I. K. Dutta, B. Ghosh, A. Carlson, M. Totaro and M. Bayoumi. (Oct. 28-31, 2020). Generative Adversarial Networks in Security: A Survey, *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, USA, 2020, pp. 0399-0405, doi: https://doi.org/10.1109/UEMCON51285.2020.9298135]

Generative Adversarial Networks in Security: A Survey

Conference Paper · October 2020

DOI: 10.1109/UEMCON51285.2020.9298135

Indira Kalyan Dutta
Arkansas Tech University

Bhaskar Ghosh
University of Louisiana at Lafayette

Albert H. Carlson
Austin Community College

Michael Totaro
University of Louisiana at Lafayette

Generative Adversarial Networks in Security: A Survey

Indira Kalyan Dutta*, Bhaskar Ghosh†
University of Louisiana at Lafayette
Louisiana, USA
*indira.dutta1@louisiana.edu,
†bhaskar.ghosh1@louisiana.edu

Albert Carlson
Kyle, Texas
ltzap1@gmail.com

Michael Totaro‡, Magdy Bayoumi§
University of Louisiana at Lafayette
Louisiana, USA
‡michael.totaro@louisiana.edu,
§magdy.bayoumi@louisiana.edu

***Abstract*—In the Information Age, the majority of data stored and transferred is digital; however, current security systems are not powerful enough to secure this data because they do not anticipate unknown attacks. With a growing number of attacks on cybersecurity systems defense mechanisms need to stay updated with the evolving threats. Security and their related attacks are an iterative pair of objects that learn to enhance themselves based upon each others' advances – a cybersecurity "arms race." In this survey, we focus on the various ways in which Generative Adversarial Networks (GANs) have been used to provide both security advances and attack scenarios in order to bypass detection systems. The aim of our survey is to examine works completed in the area of GANs, specifically device and network security. This paper also discusses new challenges for intrusion detection systems that have been generated using GANs. Considering the promising results that have been achieved in different GAN applications, it is very likely that GANs can shape security advances if applied to cybersecurity.**

***Index Terms*—Security, Generative Adversarial Networks, Cybersecurity, Machine Learning, Artificial Intelligence**

I. Introduction

Attacks against digital information, whether in the form of information at rest or information in motion, continue to grow in number, severity, and importance. The Internet grew from academic novelty to a central place in the daily life of almost every person that uses or is affected by modern technology. Hackers quickly recognized the value of the information on the Internet and the dependence that society had on the connectivity and communications that networks afforded. The next step in the evolution of modern networking is to include industrial and sensing devices known as the Internet of Things (IoT). It is estimated that by 2030, 50 billion devices will be added to the already crowded network and produce many new opportunities for entry and exploitation [1].

Cyber-attacks are a constant risk to users' digital lives. As indicated by Dutta, et al. in [2], devices and networks are vulnerable to severe attacks which can affect users in their daily lives [3]. Sophisticated algorithms are being used to develop complex intrusions in order to enter networks and systems unnoticed by detection systems which have not evolved to grapple with the growing complexity of threats. Information about the user's digital life can be stored, analyzed to plan further attacks, and/or sold by the attackers. Often these compromised systems are combined with other compromised systems to attack more targets in what becomes a snowballing action. These threats and the lack of robust detection systems leaves sensitive data exposed.

Protecting systems and networks from these attacks is a major cybersecurity goal. Although security systems are improving their resistance and security as a result of training for a wider variety of attacks, there remain various attacks that are not covered. Moreover, attacks are discovered with regularity. Thus, the question may be asked, if the defender does not know that an attack exists, how can they protect against such an attack? As a result, detection systems are used to protect networks against only known attacks. What follows are several examples [4] of attacks on systems that have failed to provide adequate protection, which motivated this survey:

- Weather Channel Ransomware - In April 2019, a ransomware attack occurred during a severe weather event in the southeastern US, which kept the cable channel inoperative for more than an hour [5]. This resulted in potential loss of property and life due to lack of vital information.
- Capital One Breach - In July 2019, thousands of credit card applicants' personal identification information, such as birthdays and Social Security numbers' were hacked [6].
- Texas Ransomware - In August 2019, the computer systems of 22 small towns in Texas suffered a ransomware attack. The result was that the government was unable to provide birth and death certificates [7].

With the advent of Machine Learning (ML), researchers began using the power of ML to improve their security systems. ML is a system where the computer algorithm adjusts itself based on past experience to improve its performance over time. The more time it is given to train on data, the more information it can gather to adapt to specified goals. Generative Adversarial Networks (GANs) [8] are one such type of ML that was introduced in 2014. GANs can be used to produce synthetic data based on the experience of training over actual data. As a result, many possible attacks, including previously unidentified attacks, are explored using this generated data, which a user would not normally present in training. This makes the GANs methodology very powerful in a scenario of system security where unforeseen data threats are regularly being developed. GANs seem to be an ideal technique to train a neural network on an established attack to model similar attacks. Using GANs allows for isolating and predicting future attacks so that a designer can create enhanced security measures to fend off those attacks before they are even conceived of in the attackers minds. It can also be used as a way of creating new threats by hackers. This paper will discuss the security that has been provided and the attacks that have been modeled using GANs.

Using GANs in the field of security is a very promising area of research. An in-depth search of the literature in the area showed no previous surveys that cover the current work involving GANs in cybersecurity. The aim of this paper is to understand how GANs have been modified and used to enhance security measures. Specifically, emphasis is placed on how GANs have been used to identify threats and attacks on systems.

The paper is organized as follows: in Section II the background of GANs, its architecture, and the concept of basics of system security are presented. In Section III, the state-of-the-art security defense methods that have been setup using GANs are surveyed. Section IV discusses attack strategies where GANs have been used to model intrusions systems. Section V presents our discussions and conclusions.

II. Background

A. Generative Adversarial Network

Generative Adversarial Networks or GANs were first introduced by Ian Goodfellow in 2014 [8]. It is a two network system which contains a Generator and a Discriminator as seen in Fig. 1 [9]. The network trains in an adversarial fashion where the Generator model *G* tries to emulate the data distribution from a random noise vector which is sent to the Discriminator model *D*. *D* assesses the sample and outputs a probability value of its assessment of whether the data came from *G* or from a real data set. *G* is trained based on the output of *D*. The aim of *G* is to maximize the probability of the *D* thinking that the data is from the real dataset. The models play a zero-sum two player mini-max game where the *G* tries to maximize the probability and *D* tries to minimize it. The loss function that is used by GANs is below:

$$min_G max_D V(D,G) = \mathbb{E}_{x\sim p_{data(x)}}[logD(x)] + \mathbb{E}_{x\sim p_z(z)}[log(1-D(G(z)))] \quad (1)$$

where x is the real sample of data, z is the random noise vector, $\mathbb{E}$ represents the expectation, $G(z)$ is the data generated from the G, $D(x)$ indicates the probability of the D on the real data x and $D(G(z))$, the probability that D outputs on the generated data G. The goal of the D is to bring $D(G(z))$ closer to 0, and the goal of the G is to bring it closer to 1. If the D outputs a probability of 0.5, this would mean that the D is unable to make a decision if the sample is real or fake [8]–[10].

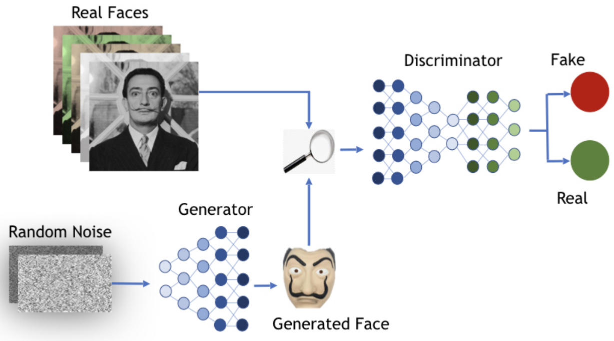

Fig. 1. Architecture of Generative Adversarial Network [9]

GANs have predominantly found success in the field of images. GANs have been utilized for Image Texture Synthesis [11], [12], Improving Image Resolution [13]–[16], and Image Generation [17]–[20]. Recently, GANs have found extensions into fields like security. GANs are being researched heavily in the realm of security as generating new, unseen threats as using a GAN gives the defense mechanism a more robust way to prepare for future attacks. The goal is to discover unknown attacks and prepare for a mechanism to defend our systems against those vulnerabilities.

B. Overview of Security

Cybersecurity plays a very important role in information technology by providing the measures for protecting systems, networks, and programs from various digital attacks. Today's world is highly connected. It is predicted that by 2030, there will be 15 connected devices owned by per person [21]. The result is a vast number of targets with wildly varying levels of protection. This makes it difficult to provide effective cybersecurity to all of those users. With the increasing number of connected devices and with the innovative approaches of attackers, cybersecurity threats are constantly evolving and the number of possible attacks only continues to increase [22].

Security is an important application for Artificial Intelligence (AI) [23]. Advancements in AI and ML algorithms ease the effort required to build more secure systems, but at the same time they create and reveal different means of breaching what are thought to be secure systems. GANs are a very new technology which provides both positive and negative changes to what is often an afterthought in system design - security.

III. GANs in Security Defenses

A. Obscuring Sensitive Information

Companies or public institutions often store very sensitive data that are unavailable to researchers. For example, healthcare organizations have a lot of sensitive information on patients. Statements and financial records are also securely stored by banks. If the secure information could be shared with researchers or analysts, this data could probably give key insights and help with further research. Research work by WWT artificial intelligence [24] shows that a well trained GAN can create new data that will be representative of the original data. Therefore, the original data can remain secure and the data generated by the GANs will likely carry the same trends and insights from the original data. The generated data indicates a close correlation with the characteristics of the original data set. This data can be further analyzed to increase the security of the original data. The authors of that research evaluated how closely the generated data is related with the original data, also testing the feasibility of building a predictive model using the generated data. Another work by Mirjalili et al. [25] mentioned that an automated analysis can potentially be misused for age-based or gender-based profiling that can undermine the use of biometrics in many applications [26]. They proposed an auto-encoder with a modified GAN which will transform an input face image, so that the transformed image can be used for facial recognition, but not for gender classification.

B. *Cyber Intrusion and Malware Detection*

Cyber intrusions are used to attack and compromise a computer by breaking the security system or by making the environment unsafe for operation. The results of cyber intrusions are many fold, such as unauthorized publication of information, tampering, and destruction of information. An Intrusion Detection System (IDS) monitors the network and detect any malicious activities and also alerts the user when it finds any such activity. Researchers have been exploring different IDSs using statistical learning and NNs [27]. Chen et al. [28] showed in their work that a GAN-based model can be a very successful candidate for implementing an IDS. GANs are used in intrusion detection by learning the features of normal data. In their work Chen, et al. have proposed a GAN-based model with a refined loss function and with multiple intermediate layers to gain moderate decisions from the discriminator.

Researchers have been using GANs for malware detection as well. Malware is software intentionally designed to damage a computer system. Not all intrusions involve malware. Anderson et al. [29] demonstrated adversarially-tuned generation of a domain and also showed that by augmenting the training set with generated adversarial examples, the classifier is able to detect more malware families than using other approaches. Burks et al. [30] demonstrated a comparative study between GANs and Variational Autoencoder (VAE) models and concluded that by using GANs malware detection effectiveness improved.

Several researchers have also proposed new defense strategies and algorithms against different attacks by using GANs. Samangouei et al. [31] proposed Defense-GAN, which is trained to model the distribution of unperturbed images. Their proposed GAN can be used as a defense against different attack methods and also improves on existing defense strategies. Most of the existing defense strategies are attack model specific. Defense-GAN can be used with any classifier and on any attack by leveraging the generative power of GANs. Yu et al. [32], and Zhao et al. [33] also demonstrated successful defense mechanisms against attacks by using GANs.

C. *Secure Image Steganography*

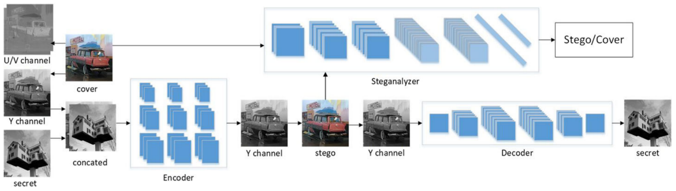

Fig. 2. Architecture of ISGAN [34]

Steganography is a process of hiding secret data within an image [35]. In this technique the image that is used to hide the data is called the cover and the image containing the embedded hidden message is called the stego image. Unlike cryptography, steganography tries to hide the presence of the message. GANs can be used to perform secure image steganography. Hayes et al. [36] described a design scheme of a steganographic algorithm, which is produced in an unsupervised manner by a GAN based model. Recently, more research has been done on image steganography by using GANs. Zhang et al. [34] proposed a novel Convolutional Neural Network (CNN) architecture named ISGAN as seen in Fig. 2. In the steganography process, their design conceals a gray image inside a color cover image. They use GANs to strengthen the security by minimizing the divergence of empirical probability distributions between the stego image and the cover image. Shi et al. [37] proposed a strategy of secure steganography based on GANs to improve the perceptibility, the security, and the diversity by making the generated images suitable for embedding. In Volkhonskiy et al. [38] the author proposed a new model for generating image-like containers based on Deep Convolutional Generative Adversarial Networks (DCGAN) [39]. Tang et al. [40] proposed a framework, which can automatically learn embedding change probabilities for every pixel in a given spatial cover image, which can further help to produce minimal-distortion embedding. Zhang et al. [41] proposed an information hiding scheme for steganography by using Auxiliary Classifier Generative Adversarial Networks (AC-GANs) [42]. Liu et al. [43] presented an automated framework of grille cipher, which simultaneously satisfies both channel and content security for secure communication in steganography. Such results should be expected because GANs are predominantly an image based method. Since steganography also deals with images, using GANs has turned into a powerful security measure and popular research topic.

D. *Neural Cryptography*

Neural Cryptography is an emerging field of research which combines NNs and cryptography. GANs play a vital role in this field. Wu et al. [44] demonstrated in their work the concept of biometric cryptography, in which they encrypted facial features by using Wasserstein Generative Adversarial Networks Encryption (WGAN-E) [45]. Abadi et al. [46] proposed

TABLE I
GANs in Security Defenses

Purpose	References	GAN Type
Obscuring Sensitive Information	WWT AI [24]	Vanilla GAN [8]
	Mirjalili et al. [25]	Modified version of GAN
Cyber Intrusion and Malware Detection	Chen et al. [28]	BiGAN [50]
	Anderson et al. [29]	Vanilla GAN
	Burks et al. [30]	Vanilla GAN
	Samangouei et al. [31]	WGAN [45]
	Yu et al. [32]	CGAN [51]
	Zhao et al. [33]	WGAN
Secure Image Steganography	Hayes et al. [36]	Vanilla GAN
	Zhang et al. [34]	Vanila GAN
	Shi et al. [37]	WGAN
	Volkhonskiy et al. [38]	DCGAN [39]
	Tang et al. [40]	Vanilla GAN
	Zhang et al. [41]	AC-GAN [42]
	Liu et al. [43]	GAN/DCGAN
Neural Cryptography	Wu et al. [44]	WGAN
	Abadi et al. [46]	Vanilla GAN
Security Analysis	Chhetri et al. [48]	CGAN

an adversarial method to protect a communication channel without a cryptographic algorithm. In their architecture, two NN systems are trained to defeat a third NN which attempts to intercept any message that is being sent, emulating the operations of a GAN.

E. Security Analysis

Cyber Physical Production Systems (CPPSs) are an emerging system which brings the electronic and the physical security layers together into a common infrastructure. The economic and the social importance of such a system is vast. CPPS is the integration of computation, networking, and physical processes of autonomous and connected subsystems [47]. Cross domain security analysis between the cyber and physical systems is a very important research topic and GANs can help to determine that the various security components (Confidentiality, Availability, and Integrity) are met. Chhetri et al. [48] suggested the GAN-Sec system, a GAN based security analysis model. GAN-Sec analyzes security by taking into consideration the signal and the energy flows of a system. As a case study to show the applicability of GAN-Sec, the authors provided a security analysis of an additive manufacturing system. The results show that the proposed model can be used for security analysis of confidentiality breach through side-channels attacks [49]. Gan-Sec can also help estimating the performance of an integrity and availability attack detection model.

IV. GANs in Security Attacks

A. Breaking (Cracking) Ciphers

Ciphertexts are encoded or encrypted messages that are used to protect the integrity of data by obscuring patterns. Encryption is the method of converting raw data into ciphertexts using encryption algorithms to save the data from being access by an unauthorized user. Symmetric Encryption is a form of encryption where the sender and the receiver use the same key to encrypt and decrypt the data of the message [52]. However, neural networks have evolved to be able to train on their mutual outputs to perform decryption. This has lead to a new emergent field called Neural Cryptography which combines NNs in the application of cryptography and cryptanalysis. Secret keys can be generated by synchronizing the output weights of two neural networks [53].

Cipher cracking is one such concept developed by Gomez et al. [54]. The authors use CycleGANs [55] where a source image can be translated into a target image by maintaining a cyclic consistency. The model learns the mapping from the source image and projects onto the target image in a way that the target image is now indistinguishable from the source image using an adversarial loss. Using this concept in cryptography, Gomez et al. [54] proposed using this cyclic consistency on discrete data to derive a cipher mapping from unpaired ciphertext and plaintext. Their architecture is more stable than CycleGAN and has achieved good results on larger messages and files encrypted by the shift and Vigenère ciphers with high degree of confidence. The proposed methodology can also be applied to different forms of cipher and to different underlying data.

B. Password Guessing

Password cracking, or password guessing, is a kind of an attack method that is used to guess a password by a brute force [49] attack. Tools like HashCat [56] and John the Ripper [57] present billions of possible passwords against password hashes or use dictionary attacks to concatenate different words to guess passwords. To improve the quality of password guessing, Hitaj et al. [58] used GANs to conduct and improve this attack. PassGAN uses the improved Wasserstein GAN [45] to learn from the data distribution of the billions of leaked passwords and uses that result to generate higher quality password guesses. *D* uses verified, known, leaked examples to train the *G* to emulate false passwords that are very close to the real password data distribution achieving higher accuracy than HashCat and John the Ripper.

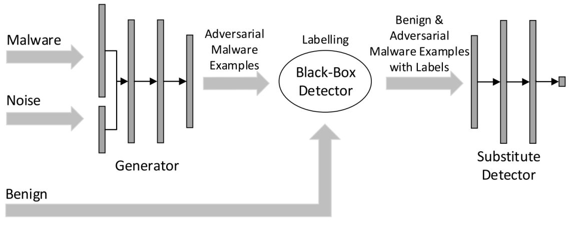
Malware
Noise
Generator
Benign
Adversarial Malware Examples
Labelling
Black-Box Detector
Benign & Adversarial Malware Examples with Labels
Substitute Detector

Fig. 3. Architecture of MalGAN [59]

Nam et al. proposed an enhancement to PassGAN increasing performance by 15% [60]. The authors used the two fold approach of first changing the current loss function to a Recurrent Neural Network (RNN) based loss function and next, they changed the architecture to a dual-discriminator network. The generator is tasked to create a pseudo password that is very similar to the authentic password. The first discriminator is set up to find only the genuine password and the second is to look for the pseudo passwords in the sample. If the generator is successful in defeating both the discriminators, then it has generated a password which neither discriminator has been able to detect. Experiments showed that the RNN based model with the dual discriminator did better by decreasing the redundancy of password guesses [60].

C. *Malware Generation and Attacks Against Intrusion Detection Systems*

Some commonly used examples of malware are viruses, worms, and Trojan horses [61]. As noted in Section III-B, GANs have been used to make IDSs stronger, but a downside of ML is that GANs can also be used to generate malware to bypass an IDS as shown in Fig. 3 by Hu et al [59] known as MalGAN. This attack generated adversarial malware examples by training on input noise and malware examples which is then sent to a substitute neural network detection system along with benign example. The GAN is trained to minimize the malicious properties so that the substitute detector can be bypassed. The probability distribution on the attack can be changed as soon as the IDS comes close to understanding the attack which can make it unpredictable. Improved MalGAN [62] was proposed by Kawai et al., where the authors injected more non-malware and a single instance of malware to decrease the maliciousness of the attack. This combination of software is sent to a substitute detector that is used as an imitative detector that the data will be sent through later. The generator is trained on this local detector to disguise the data so that it is not classified as malware by the IDS. After this step, the data is sent to the actual detector. The attack achieved better performance than MalGAN.

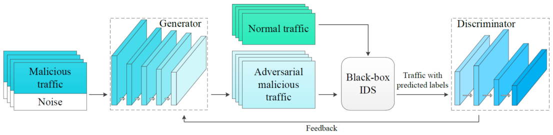

Fig. 4. Architecture of IDSGAN [63]

Rigaki and Garcia [64] proposed a GAN to generate network traffic to simulate other networks. The GAN changes the network behavior of malware and makes the detection system believe that the generated network is from a genuine application. Experiments were conducted to use a GAN to emulate real Facebook chat traffic and keep communicating the changes to the malware. The malware is updated by the generator of the trained chat traffic and avoids being detected. If the malware is detected at any point, the GAN is trained for more cycles on the trusted traffic and the malware is updated again in an effort to remain undetected. The results have shown GAN-modified malware is virtually undetectable, easily bypassing the detection systems. IDSGAN is another such attack that was developed by Lin et al. [63] to point out the drawbacks of an IDS. As seen in Fig. 4, IDSGAN uses a WGAN network to produce new malicious data from an existing dataset with the discriminator then working on distinguishing the normal traffic from the malicious traffic. This attack is sent to an IDS and the output of the IDS is sent to the discriminator so that it simulates the IDS. Lin et al. achieved good results as the detection rates for malware dropped from 70% to lower than 1%. A similar approach was taken by Lin et al. [65] for Denial of Service (DoS) attacks [66]. The author modified only portions of the attack that are unimportant to the DoS attack and preserved the functional features. This allowed the authors to reduce the current true positive rates by half to 47.6% [67].

TABLE II
GANs in Security Attacks

Purpose	References	GAN Type
Cipher Cracking	Gomez et al. [54]	CycleGAN [55]
Password Guessing	Hitaj et al. [58]	IWGAN [72]
	Nam et al. [60]	IWGAN/ RNN
Malware Generation and Attacks Against Intrusion Detection Systems	Hu et al. [59]	Vanilla GAN
	Kawai et al. [62]	Vanilla GAN
	Rigaki and Garcia [64]	Vanilla GAN
	Lin et al. [63]	WGAN
	Lin et al. [65]	WGAN
	Singh et al. [68]	AC-GAN
	Corley et al. [69]	LSGAN [71], WGANGP [72], Vanilla GAN

A lack of sufficiently labeled datasets has been an issue for generating malware attacks. To address this issue, Singh et al. [68] suggested a data augmentation technique of using AC-GANs [42] to generate more labeled datasets from existing malware images. AC-GANs have been able to make training more stable and robust. The augmentation technique has been able to give malware databases a boost with an increasing number of examples to help with training.

Corley et al. [69] have shown how botnets create and use domains as an assembly point for other botnets. Botnets [70] are a group or network of infected computers that are being controlled as a group to accomplish some task. Regular Domain Generator Algorithms (DGA) can be easily detected and hacked by ML techniques. This flaw is addressed by using three different GANs to improve DGAs in a network which is called DomainGAN [69] to make it difficult to be detected. The three versions of GANs used were LSGAN [71], WGANGP [72] and vanilla GAN [8] and a comparative analysis was done to show which GAN preformed best. Among these models, WGANGP produced the best results with DGA for generating a usable domain and GAN based DGAs for limiting detection.

V. Discussion and Conclusion

Table I lists research which has been done on GANs in security and Table II lists research which has been done using GANs on security attacks. GANs are a relatively new technology and therefore security applications research based on this technology also only began recently. Information security is an important research topic in the present computing environment. Applying GANs to security can be seen as a very powerful step forward and a valuable tool to analyze and be applied to cybersecurity issues. To date, GANs have shown promise in generating new defense techniques in the field of cyber intrusion, malware detection, and secure image steganography, although applicable research has been limited. From a security attack viewpoint, a lot of the available research has been centered on malware generation for IDSs. The new generated attacks or malware provide knowledge about previously unknown attacks and therefore helps to update defense mechanisms. This makes the research on attacks using GANs even more important.

The survey includes recent GANs research ranging from topics as diverse as image steganography and neural cryptography to malware generation, with the aim of training the system to defend itself better during adverse attack scenarios, showing us the different research opportunities for combining NNs with cybersecurity. The paper also discusses several different kinds of GANs and GAN variations that have been used by researchers to address meaningful security scenarios. It elaborates on how GANs have been used to enhance surveillance in areas like security protocols and strengthening detection systems to battle data sensitivity, work on making a better intrusion detection system, secure image steganography, neural cryptography, and security analysis. Further, GANs are being used for improving malware and intrusion attacks. The effectiveness of GANs resonate in the fact that it helps create new and unknown attacks that can point out vulnerabilities of defense systems. Researchers have trained systems to generate attacks which are difficult to be recognized and can easily circumvent detection systems. These methods can be then used to harden a software from further attacks. We have examined the architecture of these networks and the variations of GANs that have been used and discuss the results achieved in both defense and attack situations. Indeed, GANs should be developed for use in testing the robustness of security in products released by companies. GANs can produce tests for a set of known and unknown attacks that will result in significantly stronger computers, computer based products, and IoT devices. Presently, the use of GANs in security is in its infancy, but it should not remain there long.

References

[1] "Number of connected devices worldwide 2030 — Statista." [Online]. Available: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

[2] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight cryptography for internet of insecure things: A survey," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0475–0481.

[3] K. Khalil, K. Elgazzar, A. Ahmed, and M. Bayoumi, "A Security Approach for CoAP-based Internet of Things Resource Discovery," *IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020.

[4] "What is a cyber attack? Recent examples show disturbing trends — CSO Online." [Online]. Available: https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

[5] "A ransomware attack took The Weather Channel off the air - The Verge." [Online]. Available: https://www.theverge.com/2019/4/19/18507869/weather-channel-ransomware-attack-tv-program-cable-off-the-air

[6] "2019 Capital One Cyber Incident — What Happened — Capital One." [Online]. Available: https://www.capitalone.com/facts2019/

[7] "Ransomware Attack Hits 22 Texas Towns, Authorities Say - The New York Times." [Online]. Available: https://www.nytimes.com/2019/08/20/us/texas-ransomware.html

[8] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative Adversarial Networks," *NIPS'14: Proceedings of the 27th International Conference on Neural Information Processing Systems*, vol. Volume 2, no. December 2014, pp. 2672–2680, 2014.

[9] B. Ghosh, I. K. Dutta, M. Totaro, and M. Bayoumi, "A Survey on the Progression and Performance of Generative Adversarial Networks," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. Kharagpur: IEEE, jul 2020, pp. 1–8.

[10] Z. Pan, W. Yu, X. Yi, A. Khan, F. Yuan, and Y. Zheng, "Recent Progress on Generative Adversarial Networks (GANs): A Survey," *IEEE Access*, vol. 7, no. c, pp. 36 322–36 333, 2019.

[11] U. Bergmann, N. Jetchev, and R. Vollgraf, "Learning texture manifolds with the periodic spatial gan," *arXiv preprint arXiv:1705.06566*, 2017.

[12] N. Jetchev, U. Bergmann, and R. Vollgraf, "Texture synthesis with spatial generative adversarial networks," *arXiv preprint arXiv:1611.08207*, 2016.

[13] D. Mahapatra, B. Bozorgtabar, and R. Garnavi, "Image super-resolution using progressive generative adversarial networks for medical image analysis," *Computerized Medical Imaging and Graphics*, vol. 71, pp. 30–39, 2019.

[14] M. Zareapoor, M. E. Celebi, and J. Yang, "Diverse adversarial network for image super-resolution," *Signal Processing: Image Communication*, vol. 74, pp. 191–200, 2019.

[15] X. Wang, K. Yu, S. Wu, J. Gu, Y. Liu, C. Dong, Y. Qiao, and C. C. Loy, "Esrgan: Enhanced super-resolution generative adversarial networks," *European Conference on Computer Vision*, pp. 63–79, 2018.

[16] J. Guan, C. Pan, S. Li, and D. Yu, "Srdgan: learning the noise prior for super resolution with dual generative adversarial networks," *arXiv preprint arXiv:1903.11821*, 2019.

[17] J. Y. Zhu, T. Park, P. Isola, and A. A. Efros, "Unpaired Image-to-Image Translation Using Cycle-Consistent Adversarial Networks," *Proceedings of the IEEE International Conference on Computer Vision*, vol. 2017-Octob, pp. 2242–2251, 2017.

[18] P. Isola, J. Y. Zhu, T. Zhou, and A. A. Efros, "Image-to-image translation with conditional adversarial networks," *Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017*, vol. 2017-Janua, pp. 5967–5976, 2017.

[19] A. Nguyen, J. Clune, Y. Bengio, A. Dosovitskiy, and J. Yosinski, "Plug and play generative networks: Conditional iterative generation of images in latent space," *Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017*, vol. 2017-Janua, no. 1, pp. 3510–3520, 2017.

[20] C. H. Lin, C.-C. Chang, Y.-S. Chen, D.-C. Juan, W. Wei, and H.-T. Chen, "Coco-gan: generation by parts via conditional coordinating," in *Proceedings of the IEEE International Conference on Computer Vision*, 2019, pp. 4512–4521.

[21] "By 2030, Each Person Will Own 15 Connected Devices. Here's What That Means For Your Business and Content. — MarTech Advisor." [Online]. Available: https://www.martechadvisor.com/articles/iot/by-2030-each-person-will-own-15-connected-devices-heres-what-that-means-for-your-business-and-content/

[22] McAfee, "McAfee Labs Threats Report," McAfee Labs, Tech. Rep., 2019.

[23] "What to Expect from AI and Cyber Security Roles in the Future - CCSI." [Online]. Available: https://www.ccsinet.com/blog/what-to-expect-from-ai-and-cyber-security-roles-in-the-future/

[24] W. A. I. R. . Development, "Obscuring and Analyzing Sensitive Information with Generative Adversarial Networks," World Wide Technology, Tech. Rep., 2019.

[25] V. Mirjalili, S. Raschka, A. Namboodiri, and A. Ross, "Semi-Adversarial Networks: Convolutional Autoencoders for Imparting Privacy to Face Images," in *11th IAPR International Conference on Biometrics (ICB 2018). Gold Coast, Australia*, 2018.

[26] "Perpetual Line Up - Unregulated Police Face Recognition in America." [Online]. Available: https://www.perpetuallineup.org/

[27] D. P. A. R. Vinchurkar, "A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique," *International*

Journal of Engineering Science and Innovative Technology (IJESIT) Volume 1, Issue 2, November 2012, 2012.

[28] H. Chen and L. Jiang, "Efficient GAN-based method for cyber-intrusion detection," *ArXiv*, 2019.

[29] H. S. Anderson, J. Woodbridge, and B. Filar, "Deepdga: Adversarially-tuned domain generation and detection," in *Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security*, 2016, pp. 13–21.

[30] R. Burks, K. A. Islam, Y. Lu, and J. Li, "Data augmentation with generative models for improved malware detection: A comparative study," in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2019, pp. 0660–0665.

[31] P. Samangouei, M. Kabkab, and R. Chellappa, "Defense-gan: Protecting classifiers against adversarial attacks using generative models," *arXiv preprint arXiv:1805.06605*, 2018.

[32] F. Yu, L. Wang, X. Fang, and Y. Zhang, "The Defense of Adversarial Example with Conditional Generative Adversarial Networks," *Security and Communication Networks*, vol. 2020, pp. 1–12, aug 2020.

[33] Z. Zhao, D. Dua, and S. Singh, "Generating natural adversarial examples," *arXiv preprint arXiv:1710.11342*, 2017.

[34] R. Zhang, S. Dong, and J. Liu, "Invisible steganography via generative adversarial networks," *Multimedia Tools and Applications*, vol. 78, pp. 8559–8575, 2019.

[35] S. Bhallamudi, "Image Steganography, Final project – Report," Wright State University, Tech. Rep. March, 2015.

[36] J. Hayes and G. Danezis, "Generating steganographic images via adversarial training," in *Advances in Neural Information Processing Systems*, 2017, pp. 1954–1963.

[37] H. Shi, J. Dong, W. Wang, Y. Qian, and X. Zhang, "SSGAN: Secure steganography based on generative adversarial networks," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10735 LNCS, pp. 534–544, 2018.

[38] D. Volkhonskiy, I. Nazarov, B. Borisenko, and E. Burnaev, "Steganographic generative adversarial networks," *arXiv preprint arXiv:1703.05502*, 2017.

[39] A. Radford, L. Metz, and S. Chintala, "Unsupervised representation learning with deep convolutional generative adversarial networks," *arXiv preprint arXiv:1511.06434*, 2015.

[40] W. Tang, S. Tan, B. Li, and J. Huang, "Automatic Steganographic Distortion Learning Using a Generative Adversarial Network," *IEEE Signal Processing Letters*, vol. 24, no. 10, pp. 1547–1551, oct 2017.

[41] Z. Zhang, G. Fu, J. Liu, and W. Fu, "Generative information hiding method based on adversarial networks," in *Advances in Intelligent Systems and Computing*, vol. 905. Springer Verlag, aug 2020, pp. 261–270.

[42] A. Odena, C. Olah, and J. Shlens, "Conditional image synthesis with auxiliary classifier gans," in *International conference on machine learning*, 2017, pp. 2642–2651.

[43] J. Liu, Y. Ke, Y. Lei, J. Li, Y. Wang, Y. Han, M. Zhang, and X. Yang, "The reincarnation of grille cipher: A generative approach," *arXiv preprint arXiv:1804.06514*, 2018.

[44] C. Wu, B. Ju, Y. Wu, N. N. Xiong, and S. Zhang, "WGAN-E: A generative adversarial networks for facial feature security," *Electronics (Switzerland)*, vol. 9, no. 3, 2020.

[45] M. Arjovsky, S. Chintala, and L. Bottou, "Wasserstein generative adversarial networks," in *34th International Conference on Machine Learning, ICML 2017*, 2017.

[46] M. Abadi and D. G. Andersen, "Learning to protect communications with adversarial neural cryptography," *arXiv preprint arXiv:1610.06918*, 2016.

[47] L. Monostori, "Cyber-Physical Systems Theory and Application," in *CIRP Encyclopedia of Production Engineering*. Springer Berlin Heidelberg, 2018, pp. 1–8.

[48] S. R. Chhetri, A. B. Lopez, J. Wan, and M. A. Al Faruque, "GAN-Sec: Generative Adversarial Network Modeling for the Security Analysis of Cyber-Physical Production Systems," in *Proceedings of the 2019 Design, Automation and Test in Europe Conference and Exhibition, DATE 2019*. Institute of Electrical and Electronics Engineers Inc., may 2019, pp. 770–775.

[49] P. Jorgensen, *Applied cryptography: Protocols, algorithm, and source code in C*, 2nd ed. New York: John Wiley and Sons Inc., 1996, vol. 13, no. 3.

[50] J. Donahue, P. Krähenbühl, and T. Darrell, "Adversarial feature learning," *arXiv preprint arXiv:1605.09782*, 2016.

[51] M. Mirza and S. Osindero, "Conditional generative adversarial nets," *arXiv preprint arXiv:1411.1784*, 2014.

[52] I. Kalyan Dutta, B. Ghosh, A. H. Carlson, and M. Bayoumi, "Lightweight polymorphic encryption for the data associated with constrained internet of things devices," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020, pp. 1–6.

[53] W. Kinzel and I. Kanter, "Neural cryptography," in *Proceedings of the 9th International Conference on Neural Information Processing, 2002. ICONIP'02.*, vol. 3. IEEE, 2002, pp. 1351–1354.

[54] A. N. Gomez, S. Huang, I. Zhang, B. M. Li, M. Osama, and L. Kaiser, "Unsupervised cipher cracking using discrete gans," *arXiv preprint arXiv:1801.04883*, 2018.

[55] J.-Y. Zhu, T. Park, P. Isola, and A. A. Efros, "Unpaired image-to-image translation using cycle-consistent adversarial networks," in *Proceedings of the IEEE international conference on computer vision*, 2017, pp. 2223–2232.

[56] "hashcat - advanced password recovery." [Online]. Available: https://hashcat.net/hashcat/

[57] "John the Ripper password cracker." [Online]. Available: https://www.openwall.com/john/

[58] B. Hitaj, P. Gasti, G. Ateniese, and F. Perez-Cruz, "Passgan: A deep learning approach for password guessing," in *International Conference on Applied Cryptography and Network Security*. Springer, 2019, pp. 217–237.

[59] W. Hu and Y. Tan, "Generating adversarial malware examples for black-box attacks based on gan," *arXiv preprint arXiv:1702.05983*, 2017.

[60] S. Nam, S. Jeon, H. Kim, and J. Moon, "Recurrent gans password cracker for iot password security enhancement," *Sensors (Switzerland)*, vol. 20, no. 11, pp. 1–19, 2020.

[61] S. Madani, M. R. Madani, I. K. Dutta, Y. Joshi, and M. Bayoumi, "A hardware obfuscation technique for manufacturing a secure 3d ic," in *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2018, pp. 318–323.

[62] M. Kawai, K. Ota, and M. Dong, "Improved MalGAN: Avoiding Malware Detector by Leaning Cleanware Features," in *1st International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2019*. Institute of Electrical and Electronics Engineers Inc., mar 2019, pp. 40–45.

[63] Z. Lin, Y. Shi, and Z. Xue, "Idsgan: Generative adversarial networks for attack generation against intrusion detection," *arXiv preprint arXiv:1809.02077*, 2018.

[64] M. Rigaki and S. Garcia, "Bringing a gan to a knife-fight: Adapting malware communication to avoid detection," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 70–75.

[65] Q. Yan, M. Wang, W. Huang, X. Luo, and F. R. Yu, "Automatically synthesizing DoS attack traces using generative adversarial networks," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 12, pp. 3387–3396, dec 2019.

[66] "Understanding Denial-of-Service Attacks — CISA." [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST04-015

[67] N. Martins, J. M. Cruz, T. Cruz, and P. H. Abreu, "Adversarial machine learning applied to intrusion and malware scenarios: a systematic review," *IEEE Access*, vol. 8, pp. 35 403–35 419, 2020.

[68] A. Singh, D. Dutta, and A. Saha, "MIGAN: Malware Image Synthesis Using GANs," *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 33, pp. 10 033–10 034, 2019.

[69] Isaac Corley, Jonathan Lwowski, Justin Hoffman, and Booz Allen Hamilton, "DomainGAN: Generating Adversarial Examples to Attack Domain Generation Algorithm Classifiers." [Online]. Available: https://www.groundai.com/project/domaingan-generating-adversarial-examples-to-attack-domain-generation-algorithm-classifiers/1

[70] Malware, "What is a Botnet?" Norton, Tech. Rep., 2020. [Online]. Available: https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

[71] X. Mao, Q. Li, H. Xie, R. Y. Lau, Z. Wang, and S. P. Smolley, "Least Squares Generative Adversarial Networks," *Proceedings of the IEEE International Conference on Computer Vision*, vol. 2017-Octob, pp. 2813–2821, 2017.

[72] I. Gulrajani, F. Ahmed, M. Arjovsky, V. Dumoulin, and A. C. Courville, "Improved training of wasserstein gans," in *Advances in neural information processing systems*, 2017, pp. 5767–5777.