Tables

Multipart figures should be combined and labeled before final submission. Labels should appear centered below each subfigure in 8 point Times New Roman font in the format of (a) (b) (c).

1. FILE NAMING

Figures (line artwork or photographs) should be named starting with the first 5 letters of the author’s last name. The next characters in the filename should be the number that represents the sequential location of this image in your article. For example, in author “Anderson’s” paper, the first three figures would be named ander1.tif, ander2.tif, and ander3.ps.

Tables should contain only the body of the table (not the caption) and should be named similarly to figures, except that ‘.t’ is inserted in-between the author’s name and the table number. For example, author Anderson’s first three tables would be named ander.t1.tif, ander.t2.ps, ander.t3.eps.

Author photographs should be named using the first five characters of the pictured author’s last name. For example, four author photographs for a paper may be named: oppen.ps, moshc.tif, chen.eps, and duran.pdf.

If two authors or more have the same last name, their first initial(s) can be substituted for the fifth, fourth, third... letters of their surname until the degree where there is differentiation. For example, two authors Michael and Monica Oppenheimer’s photos would be named oppmi.tif, and oppmo.eps.

When referencing your figures and tables within your paper, use the abbreviation “Fig.” even at the beginning of a sentence. Do not abbreviate “Table.” Tables should be numbered with Roman Numerals.

The IEEE Graphics Analyzer enables authors to pre-screen their graphics for compliance with IEEE Access standards before submission. The online tool, located at <http://graphicsqc.ieee.org/>, allows authors to upload their graphics in order to check that each file is the correct file format, resolution, size and colorspace; that no fonts are missing or corrupt; that figures are not compiled in layers or have transparency, and that they are named according to the IEEE Access naming convention. At the end of this automated process, authors are provided with a detailed report on each graphic within the web applet, as well as by email.

For more information on using the Graphics Analyzer   
or any other graphics related topic, contact the IEEE Graphics Help Desk by e-mail at [graphics@ieee.org](mailto:graphics@ieee.org).

1. SUBMITTING YOUR GRAPHICS

Because IEEE will do the final formatting of your paper,

you do not need to position figures and tables at the top and bottom of each column. In fact, all figures, figure captions, and tables can be placed at the end of your paper. In addition to, or even in lieu of submitting figures within your final manuscript, figures should be submitted individually, separate from the manuscript in one of the file formats listed above in section VI-J. Place figure captions below the figures; place table titles above the tables. Please do not include captions as part of the figures, or put them in “text boxes” linked to the figures. Also, do not place borders around the outside of your figures.

All IEEE Transactions, Journals, and Letters allow an author to publish color figures on IEEE Xplore® at no charge, and automatically convert them to grayscale for print versions. In most journals, figures and tables may alternatively be printed in color if an author chooses to do so. Please note that this service comes at an extra expense to the author. If you intend to have print color graphics, include a note with your final paper indicating which figures or tables you would like to be handled that way, and stating that you are willing to pay the additional fee.

CONCLUSION

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

APPENDIX

Appendixes, if needed, appear before the acknowledgment.

ACKNOWLEDGMENT

The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments. Avoid expressions such as “One of us (S.B.A.) would like to thank ... .” Instead, write “F. A. Author thanks ... .” In most cases, sponsor and financial support acknowledgments are placed in the unnumbered footnote on the first page, not here.

REFERENCES AND FOOTNOTES

1. REFERENCES

References need not be cited in text. When they are, they appear on the line, in square brackets, inside the punctuation. Multiple references are each numbered with separate brackets. When citing a section in a book, please give the relevant page numbers. In text, refer simply to the reference number. Do not use “Ref.” or “reference” except at the beginning of a sentence: “Reference [3] shows ... .” Please do not use automatic endnotes in Word, rather, type the reference list at the end of the paper using the “References” style.

Reference numbers are set flush left and form a column of their own, hanging out beyond the body of the reference. The reference numbers are on the line, enclosed in square brackets. In all references, the given name of the author or editor is abbreviated to the initial only and precedes the last name. Use them all; use et al. only if names are not given. Use commas around Jr., Sr., and III in names. Abbreviate conference titles. When citing IEEE transactions, provide the issue number, page range, volume number, year, and/or month if available. When referencing a patent, provide the day and the month of issue, or application. References may not include all information; please obtain and include relevant information. Do not combine references. There must be only one reference with each number. If there is a URL included with the print reference, it can be included at the end of the reference.

Other than books, capitalize only the first word in a paper title, except for proper nouns and element symbols. For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation See the end of this document for formats and examples of common references. For a complete discussion of references and their formats, see the IEEE style manual at www.ieee.org/authortools.

1. FOOTNOTES

Number footnotes separately in superscripts (Insert| Footnote).[[6]](#footnote-6) Place the actual footnote at the bottom of the column in which it is cited; do not put footnotes in the reference list (endnotes). Use letters for table footnotes (see Table I).

SUBMITTING YOUR PAPER FOR REVIEW

1. REVIEW STAGE USING WORD 6.0 OR HIGHER

If you want to submit your file with one column electronically, please do the following:

--First, click on the View menu and choose Print Layout.

--Second, place your cursor in the first paragraph. Go to the Format menu, choose Columns, choose one column Layout, and choose “apply to whole document” from the dropdown menu.

--Third, click and drag the right margin bar to just over 4 inches in width.

The graphics will stay in the “second” column, but you can drag them to the first column. Make the graphic wider to push out any text that may try to fill in next to the graphic.

1. FINAL STAGE USING WORD 6.0

When you submit your final version (after your paper has been accepted), print it in two-column format, including figures and tables. You must also send your final manuscript on a disk, via e-mail, or through a Web manuscript submission system as directed by the society contact. You may use Zip for large files, or compress files using Compress, Pkzip, Stuffit, or Gzip.

Also, send a sheet of paper or PDF with complete contact information for all authors. Include full mailing addresses, telephone numbers, fax numbers, and e-mail addresses. This information will be used to send each author a complimentary copy of the journal in which the paper appears. In addition, designate one author as the “corresponding author.” This is the author to whom proofs of the paper will be sent. Proofs are sent to the corresponding author only.

1. REVIEW STAGE USING SCHOLARONE® MANUSCRIPTS

Contributions to the Transactions, Journals, and Letters may be submitted electronically on IEEE’s on-line manuscript submission and peer-review system, ScholarOne® Manuscripts. You can get a listing of the publications that participate in ScholarOneat http://www.ieee.org/  
publications\_standards/publications/authors/authors\_submission.html First check if you have an existing account. If there is none, please create a new account. After logging in, go to your Author Center and click “Submit First Draft of a New Manuscript.”

Along with other information, you will be asked to select the subject from a pull-down list. Depending on the journal, there are various steps to the submission process; you must complete all steps for a complete submission. At the end of each step you must click “Save and Continue”; just uploading the paper is not sufficient. After the last step, you should see a confirmation that the submission is complete. You should also receive an e-mail confirmation. For inquiries regarding the submission of your paper on ScholarOne Manuscripts, please contact oprs-support@ieee.org or call +1 732 465 5861.

ScholarOne Manuscripts will accept files for review in various formats. Please check the guidelines of the specific journal for which you plan to submit.

You will be asked to file an electronic copyright form immediately upon completing the submission process (authors are responsible for obtaining any security clearances). Failure to submit the electronic copyright could result in publishing delays later. You will also have the opportunity to designate your article as “open access” if you agree to pay the IEEE open access fee.

1. FINAL STAGE USING SCHOLARONE MANUSCRIPTS

Upon acceptance, you will receive an email with specific instructions regarding the submission of your final files. To avoid any delays in publication, please be sure to follow these instructions. Most journals require that final submissions be uploaded through ScholarOne Manuscripts, although some may still accept final submissions via email. Final submissions should include source files of your accepted manuscript, high quality graphic files, and a formatted pdf file. If you have any questions regarding the final submission process, please contact the administrative contact for the journal.

In addition to this, upload a file with complete contact information for all authors. Include full mailing addresses, telephone numbers, fax numbers, and e-mail addresses. Designate the author who submitted the manuscript on ScholarOne Manuscripts as the “corresponding author.” This is the only author to whom proofs of the paper will be sent.

1. COPYRIGHT FORM

Authors must submit an electronic IEEE Copyright Form (eCF) upon submitting their final manuscript files. You can access the eCF system through your manuscript submission system or through the Author Gateway. You are responsible for obtaining any necessary approvals and/or security clearances. For additional information on intellectual property rights, visit the IEEE Intellectual Property Rights department web page at http://www.ieee.org/publications\_  
standards/publications/rights/index.html.

IEEE PUBLISHING POLICY

The general IEEE policy requires that authors should only submit original work that has neither appeared elsewhere for publication, nor is under review for another refereed publication. The submitting author must disclose all prior publication(s) and current submissions when submitting a manuscript. Do not publish “preliminary” data or results. The submitting author is responsible for obtaining agreement of all coauthors and any consent required from employers or sponsors before submitting an article. The IEEE Access

Department strongly discourages courtesy authorship; it is the obligation of the authors to cite only relevant prior work.

The IEEE Access Department does not publish conference records or proceedings, but can publish articles related to conferences that have undergone rigorous peer review. Minimally, two reviews are required for every article submitted for peer review.

PUBLICATION PRINCIPLES

The two types of contents of that are published are; 1) peer-reviewed and 2) archival. The Transactions and Journals Department publishes scholarly articles of archival value as well as tutorial expositions and critical reviews of classical subjects and topics of current interest.

Authors should consider the following points:

1. Technical papers submitted for publication must advance the state of knowledge and must cite relevant prior work.
2. The length of a submitted paper should be commensurate with the importance, or appropriate to the complexity, of the work. For example, an obvious extension of previously published work might not be appropriate for publication or might be adequately treated in just a few pages.
3. Authors must convince both peer reviewers and the editors of the scientific and technical merit of a paper; the standards of proof are higher when extraordinary or unexpected results are reported.
4. Because replication is required for scientific progress, papers submitted for publication must provide sufficient information to allow readers to perform similar experiments or calculations and use the reported results. Although not everything need be disclosed, a paper must contain new, useable, and fully described information. For example, a specimen’s chemical composition need not be reported if the main purpose of a paper is to introduce a new measurement technique. Authors should expect to be challenged by reviewers if the results are not supported by adequate data and critical details.
5. Papers that describe ongoing work or announce the latest technical achievement, which are suitable for presentation at a professional conference, may not be appropriate for publication.

REFERENCES

*Basic format for books:*

J. K. Author, “Title of chapter in the book,” in *Title of His Published Book, x*th ed. City of Publisher, (only U.S. State), Country: Abbrev. of Publisher, year, ch. *x*, sec. *x*, pp. *xxx–xxx.*

*Examples:*

1. G. O. Young, “Synthetic structure of industrial plastics,” in *Plastics,* 2nd ed., vol. 3, J. Peters, Ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15–64.
2. W.-K. Chen, *Linear Networks and Systems.* Belmont, CA, USA: Wadsworth, 1993, pp. 123–135.

*Basic format for periodicals:*

J. K. Author, “Name of paper,” *Abbrev. Title of Periodical*, vol. *x, no*. *x,* pp*. xxx-xxx,* Abbrev. Month, year, DOI. 10.1109.*XXX*.123456.

*Examples:*

1. J. U. Duncombe, “Infrared navigation—Part I: An assessment of feasibility,” *IEEE Trans. Electron Devices*, vol. ED-11, no. 1, pp. 34–39, Jan. 1959, 10.1109/TED.2016.2628402.
2. E. P. Wigner, “Theory of traveling-wave optical laser,”   
   *Phys. Rev*.,   
   vol. 134, pp. A635–A646, Dec. 1965.
3. E. H. Miller, “A note on reflector arrays,” *IEEE Trans. Antennas Propagat*., to be published.

*Basic format for reports:*

J. K. Author, “Title of report,” Abbrev. Name of Co., City of Co., Abbrev. State, Country, Rep. *xxx*, year.

*Examples:*

1. E. E. Reber, R. L. Michell, and C. J. Carter, “Oxygen absorption in the earth’s atmosphere,” Aerospace Corp., Los Angeles, CA, USA, Tech. Rep. TR-0200 (4230-46)-3, Nov. 1988.
2. J. H. Davis and J. R. Cogdell, “Calibration program for the 16-foot antenna,” Elect. Eng. Res. Lab., Univ. Texas, Austin, TX, USA, Tech. Memo. NGL-006-69-3, Nov. 15, 1987.

*Basic format for handbooks:*

*Name of Manual/Handbook, x* ed., Abbrev. Name of Co., City of Co., Abbrev. State, Country, year, pp. *xxx-xxx.*

*Examples:*

1. *Transmission Systems for Communications*, 3rd ed., Western Electric Co., Winston-Salem, NC, USA, 1985, pp. 44–60.
2. *Motorola Semiconductor Data Manual*, Motorola Semiconductor Products Inc., Phoenix, AZ, USA, 1989.

*Basic format for books (when available online):*

J. K. Author, “Title of chapter in the book,” in *Title of Published Book*, *x*th ed. City of Publisher, State, Country: Abbrev. of Publisher, year, ch.*x*, sec. *x*, pp. *xxx–xxx*. [Online]. Available: http://www.web.com

*Examples:*

1. G. O. Young, “Synthetic structure of industrial plastics,” in Plastics, vol. 3, Polymers of Hexadromicon, J. Peters, Ed., 2nd ed. New York, NY, USA: McGraw-Hill, 1964, pp. 15-64. [Online]. Available: http://www.bookref.com.
2. *The Founders’ Constitution*, Philip B. Kurland and Ralph Lerner, eds., Chicago, IL, USA: Univ. Chicago Press, 1987. [Online]. Available: http://press-pubs.uchicago.edu/founders/
3. The Terahertz Wave eBook. ZOmega Terahertz Corp., 2014. [Online]. Available: http://dl.z-thz.com/eBook/zomega\_ebook\_pdf\_1206\_sr.pdf. Accessed on: May 19, 2014.
4. Philip B. Kurland and Ralph Lerner, eds., *The Founders’ Constitution.* Chicago, IL, USA: Univ. of Chicago Press, 1987, Accessed on: Feb. 28, 2010, [Online] Available: http://press-pubs.uchicago.edu/founders/

*Basic format for journals (when available online):*

J. K. Author, “Name of paper,” *Abbrev. Title of Periodical*, vol. *x*, no. *x*, pp. *xxx-xxx*, Abbrev. Month, year. Accessed on: Month, Day, year, DOI: 10.1109.*XXX*.123456, [Online].

*Examples:*

1. J. S. Turner, “New directions in communications,” *IEEE J. Sel. Areas Commun*., vol. 13, no. 1, pp. 11-23, Jan. 1995.
2. W. P. Risk, G. S. Kino, and H. J. Shaw, “Fiber-optic frequency shifter using a surface acoustic wave incident at an oblique angle,” *Opt. Lett.*, vol. 11, no. 2, pp. 115–117, Feb. 1986.
3. P. Kopyt *et al., “*Electric properties of graphene-based conductive layers from DC up to terahertz range,” *IEEE THz Sci. Technol.,* to be published. DOI: 10.1109/TTHZ.2016.2544142.

*Basic format for papers presented at conferences (when available online):*

J.K. Author. (year, month). Title. presented at abbrev. conference title. [Type of Medium]. Available: site/path/file

*Example:*

1. PROCESS Corporation, Boston, MA, USA. Intranets: Internet technologies deployed behind the firewall for corporate productivity. Presented at INET96 Annual Meeting. [Online]. Available: http://home.process.com/Intranets/wp2.htp

*Basic format for reports and handbooks (when available online):*

J. K. Author. “Title of report,” Company. City, State, Country. Rep. no., (optional: vol./issue), Date. [Online] Available: site/path/file

*Examples:*

1. R. J. Hijmans and J. van Etten, “Raster: Geographic analysis and modeling with raster data,” R Package Version 2.0-12, Jan. 12, 2012. [Online]. Available: http://CRAN.R-project.org/package=raster
2. Teralyzer. Lytera UG, Kirchhain, Germany [Online]. Available: http://www.lytera.de/Terahertz\_THz\_Spectroscopy.php?id=home, Accessed on: Jun. 5, 2014

*Basic format for computer programs and electronic documents (when available online):*

Legislative body. Number of Congress, Session. (year, month day). *Number of bill or resolution*, *Title*. [Type of medium]. Available: site/path/file

***NOTE:*** ISO recommends that capitalization follow the accepted practice for the language or script in which the information is given.

*Example:*

1. U.S. House. 102nd Congress, 1st Session. (1991, Jan. 11). *H. Con. Res. 1, Sense of the Congress on Approval of Military Action*. [Online]. Available: LEXIS Library: GENFED File: BILLS

*Basic format for patents (when available online):*

Name of the invention, by inventor’s name. (year, month day). Patent Number[Type of medium]. Available: site/path/file

*Example:*

1. Musical toothbrush with mirror, by L.M.R. Brooks. (1992, May 19). Patent D 326 189

[Online]. Available: NEXIS Library: LEXPAT File: DES

*Basic format for conference proceedings (published):*

J. K. Author, “Title of paper,” in *Abbreviated Name of Conf.*, City of Conf., Abbrev. State (if given), Country, year, pp. *xxxxxx.*

*Example:*

1. D. B. Payne and J. R. Stern, “Wavelength-switched pas- sively coupled single-mode optical network,” in *Proc. IOOC-ECOC,* Boston, MA, USA,1985,   
   pp. 585–590.

*Example for papers presented at conferences (unpublished):*

1. D. Ebehard and E. Voges, “Digital single sideband detection for interferometric sensors,” presented at the *2nd Int. Conf. Optical Fiber Sensors,* Stuttgart, Germany, Jan. 2-5, 1984.

*Basic format for patents:*

J. K. Author, “Title of patent,” U.S. Patent *x xxx xxx*, Abbrev. Month, day, year.

*Example:*

1. G. Brandli and M. Dick, “Alternating current fed power supply,” U.S. Patent 4 084 217, Nov. 4, 1978.

*Basic format**for theses (M.S.) and dissertations (Ph.D.):*

a) J. K. Author, “Title of thesis,” M.S. thesis, Abbrev. Dept., Abbrev. Univ., City of Univ., Abbrev. State, year.

b) J. K. Author, “Title of dissertation,” Ph.D. dissertation, Abbrev. Dept., Abbrev. Univ., City of Univ., Abbrev. State, year.

*Examples:*

1. J. O. Williams, “Narrow-band analyzer,” Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, USA, 1993.
2. N. Kawasaki, “Parametric study of thermal and chemical nonequilibrium nozzle flow,” M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.

*Basic format for the most common types of unpublished references:*

a) J. K. Author, private communication, Abbrev. Month, year.

b) J. K. Author, “Title of paper,” unpublished.

c) J. K. Author, “Title of paper,” to be published.

*Examples:*

1. A. Harrison, private communication, May 1995.
2. B. Smith, “An approach to graphs of linear forms,” unpublished.
3. A. Brahms, “Representation error for real numbers in binary computer arithmetic,” IEEE Computer Group Repository, Paper R-67-85.

*Basic formats for standards:*

a) *Title of Standard*, Standard number, date.

b) *Title of Standard*, Standard number, Corporate author, location, date.

*Examples:*

1. IEEE Criteria for Class IE Electric Systems, IEEE Standard 308, 1969.
2. Letter Symbols for Quantities, ANSI Standard Y10.5-1968.

*Article number in reference examples:*

1. R. Fardel, M. Nagel, F. Nuesch, T. Lippert, and A. Wokaun, “Fabrication of organic light emitting diode pixels by laser-assisted forward transfer,” *Appl. Phys. Lett.*, vol. 91, no. 6, Aug. 2007, Art. no. 061103.
2. J. Zhang and N. Tansu, “Optical gain and laser characteristics of InGaN quantum wells on ternary InGaN substrates,” *IEEE Photon. J.*, vol. 5, no. 2, Apr. 2013, Art. no. 2600111.

*Example when using et al.:*

1. S. Azodolmolky *et al.*, Experimental demonstration of an impairment aware network planning and operation tool for transparent/translucent optical networks,” *J. Lightw. Technol.*, vol. 29, no. 4, pp. 439–448, Sep. 2011.

FIRST A. AUTHOR (M’76–SM’81–F’87) and all authors may include biographies. Biographies are often not included in conference-related papers. This author became a Member (M) of IEEE in 1976, a Senior Member (SM) in 1981, and a Fellow (F) in 1987. The first paragraph may contain a place and/or date of birth (list place, then date). Next, the author’s educational background is listed. The degrees should be listed with type of degree in what field, which institution, city, state, and country, and year the degree was earned. The author’s major field of study should be lower-cased.

The second paragraph uses the pronoun of the person (he or she) and not the author’s last name. It lists military and work experience, including summer and fellowship jobs. Job titles are capitalized. The current job must have a location; previous positions may be listed without one. Information concerning previous publications may be included. Try not to list more than three books or published articles. The format for listing publishers of a book within the biography is: title of book (publisher name, year) similar to a reference. Current and previous research interests end the paragraph.

The third paragraph begins with the author’s title and last name (e.g., Dr. Smith, Prof. Jones, Mr. Kajor, Ms. Hunter). List any memberships in professional societies other than the IEEE. Finally, list any awards and work for IEEE committees and publications. If a photograph is provided, it should be of good quality, and professional-looking. Following are two examples of an author’s biography.

**SECOND B. AUTHOR** was born in Greenwich Village, New York, NY, USA in 1977. He received the B.S. and M.S. degrees in aerospace engineering from the University of Virginia, Charlottesville, in 2001 and the Ph.D. degree in mechanical engineering from Drexel University, Philadelphia, PA, in 2008.

From 2001 to 2004, he was a Research Assistant with the Princeton Plasma Physics Laboratory. Since 2009, he has been an Assistant Professor with the Mechanical Engineering Department, Texas A&M University, College Station. He is the author of three books, more than 150 articles, and more than 70 inventions. His research interests include high-pressure and high-density nonthermal plasma discharge processes and applications, microscale plasma discharges, discharges in liquids, spectroscopic diagnostics, plasma propulsion, and innovation plasma applications. He is an Associate Editor of the journal *Earth*, *Moon*, *Planets*, and holds two patents.

Dr. Author was a recipient of the International Association of Geomagnetism and Aeronomy Young Scientist Award for Excellence in 2008, and the IEEE Electromagnetic Compatibility Society Best Symposium Paper Award in 2011.

**THIRD C. AUTHOR, JR.** (M’87) received the B.S. degree in mechanical engineering from National Chung Cheng University, Chiayi, Taiwan, in 2004 and the M.S. degree in mechanical engineering from National Tsing Hua University, Hsinchu, Taiwan, in 2006. He is currently pursuing the Ph.D. degree in mechanical engineering at Texas A&M University, College Station, TX, USA.

From 2008 to 2009, he was a Research Assistant with the Institute of Physics, Academia Sinica, Tapei, Taiwan. His research interest includes the development of surface processing and biological/medical treatment techniques using nonthermal atmospheric pressure plasmas, fundamental study of plasma sources, and fabrication of micro- or nanostructured surfaces.

Mr. Author’s awards and honors include the Frew Fellowship (Australian Academy of Science), the I. I. Rabi Prize (APS), the European Frequency and Time Forum Award, the Carl Zeiss Research Award, the William F. Meggers Award and the Adolph Lomb Medal (OSA).

1. *FARHAN ULLAH, F. A. R. H. A. N*. (*2019, August 13*). *Cyber securitythreats detection in internet of things* <https://www.researchgate.net/publication>. *https://ieeexplore.ieee.org/stamp*. *Retrieved March 10, 2022.*  [↑](#footnote-ref-1)
2. Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-turjman, F., & Mostarda, L*. (2019). Cyber security threats detection in internet of things using Deep Learning Approach. Retrived from IEEE Access.*  [↑](#footnote-ref-2)
3. Van Camp, C., & Peeters, W. (2022). *A world without satellite data as a result of a global Cyber-Attack. Space Policy*, *https://doi.org/10.1016/j.spacepol.2021.101458* [↑](#footnote-ref-3)
4. CISA. (2021, September 7). Report cyber incidents. Cybersecurity and Infrastructure Security Agency CISA. Retrieved March 10, 2022, *Retrieved From* https://www.cisa.gov/reporting-cyber-incidents [↑](#footnote-ref-4)
5. Faisal, M., Azzid, M., & casarin, zolidah. (2020*). API Vulnerabilities In Cloud Computing Platform: Attack And Detection. International Journal of Engineering Trends and Technology, 1–14*. [↑](#footnote-ref-5)
6. It is recommended that footnotes be avoided (except for the unnumbered footnote with the receipt date on the first page). Instead, try to integrate the footnote information into the text. [↑](#footnote-ref-6)