Cyber Breaches in Smart Toilets

Prepared for: Dr. Nir Nassim, Head of Malware Lab, BGU

Prepared by: Jubeen Shah & Aditya Pratap Singh

31 July 2016

ABSTRACT

With the advent of the IOT environment, we now even have Smart Toilets to analyse human excreta. These devices can be used to measure and monitor the human excreta and provide calculative actions to not only the consumers but also send the data to the hospitals for better efficiency in providing healthcare facilities to the various patients. If such a system is compromised using various malicious methodologies, several damaging effects can occur.

In this paper what we're trying to cover is the potential ways in which Smart Toilets can be attacked and how these Cyber Attacks can have adverse effects on our life directly and indirectly. We would also be providing solutions based on Machine Learning methods to tackle and avoid such Cyber Attacks to build a system which is very secure, to protect not only the Private Data of the consumer but also prevent the Smart Toilet systems to act as a hub for further penetration into the house or organisation.

INTRODUCTION

Internet Of Things or IOT as we all know it has its roots spread far and wide with almost 50 Billion connected devices by the year 2020. The devices in this domain include devices such as Smart Watches, Smart Refrigerators, Smart Televisions, Smart ToothBrush and the list goes on. The objective of these devices is to strengthen usability and absorb more functionality.

Since the paper revolves around the notion of Cyber Attacks on Smart Toilets, we would start off by explaining what Smart Toilets are; which in basic terms could be described as internet connected toilet essentially used with the purpose of human excreta analysis. This analysis could give us insights about the medical information about a user, which can essentially be used to predict future diseases which the patient can be diagnosed with. This could potentially help the patient to get a treatment before he is actually diagnosed with a disease. The interpretation could also help the doctors to better treat the disease that the patient has been diagnosed with already. In this paper, we would focus more on *Urinalysis,* however the fact that stool analysis could give us a deeper insight into the health of the patient cannot be ignored.

Urinalysis Defined

Starting off with the very basics, *Urinalysis* can be defined as *the physical, chemical, and microscopic examination of urine. It involves a number of tests to detect and measure various compounds that are passed through the urine.* Urinalysis is a very basic test and is required by most doctors to get a deeper understanding about the patient before further tests are requested.

Urinalysis Explained

Today, *Urinalysis* is essentially done at clinics and the reports are available after a period of approximately 12 Hours, which in some cases could be considered a very long time. Smart Toilets reduces this time frame to a significantly shorter time and increases accessibility since this system is installed at the user's home. The Smart Toilets would analyse the urine sample in real time and sends the report over a WiFi network or Bluetooth to the user's PC or Smartphone. The user can then manually send this report to the Doctor in case of abnormalities as indicated by the system or in cases where the user has to send the reports every week, for example in case of Diabetics.

Urinalysis involves collection of the samples, and scanning the various aspects of the sample such as the colour and appearance, the microscopic appearance and the chemical composition of the Urine sample. Each of the aspect of the urine sample is an indication as to whether the patient is in good health or not. For example a deep yellow colour would indicate dehydration, whereas light yellow sample colour would indicate no abnormalities in the health. The presence of certain chemical components such as nitrites or proteins in the urine would indicate some irregularity in the health.

Also urinalysis measures the levels and detect presence of various chemical components of such as *proteins, ketones, bilirubin, nitrites, glucose, red blood cells, white bloods cells and the pH* of the urine. Each component either independently or in combination with other compounds beyond a certain limit can prove to be very unsafe to human health.

Normal Urine Levels

Table 1

Component	Average Range/Value
pH	5.5 - 7
Specific Gravity	1.003 - 1.035
Carbon	6.87 g/L
Nitrogen	8.12 g/L
Hydrogen	1.51 g/L
Red Blood Cells	0 - 3 HPF
White Blood Cells	0 - 2 HPF
Blood Sugar Level	70 - 140 mg/ dL

Table 1. gives us a general information about the normal levels in the components of urine.[1]

CYBER ATTACKS IN SMART TOILETS

It indeed is valuable to understand the importance of seclusion of meaningful data and with everything connected, we have to make sure that it doesn't recoil on ourselves. As per reports *70 Percent of IoT Devices are Vulnerable to Cyberattacks:* [2] *According to HP's report,"Internet of Things Security: State of the Union", a total of 250 security holes have been found in the tested IoT devices — on average, 25 per device.* The major cyber loop holes in the smart toilets can be identified as follows:

- **Wireless attacks**
- **Malicious Emails**
- **Lack of Encryption**
- **Man in the Middle**
- **Smartphone Malware**
- **Supply Chain Attack**
- **Social Engineering**

Wireless attacks

Wifi attacks can be one of the major reasons for Cyber Attacks on Smart Toilet systems. The transmission of data from the smart toilet system to the victim's PC or smartphone happens over a wireless network that involves using the Wifi because of increased accessibility. The associations that the Smart Toilet makes with a WiFi network can be both accidental and malicious.[3]

In the accidental association the Smart Toilet system can latch onto a wireless access point from a neighbour's overlapping network and the user may not even know that this has occurred.

[1] https://medlineplus.gov/ency/article/003579.htm
https://labtestsonline.org/understanding/analytes/urinalysis/tab/test/

[2] http://www.securityweek.com/70-iot-devices-vulnerable-cyberattacks-hp

[3] http://infosecawareness.in/downloads/handbooks/wifi-security-ebook.pdf

In case of malicious associations, the attacker actively makes a wireless device to connect to a victim's network through cracking their laptop, instead of the Access Point. The attacker creates these *"Soft APs"[1]* to disguise itself as a legitimate access point. Once the access is gained, the attacker can not only steal private information but also embed trojans which in our case can also manipulate the victim's data which is primarily sent to the Doctor on a periodic basis for further research and development of the victim's health related issues.

Non traditional networks such as Bluetooth devices are vulnerable to cracking and should be regarded as a security risk, as most of the IOT devices today even communicate over an insecure Bluetooth connection with the smartphone and can be compromised by the attacker if he turns out to be the neighbour of the victim or is in the vicinity of such transactions while in a hospital or a large corporation.

Network injection and Caffe Latte Attacks should can also be a source of efficient attacks launched by the attacker where in the attacker exploits non-filtered network traffics. The attacker can reconfigure networks that can affect the routers, switches and other intelligent hubs in a large corporation or a Hospital. The attacker does not have to necessarily be in the vicinity of the victim to launch an attack. He can remotely target the Windows Wireless Stack and obtain the WEP key from the victim, by exploiting the flaws of 802.11 WEP.

Other ways of compromising the wireless system in large companies where such Smart Toilets are installed is by Ad-hoc networks which are essentially peer to peer networks between wireless computers that do not have an access point in between them.

Malicious Emails

Malicious Emails can be sent by the attacker to the victim which might either contain a malicious file or link to an malicious Website which the user might be tricked into opening, which would result in downloading a malware on the device that would essentially rig the entire System. The malware could be designed in a way to manipulate data being recorded and also steal the original data at the same time to be used by the attacker to sell.

At the same time the malware can also be designed to infect every other file which the user might send in an email to other potential victims including the doctor. Once the doctor is infected with the malware, the same malware can be used to infect other patients thereby exponentially spreading the malware to more and more potential victims thereby causing a mass outrage among users of the Smart Toilet system which may receive wrong treatment based on the results.

Lack of Encryption

HP says 70% of tested IoT devices don't encrypt Internet and local network communications, with half of their applications lacking transport encryption. For 60% of devices, manufacturers haven't ensured that software updates are downloaded in a secure manner, in some cases enabling attackers to intercept them.

So attacking the smart toilet system can be carried out in similar ways, where the transported data is not being encrypted and someone can grab hold of this *data in movement* thereby infiltrating the privacy of the patient. Not only that, but also the attacker can place a dummy server to which the Smart Toilet system can accidentally connect, in order to make system updates. This fetching of new update could happen over an unauthenticated server in an insecure manner which could have a malicious copy of the software.

Man in the Middle

They are possible by exploiting inherent vulnerabilities of the TCP/IP protocol at various layers.[4] If carried out properly, users can be completely oblivious to this attack, making it difficult to detect and stop. At a macro level, the steps involved are to intercept traffic, break the authentication chain, and impersonate the endpoints seamlessly.

In such a scenario the attacker can be spoofing a connection between the victim and the doctor while not only stealing the data but also manipulating the data while the data is in movement. Sophisticated attacks are very difficult to

[4] http://www.idc-online.com/technical_references/pdfs/information_technology/Cyber_Attacks_-Explained_The_Man_In_The_Middle.pdf

detect and raises flags for concern for privacy amongst the patients and even the vendors of the Smart Toilet system.

Smartphone Malware

Smartphone malware can be one of the several routes the attacker can take to steal data from the user. Malware on smartphone can be very harmful, because usually the IOT device, in our case the Smart Toilet System would establish a connection with the smartphone most of the times for user accessibility. The malware on the smartphone can not only cause Data Leakage but also manipulate the data from the Smart Toilet System before sending it to the doctor. Manipulation of data is one of the many key concerns which will affect a huge community of people as described later in the paper.

Supply Chain Attack

It is a type of cyber attack which damages the organisations's reputation by targeting less secure elements in the supply network. The attacker can tamper with the manufacturing process by installing a *rootkit* which can in essence infect every smart toilet before it even reaches the end consumer. Such an attack is very sophisticated since the attacker does not have to explicitly infect one potential victim at a time, and can in theory affect a large number of people at the same time from different spheres like the patients, the doctors, the large corporate companies etc.

Social Engineering

Social engineering is essentially the art of stealing information from the victim in a way that he is tricked into giving in the private information voluntarily. This way of cyber attack of gaining information from the patients or even doctors is very sophisticated, because the attacker can be very convincing at exfiltrating the information from either of them. This attack can be difficult to stop without user awareness.

EFFECTS

As we have seen how the attackers can attack the smart toilet system and gain access to almost the entire network by exploiting vulnerabilities. Once the attacker has gained access into the system and planted a malware, the capabilities of the malware can be designed as per the use for the attacker. But we would be focused more on the fact that the attacker can manipulate the data that he has access to.

In this section we would like to focus more on how the cyber attacks can directly or indirectly affect the life of not only the life of not only the consumer but also the vendor in various ways which is not only life threatening but also can result in large amount of monetary loss in several aspects.

These smart toilet systems as mentioned previously are not only used by patients in their own private homes but also by doctors at their own private clinic or hospitals. These smart devices are even used in large corporation where *drug test* is mandatory for not only potential employees but also existing employees to discourage the use of narcotics amongst them.

How does it directly affect our lives?

- **Panic amongst Patients**

Manipulated data could result in panic amongst the infected patients because they would be shown the results that are far deviated from the actual the results. These could include the indication of protein levels or blood sugar levels much beyond or much lower than the *healthy* levels for the human body. Not only manipulation of levels of the existing components of the urine, but also manipulating the presence of certain components which if present could indicate the onset of certain diseases or illness.

For example, the presence of white blood cells along with the red cells in the urine could indicate Urinary Tract indication, which would essentially worry the patient, maybe even to an extent that he tries to find remedies for the *illness* he is not even suffering from leading to worsening of his condition.

In a scenario altogether different from above, the malware could also *hide* diseases that the patient might be suffering from by manipulating the data. This would lead to worsening of the condition for the patient in cases where the symptoms are not always discrete enough for the patient to realise that some this is wrong with him until it is too late. For example if the cancer in the bladder or the kidney goes untreated for a very long time it may reach a point of no turning back, being fatal to the patient. Another example can be observed with a woman if she is tested positive for a pregnancy test where in reality it is negative, the whole situation could prove to be very traumatising.

The permutation and combination of the disease being shown and hidden is very high and can all in all be summarised to be extremely traumatic to the patient and even prove to be fatal. This is a very serious issues as it can leave life long impacts on the patient lives such as Post Traumatic Stress Disorder (PSTD), Panic Disorder or anxiety Disorder.

- **Wrong diagnosis by the doctor**

Another direct effect that such a cyber attack can have on our lives is much more severe, and happens once the patient sends the data file to the doctor for further analysis. Since the data from Smart Toilet system is already manipulated before the patient sends it over to the doctor, there is no way for the doctor to concur that the data has been tampered with. The doctor would consider the received data to be the result of the patient from the Smart Toilet System and would analyse the data as is, without verifying its authenticity.

This is potentially very harmful for the patient because the doctor would perform the analysis on the tampered data, thereby misdiagnosing the disease. As in the previous point there are several permutation on what conclusion the doctor reaches based on the data. The doctor could increase the dosage of the prescribed medicines, reduce it or stop it altogether. The doctor could even prescribe more medicines that might have an adverse effect on the patient based on his actual condition rather than the *manipulated condition.*

For instance if we take a diabetic patient, who takes a certain dosage of insulin shots every day based on his previous condition, but after the diagnosis of the *allegedly* increased blood sugar levels the doctor might increase the dosage or the frequency of the insulin shots which might result in concentration problem, seizures unconsciousness and in some case can prove to be fatal to the patient.[5]

In summary, manipulated or tampered data can have many outcomes, in which either a disease is not treated at all, or treated differently based on the results. This could have potentially adverse effects directly on the life of the patient which might prove to be fatal.

- **Termination of Employees on the basis of the test**

As mentioned before, large corporations employ urine drug test before hiring new employees, or even for the existing employees. In such large corporations if the Smart Toilets systems are used for such analysis and the results of the drug test are tampered with by a malware, then it could result in several problems.

Firstly, the employees who have not been using drugs could be marked positively and could result in their immediate termination, depending on the bylaws. This could also lead to the corporation to take legal action against the employee. Even though further deterministic test would prove the employee to come clean of any charges but in essence would lead to monetary loss from the side of the employee, and the corporation which in turn could be sued for harassment by the wrongly accused employee who would now be seeking for compensation. Secondly, potential narcotic abusers could go undetected if the malware randomises the process of manipulating data. Since most of the corporation conduct a drug test quarterly the employees abusing drug usage could go undetected for a long time, before the next test happens.

To summarise this point, a cyber attack on Smart Toilet System has a direct impact on the Employee’s life.

- **Invasion of privacy**

Once the attack on an individual person or a group of people has already been to effect, there is a rising concern of the privacy for each of the user. Since privacy is considered as a high priority issue, stealing the private of victims and its availability will indefinitely raise red flags amongst the infected people. By law if such private data is made publicly available without the consent of the consumer, the consumer has the right to press charges against the body of wrong doing.

[5] http://www.healthline.com/health/diabetes/insulin-overdose#Symptoms4

How does it indirectly affect our lives?

- **Private Data available to advertisers**[6]

Once the private data is stolen, the attacker might not necessarily have a use for it for himself. He might sell the data accumulated from various victims to merchandisers and advertisers. By doing this the private information of all the victims is not only publicly available but also can be misused. Such data collectors are essentially data brokers who collect and analyse the data and can send personalised discounts, catalogues and advertisements.

The data stolen can be used in unethical ways by malpractitioners to take advantage of vulnerable group of people. This could be a potential threat to the user who could be bombarded with advertisements which could even be malicious to some extent.

Since the victim is usually unaware of the data being stolen, it doesn't directly affect him per say. Security in such a case is a very big issue. There have been a lot of cases that hackers accessed and stole big data of customers from the big corporation such as Ford Motor Credit Company, Sony etc. with so much personal and financial information available, the credit card stolen and identity theft become a big problem.[7]

- **Monetary Impact on the organisation**

One of the major effects that Cyber Attack on the smart toilet system would essentially be on the vendor of the Smart Toilet. Together with the cyber attacks the organisation would also have to deal with the raising customer complaints, which could soon turn into a law suit. Dealing with each and every person who sued and settling for the damages with compensation would result in a massive bleed in the organisation's pocket which could worry the investors and prevent other people from buying the system thereby losing business not only with individual customers but also hospitals and large corporations.

To make the matters worse, the organisation would have to deploy more people to work over time and detect, analyse and reciprocate the damage done by the attackers. That would be the case if the attackers chose to hack the Smart Toilet exploiting some vulnerability in the software. If they were compromised even before it reached the consumer, supply chain attack, then the organisation would essentially have to recall each and every infected equipment. In both the cases the organisation would be compelled to address the issue and spend a lot of money on research and development leading to a even bigger hole in its pocket.

Overall the impact on the organisation from an economic point of view could potentially be devastating and could even lead the organisation into bankruptcy.

- **Brand Deprecation**

Brand deprecation would be a side effect of the cyber attack on other entities such as the Hospitals, the Corporations and the doctors, for no fault of theirs. When a either of the entity receives tampered data, which at the time of receiving would be unknown, the initial step would be to consider the data to be valid and take actions accordingly; be it misdiagnosing a disease, overdosage of prescribed medications, wrongful termination of employees etc. Even though there is no fault of theirs, the brand value has already deprecated and rising up could be a very challenging task.

For example if an overdosage of insulin prescribed by a doctor based on certain results of a patients result in the death of the patient, would eventually lead to people not trusting the doctor anymore even if the tampering of information is revealed at a later stage.

- **Irregularities in research**

In cases where the tampered data being collected is also being sent to researchers could result in abnormalities in the research. A very good platform for this is the ResearchKit and CareKit. ResearchKit is an open source framework introduced by Apple that allows researchers and developers to create powerful apps for medical research. The researchers and developers can easily create visual consent flows, real-time dynamic active tasks, and surveys using a variety of customisable

[6] http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/

[7] http://www.zentut.com/data-mining/advantages-and-disadvantages-of-data-mining/

modules that you can build upon and share with the community.[8]

In a context where tampered data is being sent to the researchers it would lead to very unproductive results, since the data is not reliable anymore and if it goes unnoticed could also adversely affect future work in similar domains. In summary cyber attack on Smart Toilet system could have a very harmful effect on researcher's work.

As seen from the above points, the effects of Cyber Attacks on the Smart Toilet system can have a diverse effect on people from different spheres correlated with the domain. Before starting to gather information about this topic we couldn't have even imagined the severity of such a attack happening. From the information we provided above, it is safe to say that securing such IOT medical devices is of grave importance and should not be undermined.

How to deal with these severities?

After going through the ways in which Cyber Attacks can be carried out on Smart Toilets and its direct and indirect effect on different spheres associated with it, we now have reached a consensus that such Cyber Attacks need to be prevented and dealt with in a sophisticated manner so as to no hamper the user experience while at the same time putting great efforts at making the system robust and secure from potential attacks. In this section we would now slowly turn our focus into providing a preventive measures, so as to make it hard for the attackers to attack in the first place.

- **Machine Learning methodology**

It is not impossible for hackers to hack into a system, with enough resources and skills, no system can claim to be 100 percent attack free. However, with the increasing number of malware everyday, it is very difficult for a security analyst to not get overwhelmed with large amounts of raw data regarding malware, which are collected day in and day out at mature environments. Therefore, machine learning techniques are a great fit to improve the security posture of an organisation. Without the help of any form of machine learning system, the analyst would have a difficult time resolving the issues mentioned in this paper in a short timeframe.

So now we would transition from the methodologies and effects of Cyber Attack on Smart Toilets towards sturdy and reliable solution in the form of Machine Learning the next section. With a machine learning approach, many of the tasks can be automated, and even deployed in real time to catch these Cyber Attacks before any damage is done. The massive amounts of data that can be generated, along with the problems of conducting large scale analysis to find the proverbial needle in the haystack, are the perfect combination for extensive and successfully machine learning architectures.[9]

Machine Learning Defined

Very simply defined *Machine Learning is the process of training a system to learn without explicitly programming the system.*

This process of learning could be task oriented and could be used for Predicting, Classifying and Clustering new data from any domain, in our case Cyber Security Domain.

Machine Learning in Cyber Security

Solving a Cyber Security problem is a challenging issue because of several reasons. All the devices are connected to the internet, which makes the monitoring of each and every device and protecting it from threat an extremely difficult task. Moreover, the data generated by these devices is very extensive and needs a lot of automation to handle these *Data Streams*, to be able to extract each and every vital feature from the data. With advances in technology, the attackers are becoming more and more complex with their threats and attacks which makes it very difficult for Cyber Security analysts to handle such threats.

[8] http://researchkit.org

[9] http://www.cybersecurity-review.com/industry-perspective/applying-machine-learning-to-advance-cyber-security-analytics

As a result of these issues, for our paper on attacks on Smart Toilets, in this section we would try and provide a concrete solution for such attacks using Machine Learning methods

- **Intrusion Detection**

Intrusion detection is the process of monitoring real time events occurring in a computer system or network, analysing them for signs of possible incidents and often prohibiting the unauthorised access.[4]. This is typically accomplished by automatically collecting information from a variety of systems and network sources, and then analysing the information for possible security problems.

An IDS generally has to deal with issues such as humongous network traffic volumes, highly irregular data distribution, the complexity to realise decision boundaries between normal and abnormal behaviour, and a requirement for continuous remodelling to a persistently altering environment [5]. In general, the challenge is to efficiently capture and classify various behaviours in a computer network. Strategies for classification of network behaviours are typically divided into two categories: misuse detection and anomaly detection [4].

Misuse detection techniques inspect both network and system activity for known instances of misuse using signature matching algorithms. This technique is effective at detecting attacks that are already known. However, novel attacks are often missed giving rise to false negatives. To overcome this problem, IDS should not start elimination procedure as soon as the first symptom has been detected but rather it should be patient enough to collect alerts and decide based on the correlation of them.

Anomaly detection systems rely on constructing a model of user behaviour that is considered normal. This is achieved by using a combination of statistical or machine learning methods to examine network traffic or system calls and processes. The detection of novel attacks is more successful using the anomaly detection approach as any deviant behaviour is classified as an intrusion. However, normal behaviour in a large and dynamic system is not well defined and it changes over the time. This often results in a substantial number of false alarms known as false positives.

Since responding to each alert consumes relatively large amounts of time and resources, IDS should not respond to every alert it generates. Disregarding this fact may result in a self-inflicted denial-of- service. To overcome this problem, alerts should be aggregated and correlated in order to produce fewer but more expressive and remarkable alerts.

Machine Learning Based Solution

We can divide the Machine Learning based approach to intrusion detection into two categories: Artificial Intelligence (AI) techniques and Computational Intelligence (CI) techniques. Artificial Intelligence techniques refers to the methods of Statistical Modelling. Whereas Computational Intelligence includes technology that is inspired by nature to find solution to complex real world problems. CI methodologies include fuzzy logic, artificial neural networks and evolutionary computation such as genetic algorithms.

AI based Techniques [6]

In order to train the IDS system to be able to detect new attacks on the smart toilet system we must first train and test the model on different scenarios in which the model is capable of detecting malicious behaviour from same unknown distribution. In addition, we should train and the test the system on new attack patterns. This would solve the issue of generalisation with the IDS system increasing its overall accuracy , because in todays world, the attackers are far more skilled to be able to use several intrusion patterns to escape from an IDS.

Lee and Solfo [7] build a classifier to detect anomalies in networks using data mining techniques. They implement two general data mining algorithms that are essential in describing normal behaviour of a program or user. They propose an agent-based architecture for intrusion detection systems, where the learning agents continuously compute and provide the updated detection models to the agents. They conduct experiments on Sendmail system call data and network tcpdump data to demonstrate the effectiveness of their classification models in detecting anomalies. They finally argue that the most important challenge of using data mining approaches in intrusion detection is that they require a large amount of audit data in order to compute the profile rule sets.

CI based Techniques

There are several algorithms based on the core technique of Computational Intelligence such as genetic algorithms [8], artificial neural networks[9], fuzzy logic[10] and artificial immune systems[11, 12]. After having read several papers and comparing their efficiencies, we came to a conclusion that Artificial Immune Systems should be able to provide better results. However not disregarding the theory that one algorithm might always outperform the other depending on the data set, we would leave the selection of the algorithm an open discussion. Also the fact that using Evolutionary Algorithms, for such an attack, can prove to be very useful with new trends and patterns developing every day.

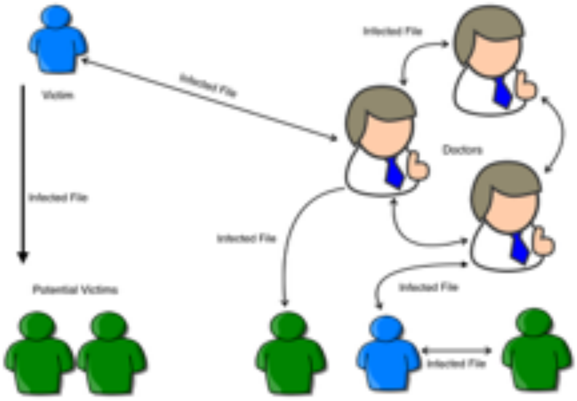
Zamani et al. [11, 12] describe an artificial immune algorithm for intrusion detection in distributed systems based on danger theory, a immunological model based on the idea that the immune system does not recognise between self and non-self, but rather between events that cause damage. The authors propose a multi-agent environment that computationally emulates the behaviour of natural immune systems is effective in reducing false positive rates. They show the effectiveness of their model in practice by performing a case study on the problem of detecting distributed denial-of-service attacks in wireless sensor networks.

Based on the several techniques for intrusion detection mentioned in this section, the attack can be prevented from even happening. We reviewed several influential algorithms for intrusion detection based on various machine learning techniques. Characteristics of ML techniques makes it possible to design IDS that have high detection rates and low false positive rates while the system quickly adapts itself to changing malicious behaviours. The use of Intrusion Detection System is a great way of detecting anomalies in the network and suspending and blocking the activity of the attacker, thereby nullifying his efforts. However, in case of supply chain attack when the Smart Toilets are infected from the point of manufacturing the IDS system may not always work efficiently, so the need for another method to examine the file being exchanged between the doctor and the patients arises. This method of file analysis is explained in the next section.

- **File Analysis**

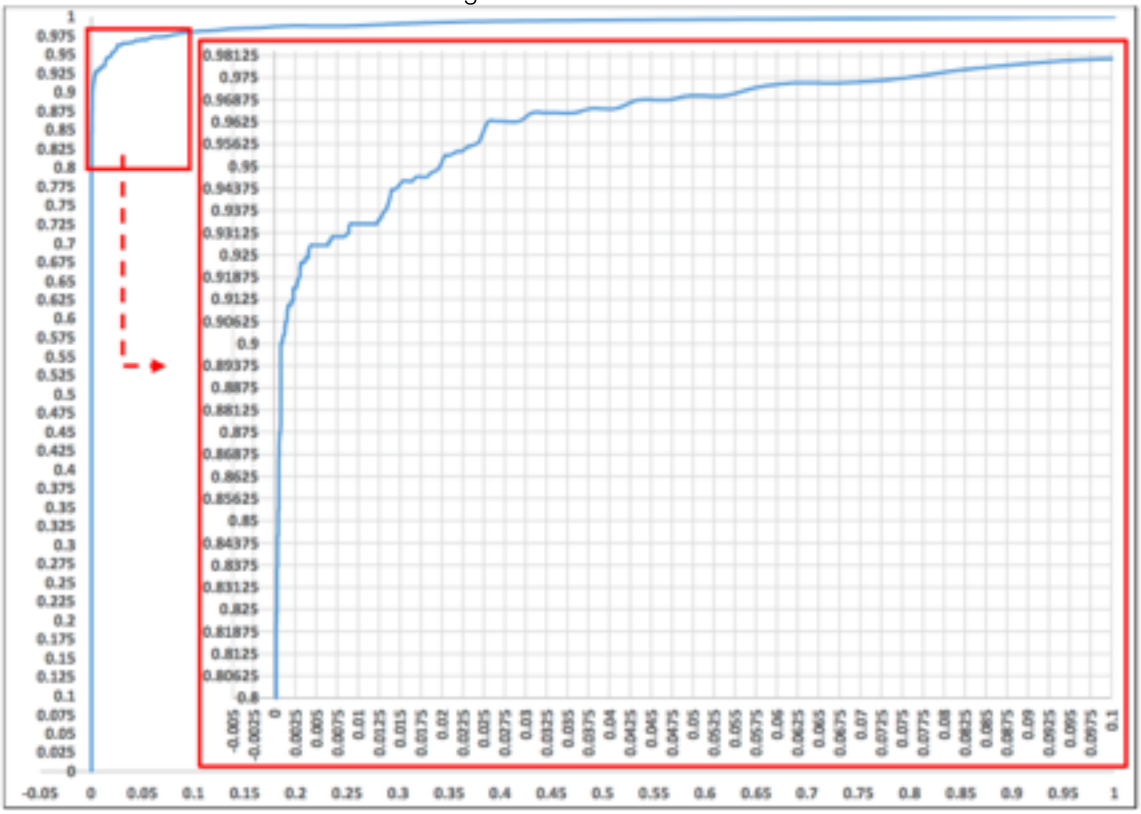
File analysis is the process of extracting useful features from any given file and examining those features to either classify the file as benign or malicious. In attacks on Smart toilets, where the attacker is able to tamper with the data generated by the system and being able to infect other files on the device of the victim to be able to propagate easily to new potential victims, File analysis becomes a huge necessity. If the attacker is able to infect other files on the system, the probability of the victim to send the infected files to his peers is very high as shown in Figure 1.

Figure 1. Propagation of infected File



Cohen et al. [13] described a methodology for file analysis which uses Structural Feature Extraction Methodology that extracts discriminative structural features from Extensible Markup Language (XML) based documents (e.g., *.docx, *.xlsx, *.pptx, *.odt, *.ods, etc.). The extracted features contribute to the discrimination between malicious and benign documents when used in conjunction with machine learning algorithms. They implemented Information Gain and Fischer Score feature selection methods while taking into consideration a large number of permutation and combination of number of features and algorithms to be used. The configuration that provides the best detection measures is based on: TFIDF, Fisher Score, Top 200, and Random Forest (500 trees), and achieved a TPR of 0.97 with an FPR of 0.049, and an AUC of 0.9912. Figure () presents the ROC curve of the Random Forest (500 trees) in the best configuration. The X-axis represents the FPR, and

Figure 2 Results of SFEM



the Y-axis represents the TPR. The area pictured in the red rectangle is enlarged and presented within. They also found that removing the number from the extracted features significantly reduces the time complexity and computational resources needed for the feature extraction and selection processes, however it does not lead to significantly better detection results.

Using SFEM, the files that are being transported between Patient and Doctor, and in between Doctors can be monitored in real time; and the malicious files can be flagged and removed. This would prevent the propagation of malicious and cut the nip in the bud. As the research suggests the method is highly accurate and would protect the system from getting infected. This method when coupled with IDS can provide significantly more secure system to prevent attacks, and propagation of malware through emails.

- **Cognitive Analysis**

Cognitive computing is the simulation of human thought processes in a computerised model.[16] These systems learn at scale, which means that they learn progressively and interact with human naturally. In this final section of Machine Learning based solution, we decided to implement and provide a cognitive solution to the problem. The main reason for using Cognitive Computing is that it can understand, extract and identify contextual elements, while being interactive at the same time. It not only gives a hypotheses but also provides reasoned arguments for the results given. Finally, cognitive computing is highly adaptive; i.e it learns and remembers the interaction from the users.

The way we are proposing to use cognitive analysis is to train a multi-class classifier in which different *emotions, weather condition, current political scenario* etc ca be used, and the user before sending the result file to the doctor has to select certain options based on the specific question being asked. For example the user may be asked to select all those alternatives which may portray *hateful* emotions. only if the user gets all the emotions correctly will he be allowed to send the file. This would add a layer of security to the system which ensure that only a human can manually send the file. Doing this would prevent a malware to automatically send the malicious files over to the doctors.

For demonstration purpose we used IBM's blue mix to develop a language classifier based on 500 different examples with two classes: Accept and Deny. In the *Accept* class we trained a classifier with a set of 250 examples of sentences which poetry certain emotions, while in the *Deny* class we trained the classifier with a set of random text related to mathematics and other domains. Set of correct inputs is needed to to pass the security to send the mail. When a malware would try to bypass the security measures it would select some options randomly in order to go unnoticed, how ever the probability of it being *allowed* is very low. Thus ensuring that only the user has the access to sending those files.

The classifier of accepting and denying users or malware is highly customisable with different questions being asked that could be specific to the user or the current weather conditions, or information that only a human can identify. This method can be used even prevent unauthorised access to the files. In summary cognitive analysis can be used in a very intuitive way to not only add usability but also a layer of security in the system.

Conclusion

IOT is a booming market which is growing day in and day out. With the Cyber threats on the rise, there surfaces a need to secure these IOT devices from different spheres against these threats. We reviewed several influential algorithms for intrusion detection, file analysis based on various machine learning techniques. Characteristics of ML techniques makes it possible to design models that have high detection rates and low false positive rates while the system quickly adapts itself to changing malicious behaviours in the Smart Toilets. Even though the Smart Toilet systems are limited in supply today, the need for them will grow exponentially in the future with everything getting automated.

We would like to conclude the paper by saying that integrating the machine learning methods mentioned above into a single *Threat Prevention Engine* would prove to be very useful and would provide several layers of security to the Smart Toilet System. Such an engine could be made generic so as to serve other devices in IOT domain.

References

1. Wireless Network Security: Vulnerabilities, Threats and Countermeasures. International Journal of Multimedia and Ubiquitous Engineering: Vol 3, No. 3, July, 2008
2. Rose, C.; Parker, A.; Jefferson, B.; Cartmell, E. (2015). "The Characterization of Feces and Urine: A Review of the Literature to Inform Advanced Treatment Technology". Critical Reviews in Environmental Science and Technology 45 (17): 1827–1879.
3. Martín Hernández E, Aparicio López C, Alvarez Calatayud G, García Herrera MA (2001). "[Vesical uric acid lithiasis in a child with renal hypouricemia]". An. Esp. Pediatr. (in Spanish) 55 (3): 273–6
4. Peter Mell Karen Scarfone. Guide to intrusion detection and prevention systems (idps). National Institute of Standards and Technology, NIST SP - 800-94, 2007. Available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50951.
5. Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin, and Wei-Yang Lin. Review: Intru- sion detection by machine learning: A review. Expert Syst. Appl., 36(10):11994– 12000, December 2009.
6. Pavel Laskov, Patrick Dssel, Christin Schfer, and Konrad Rieck. Learning intru- sion detection: Supervised or unsupervised? In Image Analysis and Processing ICIAP 2005, volume 3617 of Lecture Notes in Computer Science, pages 50–57. Springer Berlin Heidelberg, 2005.
7. Wenke Lee and Salvatore J. Stolfo. Data mining approaches for intrusion de- tection. In Proceedings of the 7th USENIX Security Symposium - Volume 7, SSYM'98, pages 6–6, Berkeley, CA, USA, 1998.
8. Chris Sinclair, Lyn Pierce, and Sara Matzner. An application of machine learning to network intrusion detection. In Proceedings of the 15th Annual Computer Security Applications Conference, ACSAC '99, Washington, DC, USA, 1999.
9. Srinivas Mukkamala, Guadalupe Janoski, and Andrew Sung. Intrusion detection using neural networks and support vector machines. In Proceedings of the 2002 International Joint Conference on Neural Network (IJCNN), volume 2, pages 1702–1707, 2002.

10. Jonatan Gomez and Dipankar Dasgupta. Evolving fuzzy classifiers for intrusion detection. In Proceedings of the 2002 IEEE Workshop on Information Assurance, West Point, NY, USA, 2002.
11. Mahdi Zamani, Mahnush Movahedi, Mohammad Ebadzadeh, and Hossein Pe- dram. A DDoS-aware IDS model based on danger theory and mobile agents. In Proceedings of the 2009 International Conference on Computational Intelligence and Security - Volume 01, CIS '09, pages 516–520, Washington, DC, USA, 2009. IEEE Computer Society.
12. Mahdi Zamani, Mahnush Movahedi, Mohammad Ebadzadeh, and Hossein Pe- dram. A danger-based approach to intrusion detection. CoRR, abs/1401.0102, 2014.
13. Aviad Cohen, Nir Nissim, Lior Rokach, Yuval Elovici. SFEM: Structural Feature Extraction Methodology for the Detection of Malicious Office Documents Using Machine Learning Methods

The word count is well under the limit, at around 7000 words, however, due to the structure of the paper, we have exceeded the page count. I was allowed this extension by Dr. Nir Nissim on 28th July, 2016.