APPROVED
NU IRB# 1708-07 Ver. 2018-8-27
VALID 8/24/18
THROUGH 8/28/19

Northeastern University, College of Computer and Information Science
Name of Investigators: Dr. David Choffnes (PI), Dr. Daniel J. Dubois, Jingjing Ren
Title of Project: Revealing and Controlling Privacy Leaks in Internet of Things' Network Traffic

Informed Consent to Participate in a Research Study

We are inviting you to take part in a research study. This form will tell you about the study, but the researcher will explain it to you first. You may ask this person any questions that you have. When you are ready to make a decision, you may tell the researcher if you want to participate or not. You do not have to participate if you do not want to. If you decide to participate, the researcher will ask you to sign this statement and will give you a copy to keep.

Why am I being asked to take part in this research study?

We are asking you to be in this study because you have badge access or are an authorized escorted visitor to room 660 of the ISEC building at Northeastern University.

Why is this research study being done?

Smart devices are no longer limited to general-purpose ones such as smartphones and tablets; they now include network-capable versions of any object, from simple light bulbs to large home appliances. These objects are "smart" in the sense that they can be used, programmed, controlled, and reconfigured remotely. These devices often require an Internet connection for all or part of their functionality, and are widely referred as the **Internet of Things** (IoT).

While IoT technology is becoming pervasive in everyday objects, our awareness of the sensitive information they get access to and use remains almost non-existent. In an ideal world, they would gather and use only the information necessary to enable essential functionality; however, if IoT devices are malicious or not configured properly, they could possibly share private information with unintended recipients or with the whole world. For example, in the case of a smart voice-controlled TV, we want to be aware if and when the TV is sharing its recorded audio with third parties.

The primary purpose of this research is to first understand what **personally identifiable information (PII)**, such as names, locations, gender, daily activity, etc., is being leaked (intentionally or otherwise) to other parties from IoT devices. In addition, we aim to develop techniques that mitigate such privacy risk without compromising the functionality of such devices.

Where will this take place?

This research will be undertaken inside an IoT "living lab," that we call the **Mon(IoT)r Lab**, for measuring IoT device network leakage. The lab consists of a "fishbowl" (glass walls) that encloses a space replete with a wide selection of smart devices from TVs to toasters, fridges to fitbits, lights to locks. Specifically, we ensure that all of the IoT devices in the lab are configured to use monitored network connections subject to traffic-recording and PII detection software, which allows us to perform the privacy analysis. In addition to the IoT devices under test, the lab is also equipped with one or more video cameras that record what is happening inside the lab. These cameras will capture information on when and how you use the IoT devices under test. The Mon(IoT)r Lab will have its access restricted to study personnel (i.e., project investigators) and study participants only, and is located inside room 660C (also access-controlled) of the ISEC building at Northeastern University, 805 Columbus Ave., Boston, MA, USA.

The purpose of the Mon(IoT)r Lab within our study is to be the physical location of all the experiments and to showcase security and privacy research through live demonstrations inside the lab, and real-time visual interfaces both inside and outside of the lab.

What will I be asked to do and how much of my time will it take?

Your experiments consist of entering the Mon(IoT)r lab and possibly using any lab-owned IoT devices (connected to any monitored network) with their lab-owned companion devices (e.g., smartphones and tablets running companion apps). When you use a device, you are expected to do so for its intended purpose (e.g., you will use a smart dishwasher to wash dishes, or a smart TV to watch TV). Your personal devices can also be freely used in

the lab, but you cannot connect them to the lab devices or network, and they will not be monitored, since access to the monitored networks will be limited to lab-owned devices.

You can enter the lab at any time that 660 ISEC is open (expected to be 24/7), and you can stay in the lab for any amount of time you want (from seconds to hours with no restrictions). The only exception is when the study personnel has to perform maintenance tasks or run private experiments. In such a case, we will put up a sign on the entrance door to prevent participants from entering and we will ask any participant inside the lab to leave.

It is your responsibility to delete any personal information stored in the devices after the end of each experiment. Any personal information that is not deleted from the devices under test (or from any companion device or from any external service used as storage by them) will never be used within this user study and will be deleted by the study personnel as soon as it is detected and during weekly devices wipe. A sign in the lab will help you remember to log out and delete your data from any lab-owned device after use.

No other activities (e.g., surveys, interviews, etc.) besides what is needed to interact with lab-owned IoT devices are required from you.

During experiments, we will capture the following information:

1. A closed-circuit video of the participants, including you, using video cameras (e.g., security cameras).
2. The Internet traffic generated by the devices connected to any of the monitored networks of the Mon(IoT)r lab, which include lab-owned IoT devices under test and any related companion devices.
3. The Bluetooth, Wi-Fi-Direct, Zigbee traffic generated for direct device-to-device wireless connections by the devices under test.

All the devices used in the experiments are furnished by our research team, not ones belonging to you or any other study participant. You can still use your own personal devices in the Mon(IoT)r lab, but they cannot be connected to the monitored networks, so that their traffic will not be recorded and analyzed for the purpose of this study.

The information captured during experiments will be used in the following way:

1. Video recordings are used to identify: (1) ongoing activity inside the Mon(IoT)r lab; (2) which devices are being used and how they are being used; (3) which participants are using the devices. This information is needed to correlate any traffic data to any activity carried out in the lab and detect some PII in the traffic (for example to find security camera images in video streams shared by IoT devices). A sign in the lab will remind study participants about active video recording in the room.

2. Internet and direct wireless traffic are used to: (1) detect the presence and the content of textual PII (i.e., names, device identifiers, credentials, etc.), (2) detect the presence and the content of non-textual PII such as pictures, audio, and video streams shared by the devices; (3) detect the presence and the content of any PII (textual and non-textual) in encrypted streams by using man-in-the-middle techniques; (4) detect the strength of the encryption used by the devices, and whether they check the validity of the certificates; (5) determine the destinations of any PII shared over the Internet; (6) determine the destinations of any PII shared over direct wireless connections.

Will there be any risk or discomfort to me?

Privacy risks: Some IoT devices are equipped with cameras, microphones and storage, and may share PII to third parties during tests or keep that information stored in in-device memory or in cloud services.
This risk is not more serious than one would expect in any modern smart home. When conducting experiments, we will require study participants to use fake information and delete their information from the device (and any related remote service) as soon as an experiment is completed. A sign in the lab will remind you to do so. We will also wipe all the data from the devices (and any related remote service) every week to limit this risk.

Physical risks: Subjects in this study may get hurt if some lab-owned devices are misused or are malfunctioning. This risk is minimal since potentially dangerous devices (e.g., toasters) will be kept locked and made available only when study personnel are in the room. However, since a minor risk is also present for less-dangerous devices, the lab has a sign with emergency contact information to be called in case of injuries or any other emergency associated with lab-owned devices.

APPROVED
NU IRB# 17-08-07
VALID 5/29/18
THROUGH 5/28/19

Psychological risks: subjects may suffer psychological discomfort of learning about potential public visibility of private information stored or captured by an IoT device.
This risk is mitigated by the fact that the devices are not owned by the participant, and the participant can simply opt out of the study to avoid any associated discomfort.

Will I benefit by being in this research?

You will have several benefits from participating to the study.

The first benefit is the possibility to use all the IoT devices under test in the Mon(IoT)r lab. For example, you will be authorized to wash your personal clothes using a smart IoT washing machine, to use the smart entertainment consoles we provide for personal enjoyment, to watch TV using the smart TV, to play with the newest wearable technologies, and so on.

The second benefit is that you will be informed if any of the devices you experimented within the lab have leaked any personal information. This will be helpful for increasing your awareness of which personal information has been shared and with whom.

The third benefit is that we will make the general public (including you) aware of how the different types of IoT devices communicate with other servers, how the data is sent and whether there are privacy risks. Learning these risks will allow you to make more informed decisions about what IoT devices to use and what to avoid to minimize any undesirable leaks of your private information.

Who will see information about me?

You will be assigned a participant ID code that does not contain PII. Data collected from you will be timestamped and either left untagged or tagged with your participant ID, depending on the type of experiment and IoT device. The mapping between your ID and your direct identifiers (i.e., name and contact information collected during the informed consent process) will be held separately in a secure cabinet that is accessible only to the study personnel.

No parties other than the study personnel will have access to your data. The traffic data and the data captured by the video cameras within the lab will be stored securely on a server that is physically hosted in a restricted area building at Northeastern University. When the data analysis is complete (up to one year after the end of the study), the collected data will be destroyed.

Any data stored on the IoT devices, companion devices, or their related services (e.g., Internet cloud storage) will not be analyzed by our study and we encourage all the participants to delete it after the end of each experiment. Some cloud services used by the IoT devices may have their own policies regarding the confidentiality of the data sent to them during the experiments: such policies are outside the control of this study and you are expected to review and accept them before using such IoT devices.

All the information detected in the captured traffic is used with the sole purpose of assessing the level of privacy risk for each device under test, and will not be shared outside of the project personnel. For example, if an IoT device during an experiment shares the data captured by its microphone, such data will be captured, decoded, and used to confirm that the device has violated the privacy of its user; however, such captured audio recording will never be released or used for any other purpose.

All the recordings and the traffic will be deleted after the analysis is complete and, in any case, within one year from the completion of the user study.

What will happen if I suffer any harm from this research?

This research does not increase your risk of injury with respect to the one you would expect in any modern smart home. Because of this if you suffer a research-related injury, your medical expenses will be your responsibility or that of your third-party payer, although you are not precluded from seeking to collect compensation for injury related to malpractice, fault, or blame on the part of those involved in the research. A sign the Mon(IoT)r lab will contain emergency contact numbers in case you get hurt while using any lab-owned device.

Can I stop my participation in this study?

APPROVED
NU IRB# 17-07-07
VALID 8/29/18
THROUGH 3/28/19

Your participation in this research is completely voluntary. You do not have to participate if you do not want to and you can refuse to answer any question. Even if you begin the study, you may quit at any time and have all your data deleted. If you do not participate or if you decide to quit, you will not lose any rights, benefits, or services that you would otherwise have. However, all the privileges obtained as part of this research, such as the access to the Mon(IoT)r lab and its IoT devices, will be revoked.

Who can I contact if I have questions or problems?

If you have any questions about this study, please feel free to contact any of the following investigators:

- David Choffnes, Assistant Professor, Principal Investigator, choffnes@ccs.neu.edu (617) 373-4239
- Daniel J. Dubois, Postdoctoral Associate, Researcher, d.dubois@northeastern.edu
- Jingjing Ren, Graduate Student, Researcher, renjj@ccs.neu.edu
- Talha Ongun, Graduate Student, Researcher, ongun.t@husky.neu.edu

Who can I contact about my rights as a participant?

If you have any questions about your rights in this research, you may contact Nan C. Regina, Director, Human Subject Research Protection, Mail Stop: 560-177, 360 Huntington Avenue, Northeastern University, Boston, MA 02115. Tel: 617.373.4588, Email: n.regina@neu.edu. You may call anonymously if you wish.

Will I be paid for my participation?

No.

Will it cost me anything to participate?

The only cost incurred by you as part of this study is the cost to physically reach the Mon(IoT)r lab premises.

Is there anything else I need to know?

The target population for this research is English-speaking individuals age 18 or older, regardless of their Northeastern University affiliation, who either: (1) have badge access rights to room 660 of the ISEC building at Northeastern University Boston campus; or (2) are authorized escorted visitors of room 660 of the ISEC building. All people who meet these criteria are eligible for inclusion and will be accepted as subjects without consideration as to their gender, sexual orientation, ethnicity, race, socio-economic level, literacy level or health.

Your participation to the study may be involuntarily terminated if you do not belong to the target population anymore or if you repeatedly fail to follow the instructions given by the study personnel.

This research is supported by the Department of Homeland Security – Science and Technology contract FA8750-17-2-0145 (Revealing and Controlling Privacy Leaks in Network Traffic).

I agree to take part in this research.

Signature of person agreeing to take part _____ Date _____

Printed name of person above _____

Signature of person who explained the study to the Participant above and obtained consent _____ Date _____

Printed name of person above _____

APPROVED
NU IRB# 17-08-07
VALID 8/29/18
THROUGH 8/28/19