Internet of Things Security

Lecture 6: Context Aware Security in IoT

Mehmoona Jabeen

Mehmoona.jabeen@au.edu.pk

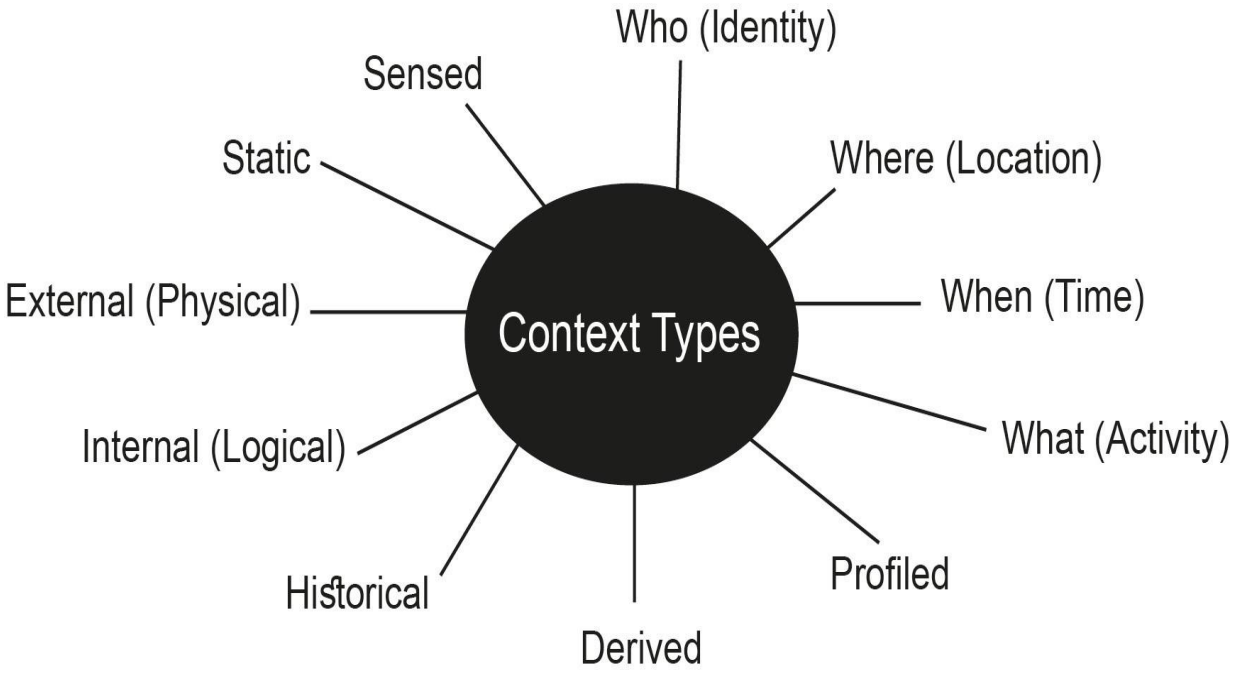
Department of Cyber Security, Air University

Lecture Outlines

- What is Context Awareness?
- Motivation
- Context Awareness in Cyber Security
- Recent Work on Context Aware Cyber Security
- Hybrid model of ML and Context Awareness in Cyber Security

What is Context

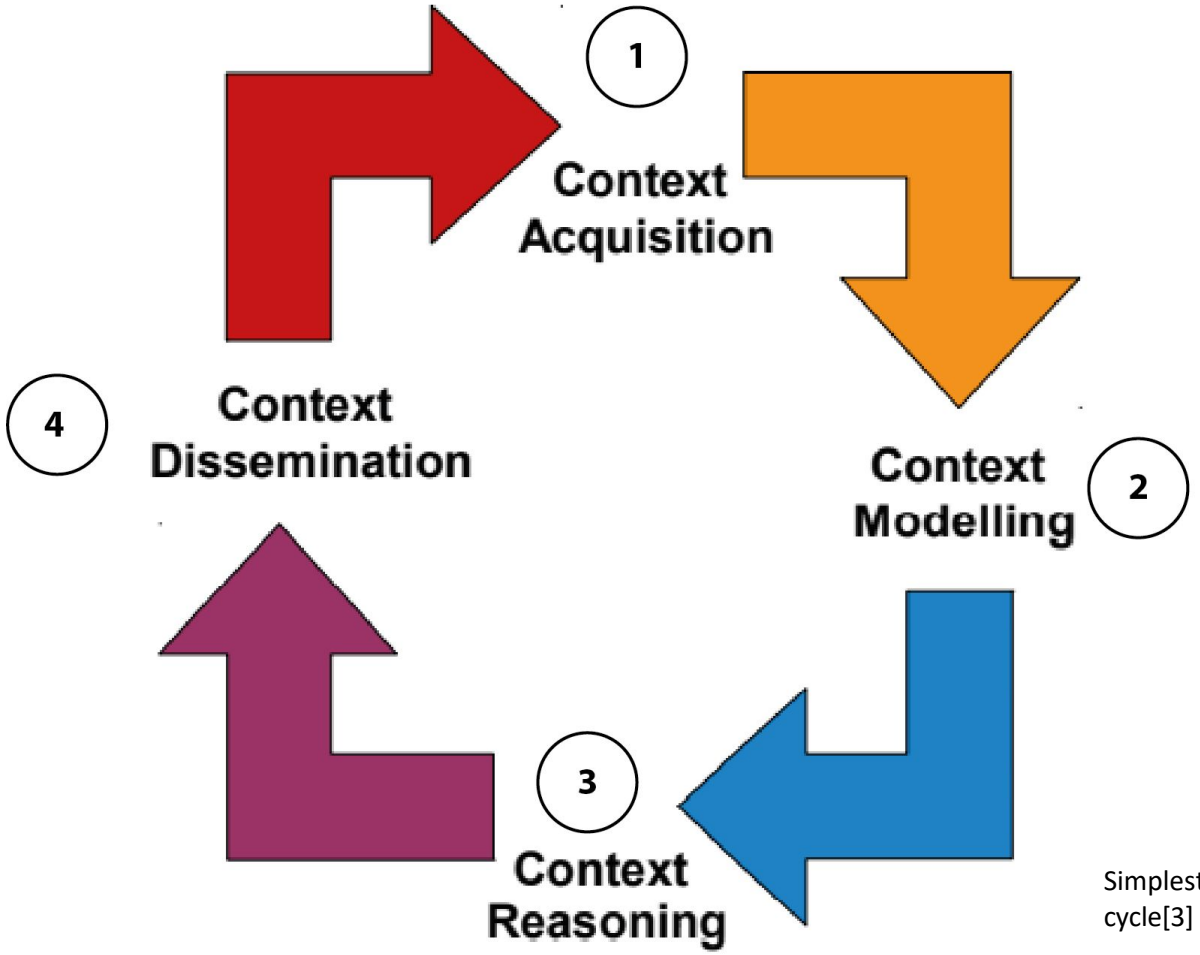
- Any information about the circumstances that characterize an event or situation.
- Context in this lecture situation could be:
  - Speaker bio
  - Topic of this lecture
  - Time schedule and duration
  - Participants
  - Dates and venue of the event
  - Anything that describes the situation...



Context Awareness

- A system is context-aware if it uses context to provide relevant information and/or services to the user.
- System dynamically adapts to the situation of the user.
- For example
  - A tablet computer switching the orientation of the screen, adapting the zoom level to the current speed, and switching on the backlight
  - A smart AC changes the thermostat to a level when a user is sleeping or gossiping at home

Context Awareness Cycle



Simplest form of a context life cycle[3]

Context Acquisition

- Techniques used to gather context are:
- Push and Pull Method
- Acquire directly from sensor Hardware
- Acquire through a middleware Infrastructure
- Acquire from context servers
- Acquire from Physical, Virtual & Logical sensors
- Manually provided, sensed & derived

Context Aware Cycle

Key-Value Modelling

It models context information as key-value pairs in different formats such as text files and binary files.

Markup Scheme

It models data using tags. Therefore, context is stored within tags.

Graphical Modelling

It models context with relationships. Some examples of this modelling technique are Unified Modelling Language (UML) and Object Role Modelling (ORM).

Object Based

It is the concepts are used to model data using class hierarchies and relationships. Object oriented paradigm promotes encapsulation and re-usability.

Logic Based

Facts, expressions, and rules are used to represent information about the context. Rules are used by other modelling techniques, such as ontologies, as well.

Ontology Based

The context is organized into ontologies using semantic technologies. A number of different standards (RDF, RDFS, and OWL).

Context Reasoning

- Method of deducing new knowledge, and understanding better, based on the available context.

Supervised Learning

For situation where the feature set is easily identifiable, possible outcomes are known, and large data sets are available in numerical terms.

Unsupervised Learning

For situations where possible outcomes are not known.

Rules

For situations where raw data elements need to be converted in to high level context information. Suitable to be used to define events.

Fuzzy Logic

For situation where low-level context need to be converted in to high-level more natural context information.

Ontology Based

For situations where knowledge is critical. Can reason both numerical and textual data.

Probabilistic Logic

For situations where probabilities are known and coming evidence from different sources are essential.

Context Distribution

- How to deliver context to the consumers?
- In consumer Perspective it is same as Acquisition.
- Query Based Method
- Subscription/ Publish

Motivation of using context awareness

- Traditional security mechanisms use static parameters and policies for decision making.
- IoT is a dynamic environment with huge scale.
- Rapid growth of IoT attacks in recent years.
- Unawareness about consequences of attacks to users.

Context Aware Security

"A set of information collected from the user's environment and the application environment and that is relevant to the security infrastructure of both the user and the application[4]."

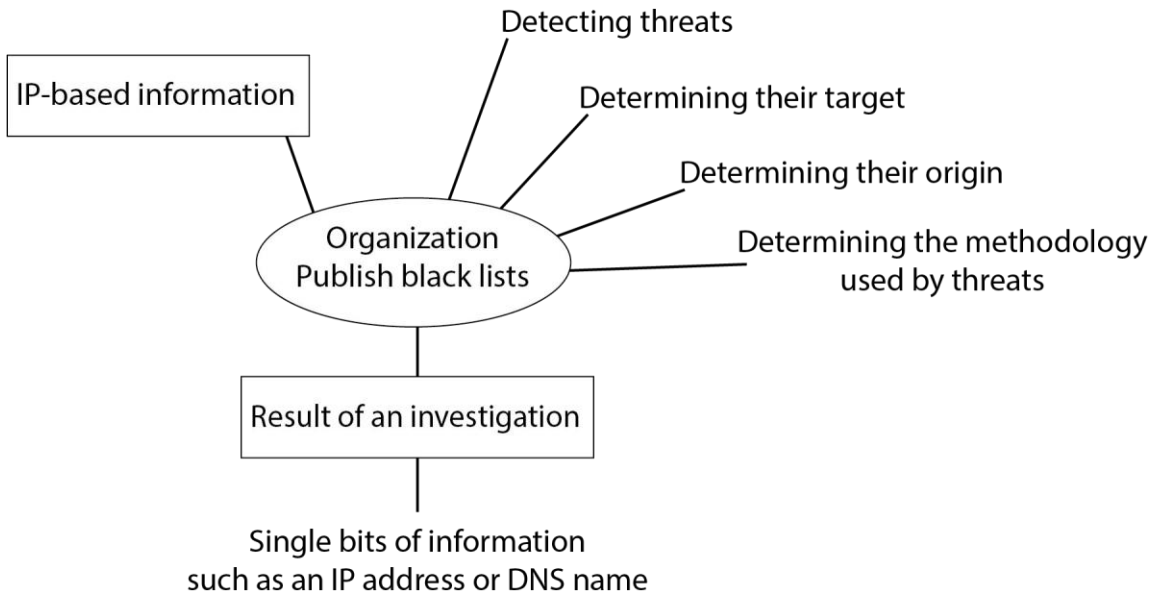
Mostefaoui and Brezillon

- Context-aware security appears as a viable choice for IoT security.
- It uses the context information of IoT environments thus providing dynamic security.

Context Awareness in Security Perspective

- Context-awareness can be used in access control for authentication. For example, access from New York can differ from access rights required from London.
- Context-awareness can also be used in anomaly detection.
- Network firewalls can benefit from the knowledge inferred from devices and user behavior

Importance of Context



Flaws of not using context

- What are the details of the Traffic that generated the alert? Is it a real attack or a false-positive?
- How much to consider it compared to other signals from their environment or how relevant it is to them.

Contextual Information

Is the alert plausible?
Is the solution known to have false positives?

Is this event common?
Whether a similar event has been previously reported as false-positive?

What is known about the source?
Is it blacklisted for visible traffic reasons?

Were there related events in the system?

Is there any additional information that would be useful?

Attacks Report

Kaspersky data showed that more than **1.5 billion attacks** have occurred against IoT devices during the first six months of 2021.

Malicious domains

Khan et al. (2020)

Checkpoint Risk Intelligence
3% of these domains are malicious
5% of them are suspicious

66 hospitals in South Africa affected by DDoS attacks

Denial of service attack

WHO (2020a) and CDC (2020)

First National Bank (FNB) in South Africa has been confronted with malware

Malware Attacks

Ganiyu and Jimoh (2018)

More than 1.7 million user accounts were hacked into at Nedbank in February 2020

Business email compromise

Dixon and Balson (2020)

Recent Work on Security without Context

A Supervised Intrusion Detection System for Smart Home IoT Devices

Problem: IoT devices introduce tremendous security flaws

Proposed Scheme: A three layer intrusion detection system (IDS)

Approach Used: Supervised Machine Learning

Use Case Used: Smart Home Devices

Future Work: Evaluate on more complex and more sophisticated attacks

Drawback:

More false positive ratio Static Approach

Eirini Anthi, Lowri Williams and Pete Burnap, Published in IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 5, OCTOBER 2019

Limitation of Machine Learning

Issue with supervised ML/DL approaches

- Producing a new labelled dataset is expensive.
- Privacy issues often limit data acquisition.
- High variability of environments, situation, sensors and infrastructure setup.

Limitation of Semantic Technology

Issue with dynamic ontology approaches

- Collection of sufficient domain-related data is expensive.
- Structure becomes complex for large amount of data.
- Cause reasoning process to be resource intensive and slow.

Hybrid Model of Context Aware Security

Context of a device gather by ontology:

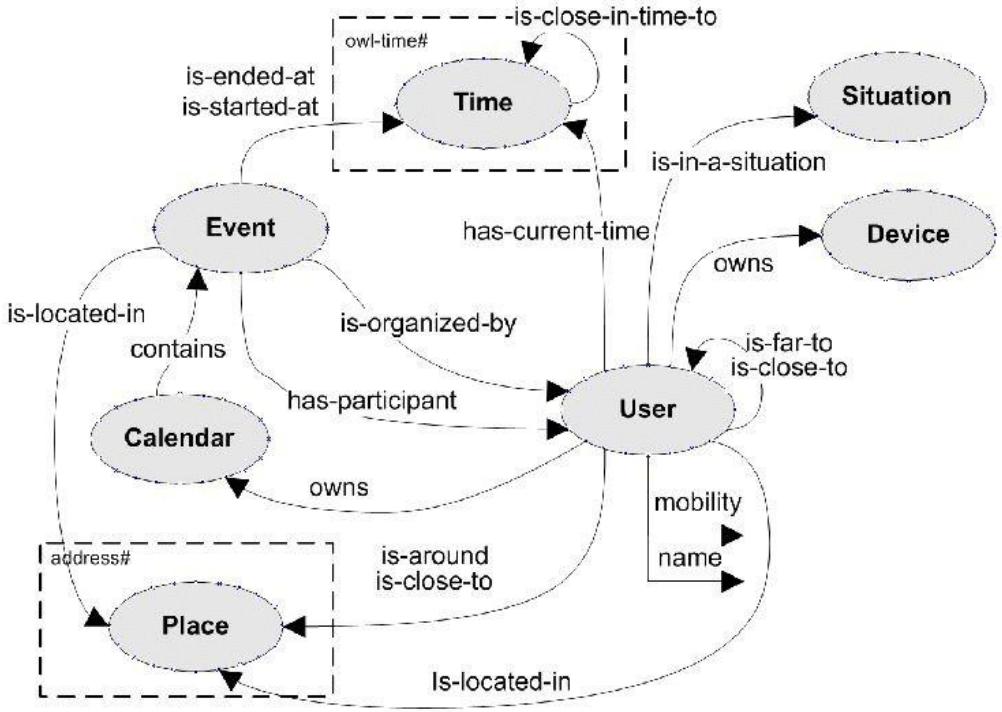


Figure 1. Visualization of User Ontology

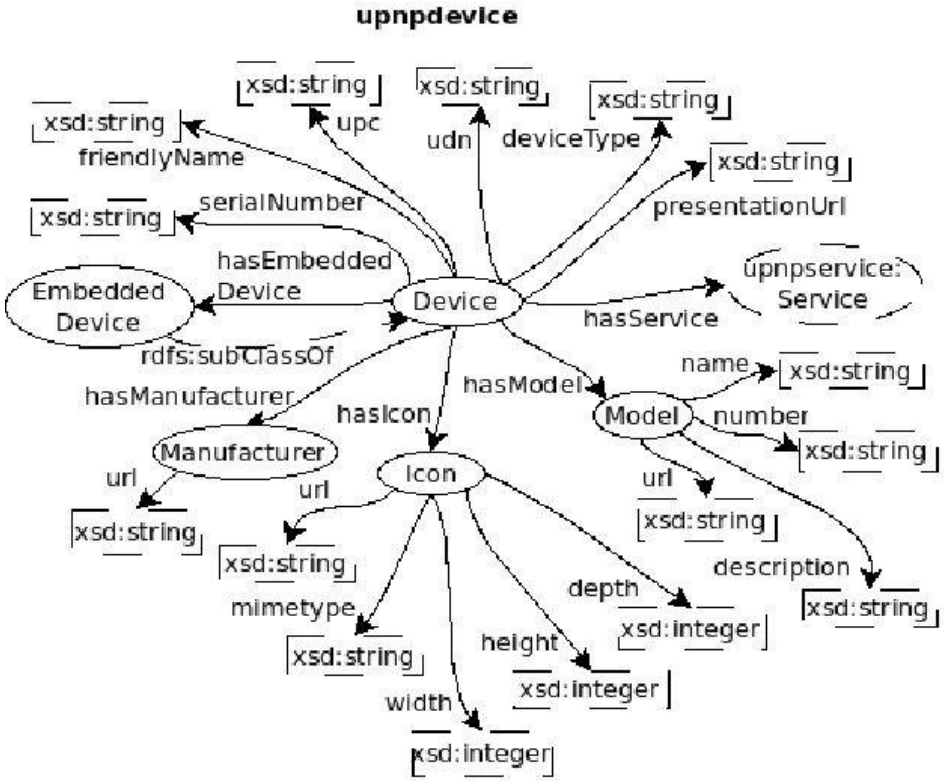


Figure 2. Visualization of UPnP Device Ontology

Context Aware Security Use case

Ransomware Attack:

Kia Motors

In February 2021, car manufacturer Kia Motors America (KMA) was the victim of a ransomware attack.

Internal and customer-facing systems affected by it.

Including mobile apps, payment services, phone services, dealerships' systems and IT systems of delivery of new vehicles.

DoppelPaymer was believed to be the ransomware family that targeted Kia.

Context Aware Security Use case

Ransomware Attack:

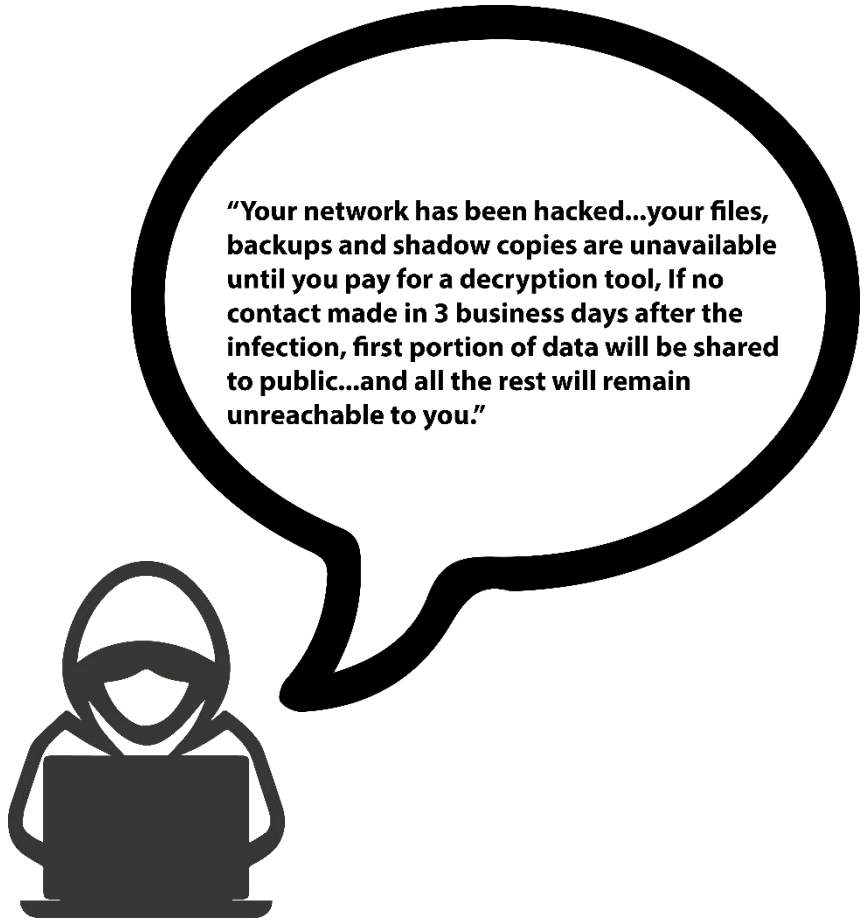
Kia Motors

An employee clicking on a phishing email.

Kia Motors America denied it

had suffered a “ransomware” attack

Because they have a backup.

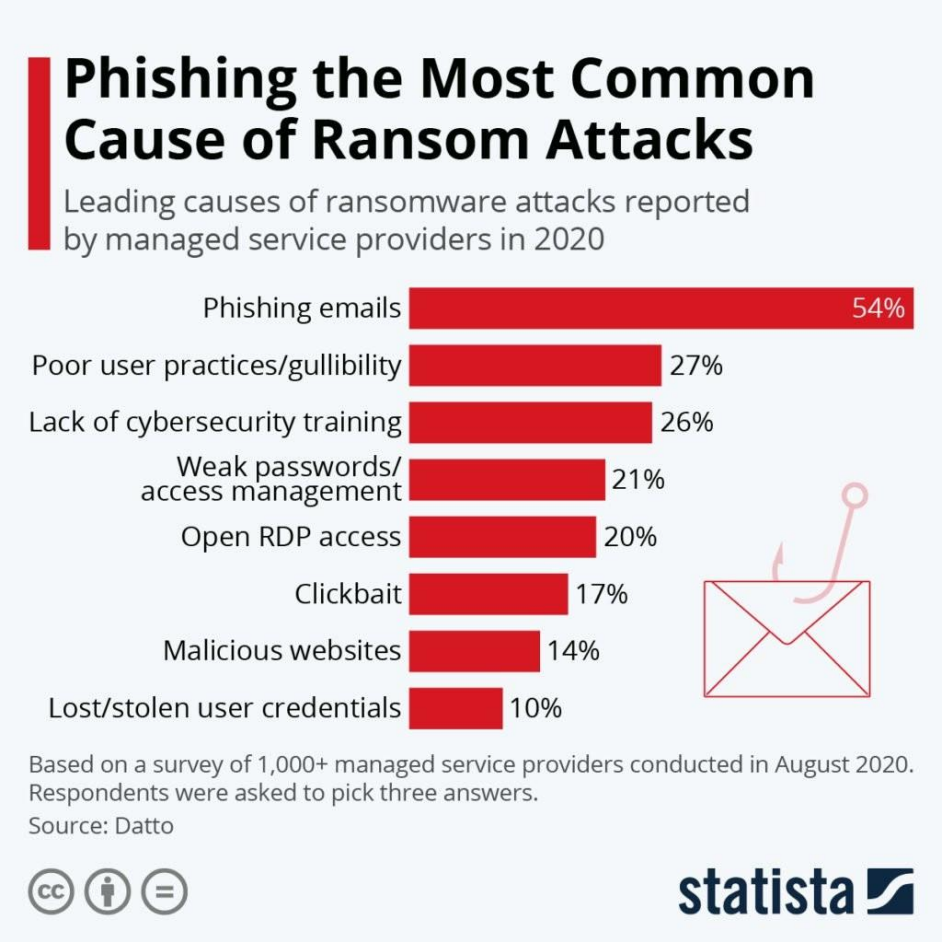


Context Aware Security Use case

Ransomware Attack Reasons:

Datto’s Global State of

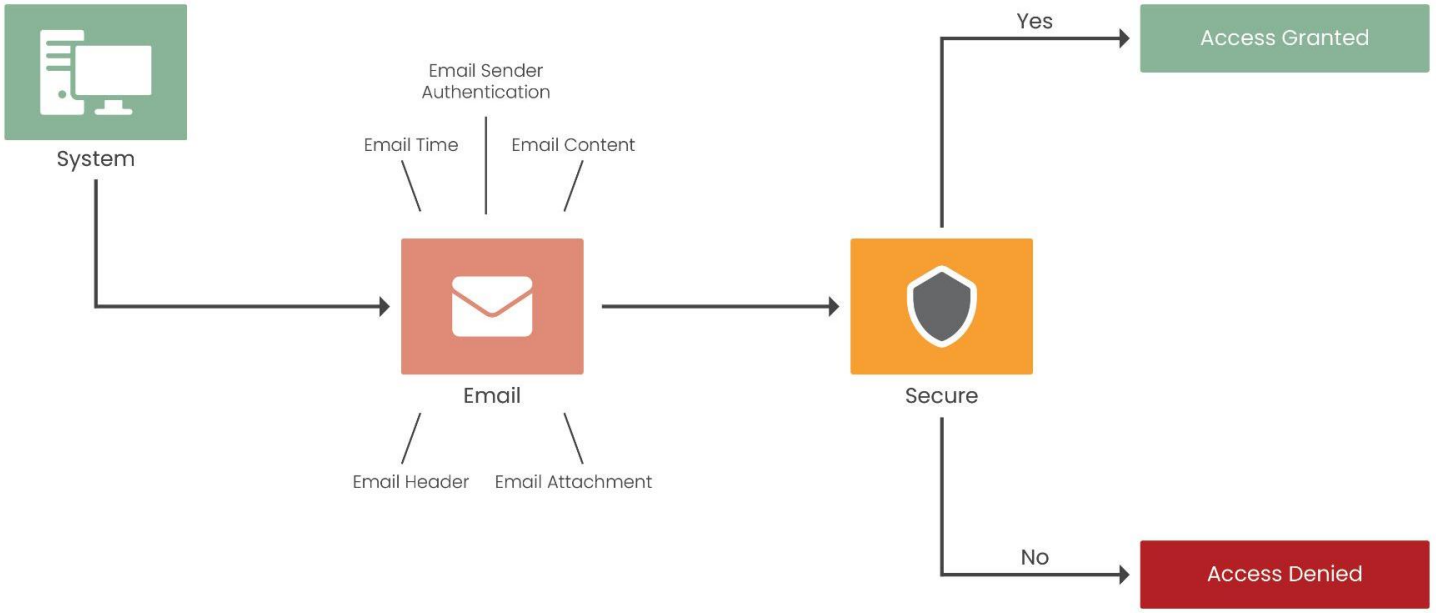
Channel Ransomware Report.



Context Aware Security Use case

Context-Aware Security Technique:

If the system had been sufficiently aware of the email context, the attack could have been avoided.



Context-Aware System Diagram

Context Aware Security Use case

IoT Attacks:

The new **BotenaGo malware botnet** discover thirty exploits to attack millions of routers and IoT devices like routers, modems, and NAS devices.

Some notable examples given below:

CVE-2015-2051, CVE-2020-9377, CVE-2016-11021: D-Link routers

CVE-2016-1555, CVE-2017-6077, CVE-2016-6277, CVE-2017-6334: Netgear devices

CVE-2019-19824: Realtek SDK based routers

CVE-2017-18368, CVE-2020-9054: Zyxel routers and NAS devices

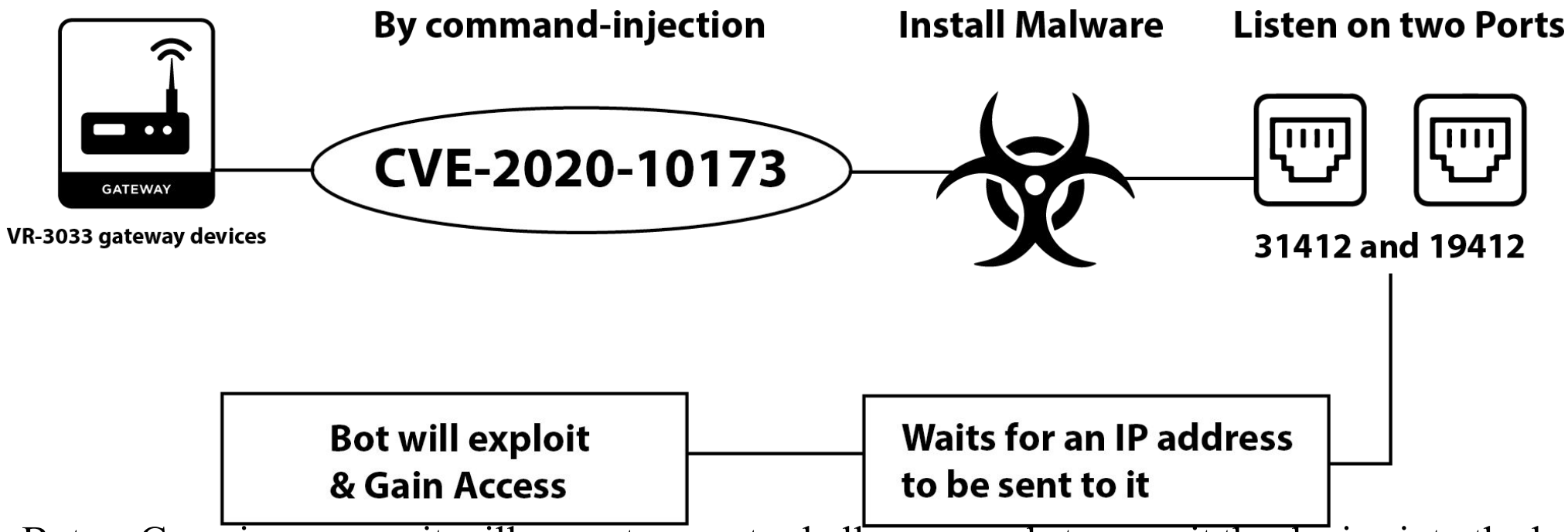
CVE-2020-10987: Tenda products

CVE-2014-2321: ZTE modems

CVE-2020-8958: Guangzhou 1GE ONU

Context Aware Security Use case

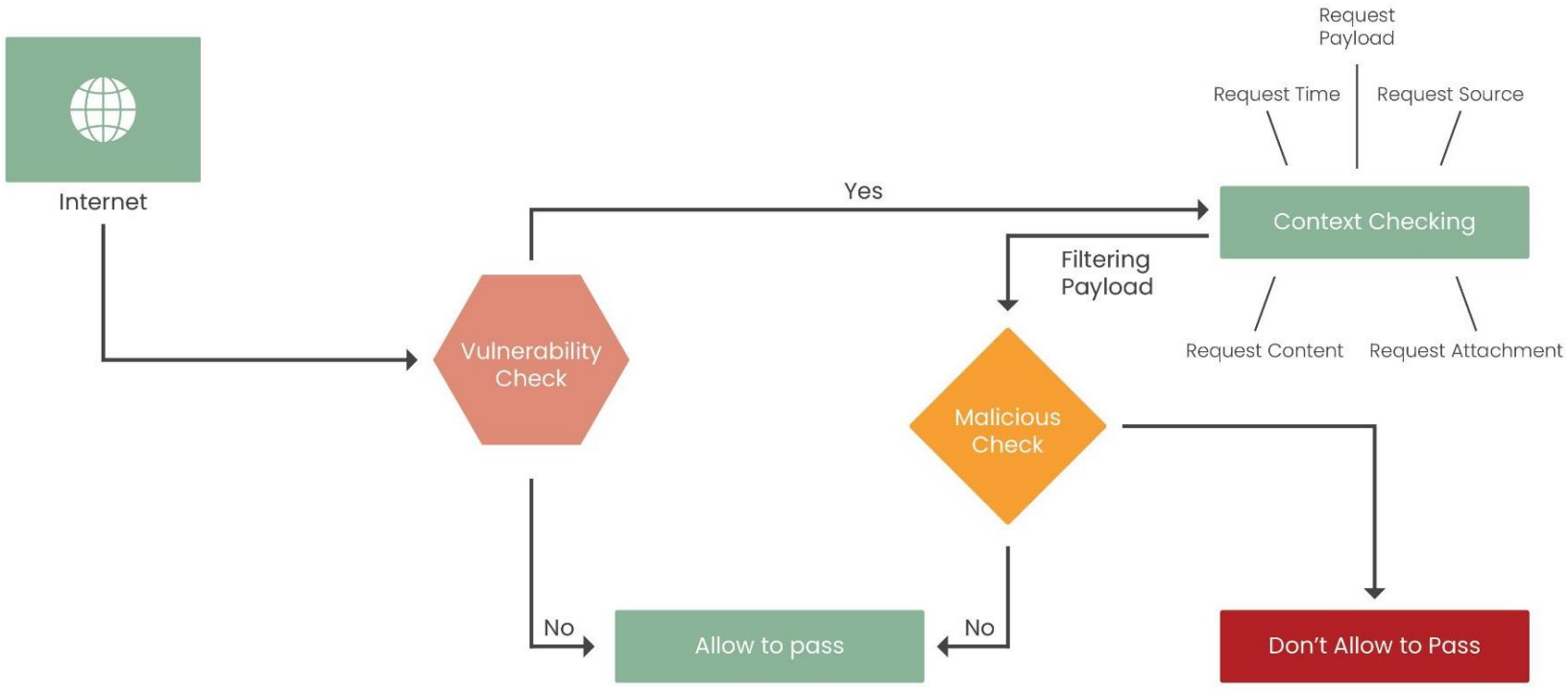
IoT Attacks Example:



Once BotenaGo gains access, it will execute remote shell commands to recruit the device into the botnet.

Context Aware Security Use case

Context-Aware Security Technique:



Context-Aware Vulnerability scanner Diagram

Readings

1 P. Patel, S. Jardosh, S. Chaudhary, and P. Ranjan, “Context aware middleware architecture for wireless sensor network,” in Services Computing, 2009. SCC ’09. IEEE International Conference on, sept. 2009, pp. 532 –535. [Online]. Available: http://dx.doi.org/10.1109/ SCC.2009.49

2 A. Arfaoui, S. Cherkaoui, A. Kribeche, S. M. Senouci, and M. Hamdi, “Context-aware adaptive authentication and authorization in internet of things,” in Proceedings of the ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1–6, Shanghai, China, May 2019.

3 Charith Perera, Student Member, IEEE, Arkady Zaslavsky, Member, IEEE, Peter Christen, and Dimitrios Georgakopoulos, Member, IEEE “Context Aware Computing for The Internet of Things: A Survey” in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. X

4 M. Trnka and T. Cerny, “On security level usage in context-aware role-based access control,” in Proceedings of the 31st Annual ACM Symposium on Applied Computing, ser. SAC ’16. New York, NY, USA: ACM, 2016, pp. 1192–1195.

5 Rowida Alfrjani, Taha Osman and Georgina Cosma, “A Hybrid Semantic Knowledge base-Machine Learning Approach for Opinion Mining”, published in data knowledge in 2016

6 Eirini Anthi, Lowri Williams, Małgorzata Słowinska, George Theodorakopoulos and Pete Burnap, “A Supervised Intrusion Detection System for Smart Home IoT Devices”, in IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 5, OCTOBER 2019

7 Omar Al-Kadri and Garikayi Madzudzo, “Context-aware Anomaly Detector for Monitoring Cyber Attacks on Automotive CAN Bus”, published in CSCS ’19, October 08, 2019, Kaiserslautern, Germany

8 Josep Soler Garrido, Dominik Dold and Johannes Frank, “Machine learning on knowledge graphs for context-aware security monitoring”, published in IEEE CS.cr in 2021