# gSOAP Security Flaws: IoT Network Segmentation

Farhad Ahmed, Defne Gunes Aydin, Fan Bu, Danny Lin, Navneet Singh

## Abstract

To combat the gSOAP (Simple Object Access Protocol) security camera exploit, we will look at a solution that properly segments the IoT networks using tightly controlled ACLs. The implementation of this solution will allow us to reduce any losses to a minimum and help to deal with future attacks as well.

## Introduction

Security cameras are used widely for the protection of goods and resources. Internet-connected security cameras, like most IoT devices, can be exploited to cause harm instead of protection. The critical exploit (Devil's Ivy) for these security cameras is found in the software development toolkit gSOAP. gSOAP, which stands for Simple Object Access Protocol, is used by a large number of technology companies. The exploit allows attackers to take over security cameras and deny service to the administrator. Flaws can arise in the supply chain of this third party software or it can be spread from a single device. The Devil's Ivy security flaw is a buffer overflow vulnerability. The security flaw enables an attacker to take control of the device and remotely execute code.

## Background

The simple solution for solving the issue of security flaws revolving gSOAP is to have send out a patch to all users to account for the bug. Updating the code behind gSOAP to fix the stack buffer overflow would solve the security issues entirely. But when it comes to practice, this solution would not seem very reasonable because of the amount of impact that this bug brings. If users do not update their systems with the newest patch timely, the longer the hackers have to perform malicious acts on the user. The main security principle that is violated by the gSOAP software is the principle of confidentiality. Confidential information (private camera footage) is being disclosed to individuals (hackers) without authorization. Another principle that is violated here is availability (withholding of information/resources) since the Devil's Ivy vulnerability can not only allow attackers to deny service to the owner, but also allow them to build large botnet to launch distributed-denial-of-service (DDoS) cyberattacks against multiple targets.

Some potential solutions for this problem include patching the system to the latest version released. This approach falls short as IoT devices generally aren't automatically updated or closely maintained. Also, this approach would not offer protection against future attacks as releasing an update after an exploit has already been discovered is a reactionary approach. Instead, proper segmentation of IoT networks using tightly controlled ACL's should be applied. This approach will help mitigate damages and loss in case of an attack and is a step in securing the system against future attacks. Implementing VLAN is one proposed solution to help

segment the IoT network. Although using VLAN is good, poor configuration will also expose the network to be exposed to attacks [3].

# Threat Model

## The threat/impact

A attacker can send a crafted SOAP message to force the gSOAP system execute arbitrary code. Such attacks are possible because a stack-based buffer overflow exists in gSOAP library.

## The risk

After getting control of gSOAP system, the attacker can remotely hack into its live video feed or lock out administrator access, and even turn the system to be part of the attacker's botnet.

## Solution

**Properly segment the IoT networks using tightly controlled ACLs.**

Pros:

1. Can reduce the loss to a minimum stage.
2. Helps survive from future unknown attack.

Cons:

1. Cannot get rid of the attack.
2. Requires sophisticated management.

# Design

One proper way to divide the IoT network is to use VLAN.

## What is VLAN?

Virtual Local Area Network (VLAN) is a set of logical devices and users. These devices and users are not restricted by physical location. They can be organized according to factors such as functions, departments, and applications. The communication is as if they are in the same network segment, hence it's named as virtual LAN. The VLAN works in Layer 2 and Layer 3 of the OSI Reference Model, hence it has good security.

## Why use VLAN?

Without VLAN, the devices connected to the same switch will be in the same LAN. This means ARP man-in-the-middle attack or other attacks are so easy to initialize. With VLAN, ARP attack

or other attacks can be narrowed down to a specific VLAN because ARP packet cannot be transmitted between different VLANs.

### How to use VLAN?

There are 2 typical ways to use VLAN: Static VLAN and Dynamic VLAN.Static VLAN is also called as Port based VLAN.  And in Dynamic VLAN, there are 3 different subtypes: MAC Based VLAN, Subnet Based VLAN, and User Based VLAN. The difference among the 3 subtypes depends on which layer of the OSI reference model determines the VLAN that the port belongs to.

- The MAC based VLAN determines which VLAN the port belongs to by querying and recording the MAC address of the computer's network card. Since the VLAN is determined by MAC address, if the computer exchanges the network card, the setting has to be changed.
- Subnet based VLAN determines which VLAN the port belongs to by checking the IP address. Unlike a MAC based VLAN, even if the computer changes its MAC address because of a network card exchange or other reason, the VLAN can still be kept.
- The User based VLAN is based on the user who is currently logged in on the computer connected to the port. The user identification typically is the username. These user information belong to the OSI layer 4 or above.

## Implementation

Implementation of VLAN on Ubuntu.

1. Install VLAN package.

   $ sudo apt-get install vlan

2. Load 8021q module.

   $ sudo modprobe 8021q

3. Add VLAN.

   $ vconfig add eth0 5

   ```
   user@cs3224:~/Desktop$ sudo vconfig add eth0 5
   Added VLAN with VID == 5 to IF -:eth0:-
   ```

4. Assign IP to the VLAN.

   $ ifconfig eth0.5 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255 up

Now we can use ifconfig to check the current status.

```
user@cs3224:~/Desktop$ ifconfig etho0.5;
etho0.5: error fetching interface information: Device not found
user@cs3224:~/Desktop$ ifconfig eth0.5;
eth0.5    Link encap:Ethernet  HWaddr 08:00:27:e8:f5:78
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee8:f578/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:7482 (7.4 KB)
```

Or we can check current VLAN's detailed information.

```
user@cs3224:~/Desktop$ sudo cat /proc/net/vlan/eth0.5
eth0.5  VID: 5   REORDER_HDR: 1  dev->priv_flags: 1001
         total frames received            0
          total bytes received            0
      Broadcast/Multicast Rcvd            0

      total frames transmitted           45
       total bytes transmitted         7656
Device: eth0
INGRESS priority mappings: 0:0  1:0  2:0  3:0  4:0  5:0  6:0 7:0
 EGRESS priority mappings:
```

## Evaluation

VLANs enhance the security of the LAN, and groups of users and devices with sensitive data can be isolated from the rest of the network, reducing the possibility of revealing confidential information. Packets in different VLANs are isolated from each other. That is, users in one VLAN cannot communicate directly with users in other VLANs. If different VLANs need to communicate, you need to pass Layer 3 devices such as routers or Layer 3 switches. Then even though some part of the network is hacked and compromised, the rest part of network can remain safe.

## Related Solutions

### Monitoring IoT Devices

As far as other relevant solutions, there exists in the market several software programs designed to monitor multiple Internet of Things (IoT) devices. One of these softwares is provided by a third-party cyber security firm named Tenable. Tenable claims to offer a "modern, cloud-based vulnerability management platform that enables you to see and track all of your

assets with unmatched accuracy”. Perhaps the most useful of their services, Tenable offers an IoT Device Summary Dashboard that leverages data from their own sensors to offer insight into all activity related to IoT devices within a network. Upon adding a subnet, IP address, or asset filter to the dashboard, the results can be specially tailored to focus on the IoT devices within the network. Ultimately, this allows for tracking network connections being made to and from IoT devices.

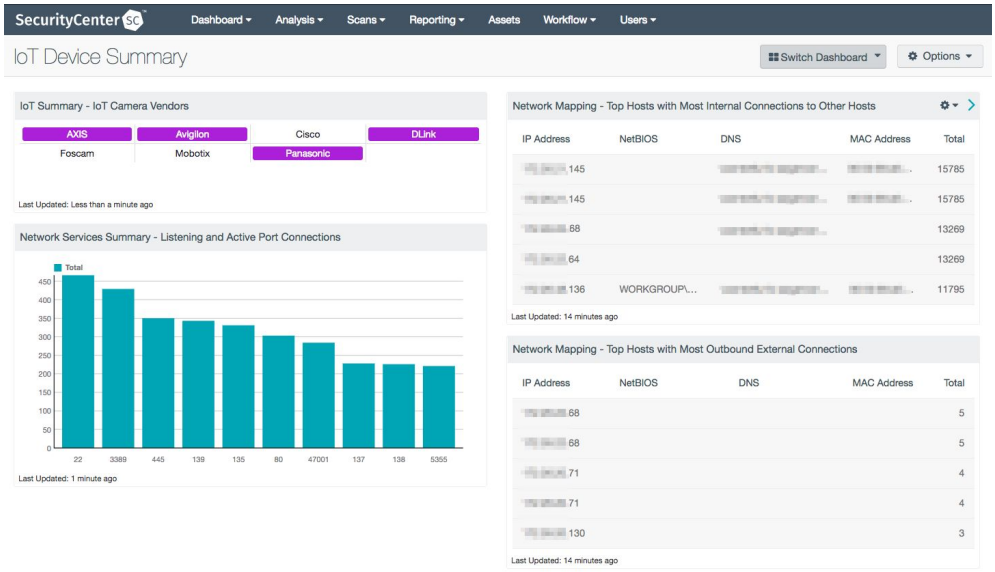


**Figure 1. Screenshot of IoT Device Summary Dashboard offered by Tenable**

## General IoT Precautions

Given that these types of devices and their functionalities will always require some level of network connectivity, it might be hard to avoid being a target for hackers with malicious intent. However, there are, as always, several general precautions that can be taken to minimize the risk and magnitude of a vulnerability.

The first and what would seem most obvious precaution is to set a strong password on the device. Many often forget to set passwords and the devices are left to be secured by default passwords or even no password protection at all.

Another precaution would be to disable Universal Plug and Play (UPnP). Universal Plug and Play is meant to help IoT devices discover other network devices easily. However, this leaves the devices susceptible for hackers to discover and so disabling this feature will prevent them from gaining access to your network.

Finally, a good solution, that might not be available right away, is the patch the software by updating to the latest firmware. The manufacturer usually does learn about vulnerabilities being

exploited by hackers at some point and releases a patch for the device software in order to mend the damage. This will cover the vulnerability and ensure that the device is at least safe from that exploit.

## Conclusion

This paper discusses using proper segmentation techniques to divide the IoT network. The ideal way to perform this segmentation is to use VLAN. Virtual Local Area Network achieves good security through the use of a set of devices and users that aren't restricted to a physical location. Virtualizing the Local Area Network allows different packets to have isolation. In addition to using general security precautions, setting up VLAN will provide the optimal solution to vulnerabilities in the software such as the Devil's Ivy vulnerability.

## References

[1] https://www.cs.fsu.edu/~engelen/soap.html

[2] https://blog.senr.io/devilsivy.html

[3] https://link.springer.com/content/pdf/10.1007%2Fs10766-018-0580-z.pdf