The Roles of Blockchain in Strengthening Security of the Internet of Things

Nir Kshetri
Professor
The University of North Carolina- Greensboro

Session: Cybersecurity and Cybercrime: New tools for better cyber protection

IoT insecurity a key concern

- October 2016 cyberattacks on DNS provider Dyn.
- Attacks originated from "tens of millions of IP addresses".
- At least some of the malicious traffic from IoT devices:
  - webcams, baby monitors, home routers and DVRs.
- Infected with Mirai.
  - easy-to-use program.
  - controls online devices: uses them to launch DDoS attacks.
  - phishing emails to infect a computer or home network.
  - spreads to other devices

A comparison of cloud and blockchain

	Cloud	Blockchain
Mechanisms related to efficiency, and cost-effectiveness	Cloud's pay as you go model: better than legacy system (building capacity by buying more computers, more software and hiring more people) Cloud's IaaS	Blockchain removes the need for third parties in transactions by creating a distributed record which is possessed and verified by other users.
Deployment models	Private, community and public	Permissionless/permissioned chains: security, privacy, and other requirements Possible to target specific members: regulators and auditors
Some mechanisms to strengthen cybersecurity	C"cyber risk free zone": constant monitoring for suspicious activities and real time response. Data encrypted Some companies (e.g., google) employ "Zero Trust" network: fine-grained control	Data fully encrypted Cryptographic hash functions
Some challenges	Many rely rely on the firewall model.	Newness: well-developed security mechanisms have not developed for some systems

Blockchain's potential to address key challenges associated with cloud-based IoT

Challenge of cloud-based IoT	Explanation	How blockchain can help to address the problem
Costs and capacity constraints	Exponential growth in IoT devices: by 2020, a network capacity at least 1k times 2016 level needed.	No need of a centralized entity: Devices can communicate securely, exchange value with each other and execute actions automatically through smart contracts.
Deficient architecture	Each block of IoT architecture acts as a bottleneck/point of failure, and disrupts the entire network: vulnerability to DDoS attacks, hackings, data thefts, and remote hijackings.	Secure messaging between devices: validity of a device's identity is verified, transactions are signed and verified cryptographically to ensure that only the originator of the message could have sent it.
Server downtime and unavailability of services	Servers are sometimes down due to cyberattacks, bugs, power, cooling or other problems.	No single point of failure: records on many computers/devices, identical information.
Susceptibility to manipulation	Information is likely to be manipulated and put to inappropriate uses	Decentralized access and immutability: malicious actions can be detected and prevented. Devices are interlocked: If one device's updates are breached, the system rejects it.

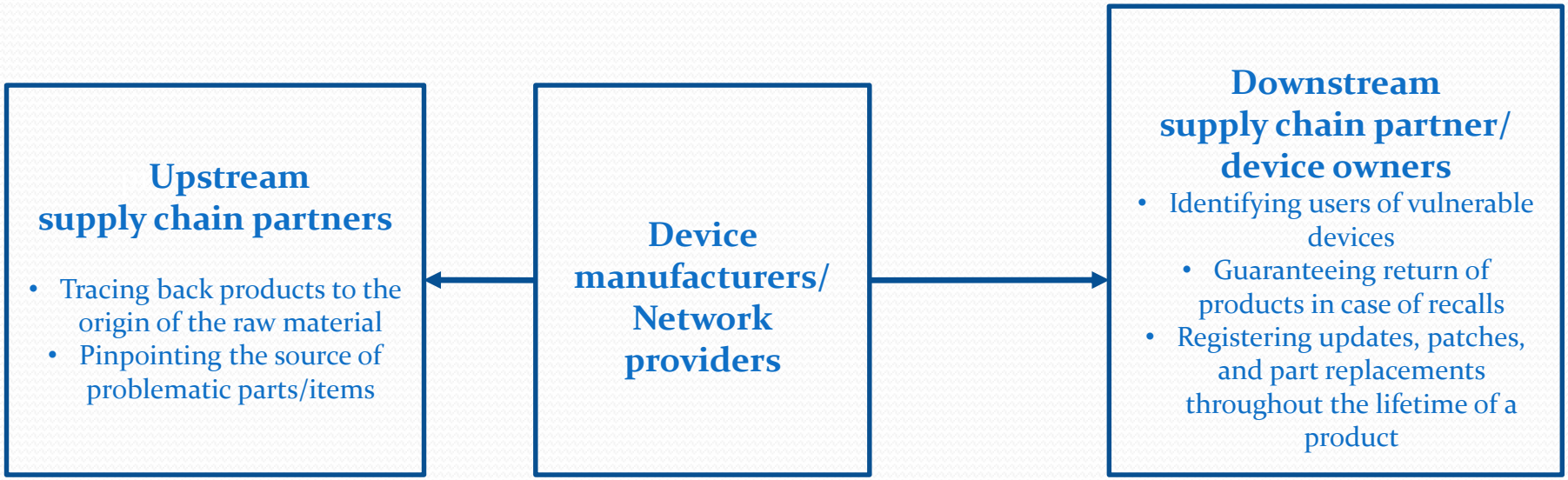
Blockchain-based identity and access management systems

- Dyn: IP spoofing attacks in the later versions of Mirai.
- Blockchain-based identity/access management: strong defense.
  - Immutability: original information entered is accurate
- Devices cannot connect by disguising/injecting fake signatures.
  - Filaments' Taps
- Used to store information: goods' provenance, identity, credentials, digital rights.
- Properties are stored securely and reliably
  - physical assets and individuals (credentials)
  - resource use (energy and bandwidth through IoT devices)
  - other relevant events.
- A private blockchain: store cryptographic hashes of device firmware.
  - a permanent record of device configuration and state.
  - verify that a device is genuine/ software/settings not tampered.

Blockchain's role in improving security in supply chain networks

- IoT-linked security crises (e.g., Dyn) could have been handled in a better way with blockchain.
- China's Hangzhou Xiongmai Technologies recalled products sold in the U.S.
  - difficult to track down the owners/contact.
- Blockchain: register time, location, price, parties involved, and other relevant information.
  - track raw materials, transformed into circuit boards/ electronic components, integrated into products, sold.
- Blockchain: register updates, patches, and part replacements

Blockchain's role in improving the overall security in supply chain networks (contd.)



Key points

- Blockchain: cybercriminals' and data manipulators' nightmare
  - can save from "another Flint-like contamination crisis"
  - smart water meters diffusing rapidly (20% in California)
    - Washington Suburban Sanitary Commission (WSSC): integrate IoT.
    - upgrade with sensors--near-infrared reflectance spectroscopy (NIRS) to include data on chemical levels
- Outperforms cloud in many aspects
- Secure storage and transmission of digitally signed documents: killer application of blockchain
  - identity and access management to stop IP spoofing attacks
- Improve security of forward and backward linkages in supply chain

Thank you