Smart grid в энергетике: исследование возможных сценариев нетехнологических потерь электроэнергии

А. А. Чухров[1,a], А. С. Минзов[2]

[1] Государственный университет «Дубна»,
Россия, 141982, г. Дубна, ул. Университетская, д. 19

[2] Национальный исследовательский университет «МЭИ»,
Россия, 111250, г. Москва, ул. Красноказарменная, д. 14

E-mail: [a] alexeych0@gmail.com

Одним из главных показателей эффективности электроэнергетического комплекса является поддержание потерь при передаче и потреблении электроэнергии на минимальном уровне. Основным видом таких потерь являются нетехнологические коммерческие потери, происходящие главным образом, от фактов хищений и безучетного потребления электроэнергии. Во многих странах кража электроэнергии ежегодно оценивается в миллиарды долларов. Несмотря на то, что современные приборы учета электроэнергии содержат более современную защиту от вскрытия и механического воздействия, по опыту внедрения в США и странах европейского союза, эти устройства не решают проблему хищений энергии. До сих пор не выработано общего стандарта безопасности передачи и обмена данными по каналам связи внутри сети.

Целью данного исследования является описание уязвимостей и возможных сценариев несанкционированного раскрытия и модификация информации об использовании электроэнергии в умных сетях, с учетом использования в них наиболее современных систем защиты. Рассмотренные в этом исследовании мошеннические схемы эксплуатируют актуальные уязвимости и в настоящее время активно используются злоумышленниками.

В исследовании показано, что эффективное решение проблемы хищений электроэнергии возможно достичь только совместно с использованием методов интеллектуального анализа данных. В настоящее время для борьбы с потерей доходов практически все крупные компании применяют традиционные методы: инвентаризацию, видеонаблюдение, контрольные замеры, инспекции, контролируемые поставки, сверку отчетности, выборку и анализ транзакций и пр. Но ограничиваться только такими методами невозможно, так как они не позволяют устранить все причины потерь доходов и имеют ряд ограничений. Во-первых, с их помощью обнаруживается уже состоявшийся факт потери доходов. Причем момент обнаружения потерь значительно отстает по времени от их возникновения. Во-вторых, применение этих методов требует серьезных затрат ресурсов компании (в первую очередь — трудовых). И, наконец, самые существенные ограничения — их выборочность и периодичность.

Ключевые слова: электроэнергетика, нетехнологические потери, информационная безопасность, экономическая безопасность, антифрод

1. Введение

За последние годы в отрасли электроэнергетики активными темпами происходила модернизация технического оборудования, замена устаревших индукционных счетчиков, на современные электронные приборы учета, позволяющие дистанционно передавать данные энергопотребления, следить за состоянием сети, качеством поставляемой энергии, а также решать множество других задач. В последующем, такие «умные счетчики» выросли в глобальную концепцию будущей электроэнергетики под названием «умная сеть». Концепция умной сети (Smart Grid, интеллектуальная сеть) представляет собой проект, распределительную сеть, которая сочетает комплексные инструменты контроля и мониторинга, информационные технологии и средства коммуникации, обеспечивающие значительно более высокую ее производительность и позволяющие генерирующим, сбытовым и коммунальным компаниям предоставлять населению энергию более высокого качества [Фардиев, Сафиуллин, 2010].

Не смотря на множество преимуществ, которые получают энергокомпании в результате стремительно растущего процесса внедрения умных сетей, до сих пор актуальной остается проблема хищений электроэнергии. Во многих странах кража электроэнергии ежегодно оценивается в миллиарды долларов [Caldeira, 2012]. Не смотря на то, что умные счетчики содержат более современную защиту от вскрытия и механического воздействия, по опыту внедрения в США и странах европейского союза, эти устройства не решают проблему хищений энергии. До сих пор не выработано общего стандарта безопасности передачи и обмена данными по каналам связи внутри сети. Усложнение умных счетчиков, при помощи добавления процессоров и защищённой памяти на практике не только повышает их стоимость, что делает их экономически неэффективными, но и создает новые угрозы информационной безопасности [Ghansah, 2012].

Целью данного исследования является предоставить описание актуальных уязвимостей и сценариев несанкционированного раскрытия и модификация информации об использовании электроэнергии в умных сетях, с учетом использования в них наиболее современных систем защиты.

2. Описание злоумышленника

Перед тем как описывать сценарии мошеннических действий, сначала необходимо классифицировать и дать характеристику лицам, заинтересованным в хищении электроэнергии.

Всех клиентов энергокомпании можно разделить на два класса:

1. Потребители бытового сектора. В большинстве своем потребители этого класса достаточно ограниченны в технических возможностях и ресурсах. Мотивация к хищениям электроэнергии носит индивидуальный характер. Однако, в некоторых случаях, клиенты бытового сектора проявляют значительные усилия в нахождении новых уязвимостей и разработке различных сценариев атак.

2. Юридические лица (бизнес, компании, производственный сектор, и пр.). Данный класс по-другому называют высоковольтные потребители. В связи с их объемами потребления, клиенты этого класса имеют прямую заинтересованность в занижении данных энергопотребления. Организовываясь в группы, имеют широкие технические возможности и ресурсы для искажения реальных значений потребления. Т.к. производству требуются крупные объемы электроэнергии, наносимый экономический ущерб, во много раз превосходит ущерб от хищений в частном секторе.

Таким образом, когда речь идет о хищении электроэнергии, под злоумышленником, главным образом следует понимать хорошо подготовленную группу лиц, способных своими действиями нанести крупный экономический ущерб энергокомпании.

3. Механическое воздействие на прибор учета

Не смотря на то, что умные счетчики изначально разрабатываются с учетом защиты от такого рода примитивных атак, этот сценарий занижения электроэнергии в некоторых случаях еще является рабочим, в зависимости от конкретной модели прибора и изобретательности мошенника. Внутри каждого умного счетчика есть датчики, осуществляющие процесс учета электроэнергии. Применив различного рода воздействия (например, магнитные, температурные, наклонив прибор и др.), возможно снизить точность регистрации датчиков.

4. Подключение скрытой проводки до прибора учета

Суть этого способа заключается в том, что часть потребляемой мощности подключается до прибора учета, в обход, и таким образом, потребленная электроэнергия остается неучтенной. Осуществляется с помощью скрытой проводки от основной электросети, с целью спрятать факт хищений и снизить вероятность обнаружения в случае инспекций энергокомпании.

Подключение скрытой проводки до прибора учета до сих пор является самым распространенным сценарием занижения реального расхода электроэнергии, т.к. является наиболее простым, не требует специальных навыков (информация наглядно предоставлена в интернете и других источниках открытого доступа) и в большинстве случаев физического воздействия на прибор учета. Однако, эта ситуация постепенно меняется с внедрением более современных приборов учета осуществляющих мониторинг, способных регистрировать несанкционированное подключение к сети и оповещать оператора [Rylatt, 2015]. Таким образом, это осложняет задачу, т.к. необходимо произвести дополнительные физические воздействия на прибор, или другие махинации с целью эмулирования работы счетчика в сети, используя уязвимости информационной безопасности. Об этом и пойдет речь далее, и как будет показано, это не предоставляет особого труда для человека со средними навыками владения компьютером, не говоря уже о профессиональных хакерах.

5. Обновление прошивки счетчика и изменение параметров процесса учета

По данным отчета ФБР [McLaughlin, et. al, 2010], в интернете широко распространены различного рода прошивки, позволяющие перепрограммировать процесс учета. Для того чтобы произвести действия по обновлению и изменению программного обеспечения счетчика и не быть обнаруженным, злоумышленнику необходимо выполнить следующие действия:

1. Подключится к устройству, используя интерфейс RS-485 или оптический порт. Обычно энергокомпании защищают этот порт пломбой.
2. Непосредственно при обновлении ПО счетчика требуется ввести мастер-пароль.
3. После обновления прошивки очистить журнал события счетчика, который регистрирует факты изменения программного обеспечения прибора, а также внешние воздействия (открытие крышки счетчика, подключения или отключения в сети).

Обход опломбирования зависит от вида используемой пломбы, они бывают: обычная свинцовая с печатью, пломба-наклейка, электронная пломба. В первых двух случаях, достаточно искусственно фальсифицировать пломбу. Принцип действия электронной пломбы заключается в том, что при открытии или подключении к счетчику соответствующая информация записывается в журнал событий прибора.

Мастер-пароли для обновления ПО являются стандартными и одинаковы в рамках модели счетчика [McLaughlin, et. al, 2010]. Для наиболее популярных моделей, пароли можно найти в

открытом доступе. Однако, энергокомпания может изменить пароль, в этом случае требуется использование специализированных инструментов подбора пароля, либо можно извлечь пароли напрямую из железа прибора (об этом речь пойдет в следующей главе).

Журнал событий, представляет собой логирование действий, список время-действие. Т.к. весь смысл перепрошивки счетчика заключается в получении полного контроля над его настройками, то после успешного обновления прошивки, очищение журнала событий является простой процедурой.

При получении контроля над счетчиком снижение реального энергопотребления возможно по следующим сценариям:

1. Возможность вручную изменять или удалять данные энергопотебления и профили нагрузки, в случае если данные отправляются с низкой частотой, например, раз в день, неделю, месяц.
2. Модификация коэффициента погрешности счетчика.
3. Модификация коэффициента трансформации. В случае высоковольтных потребителей, чтобы прибор не сгорел, он подключается через трансформатор, который понижает силу тока в несколько раз. Соответствующий коэффициент присутствует в настройках счетчика

До сих пор речь шла об атаках направленных, на модификацию данных до того как они были отправлены в центр обработки данных (фальсификация измерений перед записью в память прибора, либо изменение записанных данных). Однако наиболее серьезную опасность представляет тип атак, описанный в следующей главе, направленный на перехват передаваемого трафика сети, возможность его полной заглушки, модификации и инъекции собственных произвольный значений.

6. Перехват и модификация трафика

Само название «умный счетчик» главным образом обязано его возможности беспроводной передачи данных. Данные в центр обработки передаются с помощью беспроводного радиоинтерфейса, который использует в работе высокие частоты, близкие к 2.4 ГГц (именно на этих частотах работают практически все «умные» электроприборы). Также, сам счетчик может принимать набор команд из центра управления, на повторную передачу данных, передачу журнала событий, на отключение подсети и др.

Организация канала связи осуществляется с помощью PLC-модема, встроенного в каждый счетчик. За шифрование данных отвечает либо сам модем, либо отдельный микроконтроллер, в обоих случаях, важным фактом является то, что к модели счетчика привязан конкретный алгоритм шифрования, который распространяется на всю умную сеть, это является серьезной уязвимостью информационной безопасности. Единожды получив ключи дешифровки, хакер получает контроль над потоками данных всей сети.

Так, во время конференции Black Hat Europe, которая проходила в Амстердаме в 2014 году [Illera, 2014], испанские специалисты с информационной безопасности показали, как можно отключать электричество в целых районах, или даже по всему городу, используя сеть умных счетчиков и недостатки в шифровании передаваемых ими данных. Эти специалисты, Хавьер Видал и Альберто Иллера, изучили электросчетчики одной испанской компании, разобрав алгоритмы их работы. Как выяснилось, разработчики использовали не самый безопасный алгоритм шифрования AES-128, а ключи к дешифровке хранились в самой микропрограмме счетчика. Таким образом, получилось взломать систему передачи информации, а значит, появилась возможность в передаче ложных данных. То есть, хорошие хакеры смогут без проблем взламывать сети умных электросчетчиков для изменения их показаний или даже для отключения отдельных квартир, целых домов или районов от сети энергоснабжения.

Таким образом, заполучив неким образом один измерительный прибор, злоумышленник может полностью разобрать его, запустить на нем всевозможные встроенные программы отладки и извлечь необходимые данные (мастер-пароли, ключи дешифровки, наборы команд),

являющиеся актуальными для всех подобных приборов сети. А зная точную частоту радиосвязи, не составляет труда заглушить прием и передачу сигнала любого действующего прибора.

Хищение электроэнергии возможно по следующим сценариям мошеннических действий:

1. Модификация непосредственно данных энергопотребления
2. Замена идентификатора прибора, таким образом, счет за электроэнергию будет оплачивать другой абонент.

7. Заключение

В результате, можно сделать вывод, что в настоящее время умные приборы учета электроэнергии не являются хорошо проработанными в плане информационной безопасности. Поскольку такие приборы объединены в сеть, то они являются даже более опасными, чем устаревшие аналоговые счетчики. Данный фактор только способствует хищениям электроэнергии, к старым, уже хорошо известным сценариям хищений добавились новые.

Дальнейшее усложнение счетчиков электроэнергии, за счет внедрения различных систем защиты, в настоящее время не дает эффективных результатов, и кроме того делает их слишком дорогими и экономически неэффективными для энергокомпаний. Таким образом, проблема хищений электроэнергии должна решаться в комплексе с инструментами интеллектуальной фильтрации данных.

Список литературы

Фардиев И.Ш., Сафиуллин Д.Х. Об инновационном проекте «Умная сеть» // Энергетика Татарстана. – 2010. – №3. С. 5-12.
Fardiev I.S., Safiulin D.H. Ob innovatsionnom proekte «Umnaya set'» // Energetika Tatarstana. – 2010. – No. 3. – P. 5-12 (in Russian).

Caldeira E., Brandão G.,Campos H. Characterizing and evaluating fraud in electronic transactions // Proceedings of the 2012 Eighth Latin American Web Congress. – 2012. – P. 115-122.

Ghansah I. Smart grid cyber security potential threats, vulnerabilities and risks // Public Interest Energy Research, Prepared for: California Energy Commission. – 2012. – P. 8.

Rylatt R.M. Exploring Smart Grid Possibilities: A Complex Systems Modelling Approach // Smart Grid. – 2015. – Vol. 1, No. 1. – P. 1-15.

McLaughlin S., Podkuiko D., Delozier A., Miadzvezhanka S., McDaniel P. Embedded Firmware Diversity for Smart Electric Meters // Proceedings of the 5th Workshop on Hot Topics in Security. – 2010. – P. 1-10.

Illera A.G., Vida J.V. Lights Off! The Darkness of the Smart Meters // Black Hat Europe, URL: https://www.blackhat.com/eu-14 (12.09.2016). – 2014.

Smart grid in the energetics: survey of possible non-technical losses

A. A. Chuhrov[1,a], A. A. Minzov[2]

[1] Dubna International University, 19 Universitetskaya st., Dubna, 141982, Russia

[2] National Research University «MEI», 14 Krasnokazarmennaya st., Moscow, 111250, Russia

E-mail: [a] alexeych0@gmail.com

One of the main indicators of efficiency of electric power complex is maintenance of non-technical losses to a minimum. Non-technical losses are type of commercial losses which occurs mainly on facts of electricity thefts and unmetered electricity consumption. In many countries, theft of electricity annually is estimated at billions of dollars. Despite the fact that today's electricity metering devices contain a more advanced protection against opening and mechanical action on the implementation experience of the US and European Union countries, these devices do not solve the problem of power theft. So far there is no developed a common standard security transfer and exchange data through communication channels within the network.

The aim of this study is to describe vulnerabilities and possible scenarios of unauthorized disclosure and modification of information on the use of electricity in smart networks, taking into account their use in the most advanced security systems. The considered vulnerabilities are actively used by hackers.

Currently, to combat the loss of revenue almost all large companies are using traditional methods: inventory, control measurements, inspections, verifications of reporting, sampling and analysis of the transactions and other. But it is impossible to use only such methods because they do not allow eliminating all causes of loss of revenue and also they are having a number of limitations. First of all, with their help, the found fact of losses is already occurred. Moreover, the time of detection of losses is far behind in time than they are actually occurred. Secondly, the application of these methods requires significant expenditure of company resources. And finally, the most significant limitations are selectivity and periodicity.

Keywords: Energetics, non-technical losses, information security, economic security, antifraud