Date

Trust by Design: The Internet of Things
Security and privacy of smart-home devices and services

Internet Society

Kevin G. Chege

ISOC

The number of IoT devices and systems connected to the Internet will be more than

2.5x the global population

by 2020 (Gartner).

As more and more devices
are connected, privacy and
security risks increase.

And most consumers don't even know it.

What type of risks?

Unlocking doors, turning on cameras, shutting down critical systems and theft of personal property.

People's safety or the safety of their family might even be at risk.

Large IoT-based attacks, such as the Mirai botnet in 2016, have crippled global access to high-profile Internet services for several hours.
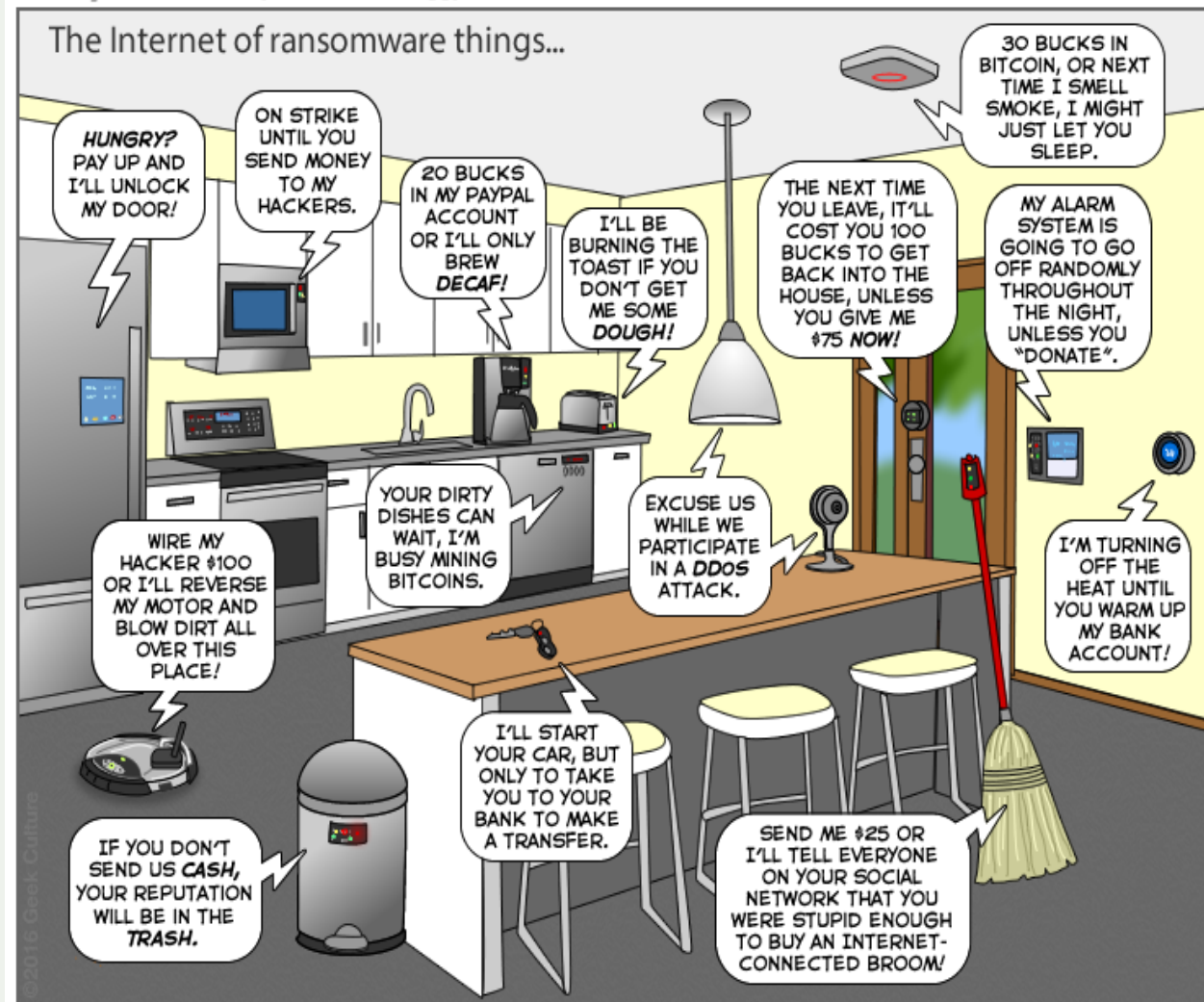
The challenges we face

A connected world offers the promise of convenience, efficiency and insight, but creates a platform for shared risk.

Many of today's IoT devices are rushed to market with little consideration for basic security and privacy protections.

Who is responsible?

Developers and users of IoT devices and systems have a collective obligation to ensure they do not expose others and the Internet itself to potential harm.

We need a collective approach, addressing security challenges on all fronts.
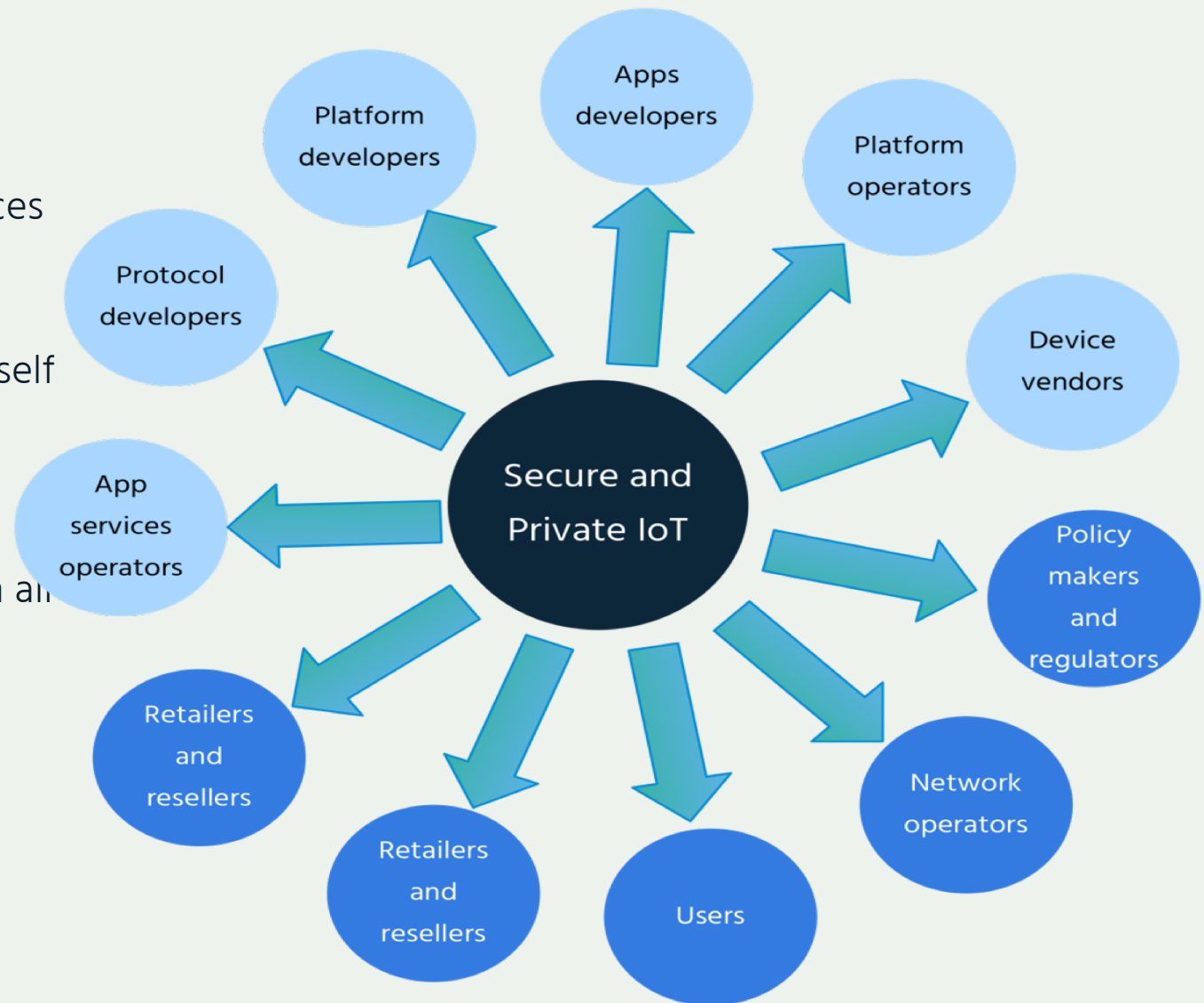
The Internet Society is working for a better Internet.

- We want manufacturers and suppliers of consumer IoT devices and services to adopt security and privacy guidelines to protect the Internet and consumers from cyber threats.

- We want to educate users on the importance of secure IoT devices and work with stakeholders involved in technology and security to better inform their communities on IoT.

Online Trust Alliance (OTA) IoT Trust Framework

- Provides a set of actions and principles to raise the level of security for IoT devices and related services to protect consumers and the privacy of their data

- More than 100+ stakeholders from industry, government and consumer advocates contributed to the Framework

- Stands apart from other IoT-related Frameworks with its comprehensive focus on security, privacy and lifecycle issues, as well as a holistic view of the entire system

- Please visit the ISOC Booth for a copy!

https://otalliance.org/iot/

Actionable principles in eight categories for manufacturers, developers and service providers

| Authentication | Encryption | Security | Updates |

| Privacy | Disclosures | Control | Communications |

IoT Framework Principles: It is a collective responsibility

IoT vendors and their supply chain

Distribution channels

Policymakers and governments

Consumer testing and product review organizations

Consumers and enterprises

Are you doing something in IoT in the African region?

- Are you doing research into the field of IoT or developing IoT products?

- Please let us know through the ISOC chapters

- This info will help us coordinate efforts in IoT and know what types of IoT devices are being developed in the region

Thank you.

chege@isoc.org