ERNW
providing security.

black hat USA 2014

When the Lights go out

Hacking Cisco EnergyWise

Version:	1.0
Date:	7/1/14
Classification:	Public
Author(s):	Ayhan Koca, Matthias Luft

Table of Content

List of Figures

List of Tables

1 Handling

The present document is classified as PUBLIC. Any distribution or disclosure of this document REQUIRES the permission of the document owner as referred in section "Document Status and Owner".

1.1 Document Status and Owner

As the owner of this report, the document owner has exclusive authority to decide on the dissemination of this document and responsibility for the distribution of the applicable version in each case to the places defined in the respective section.

The possible entries for the status of the document are "Initial Draft", "Draft", "Effective" (currently applicable) and "Obsolete".

Title:	When the Lights go out – Hacking Cisco EnergyWise
Document Owner:	ERNW GmbH
Version:	1.0
Status:	Effective
Classification:	Public
Author(s):	Ayhan Koca, Matthias Luft

1.2 Possible Classifications:

Public:	Everyone
Internal:	All employees and customers
Confidential:	Only employees
Secret:	Only selected employees

Abstract

Energy Management Protocols (herein short: EMPs) are used in a variety of devices and environments. Their purpose is always the same: Controlling and measuring the energy consumption of connected devices. However, most EMPs are designed and implemented for embedded, non-IP environments, such as HDMI or home automation networks.

Cisco EnergyWise is a proprietary, closed-source protocol that brings EMPs to the main stream IP networks (e.g. by including EnergyWise clients in widely used notebooks and phones). The resulting broad deployment in a high number of environments, such as office networks (for example, ThinkPad notebooks include an EnergyWise Client in the default configuration) or even data centers (as power consumption is always a huge issue), leads to the potential to cause huge blackouts if EnergyWise is misconfigured or contains vulnerabilities which can be abused...

This paper describes our research results on the EnergyWise architecture and protocol specification, the reverse-engineered proprietary protocol, and vulnerabilities for hijacking EnergyWise domains in order to perform DoS attacks.

2 Introduction

Data Center facilities are the heart of any corporate IT environment. Network threats like DDoS attacks or compromises of servers or clients get most of the attention [Ans13], but in the trending Internet-of-Things and connected buildings, infrastructure protocols can also put data centers and IT environments in general at significant risk. Cisco EnergyWise is an infrastructure protocol that can be used to power on and off the complete IT environment, which qualifies it as a critical infrastructure for most IT operations.

The aim of this paper is to analyze Cisco EnergyWise from a security perspective in order to determine whether it can be used for such critical tasks. We will provide detailed insight into the structure and internals of the protocol, describe our analysis process, and present vulnerabilities that we discovered in the protocol and implementation.

3 Cisco EnergyWise

Cisco EnergyWise is an IP-based energy management protocol (herein short: EMPs). EMPs are used in a variety of environments and always serve similar purposes: Gathering information about the energy consumption of devices and retrieving/changing their energy consumption levels.

This section will describe Cisco EnergyWise in detail and provide all relevant details about the technical implementation, which must be considered while performing a security assessment.

There are three important entities in an EnergyWise environment:

- Management Applications
- Domain Members
- Endpoints

Management applications are the applications and devices that use the EnergyWise protocol to monitor and manage the power consumption of domain members and endpoints. There are two kinds of applications: First-Party applications developed and distributed by Cisco (e.g. the Cisco Prime LAN Management Solution) and Third-Party applications developed by partners (e.g. the JouleX Energy Manager). The applications can either use SNMP (with a reduced feature set) or the Cisco Management Application Programming Interface (MAPI) to communicate with domain members.

Domain members are switches, routers, and other network controllers that forward messages from the management applications across the domain.

Endpoints are any devices that are managed using the EnergyWise architecture. An EnergyWise endpoint can be PoE or non-PoE, IP or non-IP. PoE endpoints do not support the full EnergyWise feature set such as supporting different levels of power consumption. Endpoints do not perform any other EnergyWise tasks than responding to queries.

All of those entities together can form a so-called EnergyWise *domain*. A domain is a logical group of EnergyWise entities that share the same *domain secret* and are addressed by the same domain name. Systems can only be part of one domain at a time.

This architecture is illustrated in the following figure:

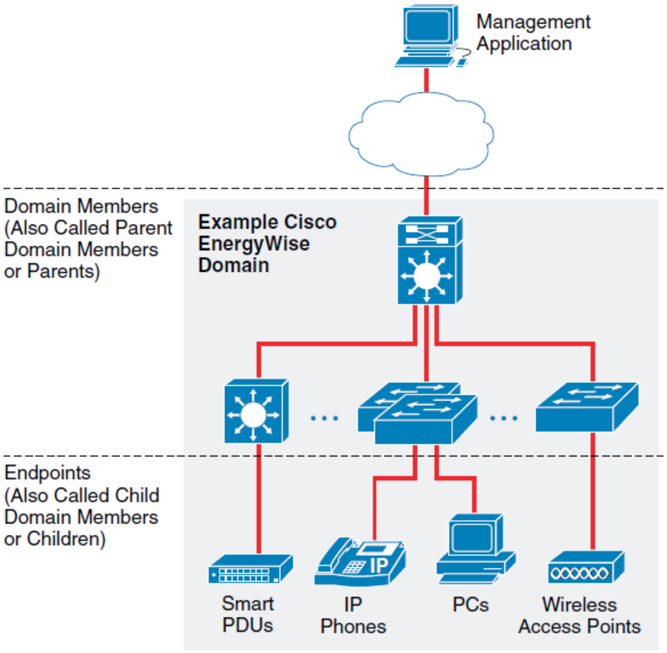

Management Application
Domain Members (Also Called Parent Domain Members or Parents)
Example Cisco EnergyWise Domain
Endpoints (Also Called Child Domain Members or Children)
Smart PDUs
IP Phones
PCs
Wireless Access Points

Figure 1: Sample EnergyWise Domain from [EWDesignGuide]

Three main activities are performed in an EnergyWise domain:

- Neighbor discovery
- Gathering of power consumption
- Setting EnergyWise levels

Neighbor discovery is carried out either using CDP or an EnergyWise flooding mechanism over UDP broadcast. The gathering of power consumption and the setting of EnergyWise levels are both performed using EnergyWise queries.

All actions are authenticated using a PSK which must be known to all domain members.

The attributes managed by EnergyWise are importance, keywords, role, levels, and name. The importance rates the business relevance of a device and can range from 0 (least important) to 100 (most important). This allows the mass-shutdown of less business critical devices. Keywords are string values that are used as tags assigned to endpoints to logically group them (e.g. by location ["lobby"] or type ["phones"]). The EnergyWise role describes the role within the EnergyWise domain and has certain default values described in [EWDesignGuide]. The name is also a string value and is used to identify a device within an EnergyWise domain. EnergyWise levels describe the level of power consumption and are defined in the following table:

Category	Level	Description
Operational	10	Full
	9	High
	8	Reduced
Standby	7	Medium
	6	Frugal

	5	Ready
	4	Low
	3	Standby
Non-operational	2	Sleep
	1	Hibernate
	0	Shut Off

Table 1: EnergyWise Levels

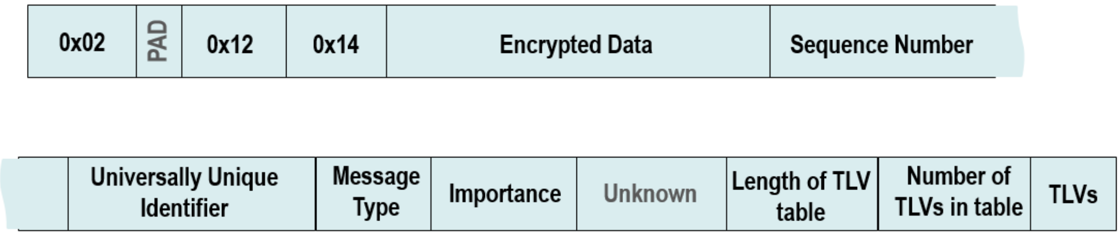
3.1 Reverse Engineering the Protocol

EnergyWise is a proprietary closed-source protocol without detailed documentation about the protocol itself. In order to perform a proper security analysis, the first step must thus be the analysis and reverse engineering of the protocol. An important piece of information from the documentation states that EnergyWise is a TLV protocol.

The following approach was used to identify all different TLV fields:

1. Identify text strings: Several strings, such as device types or domain names, are known and can easily be spotted in the protocol.
2. Identify environmental dependencies: The protocol contains time stamps, IP addresses, and MAC addresses, which can be derived from the test environment.
3. Identify Cisco EnergyWise parameters: The actual EnergyWise parameters such as importance or level where identified by repeatedly changing the values in the queries and comparing captured packets.
4. Identify lengths fields and the header: Once most of the content was identified, byte patterns in front of text strings could be compared and length information calculated and extracted.

This process resulted in the identification of the following headers, depending on whether EnergyWise is spoken via UDP or TCP:



0x02	PAD	0x12	0x14	Encrypted Data	Sequence Number

Universally Unique Identifier	Message Type	Importance	Unknown	Length of TLV table	Number of TLVs in table	TLVs

Figure 2: EnergyWise UDP Header

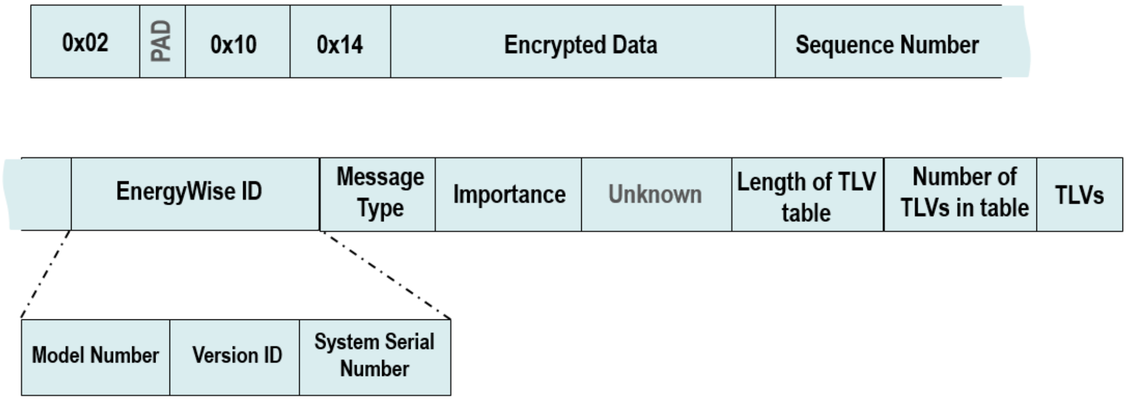
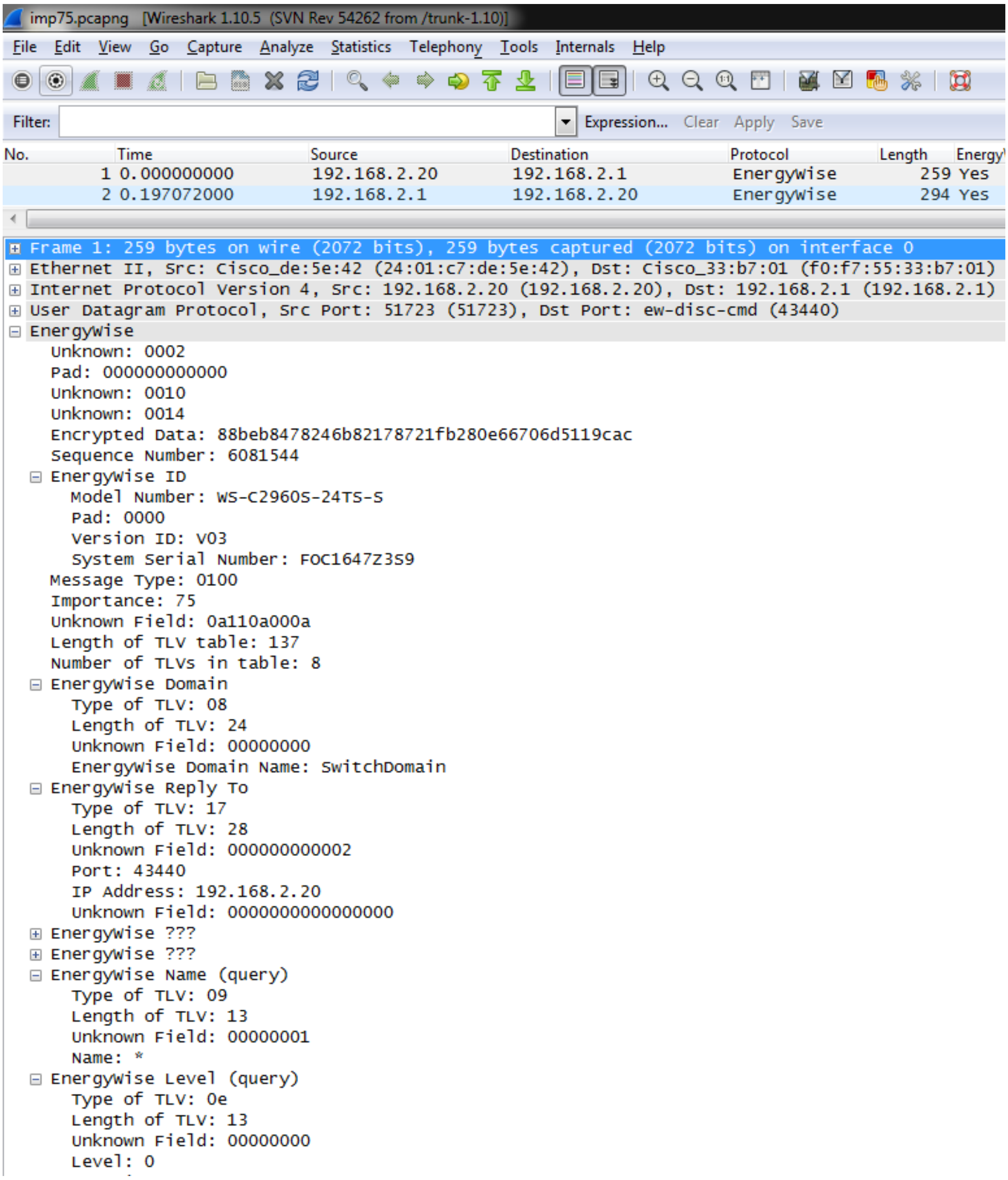


Figure 3: EnergyWise TCP Header

The complete packet definition has been documented by means of a Wireshark dissector:


imp75.pcapng [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.     Time            Source          Destination     Protocol        Length  Energy
      1 0.000000000     192.168.2.20    192.168.2.1     EnergyWise         259 Yes
      2 0.197072000     192.168.2.1     192.168.2.20    EnergyWise         294 Yes
```

```
⊞ Frame 1: 259 bytes on wire (2072 bits), 259 bytes captured (2072 bits) on interface 0
⊞ Ethernet II, Src: Cisco_de:5e:42 (24:01:c7:de:5e:42), Dst: Cisco_33:b7:01 (f0:f7:55:33:b7:01)
⊞ Internet Protocol Version 4, Src: 192.168.2.20 (192.168.2.20), Dst: 192.168.2.1 (192.168.2.1)
⊞ User Datagram Protocol, Src Port: 51723 (51723), Dst Port: ew-disc-cmd (43440)
⊟ EnergyWise
    Unknown: 0002
    Pad: 000000000000
    Unknown: 0010
    Unknown: 0014
    Encrypted Data: 88beb8478246b82178721fb280e66706d5119cac
    Sequence Number: 6081544
  ⊟ EnergyWise ID
      Model Number: WS-C2960S-24TS-S
      Pad: 0000
      Version ID: V03
      System Serial Number: FOC1647Z3S9
    Message Type: 0100
    Importance: 75
    Unknown Field: 0a110a000a
    Length of TLV table: 137
    Number of TLVs in table: 8
  ⊟ EnergyWise Domain
      Type of TLV: 08
      Length of TLV: 24
      Unknown Field: 00000000
      EnergyWise Domain Name: SwitchDomain
  ⊟ EnergyWise Reply To
      Type of TLV: 17
      Length of TLV: 28
      Unknown Field: 000000000002
      Port: 43440
      IP Address: 192.168.2.20
      Unknown Field: 0000000000000000
  ⊞ EnergyWise ???
  ⊞ EnergyWise ???
  ⊟ EnergyWise Name (query)
      Type of TLV: 09
      Length of TLV: 13
      Unknown Field: 00000001
      Name: *
  ⊟ EnergyWise Level (query)
      Type of TLV: 0e
      Length of TLV: 13
      Unknown Field: 00000000
      Level: 0
```

Figure 4: EnergyWise Protocol Definition in Wireshark

4 Security Analysis & Attacks

This section describes the approach to and results of the security analysis of the protocol that we performed. After reverse engineering the protocol definition (as described in the section above) and getting familiar with the internals of the protocol, defining attack vectors and tampering with packets revealed several vulnerabilities which are described in the next subsections.

4.1 Security Objectives and Attack Vectors

EnergyWise is used to retrieve and set the power consumption of all kinds of networked devices. Thinking of the classic security objectives confidentiality, integrity and availability, the following violations regarding the EnergyWise network traffic of those are relevant:

- Confidentiality: EnergyWise is not used to transfer highly sensitive data. The most interesting information is the power consumption queried from the devices, which is, according to the EnergyWise design, not considered to be confidential information. Hence EnergyWise is a plain text protocol without any encryption functionality, which makes attacks on the confidentiality trivial and, as no confidential data is transferred, rather uninteresting.
- Integrity: The setting of energy levels is an operation that can result in the unintended shutdown of a device if an attacker would be able to tamper with the content of the packet (e.g. modifying the desired target energy level from 8 to 0.
- Availability: Dropping packets can result in unintended behavior such as relevant devices not being powered up when they are supposed/needed to be. This can actually result in operational impact when thinking of devices such as AC, lights, phones, or access control systems.

In addition to the analysis of the network traffic, the compromise of EnergyWise components (management applications, domain members, or endpoints) must be considered as well. Even though EnergyWise is a comparatively simple protocol, the EnergyWise parsers on the devices can still contain flaws resulting in either device compromise or Denial-of-Service.

Taking those considerations into account, the following attack vectors that needed to be analyzed have been developed:

- Eavesdropping
- Interception, injection & tampering
- Replay
- Device compromise or Denial-of-Service via malformed packet
- Dropping packets & analysis of "fail-open/closed" mechanisms.

4.2 Lab Environment

For the analysis of the EnergyWise protocol, we used the lab environment visualized in the following figure:

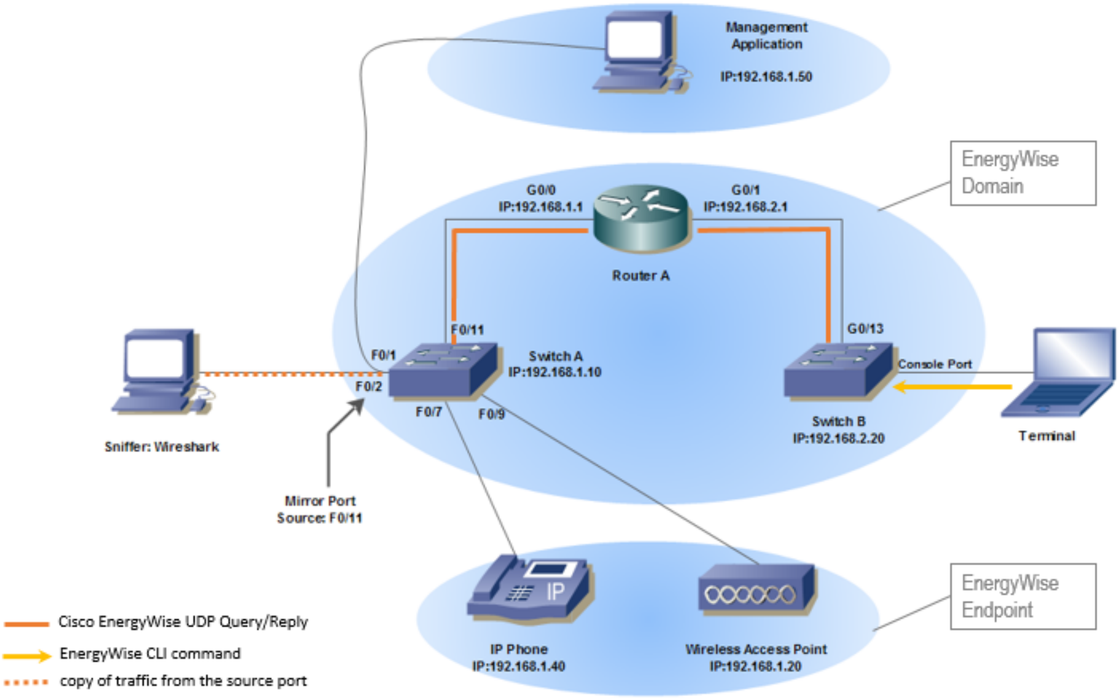


Figure 5: EnergyWise Lab Environment

This lab environment supported the evaluation of all attack vectors described above, the analysis of EnergyWise queries in a segmented network, and the testing of PoE- and Non-PoE-endpoints.

4.3 Vulnerabilities

Evaluating the attack vectors described in the previous section, we discovered several vulnerabilities by manually analyzing the protocol, reverse engineering management applications, and fuzzing all components that process EnergyWise network packets.

4.3.1 Clear Text Transport

As described above, EnergyWise traffic is unencrypted by design. While the transferred information is not confidential and it is more of a design detail than an actual vulnerability, it must still be documented that any attacker that can sniff network traffic can also read the EnergyWise content.

4.3.2 Replay

Referring to Section 3.1, EnergyWise over UDP or TCP show some differences in the header structure of the packets. As UDP-based EnergyWise does not comprise a UUID in the header, replay attacks can be possible. It also depends on a configuration option called *domain security mode*, which can either be `shared-secret` or `ntp-shared-secret`. In the case of `shared-secret`, only the PSK is used to authenticate packets, while `ntp-shared-secret` includes a timestamp into the calculation of the HMAC. If shared-secret is used, replay attacks for EnergyWise over UDP are possible and enabling an attacker that sniffed a legitimate EnergyWise packet to use the contained EnergyWise command at arbitrary times.

4.3.3 Brute-Force

The integrity and authenticity mechanisms of EnergyWise completely depend on the PSK which must be known to all members of the EnergyWise domain. This PSK is the shared secret for a custom HMAC mechanism that is not publicly documented. By analyzing `EnergyWiseTestApp.exe`, which is part of the management application, the HMAC algorithm could be determined:

```
$KEY = HMAC_SHA1(UUID, secret)
$HMAC = HMAC_SHA1(KEY, data)
```

$HMAC is the final HMAC value that is part of each EnergyWise packet. It is calculated based on a SHA1-based HMAC function that takes a key and all packet data besides the HMAC as an input (`data` in the pseudo code above). The key is calculated using the same HMAC function using a UUID, which is generated for every packet, and the PSK.

Knowing this algorithm, it is possible to implement a brute forcing tool that can be used to exploit weak PSKs.

4.3.4 Denial-of-Service

While fuzzing the different EnergyWise components, one of the switches crashed and did not forward traffic anymore. It was possible to identify one particular EnergyWise packet that can be used to crash the particular switch at any time. As we are still in the disclosure process with Cisco, we cannot release details about this vulnerability yet.

4.3.5 Malicious Insider/System Compromise/Key Leakage

Due to the nature of PSK-based authentication, every member of the EnergyWise domain knows the one secret that is used to manage the complete domain. In case this secret leaks or is abused (e.g. by compromising a client or by a malicious insider), an attacker can use it to take control of the whole EnergyWise domain.

4.4 Summary

The EnergyWise protocol contains security mechanisms that can protect the environment against the attack vectors discussed in this section, given that a strong PSK is used and the correct domain security model is configured. However, operational practice shows that infrastructure protocols are often operated with weak passwords and without additional hardening considerations. In such an environment, this analysis describes attacks that can be used to cause major outages due to the potential highjacking of the complete EnergyWise domain.

5 Conclusions & Security Considerations

This document describes potential attacks against EnergyWise domains that are not operated with security in mind. While the protocol provides basic mechanisms to protect against unauthorized EnergyWise queries, the following measures are crucial to protect the domain:

- Use ntp-shared-secret to protect against replay attacks
- Use a strong PSK (random, 20+ characters)
- Segmentation: If possible, configure different EnergyWise domains for different devices. This reduces the impact of a compromised PSK
- Filtering: The EnergyWise ports must only be accessible from within a network segment to reduce the impact of a compromised PSK and contain compromise to the local subnet.

The general design weakness of the protocol is the use of a PSK, as it can easily lead to the compromise of the whole domain. This mechanism is not appropriate anymore to protect an infrastructure protocol that can lead to the shutdown of a high number of devices (incl. relevant infrastructure such as access control systems or servers).

6 Referenced Documents

Reference	Description
[EWDesignGuide]	http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Energy_Management/energywisedg.pdf