INTERNET OF THINGS MALWARE: A SURVEY

Evanson Mwangi karanja [1], Shedden Masupe[2] , Jeffrey Mandu[1],

[1] Department of Electrical Engineering, Faculty of Engineering and Technology
University of Botswana.
[2] Botswana Institute for Technology Research and Innovation

ABSTRACT

Ubiquitous devices are rising in popularity and sophistication. Internet of Things (IoT) avails opportunities for devices with powerful sensing, computing and interaction capabilities ranging from smartphones, wearable devices, home appliances, transport sensors and health products to share information through the internet. Due to vast data shared and increased interaction; they have attracted the interest of malware writers. Internet of Things environments poses unique challenges such as device latency, scalability, lack of antimalware tools and heterogeneity of device architectures that makes malware synthesis complex. In this paper we review literature on internet of things malware categories, support technologies, propagation and tools

KEYWORDS

Internet of Things (IoT), Malware, Malware synthesis, Machine to Machine Communications (M2M).

1. INTRODUCTION

In the last two decades, computing has evolved from the context of localized desktop computing to pervasive computing where smart devices have increased in computational power and preference of usage. Internet since its invention has evolved in phases. It started with web 1.0 which is unidirectional flow of information through publishing information for the users, then evolved to web 2.0 where the refined focus was shifting away from publishing to participation through tools such as blogs, wikis, Social Network services etc. Web 3.0 now evolves from participation (internet of the people) to Internet of Things.

Honbo Zhou [1] identifies two pillars that support the evolution of the web namely: (1) web applications, internet and the protocols and (2) software such as web browsers and the standardized three layer architecture. The number of devices on the Internet of Things surpassed the human population in 2011, and the number of installed internet connected devices is predicted to grow from 7 billion in 2014 to over 50 billion in 2020 [2].

The Internet of Things has emergent range of applications domains such as in healthcare [3-5], supply chain management [6, 7], energy management [8, 9], intelligent transport systems[10-12], ambient aided living (AAL) [13-15] and smart grid power transmission [16, 17] among other domains. Detailed surveys on applications of IoT are in [18-20]. Studies on general threats and vulnerabilities of IoT includes [21-24]. Due to the sizable potential of Internet of Things there is need to analyze the potential security challenges such as malware.

2. IoT DEFINITION AND CHARACTERIZATION

The term Internet of Things was coined by Kevin Ashton in his 1998 presentation to represent interconnection of smart devices and services [25]. Internet of things is integration of various technical capabilities to bridge the gaps between the physical and virtual world. These capabilities includes communication and cooperation, addressability of devices, identification of heterogeneous devices, ability for devices to sense, actuation, ability for embedded devices to process information, constrained resources such as optimized energy usage, localization of smart devices and appropriate user interfaces [26, 27]. Various researchers have devised working definitions for IoT. We adopt the working definitions hereunder to contextualize our study. Atzori et. al [18], defines IoT as a convergence of three visions namely the internet oriented (middleware), things oriented (the sensors) and semantic oriented (the knowledge). Haller et al. [28] defines IoT as a world in which physical objects are seamlessly integrated as active participants in business processes while taking into consideration security issues. IoT can be thought as virtual objects represented as identities in internet [29]. European Research Cluster on the Internet of Things (IERC) [30] draws a consensus and defines IoT as

" *dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network*".

There are characteristics that differentiate IoT with other recent technologies. These attributes creates a unique perspective in the study of IoT malware.

a) Uncontrolled environment; variety of devices in the IoT infrastructure are highly mobile. Devices are physically accessible and sensors can generate events with minimal user involvement[31]. There exists trust models challenges due to constant change of trust status among interacting devices such as real time mobile sensors. Other Security issues includes security of routing protocols with mobility considerations. Application security aspects of IoT are detailed in [23].
b) Heterogeneity: heterogeneity arises due to device diversity brought by interactions between high level computing devices such as servers with low end sensors and actuators devices[32]. Application diversity is realized as traditional computing environments abstracted through operating systems interact with chip embedded programs in sensors.
c) Scalability; IoT is globally distributed like traditional internet however it is scalable within application areas (device can have multiple applications in numerous domains which ultimately connect to traditional networks via internet). Due to the large number of IoT devices interconnected, scalable protocols are needed [33].
d) Resource constraint; Sensors and actuators in IoT network have restricted security mechanisms due to their minimalist design[34]. They also have low energy requirements thus strong security such as cryptography cannot be used on all things.

Various reference models have been suggested by stakeholders to bridge the standards gap.We analyze in summary the reference models and their key elements. The Internet of Things Architecture (IoT-A) [35] is a reference model proposed in European Union within the 7th Framework Programme (EU7FP). The reference has modules that offer security views and maps to business processes. It has modules for identity management, network security, and privacy through Pseudonymisation of entities, device trust and reputation. The model however does not address data trust and malware aspects.

Building the environment for the Things as a Service (BeTaaS) [36] is a reference model that consists of four layers; physical layer to offer connection to devices; adaptation layer which offer abstraction for machine to machine(M2M); TaaS layer provides network access to devices and the fourth layer is service layer which manages the applications and services. The model has no specific details on privacy management and breaches caused by malware.

Efficient implementation of IoT is based on layered approach architecture, with data gathering layer on the bottom and application layer at the top. There are three categories of layered architectures namely three layer, five layer and special purpose architecture [37]. The three layer architecture consists of three abstraction levels; the application layer and device level. In [31], the authors presents a five layered generic architecture consisting of with two levels of abstraction between devices and applications, the architecture highlights the benefits of service oriented architecture (SOA) in IoT design .

3. IoT DEFINITION AND CHARACTERIZATION

3.1. Malware Definition and Characterization

Malware (malicious code) is a generic term used in computing to denote a program created deliberately to undertake unauthorized activity (payload) which may have some benefit to its creator or propagator [38, 39]. IoT malware detection is evolving, however are also evolving in complexity [40].

In classical classification of malware, various authors have categorized malware into classes based on mode of propagation or its form of existence. Zolkipli et al [41] offers seventeen classes of classification based on form of existence. Peng at al [42] in their survey of smartphone malware highlights five classes of malware based on a matrix on propagation factors, existence form and risk. Based on review of malware literature, classification of malware in IoT will follow the classical classification. We offer market examples based on classical classification:

a. Virus: Is a type of malware that gain access to the device or software without user knowledge and duplicates itself or commits the programmed malicious task. Viruses cannot exist on their own therefore require a carrier to propagate [42] which makes it hard to survive in sensors and actuators.
b. Worms: It gain access to systems without owner's permission and operates stealthily with capability to duplicate into thousands of copies. It can alter normal operations of an automated processing device. For example, Stuxnet which attacks programmable logic controllers (PLCs). Stuxnet in June 2010 struck an Iranian nuclear facility at Nantaz attacking centrifuges for separating nuclear materials [43, 44]. Linux.Darlloz is a worm that is capable of infecting wide range of devices such as home routers and set up boxes [45].
c. Trojans: is malicious piece of code that appears legitimate hence the users are tricked to activate it. After activation it attacks host device by even creating backdoors to provide malicious access to the host device. For example, the Trojan SoundMiner is capable of extracting data from keypad and audio sensors of android devices [46].
d. Rootkits: It is designed to remotely access a device by modifying the kernel of the operating systems or the device middleware. Domas [47] demonstrated a rookit vulnerability on x86 architecture in the processor's system management mode which if exploited could erase the Unified Extensible Firmware Interface (UEFI) [48].
e. Spyware: They collect user information without his knowledge and can monitor user web activities. Examples include Duqu [49], spyware variant of Stuxnet which instead of causing physical damage on controllers, it collects information. Flame

(sKyWIper) is another variant of large scale spyware that does not only steal information but listens to microphone signals, switches on Bluetooth devices if available and sends information scanned in the attacked system to the nearby device controlled by attackers [50, 51]. The Spyware demonstrated by [52] can send record video and transmit it via email hence a probable route for remote surveillance.

f. Botnets: They allow the promotor to remotely compromise devices usually for large scale attacks such as distributed denial of services or breach of privacy. Example include Zeus [53] and SpyEye [54].

New breeds of malware such as carna botnet [55] and mirai [56] have emerged as set of functional components with diversity that offer capabilities for customization and modular re-development into variants of forms with ability to detect default logins on devices. IoT devices have been used by attackers as part of malware networks, in 2014 a fridge was discovered as part of the botnet spam network sending more than 700,000 spam emails [57, 58].

To avoid detection current malware designer employ code obfuscation techniques such as polymorphism and metamorphism [59, 60]. It is therefore not easy to offer purely distinct classification of malware in IoT networks based on mode of propagation and form of existence only. IoT devices have higher latency since they are online 24/7 unlike traditional computers. They have weak security mechanisms (if available) to deter malware and have no installed anti malware solutions like antiviruses.

4. PLATFORMS AND IOT MALWARE

Traditional malware lacks cross platform capability. In heterogeneous IoT networks, different central processing unit architectures and operating systems are supported. Traditional computing environments are mainly based on X86 architecture, there exists a wide array of studies on malware propagation and analysis in X86 and/or X64 without consideration of device interaction with other architectures hence homogeneity based on specific architecture and operating system. Examples of such studies includes: on malware taxonomies [38, 61, 62], on malware detection [63-67], malware propagation [68] and malware analysis [69]. Windows variants of operating systems in both X86 and X64 architectures are most vulnerable to malware infections. Smartphones such as Lenovo K 900 and Xolo X1000 have been powered on X86 architecture using Intel atom chip. We contend that desktop computers on X86, X64 architectures based traditional operating systems are still key components of IoT global environment.

There is an increase in use of pervasive devices as mode of internet access even in developing countries. In 2012, a survey of mobile coverage in sub Saharan Africa noted that mobile devices were preferred as tools of web access compared to desktop platforms. Specific nation examples were given such as Zimbabwe with 58.1% and Nigeria 57.9% mobile device access compared to their desktop platform access of 41.9% and 42.1% respectively [70]. Smart phone penetration is on the increase in sub Saharan Africa with an estimation of one in five persons owning a smart phone [71]. Smart phones have emerged as a key component in the IoT environments. Nokia Threat Intelligence Report [72] shows that smartphones accounts for 78% of all mobile networks infections. The major operating systems for mobile phones have been a target for malware writers. The table 1 below provides a summary of mobile market share[73] and corresponding malware infection [72] in 2016.

Table **1:** Summary of malware infection vs market share

Operating System	Total Market Share	Malware Infections
Android	65.37%	74%
iOS and others	32.07%	4%
Windows	2.56%	22%

Many studies carried out on mobile phone malware are based on a single operating system or a comparative study between two operating systems. In the next part of this section we highlight several such recent studies.

Most iOS devices processors are based on ARM architecture[74]. ARMv8-M architecture offers efficient power consumption for support of embedded and IoT applications[75]. Various malware variants for iOS have been analyzed. Garcia and Rodríguez [76] studied 36 iOS malware samples collected between 2009 to 2015, the samples were categorized based on propagation channels, targeted party, attack vector and goal of attack. The study found out that most of iOS malware are distributed through official channels hence lack of user awareness on the malware threat is a key risk.

Deshotels et.al [77] analyses the role of iOS generic sandbox in containing malicious applications, using prolog based approach to analyze iOS sandbox profiles, their study discovers seven exploitable vulnerabilities. Gui et. al [78] analyzes XcodeGhost, a privacy leaking iOS malware on a large network of more than 2.59 iPhone users and discovered that over 60% of 1550 million iPhone users in China were infected. The study developed a heuristic model to differentiates XcodeGhost HTTP from usual HTTP requests from users.

Malware authors are mainly economically motivated hence prefer to develop Android malware due to its market dominance. Android Supports ARM, Intel and MIPS architecture with ARM being the most popular. In this study we review sample of recent studies on Android malware.

Saracino et al. [79] presents a multilevel and behaviour based Android malware detection using 125 existing malware families and reports 96% detection of malware. Malik et al. [80] uses pattern based detection based on Domain Name Service (DNS) queries, their approach is able to detect polymorphic malware. In [81] machine learning based detection that analyzes application behaviour using a large scale malware set of 18,677 malware and 11,187 benign apps is presented with 97.3% positive detection. Deep learning Android malware detection that does not depend on semantic pattern matching is proposed [82]. Deep learning android malware detection (Dendroid) uses text mining improves specificity of the classifier [83] .

Narudin et al. [84] evaluates logical-based, perceptron-based, static-based and instance-based classifiers evaluating in mobile applications. Arshad et al. [85] surveys static based approaches (i.e. Signature based, permission based, Dalvik bytecode) and dynamic based approaches (i.e. anomaly, taint analysis, emulation based). Six machine learning algorithms are implemented as a static analysis module for Android malware [86]. Aashima et al. [87] surveys mobile malware detection on iOS, Symbian and Android using signature and anomaly based approaches.

The operating systems platforms designed for sensors in IoT environments are usually runs on low memory and require low energy consumption. We review a sample of four common

embedded IOT operating systems on their existing malware and their respective antimalware approaches.

ARM mbed OS is an IoT operating systems supports development of microcontrollers based on ARM architecture. It supports various connectivity technologies such as Bluetooth, Wifi and Zigbee IP with intergration of IP end to end security for IP6 and IP4 [88]. ARM mbed OS implements a software hypervisor to protect against malware and data leaks among modules of the same program[89]. For device integration it implements OMA Lightweight M2M protocol.
TinyOS, a free and open source operating system popular for wireless sensor networks developed by TinyOS Alliance[90]. Embedded security architectures layers have been implemented in TinyOS such as elliptic curve cryptography[91], however scanty details exist in literature on its malware protection and attacks.

Contiki is low cost flexible open source operating system for IoT that incorporates the Cooja network simulator[92]. 6LoWPAN an intermediary layer between network layer and MAC that aids IEEE 802.15.4 links for integration of IPv6 constrained devices is supported as network protocol in Contiki stack. ContikiSec is presented as a secure network layer for wireless sensor networks in Contiki [93]. To the best of our knowledge there are no systematic studies on Contiki devices malware analysis and/or heterogeneous devices in IPv6 network that connects Contiki based devices.

RIOT is offered as micro-kernel based IoT operating system designed in modular way that supports IPv6 and supports UDP, TCP and RPL [94]. Low-Powered Wireless Personal Area Networks in IPv6 (6LoWPAN) encryption offers end to end support against spoofing and man in the middle attacks however it does not support node authentication as the nodes join the networks. Lack of strong authentication means malicious code can be injected. In IoT, node mobility is a key attribute as nodes changes their addressing characteristic. Moving Target IPv6 Defence (MTID) is implemented in 6LoWPAN as a means to curtail denial of service and man in the middle attacks. Malware studies on RIOT to the best of our knowledge have not been analyzed.

4.1. Malware modelling review and its application in IoT.

Mathematical modelling is a viable method of numerical analysis that is useful in appreciation of the behavior and parameters of systems [95]. Malware spreading models originate from classical works of Kermack and McKendrick [96, 97] on epidemic models, which forms the basis of deterministic models of malware spread. Rey classifies the models as either Deterministic or Stochastic; Continuous or Discrete ; (global or individual models. Peng et al [42] groups epidemic models as deterministic, stochastic and spatial temporal. This work adopts a mix of Rey and Peng et al classification and extends the subcategories based on recent works. We focus on models that support heterogeneity, scalability and mobility which are key attributes of IoT networks. The strength and weakness of each of the model is highlighted with regard to IoT modelling.

- **Deterministic Models**

The parameters and variables in these models over networks are not random and hence they do not follow any probabilistic distribution. They are compartmental which means metapopulation of malware prone device evolves through these stages. as; susceptible (not infected); exposed (already infected but not activated either device is online or offline[98]); infected; isolated; recovered; quarantined and vaccinated. Based on these stages the following categories of deterministic models are obtained.

a) SI (Susceptible –Infected) model

It supposes that a susceptible node after contact with infected node becomes infected and does not develop immunity from the infection. A network node can be in two states, infective (I) or susceptible (S). Using notations in [99], S(t) is the number of devices susceptible to infection and X(t) is the number of devices infected at time (t). β is the infection rate: which is the probability of contagion after contact per unit time. The system of differential equations describing the model can written as:

$$\frac{dX}{dt} = \beta \frac{SX}{n} \quad \text{and} \quad \frac{dS}{dt} = -\beta \frac{SX}{n} \tag{1}$$

Where

$\frac{S}{n}$ *is the probability of meeting a susceptible node at random per unit time.*

$\frac{XS}{n}$ is the average number of susceptible nodes that infected nodes meet per unit time.

$\beta \frac{SX}{n}$ is the average number of susceptible nodes that become infected from all infected per unit time.

This model can reduced to a logistic growth equation as follows: let $s = \frac{S}{n}$ and $x = \frac{X}{n}$ then s+x=1 and S+X=n ; this yields

$$\frac{dx}{dt} = \beta(1-x)x \quad . \tag{2}$$

Solving this differential equation yields

$$x(t) = \frac{x_0 e^{\beta t}}{1 - x_0 + x_0 e^{\beta t}} \tag{3}$$

A modified SI model is used to model the online and offline conditions of the device which can be extended to cyber physical devices that are not always online [100]. The SI model is the building block for other deterministic models.

b) SIS (Susceptible Infected Susceptible) model

In this model, a susceptible node after contact with an infectious node becomes infected but does not develop immunity. The basic governing equations based on the definition of parameters as; β

is the infection rate or the probability of contagion after contact per unit time. γ recovery rate or the probability of recovery from infection per unit time is:

$$\frac{dS}{dt} = \gamma x \; - \; \beta S x \tag{4}$$

$$\frac{dX}{dt} = \beta S x \; - \; \gamma x \tag{5}$$

Solving the derivatives analytically taking into considerations s+x=1 yields

$$x\,(t) \; = \; x_{\,0} \; \frac{(\beta-\gamma)e^{\,(\beta-\gamma)t}}{\beta-\gamma+\beta x_{\,0}\; e^{\,(\beta-\gamma)t}} \tag{6}$$

This model has been used for malware propagation for various variants. Chakrabarti et al [101] formulates a general network model for SIS based on graph theory adjacent matrix. Dadlani et al [102] uses the SIS model incorporated with infection delay and infective medium vector over complex networks and finds that these two variables accelerate the infection spread in the population. Wierman et.al [103] uses the SIS model to computer virus with possibility of reintroduction. Martin et.al. [104] investigated the propagation of mobile phone viruses based on SIS model, however their work did not take into consideration the individual characteristics of proximity based viruses or temporal spatial characteristics. Mieghem[105] predicted the influence of network topology defined in graph theory on virus spread based on SIS model. Their model did consider the heterogeneity of nodes in the network.

c) SIR (Susceptible Infected Recovered) model

It is based on the notion that when nodes get infected they develop immunity. In human epidemiology the model has been applied in maladies such as chickenpox, measles and mumps [42]. The parameters for SIR model are formulated as follows; β is the infection rate: probability of contagion after contact per unit time. γ recovery rate: probability of recovery from infection per unit time. The basic governing differential equations are as follows: S is the number of devices susceptible to malware but not yet infected, X is the infected devices; R is the devices infected and immunized or removed from network.

$$\frac{dS}{dt} = -\beta S x \tag{7}$$

$$\frac{dX}{dt} = \; \beta S x \; - \; \gamma x \tag{8}$$

$$\frac{dR}{dt} = \; \gamma x \tag{9}$$

The model has various variants used in malware propagation. Rhodes et al.[106] uses a SIR based model for propagation of wireless worms on mobile devices catering for contact and mobility. Sheng et al.[107] investigates the social network worms spread based on the uniqueness of human mobility and topology of social networks proposing the SII model. Tang et al. [108] introduced (Susceptible-Infective-Recovered with Maintenance (SIR-M) to describe the spread of virus from one node to the network in wireless sensor network. Nguyen et al [109] numerically analyses the influence of device type diversity on diffusion of malware based in both SIR and SIS.

d) SIRS (Susceptible Infected Recover Susceptible) model

It is based on the notion that an infected node can recover and is susceptible again after recovery. Various variants of this model exist. However the models of our interest are those with recovery or isolation stage.

Ramachandran et al. [110] uses a variant of SEIR, to include the exposure stage. Propagation of malware variants through internet are explored using vectors such as Bluetooth and infrared using smartphones. The model built in [110] presumes similar conditions for all devices thus not effective for modelling IoT malware. Fan et al. [111] proposes a model SEIR, using Bluetooth and SMS/MMS services. The model describes the role of pre-immunity such as antivirus on the malware propagation. Both the models have not parametrized the effect of human behavior and device heterogeneity.

The model SEIRD proposed by Xia et. al [112] introduces the stage of dormancy and Bluetooth and SMS/MMS were investigated as propagation vector on smart phones. The model did not include the influence of human behavior such as user profiles on the malware spreading. Mishra et al. [113] proposed a SEIRS model with an immunity phase and latency period as a factor. Mishra et al [114] introduced the quarantine compartment in the SEIQRS model. They argued that reproduction of infection decreases with increase in elements quarantine class.

Toutonji et al. [115] presented SEIRS with simulation on computer worms infections. The results show that security interventions on susceptible state influences propagation. Li et al. [98] built a model for mobile botnet propagation in Wi-Fi Networks namely SEIDCOOC catering for human online behavior and cloud security. The model proposes eight different states which are Susceptible S, Exposed E, Infected I, Death D, Contained C, Cloud security CI, exposed –offline (Eo).

Most of the deterministic models in their classical form have full mix assumption. This assumption is that every node has equal chances of coming into contact with others in the metapopulation which is not necessarily the case in IoT propagation where heterogeneity of communication interface is a key factor for propagation modelling.

- **Stochastic Models**

These models can classify into three categories namely;

a) Discrete Time Markov Chain (DMTC) where time and state are discrete variables.
b) Continuous Time Markov Chain, where state is discrete but time is continuous
c) Stochastic differential equations mainly based on diffusion equations and time and state which are continuous [42, 116].

Wang et al.[117] uses a discrete-state Markov model and based on various states analysis and concludes that the stationary state is key to detection of malicious code. Chen et al. [118] built a Markov model based on probabilistic graphs that incorporates temporal dependence and network topologies and obtained transient properties of malware propagation. Stochastic models are global models since they study dynamics of a population without regard to individual characteristics of the nodes such as device heterogeneity [39, 119].

Models based on Markov chains are complex for spatial temporal process such as worm propagation [120], and are suited for small networks communities. Empirical results shows that this small network should be between 102 and 105-106 [39] , compared to deterministic models

that provide better results for networks greater than 105-106 [121]. They also lack ability to model complete spatial-temporal propagation since the state transmitting matrix is fixed upfront [122].

- **Individual Based Models**

These models take into consideration the individual characteristics of nodes, local interactions between connected nodes and global dynamics. According to a survey conducted by Rey [39], very few individual models have been proposed in malware propagation. In this section we review individual models of malware propagation.

A cellular automaton is formalized as a discrete spatial temporal system which can be extended to any dimension. Formally a cellular automaton is postulated as an undirected graph G= (V, E) where V is the vertices and E are the edges; it's a 4-uple = (V, Q, N, f) where V defines the cellular space, Q defines the finite set of states that can be assumed after each transition, and N is the neighborhood of each cell where f is a transition function.

Song et al. [123] investigated wireless sensor network malware propagation using cellular automata. Using two dimensional grid of $L_{(100)} * L_{(100)}$ cells and N stationary sensors. The transition states are S-suspectibe, I-Infected, R-recovery and D-death. The state variable of a node is defined as $S_{ij}(t) \in Q$ where i and J are cell coordinates and t is time. The population S(t), I(t), R(t),D(t) are suspectible, infected, recovery and death nodes respectively. The defined state model with preceding parameters is as follows

$$\begin{cases} S(t) = \dfrac{1}{N}\sum_{i,j} S_{ij}(t) = 0 \\ I(t) = \dfrac{1}{N}\sum_{i,j} S_{ij}(t) = 1 \\ R(t) = \dfrac{1}{N}\sum_{i,j} S_{ij}(t) = 2 \\ D(t) = \dfrac{1}{N}\sum_{i,j} S_{ij}(t) = -1 \\ S(t) + I(t) + R(t) + D(t) = 1 \end{cases} \tag{10}$$

The study found that limited capability of sensors, the medium access control and node density affected the rate of propagation.

IoT networks can be modelled using topological networks such as complex networks. Song et al [122], uses modified analytical model SIS and SIR with cellular automata to evaluate malware diffusion on Erdos Renyi network and Barabasi power law network. The SIS-Cellular Automata is defined as : The state variable of a node is $S_{ij}(t) \in Q$ where i and J are cell coordinates and t is time . $Q = \{0,1\}$ with 0 being susceptible and 1 state infected. β is the probability that infected nodes attempts to infect susceptible node in unit time and δ is probability that an infected node may be cured and become susceptible. The local transition rules are defined as

$$\begin{cases} s_i(t+1) = \max\left(f_{\delta}(s_i(t)(1-\delta_i)), f_{\beta}(1-(1-\beta_i)^{m_i(t)})\right) \\ m_i(t) = \sum_{j=1}^{N} a_{ij} s_{j(t)} \\ f_{\delta}(x) = \begin{cases} 1; if \ \ x \geq \delta \\ 0; \ if \ \ x < \delta \end{cases} \\ f_{\beta}(x) = \begin{cases} 1; \ if \ \ x \geq (1-\beta) \\ 0; \ \text{if} \ \ x < (1-\beta) \end{cases} \end{cases} \quad (11)$$

The SIR-Cellular automata introduces the recovery probability γ and the state $S_{ij(t)} \in Q$ where i and J are cell coordinates and t is time . $Q = \{(0,0)(0,1)(1,0)(1,1)\}$. The local transition function becomes ;

$$\begin{aligned} S_{ix}(t+1) &= \max(f_{\delta}(s_i(t)(1-\delta_i)), f_{\beta}(1-(1-\beta_i)^{m_i(t)})) \\ m_i(t) &= \sum_{j=1}^{N} a_{ij}(t) s_{jx(t)} \end{aligned} \quad (12)$$

The model illustrates capturing spatial-temporal process in the propagation. From the simulation results malware diffuses more faster on Barabasi power law network than Erdos Renyi random graph network.

Bakhshi et al. [120] models malware using a three dimensional cellular automata and epidemic theory using Bluetooth worm as a case study. The states of node at given time t are defined as ; healthy H(t), vulnerable V(t), exposed E(t), infectious I(t), diagnosed D(t), quiet (infected but inactive) Q(t), and recovered R(t). The infection rate is determined as ratio of interaction between neighbouring cells and the resistance to infection index. The method is only effective for investigation of proximity malware and homogenous vector.

Peng et al. [124] used a two dimensional cellular automata to investigate the malware propagation in smart phones, however the model did not investigate the influence of human mobility and metamorphic viruses. The states of nodes are defined as susceptible S(t), exposed E(t), infectious I (t), diagnosed D(t) and recovered R(t) . The infection probability is calculated as ratio between interaction coefficients between neighbors(the likelihood of infection among neighbors) and resistance to infection factor.

The model proposed by Martin et al.[119], uses cellular automata to simulate mobile malware propagation using Bluetooth connections; the model placed more than one phone in a cell and allowed for smartphone mobility. Node mobility increasegd virus spread in multi-hop network [125].

Bose et al built an agent based malware modelling framework [126] for malware propagation in heterogeneous environments. The agents are segmented as domain , network or device. To cater for spatial heterogeneity, the segments can overlap. Mobility models namely Random Way point and Gaussian Markov are used for agent mobility in the framework. The framework is validated

with real life network data from Cabir virus on cellular networks through Bluetooth and worm exploits on user on a social network. The model did not cater for containment of malware spread or immunization.

Hosseini et al.[127] formulates a four state analytical SEIRS model on Barabasi–Albert scale free network topology. The four possible states in the model are S-susceptible-exposed, I-infectious, and R-stifler (nodes that lose its ability to propagate after receiving the malware). The agent model is used to cater for software diversity, device heterogeneity and autonomy to exit the network. The simulation results on immunization show that targeted immunization is more efficient on heterogeneous nodes as opposed to uniform immunization.

Individual based model for malware propagation in wireless sensor networks with capability to obtain individual transition of each sensor is proposed in [128] .The sensor devices are represented in a cellular space with local transition rules for nodes. Three classes of nodes are defined namely sensor nodes, router nodes or sink nodes. The topology of the network follows a self-organizing protocol. The infection probability is the same for all nodes in the same class. The possible nodes states are; sleep-susceptible, sleep-recovered, active susceptible, active-infectious, active recovered and damaged. The number of nodes in the network is denoted n and the i^{th} is denoted as [i] where $1 \le i \le n$. The local transition rules are defined based on infection probability $\beta[\mathrm{i}]$ e.g A node transits from active-suspectible at time t to infectious at time $t+1$ with probability $\beta[\mathrm{i}]$ if there exist active infectious node j in the neighbourhood N(i) [j]∈ N[i].

An individual based malware propagation method for industrial critical infrastructure is introduced in [129]. The model also considers characteristics that are critical for IoT malware considerations such as;

1) Operating system coefficient o[i] – which is set to 1 if the interacting agents have the same operating system otherwise set to zero. This will cater for platform heterogeneity in IoT.
2) LatencyT_L[i] – the time elapsed from malware infecting the node and its activation. In IoT devices that have no processing power it might not be possible for inactive malware to eventual activate.
3) Immunity period – this is temporal immunity when a malware specimen is removed since the agent is suspectible to other malware in its use life.
   The model proposed does not cater for device mobility.

The neigbourhood $neigh[i,t]$ is the agents reachable by agent i at time t. The state of device agent i are defined in relation to time t as state [i,t] ∈ {S,C,E,I,R,Q} where S-Susceptible, C-carrier,E-Exposed I-Infectious, R –recovered and Q-quarantined and the state of actuator agent is state[i,t] ∈{H,D} where H-Healthy and D is damaged. Infection coefficient a[i,t], the detection coefficient d[i,t], recovery coefficient b[i,t] are Boolean parameters in the model. The local transition rules are offered as logic functions based on the Boolean parameters e.g. the transition for node i from S-Susceptible at time t to E-Exposed at time $t+1$ is viable if a[i,t] AND o[i]=1. The overall transition model is derived as follows:

$$\begin{cases} S \rightarrow C; \quad \mathrm{a[i,t]} = 1 \, AND \, o[\mathrm{i}] = 0 \\ S \rightarrow E; \quad \mathrm{a[i,t]} = 1 \, AND \, o[\mathrm{i}] = 0 \\ C \rightarrow Q; \quad if \;\; d[\mathrm{i,t}] > 0 \\ E \rightarrow Q; \quad if \;\; T_L[\mathrm{i}] \neq 0 \\ I \rightarrow Q; \quad if \;\; b[\mathrm{i,t}] = 0 \\ E \rightarrow I; \quad if \;\; T_L[\mathrm{i}] < \{\mathrm{t}+1-(\mathrm{t})\} \\ \mathrm{I/C/Q} \rightarrow R; when \; b[\mathrm{i,t}] = 1 \\ R \rightarrow S; \; if \;\; T_L[\mathrm{i}] = 0 \\ H \rightarrow D \quad [\text{if } \exists \text{ infected PLC } (x) \; in \; neigh[i,t]] \end{cases} \tag{13}$$

In the synthesis of IoT malware, there is need to take into consideration individual attributes of each device with respect to the following:

1) The device architecture, firmware and operating system
2) Possible vectors of propagation supported by the device and local network that the device is connected to which may include mobility profiles.
3) Users' profiles in the possible domain as users understanding of system security is key to device vulnerability.
   To effectively model IoT malware propagation, invidualised models constructed need to cater for these needs.

5. TOOLS IN IOT MALWARE SYNTHESIS

IoT malware sythesis is still in its infancy stage. In this section we discuss various malware synthesis tools and evaluate their application for IoT malware. In malware experimental studies, the real network data and devices are not always available. Use of IoT compatible simulators, test beds, emulators, analysis sandboxes and honeypots provides a viable option for malware synthesis. We highlight free and open source examples of such tools and their possible applicability in IoT malware synthesis.

It is difficult in resource constrained environment to access large array of IoT devices for malware synthesis tests. Device emulation is a critical aspect in the IoT malware research since it offers access to device capabilities without access to physical devices. It is important to study specific malware characterization on emulated or live host IOT device. Unlike a simulator, an emulator provides complete replication of attributes in the emulated host.

Cooja is an emulator offered in the Contiki Operating system environment[92]. It allows developer to test the code before running it on target hardware if need be. This can aid in understanding device behavior before and after malware infection. The emulator has capabilities for ongoing network visualization, mote output prints and timelines. It supports two communication stacks uIP, a lightweight TCP/IP stack that enables internet communication and Rime, a lightweight communication stack for low power radio. Cooja emulates two network protocols namely; Least Interference Beaconing Protocol (LIBP) and the Routing Protocol for Low-Power and Lossy Networks (RPL)[130].

Various free and open source malware analysis tools [131],sandboxes [132] and malware visualization systems[133] exist for common platforms such as Windows, OS X, Linux, and Android. A visual grammar representation for identifying insecure IoT scenarios based on malware analysis data is discussed in [134]. IoTBOX is implemented as first sandbox that caters for 8 CPU architectures.

In the recent past, few IoT honeypots have been proposed. A multi architecture support IoT honeypot (IoTPOT) that detects at least 4 distributed denial of service malware families targeting Telnet based IoT [135]. IoTPOT is the first IOTPOT to publish its malware collected data. Other honeypots includes T-Pot[136], however no research data on their performance and collected malware dataset exists.

CONCLUSION

This survey paper explores various aspects of IoT malware namely the characterization, propagation and analysis support tools. IoT malware is a fast evolving field and has deficits in tools for experimental studies. There is need to develop new or evaluate applicability of the existing malware analysis sandboxes for IoT malware and simulators for malware propagation in heterogeneous. There lacks open IoT malware dataset for researchers to use in their experimental studies. Malware containment for heterogeneous IoT will be an interesting research avenue to pursue.

ACKNOWLEDGEMENTS

This work was supported by EU-Intra-ACP Mobility under Mobility to Enhance Training of Engineering Graduates in Africa (METEGA) grant.

REFERENCES

[1] Zhou, H., *The internet of things in the cloud: A middleware perspective*: CRC press, 2012.

[2] Murthy, D. N. and B. V. Kumar, "Internet of Things (IoT): Is IoT a Disruptive Technology or a Disruptive Business Model?," *Indian Journal of Marketing*, vol. 45, pp. 18-27, 2015.

[3] Bazzani, M., D. Conzon, A. Scalera, M. A. Spirito, and C. I. Trainito, "Enabling the IoT paradigm in e-health solutions through the VIRTUS middleware," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, 2012, pp. 1954-1959.

[4] Doukas, C., I. Maglogiannis, V. Koufi, F. Malamateniou, and G. Vassilacopoulos, "Enabling data protection through PKI encryption in IoT m-Health devices," in *Bioinformatics & Bioengineering (BIBE), 2012 IEEE 12th International Conference on*, 2012, pp. 25-29.

[5] Istepanian, R. S., A. Sungoor, A. Faisal, and N. Philip, "Internet of m-health Things “m-IoT”," in *Assisted Living 2011, IET Seminar on*, 2011, pp. 1-3.

[6] Dada, A. and F. Thiesse, "Sensor applications in the supply chain: the example of quality-based issuing of perishables," in *The Internet of Things*, ed: Springer, 2008, pp. 140-154.

[7] Gu, Y. and T. Jing, "The IOT research in supply chain management of fresh agricultural products," in *Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011 2nd International Conference on*, 2011, pp. 7382-7385.

[8] Shamszaman, Z. U., S. Lee, and I. Chong, "WoO based user centric Energy Management System in the internet of things," in *Information Networking (ICOIN), 2014 International Conference on*, 2014, pp. 475-480.

[9] Wang, M., G. Zhang, C. Zhang, J. Zhang, and C. Li, "An IoT-based appliance control system for smart homes," in *Intelligent Control and Information Processing (ICICIP), 2013 Fourth International Conference on*, 2013, pp. 744-747.

[10] Gerla, M., E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, 2014, pp. 241-246.

[11] Su, K., J. Li, and H. Fu, "Smart city and the applications," in *Electronics, Communications and Control (ICECC), 2011 International Conference on*, 2011, pp. 1028-1031.

[12] Xiong, Z., H. Sheng, W. Rong, and D. E. Cooper, "Intelligent transportation systems for smart cities: a progress review," *Science China Information Sciences*, vol. 55, pp. 2908-2914, 2012.

[13] Jara, A. J., M. A. Zamora, and A. F. Skarmeta, "An architecture based on internet of things to support mobility and security in medical environments," in *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*, 2010, pp. 1-5.

[14] Jara, A. J., M. A. Zamora, and A. F. Skarmeta, "An internet of things---based personal device for diabetes therapy management in ambient assisted living (AAL)," *Personal and Ubiquitous Computing*, vol. 15, pp. 431-440, 2011.

[15] Zhang, X. M. and N. Zhang, "An open, secure and flexible platform based on internet of things and cloud computing for ambient aiding living and telemedicine," in *Computer and Management (CAMAN), 2011 International Conference on*, 2011, pp. 1-4.

[16] Ou, Q., Y. Zhen, X. Li, Y. Zhang, and L. Zeng, "Application of internet of things in smart grid power transmission," in *Mobile, Ubiquitous, and Intelligent Computing (MUSIC), 2012 Third FTRA International Conference on*, 2012, pp. 96-100.

[17] Yun, M. and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in *Advances in Energy Engineering (ICAEE), 2010 International Conference on*, 2010, pp. 69-72.

[18] Atzori, L., A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, pp. 2787-2805, 2010.

[19] Li, S., L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, pp. 243-259, 2015.

[20] Miorandi, D., S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, pp. 1497-1516, 2012.

[21] Abomhara, M. and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, 2014, pp. 1-8.

[22] Abomhara, M. and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security*, vol. 4, pp. 65-88, 2015.

[23] Jing, Q., A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, pp. 2481-2501, 2014.

[24] Samaila, M. G., M. Neto, D. A. Fernandes, M. M. Freire, and P. R. Inácio, "Security Challenges of the Internet of Things," in *Beyond the Internet of Things*, ed: Springer, 2017, pp. 53-82.

[25] Bojanova, I., G. Hurlburt, and J. Voas, "Imagineering an Internet of Anything," *Computer*, pp. 72-77, 2014.

[26] Mattern, F. and C. Floerkemeier, "From the Internet of Computers to the Internet of Things," in *From active data management to event-based systems and more*, ed: Springer, 2010, pp. 242-259.

[27] Vasilomanolakis, E., J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems."

[28] Haller, S., S. Karnouskos, and C. Schroth, *The internet of things in an enterprise context*: Springer, 2008.

[29] Sarma, A. C. and J. Girão, "Identities in the future internet of things," *Wireless personal communications*, vol. 49, pp. 353-363, 2009.

[30] IERC-European Research Cluster on the Internet of Things. (2016, 4th February). *Internet of Things*. Available: http://www.internet-of-things-research.eu/about_iot.htm

[31] Vasilomanolakis, E., J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," in *International Workshop on Secure Internet of Things (SIoT)*, 2015.

[32] Razzaque, M. A., M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 3, pp. 70-95, 2016.

[33] Bandyopadhyay, D. and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, pp. 49-69, 2011.

[34] Xu, T., J. B. Wendt, and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," in *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*, 2014, pp. 417-423.

[35] Consortium, I.-A. (2016, 6th February). *IoT-A – Internet of Things Architecture*. . Available: http://www.iot-a.eu/public/public-documents/d1.5/at_download/file

[36] Consortium, B. (2014, 4th November). *Building the environment for the things as a service*. Available: http://www.betaas.eu/docs/deliverables/BETaaS%20-%20D1.4.2%20-%20TaaS%20Reference%20Model%20v1.0.pdf

[37] Said, O. and M. Masud, "Towards internet of things: Survey and future vision," *International Journal of Computer Networks*, vol. 5, pp. 1-17, 2013.

[38] Filiol, E., "Viruses and malware," in *Handbook of Information and Communication Security*, ed: Springer, 2010, pp. 747-769.

[39] Rey, A. M., "Mathematical modeling of the propagation of malware: a review," *Security and Communication Networks*, vol. 8, pp. 2561-2579, 2015.
[40] Zyba, G., G. M. Voelker, M. Liljenstam, A. Méhes, and P. Johansson, "Defending mobile phones from proximity malware," in *INFOCOM 2009, IEEE*, 2009, pp. 1503-1511.
[41] Zolkipli, M. F. and A. Jantan, "An approach for malware behavior identification and classification," in *Computer Research and Development (ICCRD), 2011 3rd International Conference on*, 2011, pp. 191-194.
[42] Peng, S., S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: A survey," *Communications Surveys & Tutorials, IEEE*, vol. 16, pp. 925-941, 2014.
[43] Karnouskos, S., "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*, 2011, pp. 4490-4494.
[44] Langner, R., "Stuxnet: Dissecting a cyberwarfare weapon," *Security & Privacy, IEEE*, vol. 9, pp. 49-51, 2011.
[45] Zhang, Z.-K., M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities," in *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA)*, 2014, pp. 230-234.
[46] Wolfe, H., "Are cell phones safe?," *Safety and Security Engineering IV*, vol. 117, p. 59, 2011.
[47] Domas, C., "The Memory Sinkhole," *Presentation at Black Hat*, 2015.
[48] Brook, J.-M. and R. Brooks, "A Decade of Lessons Learned: Transforming the Enterprise for Today's Cloud Architecture," in *ICCSM2015-3rd International Conference on Cloud Security and Management: ICCSM2015*, 2015, p. 16.
[49] Bencsáth, B., G. Pék, L. Buttyán, and M. Félegyházi, "Duqu: Analysis, detection, and lessons learned," in *ACM European Workshop on System Security (EuroSec)*, 2012.
[50] Bencsáth, B., G. Pék, L. Buttyán, and M. Felegyhazi, "The cousins of stuxnet: Duqu, flame, and gauss," *Future Internet*, vol. 4, pp. 971-1003, 2012.
[51] Goyal, R., S. Sharma, S. Bevinakoppa, and P. Watters, "Obfuscation of stuxnet and flame malware," *Latest Trends in Applied Informatics and Computing*, pp. 150-54, 2012.
[52] Xu, N., F. Zhang, Y. Luo, W. Jia, D. Xuan, and J. Teng, "Stealthy video capturer: a new video-based spyware in 3g smartphones," in *Proceedings of the second ACM conference on Wireless network security*, 2009, pp. 69-78.
[53] Binsalleeh, H., T. Ormerod, A. Boukhtouta, P. Sinha, A. Youssef, M. Debbabi, *et al.*, "On the analysis of the zeus botnet crimeware toolkit," in *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, 2010, pp. 31-38.
[54] Sood, A. K., R. J. Enbody, and R. Bansal, "Dissecting SpyEye–Understanding the design of third generation botnets," *Computer Networks*, vol. 57, pp. 436-450, 2013.
[55] Internet Census. (2013, 4th February). *Internet census 2012: Port scanning/0 using insecure embedded devices*. Available: http://internetcensus2012.bitbucket.org/paper.html
[56] Bertino, E. and N. Islam, "Botnets and Internet of Things Security," *Computer*, vol. 50, pp. 76-79, 2017.
[57] Chang, W., A. Wang, A. Mohaisen, and S. Chen, "Characterizing botnets-as-a-service," in *ACM SIGCOMM Computer Communication Review*, 2014, pp. 585-586.
[58] Pa, Y. M. P., S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: analysing the rise of IoT compromises," in *9th USENIX Workshop on Offensive Technologies (WOOT 15)*, 2015.
[59] Alazab, M., S. Venkatraman, P. Watters, M. Alazab, and A. Alazab, "Cybercrime: the case of obfuscated malware," in *Global Security, Safety and Sustainability & e-Democracy*, ed: Springer, 2012, pp. 204-211.
[60] Yavvari, C., A. Tokhtabayev, H. Rangwala, and A. Stavrou, "Malware Characterization Using Behavioral Components," in *Computer Network Security: 6th International Conference on Mathematical Methods, Models and Architectures for Computer Network Security, MMM-ACNS 2012, St. Petersburg, Russia, October 17-19, 2012. Proceedings*, I. Kotenko and V. Skormin, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 226-239.
[61] Subrahmanian, V. S., M. Ovelgönne, T. Dumitras, and B. A. Prakash, "Types of Malware and Malware Distribution Strategies," in *The Global Cyber-Vulnerability Report*, ed Cham: Springer International Publishing, 2015, pp. 33-46.
[62] Abed GrÉGio, A. R., V. Monte Afonso, D. S. Fernandes Filho, P. L. De Geus, and M. Jino, "Toward a Taxonomy of Malware Behaviors," *Computer Journal*, vol. 58, pp. 2758-2777, 2015.

[63] Bose, A., X. Hu, K. G. Shin, and T. Park, "Behavioral detection of malware on mobile handsets," in *Proceedings of the 6th international conference on Mobile systems, applications, and services*, 2008, pp. 225-238.

[64] Demme, J., M. Maycock, J. Schmitz, A. Tang, A. Waksman, S. Sethumadhavan, *et al.*, "On the feasibility of online malware detection with performance counters," *SIGARCH Comput. Archit. News*, vol. 41, pp. 559-570, 2013.

[65] Moser, A., C. Kruegel, and E. Kirda, "Limits of static analysis for malware detection," in *Computer security applications conference, 2007. ACSAC 2007. Twenty-third annual*, 2007, pp. 421-430.

[66] Saeed, I. A., A. Selamat, and A. M. Abuagoub, "A survey on malware and malware detection systems," *International Journal of Computer Applications*, vol. 67, 2013.

[67] Van Nhuong, N., V. T. Y. Nhi, N. T. Cam, M. X. Phu, and C. D. Tan, "Semantic Set Analysis for Malware Detection," in *Computer Information Systems and Industrial Management: 13th IFIP TC8 International Conference, CISIM 2014, Ho Chi Minh City, Vietnam, November 5-7, 2014. Proceedings*, K. Saeed and V. Snášel, Eds., ed Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 688-700.

[68] Yu, S., G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic, "Malware propagation in large-scale networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, pp. 170-179, 2015.

[69] Gandotra, E., D. Bansal, and S. Sofat, "Malware Analysis and Classification: A Survey," *Journal of Information Security*, vol. Vol.05No.02, p. 9, 2014.

[70] Deloitte and GSMA. (2012). *Sub-Saharan Africa Mobile Observatory* Available:http://www.gsma.com/publicpolicy/wp-content/uploads/2013/01/gsma_ssamo_full_web_11_12-1.pdf

[71] Tchakounté, F., P. Dayang, J. Nlong, and N. Check, "Understanding of the Behaviour of Android Smartphone Users in Cameroon: Application of the Security," *Open Journal of Information Security and Applications*, vol. 1, pp. 9-20, September 2014.

[72] Laboratories, N. T. I. (2016, 24th February). *Nokia Threat Intelligence Report* Available: http://resources.alcatel-lucent.com/asset/200492

[73] NETAPPLICATIONS. (2017). *Mobile/Tablet Operating System Market Share*. Available: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1&qptimeframe=Y

[74] Singh, M. P. and M. K. Jain, "Evolution of processor architecture in mobile phones," *International Journal of Computer Applications*, vol. 90, 2014.

[75] ARM. (2017, 23rd Feb 2017). *ARMv8-M Architecture*. Available: https://www.arm.com/products/processors/instruction-set-architectures/armv8-m-architecture.php

[76] García, L. and R. J. Rodríguez, "A Peek under the Hood of iOS Malware," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 2016, pp. 590-598.

[77] Deshotels, L., R. Deaconescu, M. Chiroiu, L. Davi, W. Enck, and A.-R. Sadeghi, "SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles," presented at the Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 2016.

[78] Gui, X., J. Liu, M. Chi, C. Li, and Z. Lei, "Analysis of malware application based on massive network traffic," *China Communications*, vol. 13, pp. 209-221, 2016.

[79] Saracino, A., D. Sgandurra, G. Dini, and F. Martinelli, "Madam: Effective and efficient behavior-based android malware detection and prevention," *IEEE Transactions on Dependable and Secure Computing*, 2016.

[80] Malik, J. and R. Kaushal, "CREDROID: Android malware detection by network traffic analysis," in *Proceedings of the 1st ACM Workshop on Privacy-Aware Mobile Computing*, 2016, pp. 28-36.

[81] Fereidooni, H., M. Conti, D. Yao, and A. Sperduti, "ANASTASIA: ANdroid mAlware detection using STatic analySIs of Applications," in *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2016, pp. 1-5.

[82] Wang, Z., J. Cai, S. Cheng, and W. Li, "DroidDeepLearner: Identifying Android malware using deep learning," in *2016 IEEE 37th Sarnoff Symposium*, 2016, pp. 160-165.

[83] Sharma, M., M. Chawla, and J. Gajrani, "A Survey of Android Malware Detection Strategy and Techniques," in *Proceedings of International Conference on ICT for Sustainable Development: ICT4SD 2015 Volume 2*, S. C. Satapathy, A. Joshi, N. Modi, and N. Pathak, Eds., ed Singapore: Springer Singapore, 2016, pp. 39-51.

[84] Narudin, F. A., A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," *Soft Computing*, vol. 20, pp. 343-357, 2016.

[85] Arshad, S., M. A. Shah, A. Khan, and M. Ahmed, "Android malware detection & protection: a survey," *Int. J. Adv. Comput. Sci. Appl*, vol. 7, pp. 463-475, 2016.

[86] Lopez, C. C. U. and A. N. Cadavid, "Machine learning classifiers for android malware analysis," in *2016 IEEE Colombian Conference on Communications and Computing (COLCOM)*, 2016, pp. 1-6.

[87] Malhotra, A. and K. Bajaj, "A survey on various malware detection techniques on mobile platform," *International Journal of Computer Applications* vol. 139, pp. 15-20, 2016.

[88] Chandra, T. B., P. Verma, and A. Dwivedi, "Operating systems for internet of things: A comparative study," in *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, 2016, p. 47.

[89] ARM. (2017, 28th Feb). *mbed uVisor*. Available: https://www.mbed.com/en/technologies/security/uvisor/

[90] Levis, P., S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo, *et al.*, "TinyOS: An operating system for sensor networks," in *Ambient intelligence*, ed: Springer, 2005, pp. 115-148.

[91] Malan, D. J., M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," in *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.*, 2004, pp. 71-80.

[92] Roussel, K., Y.-Q. Song, and O. Zendra, "Using Cooja for WSN Simulations: Some New Uses and Limits," in *EWSN 2016—NextMote workshop*, 2016, p. 319–324.

[93] Casado, L. and P. Tsigas, "ContikiSec: A Secure Network Layer for Wireless Sensor Networks under the Contiki Operating System," presented at the Proceedings of the 14th Nordic Conference on Secure IT Systems: Identity and Privacy in the Internet Age, Oslo, 2009.

[94] Baccelli, E., O. Hahm, M. Günes, M. Wählisch, and T. C. Schmidt, "OS for the IoT - Goals, Challenges, and Solutions," in *Workshop Interdisciplinaire sur la Sécurité Globale (WISG2013)*, Troyes, France, 2013.

[95] Chapra, S. C. and R. P. Canale, *Numerical methods for engineers* vol. 2: McGraw-Hill, 1998.

[96] Diekmann, O., J. Heesterbeek, and J. Metz, "The legacy of Kermack and McKendrick," *Epidemic Models: Their Structure and Relation to Data (D. Mollison, ed.)*, pp. 95-115, 1995.

[97] Kermack, W. O. and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," in *Proceedings of the Royal Society of London A: mathematical, physical and engineering sciences*, 1927, pp. 700-721.

[98] Li, N., Y. Du, and G. Chen, "Mobile Botnet Propagation Modeling in Wi-Fi Networks," in *Proceedings of the 4th International Conference on Computer Engineering and Networks: CENet2014*, E. W. Wong, Ed., ed Cham: Springer International Publishing, 2015, pp. 1147-1154.

[99] Newman, M., *Networks: an introduction*: OUP Oxford, 2010.

[100] Antonio, K. E. S., C. M. N. Pinol, and R. S. Banzon, "An Ising Model Approach to Malware Epidemiology," *arXiv preprint arXiv:1007.4938*, 2010.

[101] Chakrabarti, D., Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos, "Epidemic thresholds in real networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 10, p. 1, 2008.

[102] Dadlani, A., M. S. Kumar, S. Murugan, and K. Kim, "System Dynamics of a Refined Epidemic Model for Infection Propagation Over Complex Networks," *Systems Journal, IEEE*, vol. PP, pp. 1-10, 2014.

[103] Wierman, J. C. and D. J. Marchette, "Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction," *Computational Statistics & Data Analysis*, vol. 45, pp. 3-23, 2/28/ 2004.

[104] Juil C. Martin, Legand L. Burge III, Joseph I. Gill, Alicia N. Washington, and M. Alfred, "Modelling the spread of mobile malware," *International Journal of Computer Aided Engineering and Technology (IJCAET)*, vol. 2, 2010.

[105] Van Mieghem, P., "Epidemic phase transition of the SIS type in networks," *EPL (Europhysics Letters)*, vol. 97, p. 48004, 2012.

[106] Rhodes, C. J. and M. Nekovee, "The opportunistic transmission of wireless worms between mobile devices," *Physica A: Statistical Mechanics and Its Applications*, vol. 387, pp. 6837-6844, 2008.

[107] Wen, S., W. Zhou, J. Zhang, Y. Xiang, W. Zhou, and W. Jia, "Modeling propagation dynamics of social network worms," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, pp. 1633-1643, 2013.

[108] Tang, S. and B. L. Mark, "Analysis of virus spread in wireless sensor networks: An epidemic model," in *Design of Reliable Communication Networks, 2009. DRCN 2009. 7th International Workshop on*, 2009, pp. 86-91.

[109] Nguyen, H.-N. and Y. Shinoda, "On modeling viral diffusion in heterogeneous wireless networks," in *International Conference on Security and Privacy in Mobile Information and Communication Systems*, 2009, pp. 238-252.

[110] Ramachandran, K. and B. Sikdar, "Modeling malware propagation in networks of smart cell phones with spatial dynamics," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, 2007, pp. 2516-2520.

[111] Fan, Y., K. Zheng, and Y. Yang, "Epidemic model of mobile phone virus for hybrid spread mode with preventive immunity and mutation," in *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on*, 2010, pp. 1-5.

[112] Xia, W., L. Zhao-hui, C. Zeng-qiang, and Y. Zhu-zhi, "Commwarrior worm propagation model for smart phone networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, pp. 60-66, 2008.

[113] Mishra, B. K. and S. K. Pandey, "Dynamic model of worms with vertical transmission in computer network," *Applied Mathematics and Computation*, vol. 217, pp. 8438-8446, 2011.

[114] Mishra, B. K. and N. Jha, "SEIQRS model for the transmission of malicious objects in computer network," *Applied Mathematical Modelling*, vol. 34, pp. 710-715, 2010.

[115] Toutonji, O. A., S.-M. Yoo, and M. Park, "Stability analysis of VEISV propagation modeling for network worm attack," *Applied Mathematical Modelling*, vol. 36, pp. 2751-2761, 2012.

[116] Allen, L. J. and A. M. Burgin, "Comparison of deterministic and stochastic SIS and SIR models in discrete time," *Mathematical biosciences*, vol. 163, pp. 1-33, 2000.

[117] Peifeng, W., M. Shang, Z. Hui, and W. Jichao, "Markov Model of Malicious Code Propagation," in *Innovative Computing & Communication, 2010 Intl Conf on and Information Technology & Ocean Engineering, 2010 Asia-Pacific Conf on (CICC-ITOE)*, 2010, pp. 260-263.

[118] Zesheng, C. and J. Chuanyi, "Spatial-temporal modeling of malware propagation in networks," *Neural Networks, IEEE Transactions on*, vol. 16, pp. 1291-1303, 2005.

[119] Rey, Á. M. and G. R. Sánchez, "A CA Model for Mobile Malware Spreading Based on Bluetooth Connections," in *International Joint Conference SOCO'13-CISIS'13-ICEUTE'13: Salamanca, Spain, September 11th-13th, 2013 Proceedings*, Á. Herrero, B. Baruque, F. Klett, A. Abraham, V. Snášel, C. P. L. F. A. Carvalho, *et al.*, Eds., ed Cham: Springer International Publishing, 2014, pp. 619-629.

[120] Bakhshi, Z., M. Z. Lighvan, and R. Mostava, "MP-CA: A Malware Propagation Modeling Methodology Based on Cellular Automata," *International Journal of computer Networks and Communication Security.*, vol. 3, March 2015.

[121] Zou, C. C., W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," in *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 138-147.

[122] Song, Y., G.-P. Jiang, and Y. Gu, "Modeling malware propagation in complex networks based on cellular automata," in *Circuits and Systems, 2008. APCCAS 2008. IEEE Asia Pacific Conference on*, 2008, pp. 259-263.

[123] Yurong, S. and J. Guo-ping, "Modeling malware propagation in wireless sensor networks using cellular automata," in *Neural Networks and Signal Processing, 2008 International Conference on*, 2008, pp. 623-627.

[124] Peng, S., G. Wang, and S. Yu, "Modeling the dynamics of worm propagation using two-dimensional cellular automata in smartphones," *Journal of Computer and System Sciences*, vol. 79, pp. 586-595, 8// 2013.

[125] Li, P., S. Liu, J. Jin, and Z. Wang, "Influence of node mobility on virus spreading behaviors in multi-hop network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, p. 172, 2016.

[126] Bose, A. and K. G. Shin, "Agent-based modeling of malware dynamics in heterogeneous environments," *Security and Communication Networks*, vol. 6, pp. 1576-1589, 2013.

[127] Hosseini, S., M. Abdollahi Azgomi, and A. Rahmani Torkaman, "Agent-based simulation of the dynamics of malware propagation in scale-free networks," *Simulation*, vol. 92, pp. 709-722, 2016.

[128] del Rey, A. M., A. H. Encinas, J. H. Guillén, J. M. Vaquero, A. Q. Dios, and G. R. Sánchez, "An Individual-Based Model for Malware Propagation in Wireless Sensor Networks," in *Distributed Computing and Artificial Intelligence, 13th International Conference*, 2016, pp. 223-230.

[129] del Rey, A. M., A. H. Encinas, J. M. Vaquero, A. Q. Dios, and G. R. Sánchez, "A method for malware propagation in industrial critical infrastructures," *Integrated Computer-Aided Engineering*, vol. 23, pp. 255-268, 2016.

[130] Pignolet, Y.-A., I. Rinis, D. Dzung, and A. Karaagac, "Heterogeneous multi-interface routing: networking stack and simulator extensions," in *Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on*, 2012, pp. 1-6.

[131] Zeltser, L. (2015, 31st January). *Free Toolkits for Automating Malware Analysis*. Available: https://zeltser.com/malware-analysis-tool-frameworks/

[132] Zeltser, L. (2016, 31st January). *Free Automated Malware Analysis Sandboxes and Services*. Available: https://zeltser.com/malware-analysis-tool-frameworks/

[133] Wagner, M., F. Fischer, R. Luh, A. Haberson, A. Rind, D. A. Keim, *et al.*, "A survey of visualization systems for malware analysis," in *EG Conference on Visualization (EuroVis)-STARs*, 2015, pp. 105-125.

[134] Rodríguez-Mota, A., P. Escamilla-Ambrosio, J. Happa, and J. Nurse, "Towards IoT cybersecurity modeling: From malware analysis data to IoT system representation," in *Communications (LATINCOM), 2016 8th IEEE Latin-American Conference on*, 2016, pp. 1-6.

[135] Pa, Y. M. P., S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," *Journal of Information Processing*, vol. 24, pp. 522-533, 2016.

[136] Project, D. T. A. H. (2015, 14th Nov). *T-Pot: A Multi-Honeypot Platform*. Available: http://dtag-dev-sec.github.io/mediator/feature/2015/03/17/concept.html

AUTHORS

Evanson Mwangi Karanja is currently a PhD Research student at the University of Botswana, Department of Electrical Engineering, Faculty of Engineering and Technology . His research focuses on Internet of Things malware synthesis. He holds a M.Sc. in Computer Science from Makerere University in Uganda and a Bsc from Jomo Kenyatta University of Agriculture and Technology.

Shedden Masupe is Professor in Computer Engineering at the School of Engineering and Technology, BIUST and an executive director in charge of Technologies at Botswana Institute for Technology Research and Innovation. He holds a Ph.D. in Electronics (Edinburgh University), M.Sc. in Electronics Engineering (Digital Systems) from Cardiff University, Cardiff, United Kingdom. Prof Masupe also holds a BSc Eng.(Electrical), specialising in Communications and Fields from University of New Brunswick, Fredericton, New Brunswick, Canada. and a BSc (Maths & Physics) from Mount Allison University, Sackville, New Brunswick, Canada.

Mandu Gasennelwe-Jeffrey received her PhD in Electronic Engineering (Control Systems) from the University of Pretoria, South Africa. She also holds an MSc in Systems Engineering from the University of Wales, Cardiff, UK; a BA degree in Mathematics from York University, Toronto, Canada; and a BEng degree in Electrical Engineering from Ryerson Polytechnical Institute, Toronto, Canada.