Private Memoirs of IoT Devices: Safeguarding User Privacy in the IoT Era

Dong Chen, Phuthipong Bovornkeeratiroj, David Irwin, and Prashant Shenoy
University of Massachusetts Amherst
{dongchen,pbovornkeera}@umass.edu, irwin@ecs.umass.edu, shenoy@cs.umass.edu

***Abstract*—The rise of the Internet-of-Things (IoT) holds great promise to transform people's lives by making society more efficient in many areas, including energy, transportation, healthcare, commerce, manufacturing, etc. At their core, IoT devices use sensors to collect data on real-world physical processes and then transmit it over the Internet to cloud servers, which store, process, and learn from the data to better optimize these processes, either directly (by issuing remote commands that actuate IoT devices) or indirectly (by issuing notifications that direct users to take some action). Unfortunately, IoT devices also expose users to multiple new types of privacy attacks. In particular, the sensor data collected from IoT devices can indirectly reveal a variety of sensitive private information. In addition, users generally connect IoT devices to local networks, which they implicitly trust, with little understanding of what the IoT device is doing on the network.**

In this vision paper, we discuss recent work on sensor data privacy in the context of energy systems to provide examples of i) the surprising types of private information that we can glean from seemingly innocuous IoT data and ii) the different types of defenses that we have employed to preserve IoT data privacy for energy systems. These defenses lie at different discrete points in the tradeoff between user privacy and IoT functionality, which motivates our current work on developing defenses that provide a more tunable tradeoff. We also discuss the privacy implications of connecting tens-to-hundreds of untrusted IoT devices to implicitly trusted local networks, and avenues for research to mitigate these privacy concerns.

I. Introduction

The rise of the Internet-of-Things (IoT) holds great promise to transform people's lives by making society more efficient in many areas, including energy, transportation, healthcare, commerce, manufacturing, etc. In each industry, new IoT-enabled devices are rapidly being developed, while, in parallel, existing devices are also being augmented with IoT functionality, i.e., Internet connectivity, remote programmability, and automation. The dominant operational paradigm for IoT devices is to collect sensor data about real-world physical processes and then transmit it, often in real time, to cloud servers, which are able to store, process, and learn from this data to better optimize those physical processes. Such a cloud-based IoT paradigm has become increasingly common and there are hundreds of commercial IoT products that have adopted it. For example, in the domain of smart home automation, IoT versions of power outlet and switches, light bulbs, door locks, and thermostats are now readily available in home improvement stores.

These IoT devices connect to the cloud to enable users to monitor and control them via smartphone applications and web-based dashboards. In many cases, the cloud backend not only stores and analyzes sensor data, but also enables remote actuation, where a device, such as a smart switch, can be controlled remotely over the Internet. Similarly, in the domain of smart health, numerous fitness trackers and bands are available that track daily activities, such as steps, exercise, sleep, and heart rate, which also connect to the cloud to store and analyze the data they collect. From the IoT service provider's perspective, collecting real-world data from large numbers of devices enables them to develop new analytic techniques and learn faster by leveraging much more data than can be collected from any single device.

The operational data gathered by IoT devices is often considered innocuous by users and enterprises—users tend to believe they own the data produced by their IoT devices and often do not have a clear understanding of how the data is being used by cloud services or what it may reveal. In many cases, the data is transmitted over the Internet in plaintext, stored unencrypted in the cloud, shared with third-party analytics companies, and even made publicly available over the Internet. Recent studies have shown that IoT data can leak sensitive or private information, and can often contain side-channel information that reveals information well beyond the primary purpose for which the data was generated. For instance, data from smart switches, smart thermostats, and smart power meters can reveal whether a home is occupied, as well as the types and usage patterns of common electrical appliances [1]–[3], while power data from rooftop solar panels can reveal their location [4], [5].

Smart fitness trackers explicitly track the locations of users as part of monitoring their daily activities, which can also leak sensitive information about the user or the location itself. The most recent example of this to gain broad attention in the press was the Strava fitness app that publicly posts a map of its users' activity on the Internet. Security researchers recently showed that this public activity map posed a serious threat to U.S. national security by indirectly revealing the locations and behaviors of U.S. military bases and personnel in Iraq and Syria [6]. In other cases, many IoT devices make their data anonymously visible over the Internet through searchable web links under the assumption that such "anonymous" data is harmless. However, many of the privacy attacks above can cause such anonymous data sources to reveal sensitive information about the users.

While the examples above are from widely different application domains, the sensitive information they reveal is similar, and focuses on user behavior, e.g., what are users doing and when?, and user location, e.g., where are users? In this vision paper, we outline answers to these questions that can be drawn from analyzing energy data recorded by advanced metering infrastructure (AMI), i.e., smart meters and other Internet-connected energy sensors, to demonstrate the, often unknown, privacy threat posed by mass data collection from IoT devices. Smart meters represent one of the most widely deployed IoT devices in the world with installations estimated to hit 70M by the start of 2017 and 90M by 2020 [7]. Smart meters are particularly interesting because they are generally not installed voluntarily by users, but instead are owned and managed by utilities to improve the electric grid's efficiency and its ability to handle increasing penetrations of intermittent renewable generation, e.g., from solar modules and wind turbines. Even so, as we discuss, data collected from smart meters is being used for a wide range of purposes beyond utility operations, often without the consent of users. After describing various analytics that can reveal user behavior and location from smart meter data, we then outline the different types of defenses that we have employed to preserve energy data privacy and prevent answering the questions above, and how they might generalize to other types of data.

Of course, a simple way to protect user privacy is to simply prevent IoT devices from collecting any data, and forego any of the functionality or efficiency benefits they provide. Thus, a key research challenge is to determine how to maximize the functionality and benefits of IoT devices, while concurrently preserving user privacy, preferably at a low cost. The defenses we describe in the context of energy systems generally lie at different discrete points in this tradeoff between user privacy, IoT functionality, and cost. For example, one of the defenses strongly protects user privacy by revealing the minimal necessary information about a building's energy usage, e.g., only the information necessary to correctly bill users for their energy usage, but to the detriment of functionality, e.g., by preventing a wide range of energy analytics that could improve the grid's energy efficiency. In contrast, we discuss another type of defense that actively modifies energy usage, e.g, by controlling batteries or large loads, to mask the information that it reveals, but at a potentially high cost. These examples motivate our ongoing work on designing low-cost defenses that enable accurate grid-scale analytics on large-scale energy data that can improve grid operations, but prevent fine-grained analytics capable of identifying the behavior and location of individual users. In addition, our ongoing work also enables a more tunable tradeoff between user privacy and functionality, enabling users to better control the private information their energy data reveals.

In addition, we also examine the threat posed by numerous untrusted IoT devices being connected to implicitly trusted local networks. Users often have little understanding of what IoT devices are doing on the network, and little way to verify their operation, as many devices have narrow user interfaces that reveal little about their underlying status or operation. As a result, IoT devices are increasingly being compromised and actively used in Distributed Denial of Service (DDoS) attacks [8]. In addition, compromised IoT devices could also be used to launch indirect attacks on infrastructure, e.g., by turning off the thermostat in cold weather and causing pipes to freeze. Finally, from a privacy standpoint, compromised IoT devices also have the ability to passively monitor local networks enabling them to profile user behavior with little chance of detection. Collectively, these threats warrant greater external monitoring and visibility into the behavior of IoT devices attached to local networks.

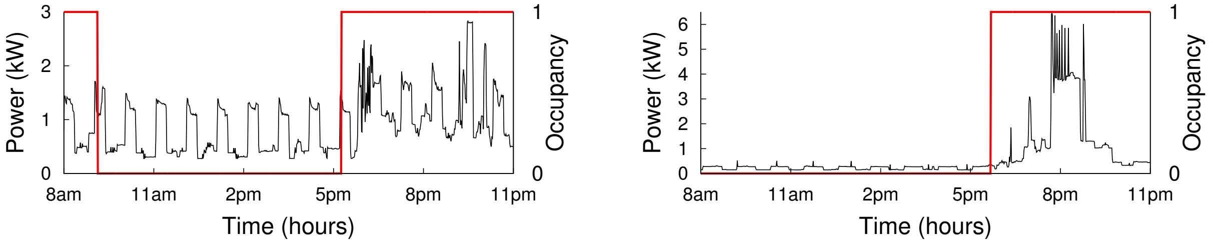
II. Private Memoirs of IoT Devices

In this section, we provide several examples to highlight the privacy implications of IoT devices and cloud-based IoT services. Our examples show how seemingly innocuous data gathered by IoT devices can contain sensitive side-channel information, and how we can employ simple analytics techniques to reveal private information that goes beyond the original purpose for which the data was collected.

A. Smart Home Devices

Recent years have seen an explosion of smart home IoT devices that enable home automation, remote control, and user convenience. Home owners may now choose from a plethora of IoT devices that make many aspects of a home "smart"—ranging from smart power outlets and switches, such as the Belkin Wemo [9], smart thermostats, such as the Nest [10], Lyric [11], and Ecobee [12], and smart locks, such as August [13]. These devices typically connect to a cloud service, which acts as a proxy that receives data and events from the device and sends remote commands (often received from users via a smartphone app) to the device.

The cloud service typically maintains a log of historical events, i.e., a "memoir," for the device, which can reveal private information about users. In the simplest case, events, such as flipping a light switch or unlocking an entry door, reveals the presence of occupants in a home. Smart thermostats may also include motion sensors that directly monitor occupancy to learn occupancy patterns, which they use to derive thermostat schedules that improve energy-efficiency without reducing user comfort. These occupancy patterns directly reveal when users leave from and return to the home on a day-to-day basis, as well as when and how frequently they are away for extended periods of time, e.g., for vacations. In recent years, electric utilities have also been replacing traditional electromechanical energy meters with smart meters, which monitor and record home energy usage at much finer granularities, e.g., every few minutes rather than once per month. Consumer-grade energy meters are also widely available that enable end-users to monitor



(a) Home-A

(b) Home-B

Figure 1. Overlay of average power usage every minute (black) with binary occupancy (red), where one indicates at least one occupant is present and zero indicates no occupants are present, over one day (8am-11pm) for two homes.

their home's total electricity usage. Interestingly, even these "coarse-grained" devices that are simply measuring a home's total electricity usage can reveal sensitive activities within the home. Below, we describe two examples of such analytics techniques that have been developed recently.

Non-intrusive Occupancy Monitoring (NIOM) is a class of analytics techniques that learn occupancy information from the energy usage data of a home or building. The methods are non-intrusive, in that they do not require any direct instrumentation or sensors to monitor occupancy, and only indirectly learn occupancy via "side-channel" information embedded in energy usage data. The primary intuition behind NIOM is that when a home is occupied, occupants perform activities that manifest themselves as an increase in the home's total energy usage, its burstiness, or both. For example, occupants may use a microwave to cook food, do their laundry, or simply turn lights on and off, when home, all of which cause changes to a home's energy usage.

In contrast, when a home is not occupied, many of these changes in energy from these interactive devices that require manual operation do not occur. As result, statistical analyses of energy data traces over time, as recorded by a smart energy meter, enables NOIM methods to accurately identify periods when a home is occupied and when it is not. A practical challenge in designing such analytics techniques is to account for the presence of background appliances that operate regardless of occupancy. For example, a refrigerator will continue to operate regardless of whether someone is home or not, requiring its energy usage to be filtered out when performing NIOM analysis.

To illustrate, Figure 1 shows an annotated trace of energy usage of two different homes that are marked with periods when a home is occupied or not [1]. As the figure shows, periods of occupancy correlate well with higher and more bursty energy usage. While the figure also shows the energy usage from background devices, it illustrates that their statistical characteristics are different than interactive foreground devices that users control, e.g., such as a microwave or lighting. Interestingly, prior work [1], [14] reports occupancy detection accuracies of 70-90% for a range of homes, which is indicative of the amount of side-channel occupancy information embedded in smart meter energy data.

Non-intrusive Load Monitoring (NILM) is a family of analytics techniques that disaggregate the total energy usage of a home into its individual appliances [15]–[17]. Thus, given a trace of a home's aggregate electricity usage, a NILM technique decomposes this total energy usage into the energy used by each individual device or appliance. In doing so, NILM determines what appliances are present in a home and their usage patterns and frequency. NILM methods have been studied for nearly three decades, and a variety of techniques to perform NILM exist, ranging from edge detection and signal processing to machine learning. For example, PowerPlay [2] is a recently proposed method that uses a model-driven approach and defines the notion of virtual sensors for each device to track its individual energy usage. PowerPlay differs from many prior NILM techniques in its focus on tracking the real-time power usage of individual devices, rather than focusing on disaggregating every device's energy usage over a long period of time. In addition, PowerPlay assumes that detailed models of each device being tracked are known *a priori*. PowerPlay's model-driven approach detects a small number of identifiable load features in smart meter data, which derive from a parameterized model of a load's energy usage profile over time, which is based on a small number of fundamental electrical characteristics, i.e., whether a load is resistive, inductive, non-linear, or cyclical. Prior work provides a detailed description of these load types, and their corresponding models [18].

Figure 2 compares PowerPlay's error in disaggregating the energy usage of common household devices with that of a conventional NILM technique that uses an approach based on Factorial Hidden Markov Models (FHMM) [19]. Rather than leverage a well-known model, the FHMM approach must learn a model using training data. Here, disaggregation error is the difference between a device's actual energy usage and its inferred energy usage, normalized by its total energy usage. Lower values are better, with an error factor of zero indicating perfect tracking. While there is no upper bound on the tracking error factor, an error factor of one indicates that the errors are equal to the device's energy usage. In general, a tracking error factor near one is not considered

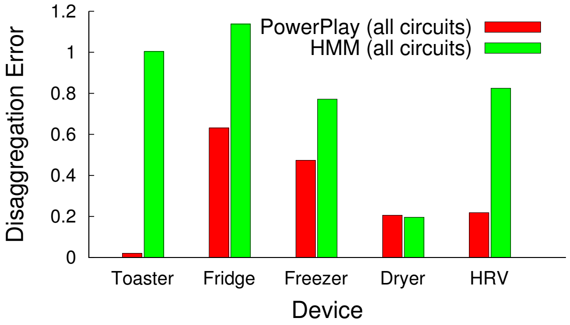


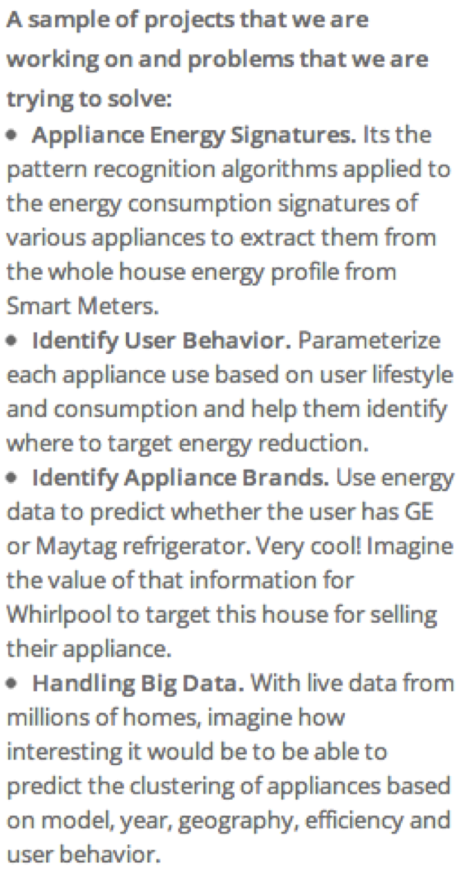
Figure 2. PowerPlay is more robust to noisy smart meter data when tracking loads than the conventional FHMM-based NILM approach.

good, since simply inferring a load's energy usage to be zero at each time t results in a tracking error of one. Our result shows that PowerPlay has significantly less error in tracking device energy usage than the FHMM approach, especially for device's with lower energy usage. The exception is the clothes dryer, which has a large energy usage that both approaches are able to accurately disaggregate and track.

Although NILM was devised as a method to track load-level energy usage without instrumenting each load, it has numerous privacy implications. First, it demonstrates that even a simple dataset, such as the electricity usage of a home, embeds a significant amount of information that permits disaggregation. Second, disaggregating loads reveals not only the energy used by each device, but also information about the daily activity patterns of the users. For instance, we can infer whether users like to eat out and when by examining the energy usage of cooking-related devices. Similarly, based on the usage of the microwave versus a cooktop, do users eat frozen dinners or prepare fresh meals? What days of the week do the users do their laundry? Do they watch a lot of TV? What time do the occupants go to bed? When do they take showers (e.g., from usage of electric water heaters)? Are there children in the household (e.g., inferred from the alignment of energy usage and occupancy to the school calendar)? Clearly, this type of information is private, and the users may not wish for their energy usage to reveal such information about their daily lives. However, this information is also potentially highly profitable, especially if collected at large scales, as it enables companies to profile user behavior and better target their advertising campaigns. There are indications that companies focused on energy data analytics are interested in information for these purposes. For example, Figure 3 shows a job ad from a NILM-focused startup, which highlights the ability to profile users and identify specific appliance brands in energy data.

B. Solar Energy Analytics

While the privacy attacks above focus on inferring human activities from IoT data, we now discuss how energy data can also leak location information, opening up the possibility of location-based privacy attacks. With the growing popularity and falling costs of photovoltaic solar technologies, rooftop solar deployments are growing rapidly in many parts of the world. Electricity generated by rooftop solar arrays can be used to satisfy the energy demands of devices and appliances within the home, while feeding any excess solar electricity to the grid. Thus, the grid is used to compensate for any differences between solar generation and local demand. Nearly all solar deployments are instrumented with IoT sensors that track generation at fine granularities, and expose this data to users via smartphone apps or web-based dashboards. Our recent work has demonstrated that solar generation data at a particular site also embeds the location of that site, and this location information can be extracted from the generation trace using solar analytics methods.

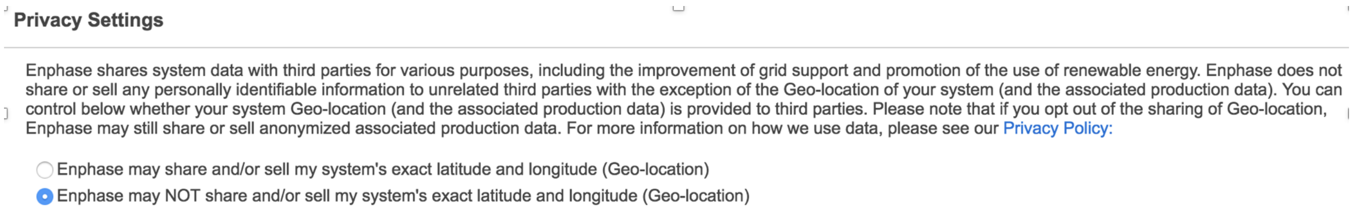


A sample of projects that we are working on and problems that we are trying to solve:

- **Appliance Energy Signatures.** Its the pattern recognition algorithms applied to the energy consumption signatures of various appliances to extract them from the whole house energy profile from Smart Meters.
- **Identify User Behavior.** Parameterize each appliance use based on user lifestyle and consumption and help them identify where to target energy reduction.
- **Identify Appliance Brands.** Use energy data to predict whether the user has GE or Maytag refrigerator. Very cool! Imagine the value of that information for Whirlpool to target this house for selling their appliance.
- **Handling Big Data.** With live data from millions of homes, imagine how interesting it would be to be able to predict the clustering of appliances based on model, year, geography, efficiency and user behavior.

Figure 3. Job ad scraped from the web posted by a NILM-focused startup, which highlights the ability to profile users using energy data.

Intuitively, solar generation at a site depends on the amount of sunlight received at that location, which in turn depends on the length of the day, i.e., from sunrise to sunset, among other factors. The sunrise, solar noon, and sunset times are governed by the latitude and longitude of each specific location—the longitude determines when the sun rises and sets, while the latitude determines the length of the day over the course of the year. Consequently, given the sunrise, solar noon, and sunset times for a particular data,



Privacy Settings

Enphase shares system data with third parties for various purposes, including the improvement of grid support and promotion of the use of renewable energy. Enphase does not share or sell any personally identifiable information to unrelated third parties with the exception of the Geo-location of your system (and the associated production data). You can control below whether your system Geo-location (and the associated production data) is provided to third parties. Please note that if you opt out of the sharing of Geo-location, Enphase may still share or sell anonymized associated production data. For more information on how we use data, please see our Privacy Policy:

○ Enphase may share and/or sell my system's exact latitude and longitude (Geo-location)

● Enphase may NOT share and/or sell my system's exact latitude and longitude (Geo-location)

Figure 4. Enphase does not give users an option to prevent the sharing or selling of their solar data. The only option is whether the data is anonymized by removing the geo-location. However, our work shows that analytics companies can extract the system location from the data itself.

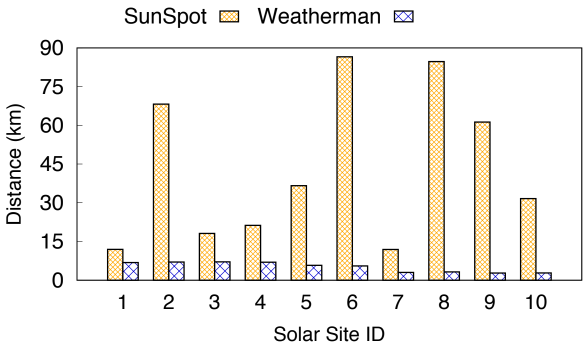


Figure 5. Localization accuracy using both solar and weather signatures.

it is straightforward to compute the latitude and longitude that corresponds to those times. Solar data indirectly reveals when the sun rises and sets based on when panels start and stop generating energy and solar noon is revealed from when the generation peaks. While the solar modules do not precisely start and stop generating energy when the sun rises and sets, respectively, we can analyze generation data over many days to infer the location of solar panels with high accuracy using the solar signature embedded in the data [4].

In addition, solar panels also exhibit a unique weather signature, since the weather conditions at each location also tend to be unique. Since detailed weather data is publicly available throughout the world, we have also developed techniques that localize solar sites by correlating changes in generation with changes in the weather. This weather-based localization can further increase localization accuracy [5]. In addition, when combined with techniques that are able to identify and characterize rooftop solar arrays from publicly-available satellite imagery, these techniques have the potential to identify the specific homes that generated the solar data [20]. Figure 5 illustrates the accuracy of solar localization (in terms of the distance from the actual location) using solar signatures (labeled SunSpot) and weather signatures (labeled Weatherman) for 10 solar sites in different states. Here, the SunSpot bar shows localization accuracy on 1-minute resolution solar data, while the Weatherman bar shows localization accuracy on 1-hour resolution solar data. The figure shows that solar localization often has high accuracy, to within a few kilometers, when using high resolution 1-minute solar data, although a few sites exhibit a high inaccuracy. Localization using weather signatures improves the localization accuracy to within a few kilometers in all cases using significantly coarser 1-hour data.

Overall, our work shows the feasibility of location attacks on anonymous solar datasets. While smart meters typically report only “net” meter data, which combines energy consumption and solar generation, our recent work on solar disaggregation shows that we can accurately separate net meter data into energy consumption and solar generation [21]. Solar disaggregation both enables analytics companies to extract solar generation and its location information from net meter data *and* extract energy consumption data with its information about user behavior, e.g., using NIOM and NILM. This privacy attack is important, since many utilities provide energy analytics companies, such as the one in the job ad from Figure 3, with anonymized energy datasets from smart meters, i.e., by stripping the data of identifying account information. In addition, Figure 4 shows a screenshot of the privacy settings from the web dashboard for Enphase microinverters, the largest manufacturer of solar microinverters, which convert DC power from solar modules to AC power in-phase with the grid. Users have no option to prevent Enphase from sharing or selling their data: their only option is whether or not Enphase anonymizes their data by removing their geo-location. This practice is now so common that the Department of Energy recently released a Voluntary Code of Conduct (VCC) for how utilities should manage user energy data [22]. Importantly, the VCC *does not* require user consent to release anonymized energy data with names and addresses stripped. Consent is likely not required because the energy analytics above do not reveal location, which prevents third-parties from associating private behavior above with a specific home. However, our work demonstrates that, for solar-powered homes, these anonymized datasets are not actually anonymous, as their location is embedded in the data itself.

C. Smart Health Devices

While our examples above focus on IoT devices that monitor energy consumption and generation, there are numerous other IoT devices that expose users to similar privacy threats. For example, wearable fitness tackers and health bands that have become popular in recent years also raise numerous privacy concerns. These trackers monitor activities, such as walking, running, sleeping, many types of exercises, heart rate, skin temperature, and other metrics. In many cases, they also record the GPS locations of where these activities are being performed. Users often share the recorded data with friends using social media features of these cloud services. Sharing of health data, by itself, has privacy implications since it can reveal details of a person's health. For example, the Apple Watch captures heart rate data for its users and Apple researchers found that heart rate patterns can be mined to detect irregular heart rate and atrial fibrillation (AFib), a leading cause of stroke [23]. Another study analyzed this data to detect early signs of diabetes [24]. While there are benefits to detecting such health problems, such private data is also prone to misuse by third parties. For example, depending on the regulations in place, health insurers could use this information in setting rates, or employers could use it in making hiring decisions. The location information gathered by fitness trackers also leaks private information. For example, the start and end location of a run recorded by the fitness tracker will reveal the user's home or work location. In the case of Strava, user running routes inadvertently revealed the location of secret military bases when anonymized user data was released for visualization [6].

III. Challenges in Safeguarding User Privacy

In this section, we present ideas for safeguarding user privacy in light of potential leakage of private side-channel information embedded in IoT data.

A. *Differential Privacy*

Differential privacy is a class of techniques that adds probabilistic transformations to each data item in a large database to prevent any individual from being identified from the larger set. Differential privacy has emerged as an important tool for anonymizing identities in large datasets. While differential privacy techniques have significant promise, they are not directly applicable in many IoT scenarios. For example, many cloud IoT services already know the identity of the users, since they are actively providing services to users (such as the ability to remotely control lights, AC or locks in their home). In such cases, users are more interested in preventing this data from leaking other side-channel information about their activity (e.g., occupancy) rather than masking their identity. Similarly, many services need location data to perform their tasks. For example, a smart door lock may auto-lock itself when the user is more than a certain distance from their home. Precise location information is needed in this case, but it is also desirable to mask other information in the location data, such as where the user goes to shop or where they work. Techniques that go beyond differential privacy are needed in these scenarios. Of course, differential privacy is still applicable to IoT datasets that are being publicly released in anonymized form to prevent de-anonymization of individuals from the data.

B. *Obfuscation*

Data obfuscation techniques modify or transform the data that is being collected to prevent others from performing analytics on the data. This is done by adding noise or other transformations to "significantly" modify the data and prevent analytics from learning anything useful from it. For example, researchers have studied both noise injection and smoothing as techniques to prevent occupancy detection from electricity meter data [25]–[27]. These approaches control large electrical loads, such as large batteries and electric water heaters, to significantly alter the energy usage pattern and mask the features that reveal sensitive information. Figure 6 demonstrates a obfuscation approach using a water heater, which we call Combined Heat and Privacy (CHPr) [25]. CHPr varies the rate water is heated in an electric water heater to mask low and non-bursty periods of electricity caused by a lack of occupancy. Since electric water heaters have a large thermal energy storage capacity relative to the electricity usage of most homes, it can typically mask occupancy without running out of hot water.

The top graph shows a home's original week-long power usage and its ground truth occupancy, while the bottom graph shows its power usage after applying CHPr. A home's original week-long power usage and ground truth occupancy (top), as well as its power usage when using a CHPr-enabled 50 gallon water heater and detected occupancy when using NIOM. We also quantify the performance of the occupancy detection attack on the original demand and the CHPr-modified demand in terms of the Matthews Correlation Coefficient (MCC) [28], which is a standard measure of a binary classifier's performance, where values are in the range -1.0 to 1.0, with 1.0 being perfect detection, 0.0 being random prediction, and -1.0 indicating detection is always wrong. MCC values closer to 0.0, or random prediction, are better for masking occupancy. In this case, our results show that the MCC of the attack on the CHPr-modified data (on the bottom) is only 0.045, which is nearly the same as random prediction, i.e., an MCC of 0.0, and is a factor of 10 less than the MCC of the attack on the original data in the top graph, which is 0.44.

Preventing occupancy detection through obfuscation is a particularly challenging problem, since it requires shifting a large amount of load. Obfuscating NILM is less challenging, since it does not require shifting as much load. As a result, prior work examines different techniques for using a battery to protect against using NILM to identify appliances [26], [27]. Of course, unlike CHPr, which is "free" since the water heater must heat the water anyway, these battery-based methods incur a high cost to install and maintain the battery. Of course, another significant downside to data obfuscation is that it is a blunt instrument that prevents all analytics—both useful analysis on the data, as well as those that leak private information. It is an open research question as to how

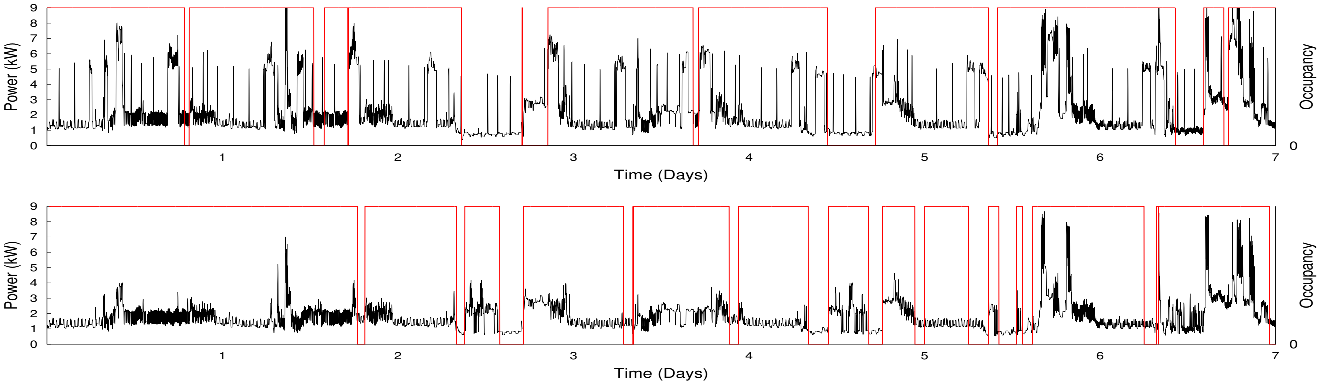


Figure 6. A home's original week-long power usage and ground truth occupancy (top), as well as its power usage when using a CHPr-enabled water heater and detected occupancy when using NIOM.

obfuscation can suitably modify data to allow only certain kinds of analytics, while preventing others.

C. Cryptographic Methods

Cryptographic methods have also been used to safeguard the privacy of users in IoT environments. One approach consists of storing all IoT data locally at the device and allowing the cloud service to query the device as needed. Responses to each query are sent as a verifiable cryptographic proof rather than sending a portion of the data (since the latter can leak private data). The cryptographic proof enables the cloud server to verify that the response to the query is correct without ever seeing the data used to construct the response. An example of this approach is Zero-Knowledge Proofs, which have been used to design a privacy-preserving smart meter in prior work [29], [30]. This work showed how the meter can be queried for the total recorded electricity usage over a period, such as the month, and the response can be sent in the form of a verifiable cryptographic proof without sending the raw usage data. Such cryptographic methods are promising from a privacy perspective but a general approach for arbitrary queries and IoT service is an open question–in the current approach, specific proofs need to be designed for particular types of queries. Furthermore, the approach does not yet generalize to two way communication between the IoT device and the cloud service. Finally, the approach permits only a narrow set of queries and thus may prevent utilities from performing a number of useful analytics that increase grid reliability and efficiency.

D. Local IoT services

The primary idea that underlies the cryptographic method above is to keep data locally at the device and not send it to the cloud server. This is a broad principle that is useful for building any privacy-preserving IoT application. In general, if the data is kept locally and never sent to third parties, the user stays in control of the data and privacy attacks on the data can be minimized. Such approaches are becoming more feasible, since IoT devices or local IoT hub are gaining more processing and storage capabilities that make high-performance local services more feasible. In such a scenario, the cloud service may still play a role–for instance, the cloud service may learn a general model over the data and send the model to the local IoT device, which then executes it locally on local data. Techniques, such as transfer learning, can be used in such scenarios, which allows general models to be applied to specific contexts. More generally, the approach implements all the "intelligence" of smart devices locally at the device and eliminates the cloud service or vastly reduces reliance on the cloud backend.

E. User Controllable Privacy

The above discussion of leakage of private information embedded in IoT data, and the need to mitigate such privacy attacks, broadly points to the need to allow users to have full control over their data, including how it is used by third parties and what can be gleaned from the data. We refer to this "holy grail" of IoT privacy as *user controllable privacy*. Some researchers have argued for an abstract "knob" that is controlled by users and represents their privacy preferences: the knob can be adjusted to tradeoff the loss of privacy that comes with sharing data with third parties with the value or utility offered by the service that comes from sharing the data. Of course, users should also be able to prevent side-channel leakage by ensuring that data is shared for a certain purpose and no other information can be learned from it. For example, a smart meter should provide usage information to a utility to calculate monthly electric bill, but should do so in a way that prevents occupancy or NILM-based analytics from being performed on the data. Location data poses particular challenges since location information is necessary to tailor the service in a location-specific manner, but user should be able to thwart location analytics from gleaning other side-channel information from such data. There are many open challenges to achieving user controllable privacy. However, it remains a worthy goal for researchers so as to ensure IoT devices and services can provide convenience to end users without compromising their privacy.

IV. IoT Network Vulnerabilities

Finally, while the privacy attacks and defense above focus on the data that IoT devices collect, IoT devices also expose users to new network vulnerabilities, since they are connected to implicitly trusted local networks. As embedded IoT devices proliferate, the probability that attackers will compromise them increases. Embedded IoT devices use increasingly high-power general-purpose processors capable of running sophisticated software stacks atop commodity operating systems, such as Linux, that expose a much larger attack surface than earlier embedded devices, which generally used custom software on lower-power processors with narrower functionality. Similar to smartphones, some IoT devices now enable users to install third-party apps, which exposes them to, not only external attacks via the network, but also internal attacks via their software interfaces.

A key difference between IoT devices and more general-purpose devices, such as laptops, smartphones, tablets, etc., is that they have very narrow, potentially non-existent, user-facing interfaces. Further, most IoT devices do not allow administrative-level access to devices that enables users visibility into their internal operations. As a result, users are much less likely to know if an IoT device has been compromised by an attacker. In general, users do not have a deep understanding of how most IoT devices work or how they interact with external entities over their network.

In some cases, as network management becomes more automated, users may not even realize that a device runs software at all and connects to remote servers on the Internet via their local network. For example, a typical home today may have over 40 IoT devices connected to its network, including multiple smart thermostats, plug-level energy monitors, a solar inverter, a smart washing machine and dryer, a hub for IoT devices, multiple smart televisions, etc. Many of these devices are running some version of Linux, often with an open ssh port that cannot be accessed by the consumer.

Importantly, such IoT devices operate behind the firewall, e.g., provided by the gateway router, in private local area networks that are implicitly trusted. This firewall typically protects network devices on these private networks from the numerous bots that probe servers on the public Internet for known vulnerabilities. As a result, servers that exclusively operate behind firewalls are often significantly more vulnerable than servers on the public Internet, since users are not accustomed to frequently updating their software to install the latest security patches and prevent breaches. In some cases, servers on these private networks may not have ever had (or needed) a security software update.

Since IoT devices generally operate behind such firewalls on local area networks, and open network connections to remote servers "in the cloud," they allow those external servers an avenue for tunneling into trusted local area networks. Such tunneling is required for an IoT device to operate, as the basic control loop is to send sensor data to the cloud, where it is processed, and then results and/or actuation commands are sent to the device by tunneling through the firewall via the device's initial network connection. Unfortunately, this basic control loop opens up multiple possible vulnerabilities that an attacker may exploit.

For example, an attacker could compromise the remote server, enabling them to steal data sent by the device or send the device erroneous data or commands that cause the device to misbehave. In addition, an attacker could compromise a software upgrade, enabling them to install their own software on the device, allowing them to attack other devices within the local area network or in the Internet. For instance, a recent distributed denial of service attack on the DNS system stemmed from millions of compromised IoT devices, e.g., routers, IP cameras, DVRs, etc. [31]. Importantly, from a privacy standpoint, an attacker could also set the compromised device's network card in promiscuous or monitor mode and passively monitor the local network traffic, and either perform deep packet inspection to learn sensitive information and profile the occupants of the building, the types of devices they own, their habits, etc. This type of vulnerability is particularly harmful since it is unlikely that users would ever detect or notice such passive monitoring of their networks.

These examples demonstrate that the nature of network and computer security is poised to dramatically change with the proliferation of next-generation IoT devices. Users can no longer assume that their local area networks are secure, and that attacks originate from outside their local network. In addition, as the examples above illustrate, securing the network is much harder since users typically do not have administrative access to IoT devices, and they cannot necessarily trust the company that sells the device to ensure its security, since that company may become compromised, e.g., from an an external attack or by their own employees. As a result, users will need to monitor their local networks to identify suspicious network traffic patterns from devices based on their frequency of transmission, the amount of data they transmit, and where those transmissions are directed in the Internet. Upon identifying suspicious traffic, local networks will need to be able to automatically configure themselves to isolate suspicious devices from other devices on the network and potentially cut off their network access.

Thus, a promising area of research is designing ”smart” gateway routers and access points that classifies devices based on their typical traffic patterns, and are able to automatically configure the network to isolate IoT devices from other local network elements. In general, gateway routers should follow the principle of least privilege, where IoT devices connected to local area networks that users cannot readily observe or control are isolated as much as possible from other devices on the local network.

V. Conclusion

This vision paper discusses recent work on sensor data privacy in the context of energy systems to provide examples of i) the surprising types of private information embedded in IoT sensor data and ii) the different types of defenses that have been employed to preserve IoT data privacy, particularly in the context of energy systems. These defenses have different tradeoffs between privacy, IoT functionality, and cost, which motivates new research on developing defenses that enable users to control this tradeoff. We then outline the privacy implications of untrusted IoT devices connecting to implicitly trusted networks, and possible future research directions to mitigate these privacy implications.

Acknowledgment

This research is supported by NSF grants IIP-1534080, CNS-1645952, CNS-1405826, CNS-1253063, CNS-1505422, and the Massachusetts Department of Energy Resources.

References

[1] D. Chen, S. Barker, A. Subbaswamy, D. Irwin, and P. Shenoy, “Non-Intrusive Occupancy Monitoring using Smart Meters,” in *BuildSys*, November 2013.

[2] S. Barker, S. Kalra, D. Irwin, and P. Shenoy, “Powerplay: Creating Virtual Power Meters through Online Load Tracking,” in *BuildSys*, November 2014.

[3] D. Chen, S. Kalra, D. Irwin, P. Shenoy, and J. Albrecht, “Preventing Occupancy Detection from Smart Meter Data,” in *ToSG*, July 2015.

[4] D. Chen, S. Iyengar, D. Irwin, and P. Shenoy, “SunSpot: Exposing the Location of Anonymous Solar-powered Homes,” in *BuildSys*, November 2016.

[5] D. Chen and D. Irwin, “Weatherman: Exposing Weather-based Privacy Threats in Big Energy Data,” in *BigData*, June 2017.

[6] R. Perez-Pena and M. Rosenberg, “Strava fitness app can reveal military sites, analysts say,” New York Times, January 28th 2018.

[7] J. John, “US Smart Meter Deployments to Hit 70M in 2016, 90M in 2020,” in *GreenTechMedia*, October 26th 2016.

[8] D. Goodin, “New IoT botnet offers DDoSes of once-unimaginable sizes for $20,” Ars Technica, February 1st 2018.

[9] “Belkin WeMo,” http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation/, February 2018.

[10] “Nest,” http://nest.com, February 2018.

[11] “Honeywell Lyric,” http://lyric.honeywell.com, February 2018.

[12] “Ecobee,” http://ecobee.com, February 2018.

[13] “August Smart Locks,” http://august.com/, February 2018.

[14] W. Kleiminger, C. Beckel, T. Staake, and S. Santini, “Occupancy Detection from Electricity Consumption Data,” in *BuildSys*, November 2013.

[15] K. Armel, A. Gupta, G. Shrimali, and A. Albert, “Is Disaggregation the Holy Grail of Energy Efficiency? the Case of Electricity,” *Energy Policy*, vol. 52, no. 1, 2013.

[16] G. Hart, “Residential Energy Monitoring and Computerized Surveillance via Utility Power Flows,” *IEEE Technology and Society Magazine*, vol. 8, no. 2, June 1989.

[17] M. Zeifman and K. Roth, “Nonintrusive Appliance Load Monitoring: Review and Outlook,” *IEEE Transactions on Consumer Electronics*, vol. 57, no. 1, February 2011.

[18] S. Barker, S. Kalra, D. Irwin, and P. Shenoy, “Empirical Characterization and Modeling of Electrical Loads in Smart Homes,” in *IGCC*, June 2013.

[19] J. Kolter and M. Johnson, “REDD: A Public Data Set for Energy Disaggregation Research,” in *SustKDD*, August 2011.

[20] J. Malof, R. Hui, L. Collins, K. Bradbury, and R. Newell, “Automatic Solar Photovoltaic Panel Detection in Satellite Imagery,” in *ICRERA*, November 2015.

[21] D. Chen and D. Irwin, “SunDance: Black-box Behind-the-Meter Solar Disaggregation,” in *e-Energy*, May 2017.

[22] “Voluntary Code of Conduct (VCC),” U.S. Department of Energy, Tech. Rep., January 12 2015.

[23] T. Ong, “The Verge, Apple launches study to identify irregular heart rhythms with the Apple Watch,” https://www.theverge.com/2017/11/30/16719458/apple-watch-study-irregular-heart-rhythms-stanford-university, November 30th 2017.

[24] S. Buhr, “TechCrunch, The Apple Watch can detect diabetes with an 85accuracy, Cardiogram study says,” https://techcrunch.com/2018/02/07/the-apple-watch-can-detect-diabetes-with-an-85-accuracy-cardiogram-study-says/, February 6th 2018.

[25] D. Chen, D. Irwin, P. Shenoy, and J. Albrecht, “Combined Heat and Privacy: Preventing Occupancy Detection from Smart Meters,” in *PerCom*, March 2014.

[26] S. McLaughlin, P. McDaniel, and W. Aiello, “Protecting Consumer Privacy from Electric Load Monitoring,” in *CCS*, October 2011.

[27] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, “Minimizing Private Data Disclosures in the Smart Grid,” in *CCS*, October 2012.

[28] B. Matthews, “Comparison of the Predicted and Observed Secondary Structure of T4 Phage Lysozyme,” *Biochimica et Biophysica Acta.*, vol. 405, no. 2, October 1975.

[29] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, “Private Memoirs of a Smart Meter,” in *BuildSys*, November 2010.

[30] A. Molina-Markham, G. Danezis, K. Fu, P. Shenoy, and D. Irwin, “Designing Privacy-preserving Smart Meters with Low-cost Microcontrollers,” in *FC*, February 2012.

[31] B. Krebs, “KrebsOnSecurity Hit with Record DDoS,” https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, September 21st 2016.