Research Repository UCD

Title	Generating power footprints without appliance interaction : an enabler for privacy intrusion
Authors(s)	Sintoni, Alex, Schoofs, Anthony, Doherty, A., Smeaton, Alan F., O'Hare, G. M. P. (Greg M. P.), Ruzzelli, Antonio G.
Publication date	2011-06-27
Publication information	Sintoni, Alex, Anthony Schoofs, A. Doherty, Alan F. Smeaton, G. M. P. (Greg M. P.) O'Hare, and Antonio G. Ruzzelli. "Generating Power Footprints without Appliance Interaction : An Enabler for Privacy Intrusion." IEEE, 2011.
Conference details	Paper presented at the 1st HOBNET Workshop on IPv6 Sensor Networking for Smart/Green Buildings, at the 7th IEEE International Conference on Distributed Computing in Sensor Systems DCOSS '11, June 27 - 29, 2011, Barcelona, Spain
Publisher	IEEE
Item record/more information	http://hdl.handle.net/10197/3191
Publisher's statement	Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Publisher's version (DOI)	10.1109/DCOSS.2011.5982180

Downloaded 2023-04-07T10:52:29Z

The UCD community has made this article openly available. Please share how this access benefits you. Your story matters! (@ucd_oa)

© Some rights reserved. For more information

Generating Power Footprints without Appliance Interaction: an Enabler for Privacy Intrusion

A. Sintoni[†], A. Schoofs[†], A. Doherty*, A.F. Smeaton*, G.M.P. O'Hare[†], A.G. Ruzzelli[†]

CLARITY: Centre for Sensor Web Technologies

[†]University College Dublin

*Dublin City University

Dublin, Ireland

Abstract—Appliance load monitoring (ALM) systems are systems capable of monitoring appliances' operation within a building using a single metering point. As such, they uncover information on occupants' activities of daily living and subsequently an exploitable privacy leak. Related work has shown monitoring accuracies higher than 90% achieved by ALM systems, yet requiring interaction with appliances for system calibration. In the context of external privacy intrusion, ALM systems have the following obstacles for system calibration: (1) type and model of appliances inside the monitored building are entirely unknown; (2) appliances cannot be operated to record power footprints; and (3) ground truth data is not available to fine-tune algorithms. Within this work, we focus on monitoring those appliances from which we can infer occupants' activities. Without appliance interaction, appliances' profiling is realised via automated capture and analysis of shapes, steady-state durations, and occurrence patterns of power loads. Such automated process produces unique power footprints, and naming is realised using heuristics and known characteristics of typical home equipment. Data recorded within a kitchen area and one home illustrates the various processing steps, from data acquisition to power footprint naming.

I. INTRODUCTION

A. Fine-Grained Electricity Monitoring

Electricity represents 41% of the total energy used in the United States [1], and about one third of it is wasted [2]. Recent efforts for a modernised electrical grid—*smart grid*—are primary triggers to counterbalance and reduce electricity consumption [3]. Smart meters are being introduced within homes for providing real-time access to power readings remotely [4], [5], facilitating utilities' global control and management of electricity consumption and generation, respectively.

As a short-term alternative to longer-term smart meter widespread deployment, commercial electricity monitors reduced to mere electricity reading and local reporting are also being made available. Such devices can be clamped to buildings' main circuit board to measure a rich cocktail of electrical parameters and provide real-time power consumption feedback to electricity consumers.

This work demonstrates that access to electricity readings via the introduction of smart meters and electricity monitors enables illicit monitoring of private activities of daily living.

B. Enabler for privacy intrusion

Activities of Daily Living (ADLs) include, but are not limited to cooking, showering, washing, and sleeping; they therefore involve interactions with electrical equipment. Appliance load monitoring (ALM) systems are systems capable of monitoring appliances' operation within a building using a single metering point. As such, they uncover information on occupants' interactions with electrical equipment and subsequently an exploitable ADL privacy leak. The privacy of ADLs is a matter well-discussed elsewhere [6], [7], [11]. For instance, such privacy intrusion may be inappropriately used to infer medical conditions [8] or to simply inquire a person's presence for a potential burglary [11]. Related work has shown monitoring accuracies higher than 90% achieved by ALM systems, yet requiring interaction with appliances for system calibration. In the context of external privacy intrusion, ALM systems have the following obstacles for system calibration: (1) type and model of appliances inside the monitored building are entirely unknown; (2) appliances cannot be operated to record power footprints; and (3) ground truth data is not available to fine-tune algorithms.

Within this work, we focus on monitoring those appliances from which we can infer occupants' activities. Without appliance interaction, appliances' profiling is realised via automated capture and analysis of shapes, steady-state durations, and occurrence patterns of power loads. Such automated process produces unique power footprints, and naming is realised using heuristics and known characteristics of typical home equipment.

II. RELATED WORK

The potential abuse of ALM systems for surveillance purpose has been discussed abundantly. Power-based surveillance for monitoring the activities of suspected criminals or political opposition; identifying the movements of occupants to time a break-in; advertising consumers lacking consumer appliances; taxing bad electricity users turning on their air-conditioning system in restricted hours are exemplars. Privacy intruders may range from single individuals to enterprises and utilities themselves.

Appliance load monitoring systems are designed to achieve a building's power decomposition, down to equipment level.

Appliance *signatures* are measurable parameters of the total load that give information about the nature or operating state of individual appliances in the load [14]. They are therefore the patterns that ALM systems try to extract from a congregated building power signal. Knowing appliances' signatures, complex pattern recognition techniques return the list of appliances which combination of signatures provides the best match with the measured signal, e.g. [9], [14].

Mature research in the area of appliance load monitoring has as yet not been transferred to actual commercial integration. Indeed, most ALM systems require complex calibration and verification to be carried out by a trained technician or an auxiliary system [10] before it can be used in a domestic or commercial environment. Hart *et al.* proposed an automatic set-up nonintrusive appliance load monitoring system (AS-NALM), setting the basic steps for an automated capture and naming of appliance signatures. Since then, a number of calibration-free systems have been proposed. Molina-Markham *et al.* [12] utilise statistical methods to derive complex appliances' usage patterns from electricity readings, claiming no prior knowledge of household activities and no training phase. They however relate to power activity journals annotated by home occupants and used to map opaque labels to real-life events. Unless occupants agree to be monitored and provide such brief logs, those cannot be assumed for configuring appliance load monitoring systems. Lisovich *et al.* [13] provide a technical study showing how activity information can be extrapolated from power-consumption data. They assume that the adversary has a list of appliances present inside, as well as their turn-on/turn-off profiles.

Although automated calibration and risks of privacy issues are well-known, few systems have been implemented and evaluated for exploiting effectively such privacy leaks in a real-world scenario where pre-calibration is impossible. This work proposes an initial experimental evaluation of such system in an ADL privacy case study. We argue that identifying the monitoring purpose and objective prior to operation is essential to achieving high accuracy, focusing monitoring on the subset of appliances of interest and discarding uninteresting power activity.

III. MONITORING ACTIVITIES OF DAILY LIVING USING A SINGLE ELECTRICITY MONITOR

Primary challenges in deriving activity patterns of a building occupant from a single electricity monitor are threefold. First, the attacker needs to have access to the building power flow. Second, the attacker requires an appliance load monitoring system that can disaggregate a power load without prior knowledge of the building appliances' signatures. Finally, appliance activities need to be matched to ADLs.

We investigate the case of power flow captured at the live wire, via illicit clamping of an electricity monitor, see Figure 1. Electric meters may be located in the power pylon serving the property; in a meter-box external to the house; in a public space such as a building's corridor or an office open distribution board; or inside the premises. Once the

Fig. 1. Illicit clamping of an electricity monitor to the live wire of the monitored building.

Fig. 2. Four-step processing of the raw electricity data captured at the electric meter to profile appliance signatures passively.

electricity monitor is clamped, raw electricity consumption of the building under surveillance is reported wirelessly to the attacker's PC-class machine.

A. Profile-free Appliance Load Monitoring System

In order to disaggregate a building's power flow without access to the premises, the appliance load monitoring system used by the attacker needs to be free of any human supervised calibration procedure.

The technique we propose takes advantage of the attacker's prior knowledge of the kind of appliances and patterns that he wishes to recognise. In an ADL intrusion context, appliances that will indicate an occupant activity are the ones of interest, reducing the monitoring objectives to their detection. For instance, detecting the activity of a fridge compressor has no intrinsic value as it is not linked to any user activity, and is either filtered out or kept unnamed.

Fig. 3. (a) Capture of power flow over one day illustrating appliance activity, and (b) Filtered power flow over one day revealing only the significant appliance activity.

Fig. 4. (a) Zoom to the 8am-9am time slot indicates superposition of appliance signatures, and (b) Zoom to the 9pm-10pm time slot indicates single appliance signatures.

The proposed technique follows a four-step processing on the raw power flow, as shown in Figure 2. The following describes in greater details the four steps of data processing conducted to retrieve appliances' signatures, illustrated with experimental data.

1) Noise filtering and capture of power signatures: These two initial processing steps consist of detecting and recording any power steps on the electricity reading that may be useful for the attacker. At this point, the attacker does not know anything about the appliances, habits and patterns of the occupant being tracked. Figure 3(a) shows the apparent power of a one-person household, captured by the electricity monitor over a period of one day. Activity is visible in the morning

between 8 and 9am, and in the evening between 7 and 10pm.

In an ADL attack context, noise is considered as being power associated to always-on appliances and periodic patterns such as the periodic power step visible on Figure 3(a). A first processing step is therefore to cancel out the noise via filtering with thresholds and pattern recognition. The output of Figure 3(a) after filtering is given in Figure 3(b).

Resulting peaks will often be a superposition of multiple appliances signatures, when several appliances are used concurrently—see zoom to 8-9am time slot on Figure 4(a). However, as Figure 4(b) shows via a zoom on the 9-10pm apparent power data, single appliance signatures often appear on a power reading, facilitating their capture. The range of electrical parameters as well as a timestamp are recorded for each of the unique power footprints that are detected after filtering. The objective of this second processing step is to aggregate a pool of power footprints to later cluster them type and time wise, in order to facilitate their naming.

2) Clustering of identical power signatures: The third processing step is to cluster identical power footprints, and analyse the times at which they appear. The goal is to derive a distribution of occurrences for each power footprint that will be used for understanding the nature of the appliances.

Fig. 5. Distribution of occurrences of the power footprint shown at the right of Figure 4(b) over a period of 7 days. Vertical lines indicate when the power footprint has been detected.

Figure 5 shows as an example the distribution of occurrences of the power footprint that appears at the very right of Figure 4(b). This clustering was produced from one week of data captured at the electricity monitor over a different period. At this point, the attacker has in his hands the power characteristics of a given appliance, such as an apparent power of 2.6kW in that case, and the times at which such signature has appeared.

3) Naming of appliances signatures: Naming is facilitated by the fact that the attacker knows the typical shape and power characteristics of the appliances signatures he is interested in. Figure 6 recalls generic power footprints for three appliances that can be used for detecting ADLs. They are signatures of an

hair-dryer, a toaster, and an oven, used for monitoring cleaning duties, eating, and cooking respectively. These signatures are not the footprints of appliances present within the building, but are footprints of similar appliances procured by the intruder beforehand. Ideally, the intruder will possess a library of signatures which footprints captured within the building can be compared to.

Fig. 6. Generic power signatures of an hair dryer, a toaster, and an oven.

Naming of the building’s appliances’ signatures is realised by comparing the power characteristics of power footprints detected from the electricity readings with typical appliances’ signatures, and reasoning on the produced time distributions of occurrences. In this example, figure 5 does not give a direct indication for concluding on the appliance name. A morning-only distribution of occurrences would be helpful for characterising breakfast-type of machines such as toaster and coffee machines. We however see that the given appliance is used at random times during the day, and several times per day. Such facts rule out appliances such as hair dryers that are used at maximum a few times per day. Furthermore, the distribution of occurrences shows that the appliance is sometimes used many times over relatively short periods of time. This extra indication together with the observed power characteristics give indication that such signatures corresponds with high probability to a kettle.

Once names are given to each power footprint, the appliance load recognition system is ready to disaggregate in real-time the power flow. The last step of the ADL monitoring consists of bridging appliances’ activities to ADLs.

TABLE I
ADLS AND ASSOCIATED APPLIANCES.

	Eating	Toileting	Moving
Dish-washer	x		
Electric heater		x	
Electric shower		x	
Fitness equipment			x
Hair-dryer		x	
Induction cookers	x		
Kettle	x		
Microwave	x		
Oven	x		
Toaster	x		

B. Matching appliances’ activities to ADLs

There exist a number of basic ADLs including eating, dressing, washing, and transferring (moving). Such ADLs can be inferred when interaction with appliances exists. For instance, detecting that the microwave is on is a good indication of eating activity. Table I categorises the set of ADLs and associated home appliances that may be used by an attacker in the context of an health condition privacy intrusion. Health condition relates importantly to the ability of a person to eat, wash and move independently. As shown in Table I, there are only few direct activity relationships between appliances and ADLs. Yet, more reasoning may provide extra information not visible in Table I. For instance, observing appliances being switched on consecutively in supposed different rooms, say the oven and the hair dryer, may indicate an occupant’s mobility.

IV. IMPLEMENTATION

We developed RECAP-free, a calibration-free appliance load monitoring (ALM) system, based on RECAP, an ALM system capable of recognising appliance activities in real-time using a neural network machine learning technique and prior appliance profiling [9]. RECAP-free reuses the recognition components from RECAP, but handles discovery and naming of power footprints without equipment interaction.

RECAP-free has been implemented in Java. The four conceptual processing steps described in Section III-A have been integrated to provide more efficient coding and have been automated to minimise human supervision. Noise filtering is realised as soon as electricity readings are read. Whether a power step is detected, the program makes a record of a new signature; other small variations are filtered out. When a new signature is recorded, the program captures the associated power parameters, and check whether a similar power footprint exists in the signature database. The objective is to immediately cluster occurrences of identical signatures. If a similar signature exists, the system records the new timestamp at which the signature has been observed, generating over time a list of timestamps for each single signature. In case the signature does not exist, a new entry is created. At the end of the process, RECAP-free profiling engine provides a list of single signatures and associated timestamps at which they occurred. At this stage, naming of power signatures is the only step done manually. We are currently populating a database of power signatures, that we plan to use to develop automated power signature comparison for further deployments.

V. EXPERIMENTATION

We have initially restricted our tests to a kitchen area, in order to fine-tune our algorithms in a controlled environment with a limited subset of appliances. After validation, we ran our algorithms within a real domestic environment for a period of one week.

A. Fine-tuning the system

A kitchen area has been equipped with an Episensor electricity monitor [15]. The monitoring setup is similar to that

presented in Figure 1. The PC-class unit stores data readings transmitted by the electricity monitor at a granularity of one sample every 10 seconds and runs RECAP-free.

Fig. 7. Data retrieved in CLARITY's kitchen area over a period of one hour.

Table - dbo.AppliancesProfiling		Table - dbo.Appliances		Table - dbo.ApplianceON		Table - dbo.A...	
	ApplianceID	Timestamp	RealPower	ApparentPower	PeakCurrent		
	u1272471654796	28/04/2010 16:20:46	40888.000000	74000.000000	0.000000		
	u1272471654796	28/04/2010 16:20:51	2627296.000000	2606866.000000	10201.000000		
	u1272471654796	28/04/2010 16:20:51	2633112.000000	2612000.000000	10208.000000		
	u1272472270546	28/04/2010 16:31:00	41193.000000	73873.000000	0.000000		
	u1272472270546	28/04/2010 16:31:05	840329.000000	813397.000000	2946.000000		
	u1272472270546	28/04/2010 16:31:05	837807.000000	811127.000000	3076.000000		
	u1272472463640	28/04/2010 16:34:15	41599.000000	74357.000000	0.000000		
	u1272472463640	28/04/2010 16:34:20	1026420.000000	1083534.000000	4014.000000		
	u1272472463640	28/04/2010 16:34:20	1028401.000000	1083643.000000	4111.000000		
*	NULL	NULL	NULL	NULL	NULL		

Fig. 8. Power footprints generated by RECAP-free from the kitchen area data capture.

Figure 7 represents one hour of data captured by the electricity monitor, showing both single and combined activity of various appliances. Figure 8 shows that 3 unique power footprints have been discovered by RECAP-free. When registering a power footprint, RECAP-free records a portfolio of electric parameters for three successive data readings, as highlighted in Figure 8. The first data reading is taken before the power step has been detected, and the two other data readings correspond to moments after the power step has been detected. The third data reading is recorded to handle cases when the second data reading has been sampled while the power level was in a transient state between the appliance off and on power states. Power footprint registration with RECAP-free is also timestamped, but discrepancies in software configuration generated a one-hour time difference between table timestamps and graph timing. Furthermore, as one can see on Figure 7 and Figure 8, RECAP-free appliances' signatures have been generated once a power footprint has appeared 3 times. For instance, the first signature has been generated at 16:20 (17:20 on Figure 7), even if the same power footprint has appeared at 17:05 and 17:15.

Figure 8 shows that the three appliances have been instrumented several times during data capture but without any meaningful usage pattern, see Figure 7. Within this study, longer data capture has however provided a better view on appliances' frequency of usage. Figure 9 shows a data capture

made during afternoon working hours, exhibiting numerous repetitions of one power signature at lunch time, and random appearance of another power signature throughout the day. Such usage pattern information is vital to associate names to the discovered footprints. Based on these times of occurrence as well as power characteristics of discovered power footprints, the first signature captured is named as a kettle, and the third one as a microwave. More data will however be necessary to name confidently the second power footprint. This example has shown the importance of the amount of data that needs to be gathered to achieve an accurate and effective processing.

Fig. 9. Data retrieved in the kitchen area during working hours exhibiting the random use of the kettle and the use of the microwave at lunch time.

B. Real world testing

One home has been equipped with an Episensor electricity monitor [15] for a period of 7 days. In that deployment, data readings are sampled every minute.

Fig. 10. Power measurement within a family home over a period of 7 days.

Figure 10 shows the apparent power measurement over the 7-day period. Immediately, one can see the difficulty at hand with real world experimentation; noise and number of appliances are increased. We ran RECAP-free over that data and Figure 11 shows that 4 primary power footprints have been discovered. The power consumption for those power footprints is given, and they are initialised with a non-meaningful name.

RECAP-free generated as well a table of activities, showing the power state of those four power footprints over time. The

id	Name	PowerConsumption
MonoPahse1302275040218	NULL	147714.290000
MonoPahse1302275063937	NULL	1716571.430000
MonoPahse1302275070765	NULL	862888.890000
MonoPahse1302275082421	NULL	389000.000000
Others000D6F00001E617D	Others000D6F00001E617D	102000.000000

Fig. 11. Power footprints discovered by RECAP-net.

Results	Messages	ID	TimeStamp	UnknownLoad	MonoPahse1302275040218	MonoPahse1302275063937	MonoPahse1302275070765	MonoPahse1302275082421
1		4277	2011-01-24 21:25:17	0	1	0	1	0
2		4278	2011-01-24 21:33:49	0	0	0	0	0
3		4279	2011-01-24 21:57:17	0	1	0	0	1
4		4280	2011-01-24 22:02:37	1	1	0	0	1
5		4281	2011-01-24 22:03:41	0	1	1	0	0
6		4282	2011-01-24 22:25:01	0	0	1	1	0
7		4283	2011-01-24 22:26:05	0	0	1	0	0
8		4284	2011-01-24 22:49:33	0	1	0	1	0
9		4285	2011-01-24 23:17:17	0	0	0	1	0
10		4286	2011-01-24 23:22:37	0	1	0	0	1
11		4287	2011-01-24 23:25:49	0	0	0	0	1
12		4288	2011-01-24 23:39:41	0	1	0	0	1
13		4289	2011-01-24 23:55:41	2	0	0	0	1
14		4290	2011-01-25 00:10:37	0	1	0	0	1
15		4291	2011-01-25 00:24:29	0	0	0	0	1
16		4292	2011-01-25 00:46:53	0	0	0	0	0
17		4293	2011-01-25 00:51:09	0	1	0	0	0
18		4294	2011-01-25 01:01:49	0	0	0	0	0
19		4295	2011-01-25 01:02:53	0	1	0	0	0
20		4296	2011-01-25 01:08:13	0	0	0	0	0
21		4297	2011-01-25 01:26:21	0	1	0	0	0
22		4298	2011-01-25 01:27:25	0	0	0	0	0
23		4299	2011-01-25 02:39:57	0	1	0	0	0
24		4300	2011-01-25 02:52:45	2	0	0	0	0
25		4301	2011-01-25 02:55:57	0	1	0	0	0
26		4302	2011-01-25 03:10:53	1	0	0	0	0

Fig. 12. Appliances' power states generated by RECAP-net.

table, shown in Figure 12, contains the times of occurrence of each footprint and will be used to name power footprints.

In order to depict the recognition process with an example, we focus in the following on the Jan 28, 2011, see Figure 13. We can see that the power measurement is composed of a baseline power, as well as a recurrent power block pattern, and power peaks.

Fig. 13. Power measurement within a family home over a period of one day.

Figure 14 illustrates the filtering done by RECAP-free. Periods with insignificant power activities have been cut off (in effect filtered out by RECAP-free). We remove those periods from Figure 14 to improve visualisation. As highlighted with various symbols, a number of similar power steps can be grouped together. Those similar power footprints are those discovered by RECAP-free and registered in the appliance tables, see Figure 11.

[TO DO: Naming of the 4 footprints]

Fig. 14. 1-day power measurement after suppression of out of hours power activities.

VI. CONCLUSIONS

ACKNOWLEDGMENT

This work is supported by Science Foundation Ireland under grant 07/CE/I1147 and through the SFI-funded National Access Programme (NAP 252).

REFERENCES

- [1] US Energy Information Administration, *Use of Energy in the United States Explained*, 2009
- [2] US Energy Information Administration, *Commercial buildings energy consumption survey*, 2003
- [3] US Department of Energy, *President Obama Announces \$3.4 Billion Investment to Spur Transition to Smart Energy Grid*, 2009
- [4] Enel Smart Metering System, http://www.enel.com/en-GB/innovation/project_technology/zero_emission_life/smart_networks/-smart_meters.aspx?it=0
- [5] PG&E SmartMeter Program Deployment, <http://www.pge.com/myhome/customerservice/meter/smartmeter/deployment/deployment.shtml>
- [6] Elias Leake Quinn, *Smart Metering and Privacy: Existing Law and Competing Policies—A Report for the Colorado Public Utilities Commission*, 2009
- [7] National Institute of Standards and Technology (NIST), *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, August 2010
- [8] K. E. Covinsky, R. M. Palmer, R. H. Fortinsky, S. R. Counsell, A. L. Stewart, D. Kresevic, C. J. Burant, C. S. Landefeld, *Loss of Independence in Activities of Daily Living in Older Adults Hospitalized with Medical Illnesses: Increased Vulnerability with Age*, Journal of the American Geriatrics Society, Vol.51, Nb.4, pg.451-458, 2003
- [9] A.G. Ruzzelli, G.M.P. O'Hare, A. Schoofs, C. Nicolas, *Real-Time Recognition and Profiling of Appliances through A Single Electricity Sensor*, In IEEE SECON'10, 2010
- [10] A. Schoofs, A. Guerrieri, D.T. Delaney, G.M.P. O'Hare, A.G. Ruzzelli, *Annot: Automated Electricity Data Annotation Using Wireless Sensor Networks*, In IEEE SECON'10, 2010
- [11] G.W. Hart, *Residential energy monitoring and computerized surveillance via utility power flows*, IEEE Technology and Society Magazine, 1989
- [12] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, *Private Memoirs of a Smart Meter*, In 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Buildings (BuildSys 2010), Zurich, Switzerland, November 2010
- [13] M. A. Lisovich, D. K. Mulligan, S. B. Wicker, *Inferring Personal Information from Demand-Response Systems*, In IEEE Security & Privacy, vol.8, no.1, pp.11-20, January-February 2010
- [14] G.W. Hart, *Non-intrusive Appliance Load Monitoring*, in IEEE, vol. 80, No 12, 1870-1891, 1992
- [15] Episenor ZEM-30 Electricity monitor, <http://www.episenor.com/products/wireless-nodes/zem-30/>