# IoT Security Threats and Risks Mitigation

## Information Security Threats by "One Alert Way"

Ashok Kumar N R [1]
BE 7th Sem:
Dept of Information Science & Engineering Dayananda Sagar College of Engineering, Bengaluru

Chandrakala B M [2]
Asst Prof:
Dept of Information Science & Engineering Dayananda Sagar College of Engineering, Bengaluru

***Abstract*—Security is one of the major issues which today's advanced IoT threats need a detailed incident response strategy when sophisticated hacking attacks. This paper presents straightforward and modular lightweight high interaction honeypot with checksum approach can investigate further mitigate undetected security risks.**

***Keywords—Honey tokens; IoT Security challenges; Defender; Incident response;***

## I. INTRODUCTION

Cities around the world are progressively becoming smart not surprisingly, It's been IoT (Internet of Things) to IoE (Internet of Every Thing) era, Sapless security may affect the lives of millions of users privacy, Security and Trust. 2015 has also been the year of international cyber treaties to help impede attacks. Security threats are everywhere the typical Insider threats or Zero-day attack lasts an average of eight months or years without knowing it. That unleash attacks adequate time to steal valuable assets . Due to number and types of vulnerabilities continuing to grow exponentially with the propagation of emergence of IoT(Internet of Things), Bring Your Own Device (BYOD).Intrusion detection system (IDS), Anti-virus(AV) and intelligence feeds generate so much data technologies to collect, analyze, and report data network architecture is only half the battle, implements controls. Today's IoT related threats need a detailed incident response strategy when it matters to follow when you become breached. The remaining of the paper is organized as follows. In section 2 literature survey discuss ENISA top threat Landscape trends. Problem definition on section 3. Section 4 proposed method on section 5 and 6 deals with the experiment setup and observations results.

## II. LITERATURE SURVEY

*The European Union Agency for Network and Information Security (ENISA)[3].*

Threat Landscape 2015 | 2016 top emerging threats to smart environments/connected devices are:

1. Malware
2. Botnets (IoT components as botnet nodes and/or C2 servers)
3. Identity theft
4. Web based attacks
5. Physical theft/damage/loss
6. Phishing
7. Insider threat
8. Information leakage
9. Web application attacks
10. DNS poisoning

Well deployed sensors can be invaluable tools in the defenders arsenal aim to reveal attacker tools, techniques and undiscovered vectors, by entrapping attackers through emulation of common protocols and services and don't need to look anything like the honeypots of old.

## III. THE IOT RISKS

Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices. Criminals can use these opportunities to remotely facilitate attacks on other systems, send malicious and spam e- mails, steal personal information, or interfere with physical safety.[7]

### *A. The IoT dynamics:*

An exploitation of the Universal Plug and Play protocol (UPnP) to gain access to many IoT devices. UPnP is designed to self-configure when attached to an IP address, making it vulnerable to exploitation. Cyber actors can change the configuration, and run commands on the devices, potentially enabling the devices to harvest sensitive information or conduct attacks against homes and businesses, or engage in digital eavesdropping;[7].

### *B. Possible Attack Vectors*

An exploitation of default passwords to send malicious and spam e-mails, or steal personally identifiable or credit card information.

Compromising the IoT device to cause physical harm.
Overloading the devices to render the device inoperable

Interfering with business transactions [7].

### *C. Characteristics of the IoT security model*

Characteristics of the IoT security model.
Precise control over security policy: Response to the same threat can vary depending on the system the threat is targeting.
Comprehensive cyber security threat detection and mitigation.

Actionable intelligence: Fog nodes analyze real-time data from switches, routers, video surveillance cameras, door controllers, and other IoT devices to detect security threats.

Automated decisions: The fog nodes instruct other IoT devices to take action based on policy. Avoiding the need for human intervention when appropriate speeds up response and improves outcomes.

## IV. PROBLEM DEFINITION

A physical honeypot is a genuine host machine on the system with its own particular IP are often high-interaction, so allowing the sensors to be fully compromised, The estimation of a honeypot is controlled by the data that we can get from it, They are expensive to install and maintain for large address spaces, it is impractical to deploy a physical honeypot for each IP address on each IoT devices such as single board computers.

In that case, Deploy virtual honeypots to detect malicious behavior, NIDS (Network Intrusion Detection System) require signatures of known attacks and often fail to detect compromises that were unknown at the time it was deployed.

On the other hand, honeypots can detect vulnerabilities that are not yet understood. Consequently, forensic analysis of data collected from honey pots is less likely to lead to false positives than data collected by NIDS bringing honeypots back an awesome thought tempered by over decade of sublime misapplication resulting in a slow relegation to the realm of academia and slightly dubious research,

But it doesn't have to be that way because a honeypot has true production value.

## V. PROPOSED METHOD

Modular and decentralized open source honeypot attempt to contact suspicious to analyze various attacks regarding the honeypot as an internal distributed sensor rather than a standalone alert generator.[8]

Each event reported is a high-quality indicator of investigation-worthy activity and each open canary instance feeds event data to a correlators which produces single alerts even in the face of network-wide scans. With such a high signal-to-noise ratio, every alert requires investigation. This is in contrast to the stream of alerts produced by tools such as anti-virus, network IDS or traditional honeypots.

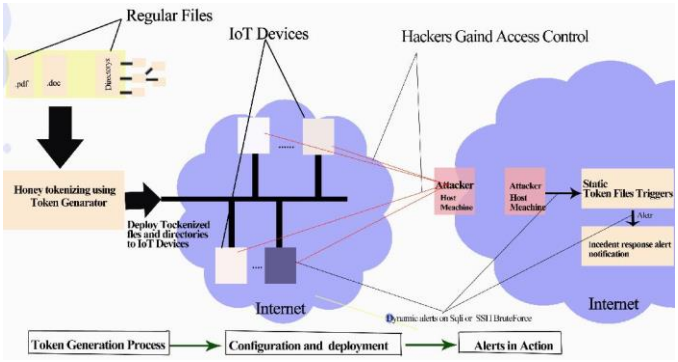


Fig. 1. On premise deployment architecture

Implementing hashing mechanism to prevent malware targeted to exploit the original application source code on production nodes for the proactive protection the honey token system are deployed tokens can be activated in a verity of ways, including on file I/O's, Database queries, Cloned websites, Process executions and changes in order to detect unauthorized attempts to use information breaches happens organizations to governments smart computing environment including smart city solutions requires painless way to help defenders discover they've been breached.

## VI. EXPERIMENT SETUP

Several Popular programming languages and Linux based systems ships several built-in functionality including hashing utilities like md5 (md5sum) sh1 and so on., Shell scripts and cron jobs great way automate hash generation and comparison for a large number of files on the system to verify its integrity. The original application source code file hashes are generated and tested across all on production nodes if any changes are found on checksum value rather the trusted hash values from original source file can be easily detected and continue further action on it. The sums are computed as described in RFC 1321.

For the proactive protection honey tokens helps track activity and actions on your network by spinning up dockerized canary tokens container requires At least one public IP and Domain name.

Configure A record type on DNS records if using Top-level domain (TLD) or ccTLD (country code top-level domain) or add CNAME record type to DNS (Domain Name System) records if you are using sub domain according your needs and wait for propagation changes on DNS after visit enter your email and tag and click generate button and you ready to trigger the generated tokens via several different ways variety of ways, including email addresses, DNS requests on cloned websites, Social Networking profiles, database queries and changes.

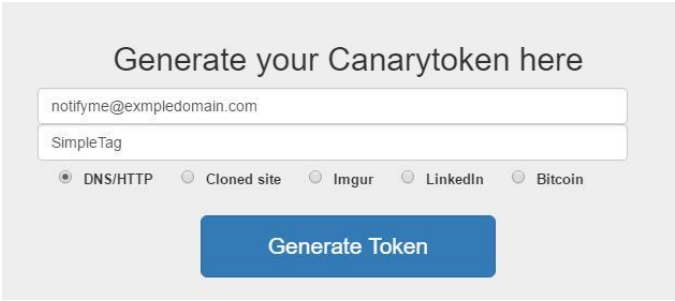


Fig. 2. Web UI for generating tokens

Generated token can be triggered in a numbers of ways, including process executions, DNS requests, email addresses, file reads, Social networking profiles, database DML queries changes,

*OBSERVATIONS AND RESULTS*

It is very essential to provide the security to IoT devices so one can share the information without any interference.


Fig. 3. Sample email notification when token was triggered

Initially by applying the appropriate updates to the operating system and application level regularly helps to keep the systems healthier.

Periodically check the web server directories and application source files for any malicious or unknown changes with File Checksum Integrity Verifier. Example usage on Linux based systems:

Example usage on Windows based

systems: C:\md5x>fciv.exe testdb.sql

Generated 32 bytes of checksum 96789f31bba08906f92fd7718823581c testdb.sql

## CONCLUSION

In this paper, We have presented when sophisticated hacker prowling a target IoT network look for juicy info leads to a trap and triggering email alert help defenders discover they've been breached we choose a simplistic way to implant traps in production systems incredibly flexible to defend the further attacks and secure the hosts making use of checksum integrity verifier utilities.

## REFERENCES

[1] "2010 DATA BREACH INVESTIGATIONS REPORT, A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service", Available: http://www.verizonenterprise.com/resources/reports/rp_20 10-data-breach-report_en_xg.pdf
[2] Cesar Cerrudo,"An Emerging US (and World)Threat: Cities Wide Open to Cyber Attacks," [Online] Available: http://securingsmartcities.org/wp-content/uploads/2015/05/CitiesWideOpenToCyberAttacks.pdf
[3] ENISA Threat Landscape 2015 | January 2016 Report [Online]. Available: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015.
[4] Fortinet,"Solution Guide: Secure Access Architecture"
[5] Ministry of Security and Public Administration, "Software development security guide for electronic government SW development operator", May (2012)
[6] "Ministry of Security and Public Administration", Secure Coding Inspection Guide for e-gov SW, (2014)
[7] www.mit.gov.in
[8] https://github.com/thinkst/canarytokens
[9] https://github.com/thinkst/opencanary
[10] https://www.rt.com/usa/217495-sony-hack-fbi-north- korea/
[11] http://canarytokens.org/generate
[12] http://blog.thinkst.com/p/canarytokensorg-quick-free-detection.html