IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DUAL NATURE OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

Dr. Nitika Arora
Assistant Professor of Computer Science
Pt. C.L.S Govt.College Karnal, Haryana, India

ABSTRACT: Cyber security has become major concern over the years because of ever increasing cyber attacks and crimes which are posing a great threat with the increasing growth of artificial intelligence. Data breaches increasing day by the day with the digital transformation of each information .Artificial Intelligence (AI) is rapidly growing technology in every field. Due to its high potential AI has been treated in Industry revolution 4.0. AI has been used in every walk of our lifelike in Cyber Security, Healthcare, Education, finance, e-commerce, Transport, Customer care, Law and many more. One crucial application that uses AI to great extent more than any other today is data security. On the other hand artificial intelligence tools could be exploited by malicious hackers. Businesses and Government are worried about cyber attacks because one successful cyber attack causes a lot of financial and economic loss. It is important for business leaders to identify the potential dangers and benefits of using AI in cyber security. This paper provides challenges and usage of AI in cyber security.

Keywords: Deepfake, Advanced Persistent threat, malvertising

INTRODUCTION

Artificial intelligence is the ability of machines to think and understand from the existing data to perform specific goals. The idea of artificial intelligence was first coined by John McCarthy in 1955 and then this idea led to the creation of Natural language processing, Machine learning, Deep Learning and Predicative analysis. In the today's scenario we are surrounded by artificial intelligence everywhere like Amazon's alexa to every advertisement or news which is displayed on our mobiles depending on what we like to see or going to buy in future.

As per a study, AI is expected to double the annual economic growth rate of 12 developed countries by 2035 .As digital technologies are becoming so important for businesses and Government ,the possibility of cyber attacks and cyber crimes have increased. Cybercrime causes loss of sensitive information which leads to production loss, Economic loss, damaged brand, fines [17] , penalties and litigations and then forensic investigation causes restoration and deletion of hacked data and systems which causes a lot of reputational harm to that organization.

Cyber Attacks includes Phishing, malware, and ransomware and DDO/IoT attacks.

- Phishing attack is cyber attack where attackers send suspicious mails that look alike legitimate emails. In 2022, on an average phishing took 295 days to detect and 710 million [20] phishing emails were blocked per week.Malware is attack where malicious software is designed by the attackers to steal sensitive information or data. In 2022 malware attacks recorded to 2.8 billion attacks and 30% of breaches were done through malware. The top three states were Florida having 140.1 million attacks, California having 140 million attacks, and New York having 133.5 million attacks [2].
- Ransomware is attack where victim's data get encrypted and unable to use system until ransom is paid by them. Ransomware is presently 30% of all the malware. Ransomware caused losses over $20 billion by 2021 which is

57 times more than that in 2015. There were still 236.1 million[5] attacks worldwide despite a 23% decrease in global ransomware attacks in 2022,

- DDoS attack can make website totally offline because attackers attack on network or online systems by flooding too many requests which make users to unable to use that website. No employees are able to access network resources in the case of Web servers running E-Commerce sites and no consumers will be able to purchase products or receive assistance. Companies can lose $20,000 per hour in the event of a successful [8] DDoS attack. In 2019, the average cost of a DDoS attack was $2.6 million, up from $1.6 million [6] the year before.

DUAL NATURE OF AI

Artificial intelligence has changed our way of living and the way how we interact with the world. In generally artificial intelligence and machine learning were shown in Sci-fi movies but now days these technologies have become so common that we are using many applications like face recognition [16], voice assistant, chatbots and camera quality. AI is used in detecting threats more accurately and then prioritizes responses based on real world risk. Artificial intelligence and machine learning are playing an important role both as blessings and curse in cyber security. Organizations can use AI to great extent for detecting BotNet, predicting risks, fraud detection and filtration of spam Emails. But nothing comes without paying a price. Technologies are developed to make life easier by providing access to different tools and products.

According to the latest reports, from Figure 1 it s clear that 328.77 million [9] terabytes of data are created each day and 181 zettabytes of data will be generated in 2025.

Figure 1 : Amount of Data Generated Annually (in TB).

Now as most of the data is available on internet, it is most likely to get targeted by cyber attack through phishing, malicious ads [23] spyware, ransomware, IoT attacks or anything else. According to Gartner [29]worldwide 45% of organizations have been attacked by cyber world which is three times as in 2021.According to Statista, global cost of cybercrime is expected to rise from $8.44 trillion in 2022 to $23.84 trillion by 2027.

Today new attacks are emerging which are called AI attacks [10] which specifically target AI system and associated physical entities to execute cyber attacks. In case of misuse of artificial intelligence by cyber attackers may purposefully fed the algorithms with false or misleading data to commit fraud or crime. The hacker's input can be used to train the AI system, which will then learn how to defeat AI-based cyber defenses [3]. So it is this dual nature of AI that that is bringing enormous risks [21] not only to Government, businesses, institutions, organizations but also to humanity. With the increasing applications of machine learning, deep learning and data availability might also leads to mass destruction on large scale. Artificial intelligence, robotics, and drones have potential benefits for human kind. However, these same advances can also bring dangers such as unchecked intelligence, surveillance, and biased or lethal algorithms. No one is prepared for

these perils. The global market for AI-based cyber security products is estimated to reach $133.8 billion [31] by 2030, up from $14.9 billion last year.

AI POWERED CYBER ATTACKS

AI hacks are posing a tremendous security risk to both government organizations and the general public. As these techniques proliferate on the web, it is now simpler for hackers to create machine learning algorithms using hacking techniques or employ botnets to their fullest potential. A bot system becomes better each time it tries to launch a spam attack. To properly protect the data of its consumers, cyber security organizations and website developers will need to respond with even more creative solutions. There are many AI-powered cyber attacks [30].

DEEPFAKE ATTACKS

Deepfake is the term for the creation of synthetic video, audio, pictures or textual data using advanced artificial intelligence and machine learning technologies. The technology can create media (Persons, 2020) that copies a person's voice and appearance. Real time voice cloning [15] and deep learning algorithms are used in swapping faces in videos, images and other media to make fake to appear [28] as real. The underlying technologies in Deepfakes are Autoencoders and Generative Adversial Networks (GAN). Deepfake scams have caused financial losses to individual victims between $24.3 million to $35 million [11]

Sensity, a company that monitors Deepfake films online, claims that since 2018, the number has doubled every six months, reaching 85,047 videos as of December 2020 [12] .As shown in Figure 2 broadcast of Deepfake videos .

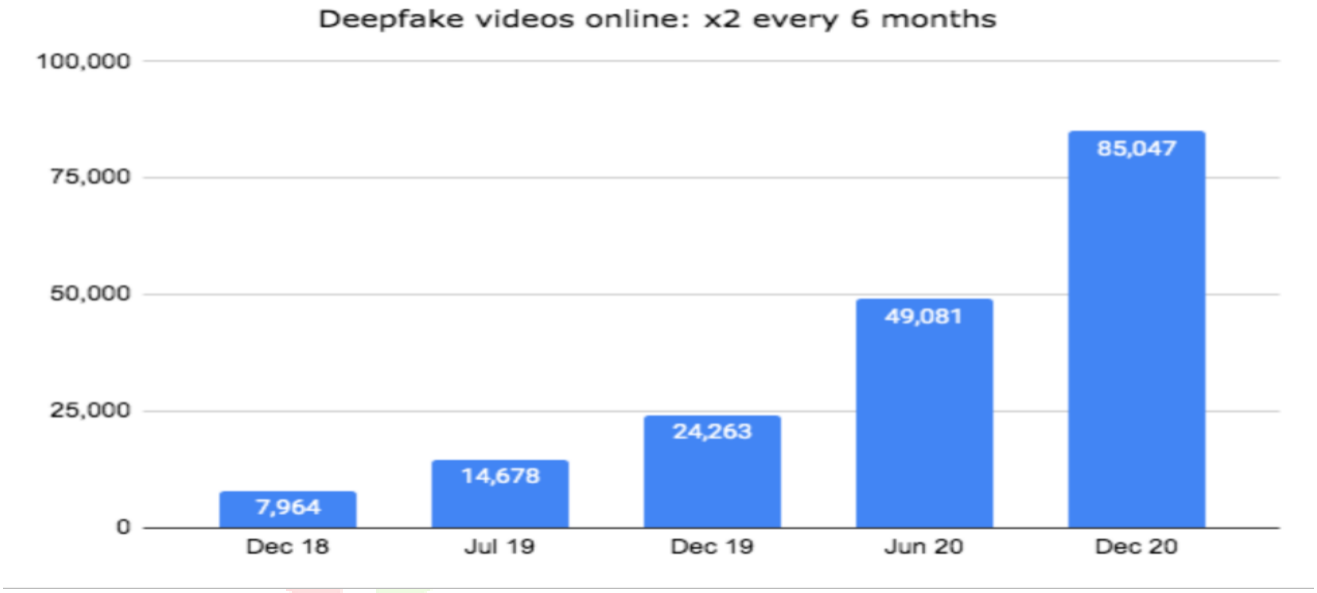

Figure 2: Growth of Generation of Deepfake videos online

DATA POISONING

Data Poisoning is an adversarial attack that manipulate training dataset by injecting malicious or polluted data to control the behavior [18] of machine learning model such that model will produce outcome of malicious example into accurate outcomes. This attack is most dangerous as training dataset is infected with tampered data which lowers its overall accuracy and target the model by adding backdoor .Backdoor may go unnoticed for a long time because it will produce desired result until it meets certain conditions for executing that attack. The most famous case of data poisoning is Gmail' spam [14] filter applications where spam emails were not marked as spam and several emails were sent by attackers containing malware or other cyber security threats without noticing them.AI industry is aware of this threat data poisoning and experts are suggesting to check all the labels in dataset at regular intervals.

The enormous machine-learning models being trained today—like ChatGPT, Stable Diffusion, or Midjourney—needs so much data to train [7] Because of this, maintaining any level of quality control is incredibly difficult.

AI PHISHING ATTACKS

Phishing attacks as we know is stealing of information including login credentials and personal information from user by clicking an attachment sent in email or message on phone or responding to social media friend without realizing it as cyber attack. Generally, the different forms of phishing attacks are email phishing, spear phishing, fake website, session hijacking, mobile phishing, voice phishing, malvertising. According to research done in 2021, about 45% of email traffic was spamming [1].

Figure 3 shows how an activity of phishing [2]attacks happen in cyber world.

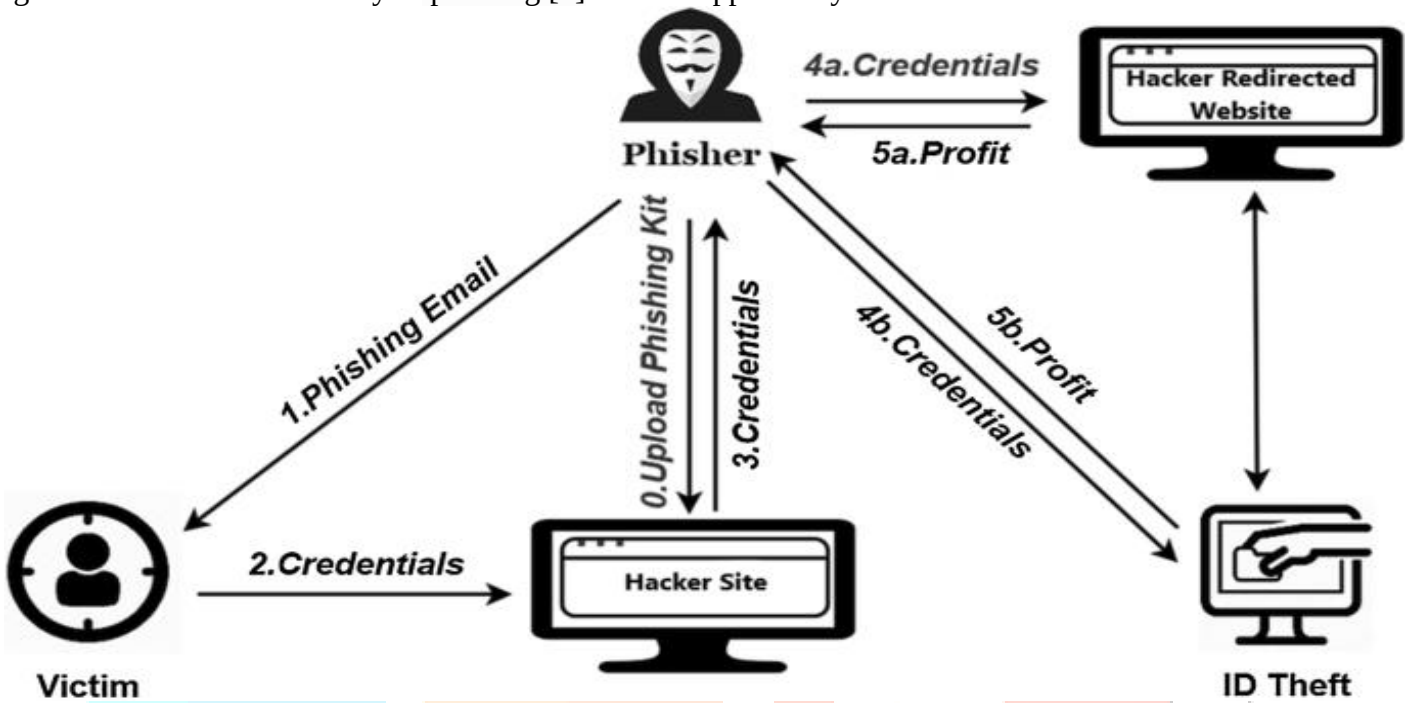

Figure 3: How Phishing takes place?

The artificial intelligence technology is being used to create convincing phishing emails that contain accurate language and grammar using ChatGPT [19] that victim cannot easily detect any error and gathering of information about the target organization, its leaders, and the general public. Rapid and intelligent answers to communications are also powered by AI [24]. AI is capable of quickly producing documents or webpages (Sayegh, 2023)with payloads that appear authentic to users. Additionally, AI is employed to deliver a deep faked voice in real time in response to suspicious unwanted spam calls that record actual voices.

According to the most recent phishing report released by Zscaler ThreatLabz [4] global phishing attacks increased by 29% over the previous 12 months. The Anti-Phishing Working Group (APWG) also reported that there were a record 1,025,968 phishing attacks in the first quarter of 2022.The way to protect from phishing attack is raising awareness of the dangers of phishing attacks regarding how to spot them and putting strong authentication techniques, such multi-factor authentication into practice and utilizing anti-phishing software to recognize and putting cyber security solutions powered by AI into use to identify and stop phishing assaults powered by AI and collaborating with a trustworthy Managed Security Services Provider (MSSP)[26] that possesses the depth, scope, and technology to thwart these threats

ADVANCED PERSISTENT THREATS (APTs)

A sophisticated, sustained cyber attack known as an advanced persistent threat (APT) [30]occurs when an intruder enters a network undetected and stays there for a long time in order to steal sensitive data. They frequently involve the use of artificial intelligence to avoid detection and target specific organizations or individuals. APT attackers frequently have the following objectives: theft of intellectual property, personally identifiable information (PII), or Data deletion or tampering (sabotage), misuse of resources, surveillance for potential attacks, Theft or fabrication of administrative credentials

Additionally, AI may be used to reduce APTs, which is notoriously [13] difficult to detect and highly targeted, enabling organizations to see threats before they seriously harm their operations. Cyber security personnel may concentrate more on strategic duties, including threat hunting and incident response, by using AI to automate

repetitive security management tasks. The way to protect your system against APT is to maintain [27]a secure network, keep operating system and software up to date, regular review access to network resources, use end to end encryption on sensitive information because once APT enters into system may go unnoticeable until it causes serious damage to systems.

CONCLUSION

Although AI has the potential to significantly enhance cyber security, it also has drawbacks. Building and maintaining AI systems requires skill, talent, increased organizational resources and financial commitments, and gathering varied data sets to train these systems which can be time and money-consuming.

AI may generate false positives and inaccurate results if there is insufficient data. Cybercriminals can also employ AI to carry out more sophisticated attacks. In summary, applying AI to cyber security is a two-edged sword. While it presents new opportunities for hackers to exploit, it also presents a chance for us to keep ahead of cyber dangers. It is our responsibility to use AI ethically and responsibly as it develops and to guard against those who would misuse it. These are a few of the additional cyber security concerns fueled by AI that the tech sector is worried about. To defend themselves, people and organizations need to keep up with the most recent AI-powered cyber threats and put strong security measures in place.

Only time will tell which group—hacktivists or cyber professionals who will figured out how to exploit this technology the most effectively. In the interim, it's essential to prioritize AI on your list of desired cyber technology tools and learn how to fight fire with fire if you want to advance before it's too late.

REFERENCES

[1] 19 examples of common phishing emails and how to avoid them. (2022, February 24). Retrieved April 2023, from terranovasecurity.com: https://terranovasecurity.com/top-examples-of-phishing-emails/

[2] A comprehensive survey of AI-enabled phishing attacks detection techniques. (n.d.). link.springer.com .

[3] Chin, K. (2023, April 12). The Impact of AI on Cybersecurity: Predictions for the Future. Retrieved April 2023, from upguard.com: https://www.upguard.com/blog/the-impact-of-ai-on-cybersecurity#:~:text=Through%20automation%20and%20machine%20learning,solutions%20beyond%20current%20human%20capabilities.

[4] Crumbaugh, J. (2022, October 10). How AI and machine learning are changing the phishing game. Retrieved April 2023, from venturebeat.com: https://venturebeat.com/ai/how-ai-machine-learning-changing-phishing-game/

[5] Cyber threat report. (2022, March). Retrieved March 16, 2023, from sonicwall.com: https://www.sonicwall.com/medialibrary/en/infographic/mid-year-update-2022-sonicwall-cyber-threat-report.pdf

[6] DDoS Attack Cost Bandwidth.com Nearly $12 Million- How to Protect Your Site Against One? (2022, September 27). Retrieved April 2023, from Indusface: https://www.indusface.com/blog/ddos-attack-cost-bandwidth-com-nearly-12-million-how-to-protect-your-site-against-one/#:~:text=Leading%20Causes%20of%20Sophisticated%20DDoS%20Attacks&text=The%20cost%20of%20DDoS%20attacks%20has%20risen%20in%20recent%20years,

[7] DHAR, P. (2023, March 24). Protecting AI Models from “Data Poisoning”. Retrieved April 2023, from spectrum.ieee.org: https://spectrum.ieee.org/ai-cybersecurity-data-poisoning

[8] Distributed Denial of Service: Anatomy and Impact of DDoS Attacks. (n.d.). Retrieved April 20, 2023, from https://usa.kaspersky.com/resource-center/preemptive-safety/how-does-ddos-attack-work

[9] Duarte, F. (2023, April 03). Amount of Data Created Daily. Retrieved april 2023, from explodingtopics.com: https://explodingtopics.com/blog/data-generated-per-day

[10] Editorial. (2022, January 22). Types Of AI Attacks Against AI Systems And Best Practices. Retrieved April 2023, from roboticsbiz: https://roboticsbiz.com/types-of-ai-attacks-against-ai-systems-and-best-practices/

[11] Fraud. (2022, October 28). Why Deepfake Fraud Losses Should Scare Financial Institutions. Retrieved April 2023, from feedzai.com: https://feedzai.com/blog/why-deepfake-fraud-losses-should-scare-financial-institutions/

[12] How deepfakes are a problem for us all and why the law needs to change. (n.d.). Retrieved April 2023, from informationmatters.net: https://informationmatters.net/deepfakes-problem-why-law-needs-to-change/

[13] Jackson, J. (2023, February 13). We are less than a year away from a cyber attack credited to ChatGPT. Retrieved April 2023, from cshub.com: https://www.cshub.com/attacks/articles/chatgpt-cyber-attack-threat

[14] Joshi, N. (2022, May 17). Countering The Underrated Threat Of Data Poisoning Facing Your Organization. Retrieved April 2023, from forbes.com: https://www.forbes.com/sites/naveenjoshi/2022/03/17/countering-the-underrated-threat-of-data-poisoning-facing-your-organization/?sh=539ba107b5d8

[15] Kepczyk, R. H. (2022, September 28). Deepfakes emerge as real cybersecurity threat. Retrieved April 2023, from aicpa-cima.com: https://www.d/news/article/deepfakes-emerge-as-real-cybersecurity-threat

[16] Khan, W. (2022, Feb 25). How To Use Artificial Intelligence In Mobile Apps. Retrieved March 2023, from https://elearningindustry.com/how-to-use-artificial-intelligence-in-mobile-apps

[17] Lobo, S. (2019, March 31). Understanding the cost of a cybersecurity attack: The losses organizations face. Retrieved March 2023, from packtpub.com: https://hub.packtpub.com/understanding-the-cost-of-a-cybersecurity-attack-the-losses-organizations-face/

[18] Menon, A. (2023, January 23). Data Poisoning and Its Impact on the AI Ecosystem. Retrieved April 2023, from themathcompany.com: https://themathcompany.com/blog/data-poisoning-and-its-impact-on-the-ai-ecosystem#:~:text=A%20form%20of%20adversarial%20attack,model%20and%20deliver%20false%20results.

[19] Milmo, A. H. (2023, March 29). AI chatbots making it harder to spot phishing emails, say experts. Retrieved April 2023, from theguardian.com: https://www.theguardian.com/technology/2023/mar/29/ai-chatbots-making-it-harder-to-spot-phishing-emails-say-experts

[20] Morgan, t. (2020, November 13). Cyberwarfare In The C-Suite. . Retrieved February 15, 2023, from cybersecurityventures.com: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[21] Pandya, J. (2019, January 7). The Dual-Use Dilemma Of Artificial Intelligence. Retrieved April 2023, from forbes.com: https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/?sh=433fea526cf0

[22] Persons, T. M. (2020, February). GAO SCIENCE & TECH SPOTLIGHT:Deepfakes. Retrieved April 2023, from gao.gov: https://www.gao.gov/assets/gao-20-379sp.pdf

[23] Rees, K. (2022, December 8). 6 Ways Your Privacy and Security Were Threatened in 2022. Retrieved March 2023, from makeuseof.com: https://www.makeuseof.com/ways-privacy-threatened-2022/

[24] Sajid, H. (2023, April 1). AI in Cybersecurity: 5 Crucial Applications. Retrieved April 2023, from v7labs.com: https://www.v7labs.com/blog/ai-in-cybersecurity

[25] Sayegh, E. (2023, April 11). Almost Human: The Threat Of AI-Powered Phishing Attacks. Retrieved April 2023, from forbes.com: https://www.forbes.com/sites/emilsayegh/2023/04/11/almost-human-the-threat-of-ai-powered-phishing-attacks/?sh=60cc002a3bc9

[26] Sayegh, E. (2023, April 11). Almost Human: The Threat Of AI-Powered Phishing Attacks. Retrieved April 20, 2023, from forbes.com: https://www.forbes.com/sites/emilsayegh/2023/04/11/almost-human-the-threat-of-ai-powered-phishing-attacks/?sh=60cc002a3bc9

[27] shaw, M. (2023, February 9). WHAT ARE THE BEST MEASURES TO AVOID APT ATTACKS? Retrieved May 20, 2023, from https://www.dnif.it/en/blog/measures-to-avoid-apt-attacks#:~:text=Maintain%20a%20secure%20network%20perimeter,systems%20regularly%2C%20and%20monitoring%20activity.

[28] Team, B. G. (2022, November 21). All You Need to Know About Deepfake AI. Retrieved April 2023, from mygreatlearning.com: https://www.mygreatlearning.com/blog/all-you-need-to-know-about-deepfake-ai/#:~:text=Deepfake%20content%20is%20created%20by,content%20is%20real%20or%20artificial.

[29] Technologies, S. (2023, March 08). Recent Cyber-Attacks of 2022: The Pandemic of Cybercrime. Retrieved April 2023, from sangfor: https://www.sangfor.com/blog/cybersecurity/recent-cyber-attacks-2022

[30] Trends, M. (2023, January 21). Top 5 AI-powered Cybersecurity threats in 2023. Retrieved April 2023, from analyticsinsight.net: https://www.analyticsinsight.net/top-5-ai-powered-cybersecurity-threats-in-2023/

[31] Violino, B. (2022, September 13). Artificial intelligence is playing a bigger role in cybersecurity, but the bad guys may benefit the most. Retrieved April 2023, from cnbc.com: https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html