Workshop Title

Internet of 'Hidden' Things: How to Build a Confidential IOT Network using TOR & Docker Containers

Abstract

TOR (The Onion Router) is a volunteer-based distributed overlay network that allows anonymous publishing of TCP services. These location Hidden Services (HS) operate under the. onion Top-Level Domain & can only be accessed through the TOR network, whilst maintaining anonymity of the Client as well as the Hidden Server. Docker on the other hand is a software containerization technology which provides an additional layer of abstraction & automation to OS-level virtualization, allowing a developer to package up an application with all of its libraries & dependencies into one container and ship it. Docker containers are lightweight by design and ideal for enabling accelerated development of microservices, which make it easy to compose, deploy and maintain complex cloud applications.

Now, with the advent of IOT, every electronic 'Thing' is getting Smart, which brings a plethora digital threats into the physical world. The ubiquitous connectivity to Internet is bringing up new Privacy & Anonymity challenges which are rising as never before. Our purchasing patterns, browsing patterns, driving habits, eating habits, health indicators, places we visit, social data, contacts and pretty much every personally identifiable data is being collected by Smart devices and are sent to huge Server Farms or the Cloud which then knows all, remembers all, and happily shares and/or monetizes them all. There's a lack of transparency between the data being collected and what it is being used for. Hence, the contemporary situation demands a paradigm shift in the existing infrastructure of IOT Businesses, where Proprietary protocols, indigenous hardware & air-gapped networks are not just enough for security & privacy in the era of Industry 4.0.

This workshop will sensitise the audience about how we can leverage the anonymity & containerisation benefits of TOR & Docker technologies to address the security & privacy challenges in IOT Businesses and stop Surveillance Capitalism. There will be several Live Demos on how to build an Internet of 'Hidden' Things by creating confidential, authenticated and anonymous IOT Applications using TOR Hidden Services amalgamated with Docker Containers. The demos will show that these 'Hidden' Things/Devices can even hide the fact they exist at all, if you don't know the necessary cookie. One can neither crawl nor probe your IOT device through the Internet while your device uses the Onion Authentication feature of TOR Hidden Services. The workshop would also cover the dark-side of using Internet of Hidden Things in future.

Following is the digest of the presentation:

1. Introduction to TOR Hidden Services (HS)

- HS Rendezvous Protocol
- Analysis of hiddenness of HSs

2. Introduction to Docker Containers
- Virtualization vs Containerization
- Security Advantages of using Docker Containers

3. Dark-Side of Internet of Things
- How Smart Devices are bridging the gap between Digital threats & Physical threats?
- Top recent IOT Hacks: Chrysler's Jeep Cherokee, Mattel's Wi-fi Hello Barbie, Mirai DDoS Botnet
- Era of Ubiquitous Surveillance: Data being the new Oil of 21st century
- Security vs Privacy vs Anonymity: Importance of Trust in IOT Privacy

4. Need for Internet of 'Hidden' Things
- Security by Obscurity vs Security by Design
- Achieving Privacy with Hidden IOT Devices
- How to leverage the anonymity & containerisation benefits of TOR & Docker in IOT
- How hidden & anonymous IOT Devices can stop Surveillance Capitalism

5. Live Demos:
- Hosting Tor Hidden Service in seconds with Docker Containers
- Pushing Tor-enabled hidden containers to Linux-based IOT devices for hiding them & avoid probing
- Connecting anonymously to hidden IOT devices with proper authentication

6. Dark-Side of Internet of Hidden Things
- How hidden IOT devices can be exploited for malicious purposes

7. Discussion & Takeaways
- Conclusion & Futuristic Thoughts.

Audience Information

Anyone from techies, design engineers, developers, system architects and entrepreneurs who want to learn & know about IOT Privacy Challenges and its possible solutions.

Attendee Takeaways

1. Demystifying IOT Infrastructure fundamentals & Learning how every electronic device is getting Smarter.
2. Advance the state of knowledge in the field of IOT Security & Privacy Challenges
3. Understanding why Privacy & Anonymity are taking lead over Security in the IOT Ecosystem.
4. In depth analysis into Tor Anonymity Protocol and its application in latest state-of-the-art IOT Business Models.
5. Identifying the key elements in establishing an Internet of 'Hidden' Things for Smart & Privacy-aware IOT services.

Prerequisite knowledge

Basic knowledge about Enterprise Computer Networks, Cryptography, Cyber Security and Smart Devices