IRT - IoT Projects

1. Identify IoT devices and Network Behavior

Device identification is critical for a number of IoT security and privacy initiatives under research in our group. We have worked on a few methods locally and many others have been the subject of research across the community. One research goal would be to scan the literature for useful algorithms that can be used as the foundation for policy enforcement such as MUD-based efforts, as well as input to our privacy database aimed at comprehensively covering the privacy landscape for IoT devices.

Task:

1. Survey paper: review current research publications in a systematic way.
2. Feature vectors foundation: link, network and protocol behavior.
3. Propose a ML model for device identification and behavior.
4. Develop a prototype for device identification using the proposed method.

Background Required:

1. Python programming.
2. Networking background.
3. Machine Learning Background.

References:

Machine Learning for the Detection and Identification of Internet of Things (IoT) Devices: A Survey
https://arxiv.org/pdf/2101.10181.pdf

Machine Learning DDoS Detection for Consumer Internet of Things Devices
https://ieeexplore.ieee.org/abstract/document/8424629
https://www.cylab.cmu.edu/news/2020/12/03-iotassistant.html

Position paper: A systematic framework for categorising IoT device fingerprinting mechanisms
https://arxiv.org/pdf/2010.08466.pdf

MeDI: Measurement-based Device Identification Framework for Internet of Things
https://acris.aalto.fi/ws/portalfiles/portal/28992701/DeviceID.pdf

Behavioral Fingerprinting of IoT Devices
https://dl.acm.org/doi/pdf/10.1145/3266444.3266452

IoT Device Identification Using Deep Learning
https://arxiv.org/pdf/2002.11686.pdf

A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic
https://arxiv.org/pdf/1705.06805.pdf

Exploring How Privacy and Security Factor into IoT Device Purchase Behavior
https://dl.acm.org/doi/pdf/10.1145/3290605.3300764

HOMESNITCH: Behavior Transparency and Control for Smart Home IoT Devices
https://enck.org/pubs/oconnor-wisec19a.pdf

IoT Devices Recognition Through Network Traffic Analysis
https://hal.archives-ouvertes.fr/hal-01994156/file/IEEE_BigData2018_IoT_devices_recognition_through_network_traffic_analysis.pdf

BRIoT: Behavior Rule Specification-Based Misbehavior Detection for IoT-Embedded Cyber-Physical Systems
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8715740

Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey
https://arxiv.org/pdf/2004.05289.pdf

Verifying and Monitoring IoTs Network Behavior using MUD Profiles
https://arxiv.org/pdf/1902.02484.pdf

D˙IOT: A Federated Self-learning Anomaly Detection System for IoT
https://arxiv.org/pdf/1804.07474.pdf

IoTArgos: A Multi-Layer Security Monitoring System for Internet-of-Things in Smart Homes
https://par.nsf.gov/servlets/purl/10191612

2. Synthetic Devices and Digital Twins

Task

1. Define state machines for standard IoT devices/sensors - light Switches, lightbulbs, locks, smoke alarms, speakers, thermostats, environmental sensors, … (Use real devices as models.)
2. Implement synthetic IoT devices (digital twins) to simulate device state machines.
3. Generate real networking traffic using existing device behavior models.

Background

1. Python programming
2. Networking background.
3. Machine learning background (optional).

Reference

Tasmota (open source firmware for ESP32)
ZigBee device profiles, AWS IoT Device Emulator

Digital Twin Paradigm: A Systematic Literature Review

https://hal.archives-ouvertes.fr/hal-03218786/file/Semeraro%20et%20al.pdf

VIoLET: A Large-scale Virtual Environment for Internet of Things
https://arxiv.org/pdf/1806.06032.pdf

Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook
https://www.researchgate.net/publication/337139416_Digital_Twins_for_Cyber-Physical_Systems_Security_State_of_the_Art_and_Outlook

Towards Security-Aware Virtual Environments for Digital Twins
https://publications.sba-research.org/publications/201806-AEkelhart-Environmentfordigitaltwins.pdf

A Specification-based State Replication Approach for Digital Twins
https://publications.sba-research.org/publications/201810-AEkelhart-Specification-based.pdf

Exploring city digital twins as policy tools: A task-based approach to generating synthetic data on urban mobility
https://www.cambridge.org/core/services/aop-cambridge-core/content/view/D89BEAEA571454D37BEEBC5BC31CD8E7/S2632324921000171a.pdf

Synthetic Data Generation for the Internet ofThings
https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=1035&context=computing_pubs

Generative Deep Learning for Internet of Things Network Traffic Generation
https://hal.archives-ouvertes.fr/hal-03127899/document

IoTNetSim: A Modelling and Simulation Platform for End-to-End IoT Services and Networking
https://dl.acm.org/doi/pdf/10.1145/3344341.3368820

MobIoTSim: Towards a Mobile IoT Device Simulator
http://publicatio.bibl.u-szeged.hu/11702/1/mobiotsim_ficloud_accepted_u_.pdf

Blockchain-based Digital Twins: Research Trends, Issues, and Future Challenges
https://arxiv.org/pdf/2103.11585.pdf

3. Context-aware IoT Authentication Framework

Create a context-aware authentication framework for IoT devices. The framework should provide enhancements to existing network-based access control lists, specifically targeting IoT services and devices based upon location restrictions such as proximity (short range/indoor locations), geofencing (polygon), identity, affiliation and time. The policies can be defined using existing data formats such as JSON/XML/YANG or may take the form of a domain-specific language.

Task

1. Define the policy data model, after literature review.
2. Implement the context-aware policy framework for a test environment, e.g. Smart Home (Smart Lock / Smart Bulb / ..)

Background:

1. Foundational programming languages theory.
2. Python programming.
3. Networking & security background.
4. Web-development experience.

References

Policy-based Access Control for the IoT and SmartCities
https://dl.gi.de/bitstream/handle/20.500.12116/20984/proceedings-13.pdf

DACIoT: Dynamic Access Control Framework for IoT Deployments
http://www.queenstrl.ca/uploads/4/6/3/1/4631596/daciot_dynamic_access_control_framework_for_iot_deployments.pdf

Automatic Device Selection and Access Policy Generation based on User Preference for IoT Activity Workflow
https://arxiv.org/pdf/1904.06495.pdf

Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things
https://vbn.aau.dk/ws/files/74574200/PNM_IACAC_River.pdf

Context-Sensitive Policy Based Security in Internet of Things
https://ebiquity.umbc.edu/_file_directory_/papers/789.pdf

A Dynamic Continuous Authentication Framework in IoT-Enabled Environments
https://webs.um.es/mattia.zago/assets/papers/IoTSMS2018.pdf

CyprIoT: framework for modelling and controlling network-based IoT applications

https://hal.archives-ouvertes.fr/hal-02333578/document

4. Privacy Enforcement

Build a MUD-like user-control language that describes and implements privacy policy restrictions in the network. For example, allow devices to send data only to X location servers. (Example: “only send data to servers based in the US.”).

The tools can be used for network data behavior modeling and validation with potential regulatory policy exploration and experimentation of various privacy models.

Task:

1. Define the MUD-like privacy language using YANG models.
2. Implement the privacy enforcing engine on the network gateway.
3. Extra Points - Given a privacy policy document, how to convert it into a network policy that can be implemented at a network gateway.

Background:

1. Python programming.
2. Networking.
3. NLP - Document modeling.

References

Privacy in Internet of Things: from Principles to Technologies
https://arxiv.org/pdf/1808.08443.pdf

Privacy Mediators: Helping IoT Cross the Chasm
https://dl.acm.org/doi/pdf/10.1145/2873587.2873600

On the Case of Privacy in the IoT Ecosystem: A Survey
https://www.researchgate.net/publication/334883432_On_the_Case_of_Privacy_in_the_IoT_Ecosystem_A_Survey

IOTGUARD: Dynamic Enforcement of Security and Safety Policy in Commodity IoT
https://cs.uwaterloo.ca/~yaafer/teaching/papers/ndss2019_07A-1_Celik_paper.pdf

Enforcement of Security Policy Rules for the Internet of Things
http://faratarjome.ir/u/media/shopping_files/store-EN-1486555503-8222.pdf

Towards a Lightweight Policy-Based Privacy Enforcing Approach for IoT
https://www.researchgate.net/publication/338365683_Towards_a_Lightweight_Policy-Based_Privacy_Enforcing_Approach_for_IoT

User-driven Privacy Enforcement for Cloud-based Services in the Internet of Thing
https://arxiv.org/pdf/1412.3325.pdf
A Scalable and Privacy-Aware IoT Service for Live Video Analytics
https://dl.acm.org/doi/pdf/10.1145/3083187.3083192