Texas A&M University at Qatar

ECEN 403 - Electrical Design Lab 1

Semester: Fall 2019

Customer Needs Survey Report

Anomaly detection in BACnet protocol systems

Team Members: Sofian Ghazali

Muhammed Zahid Kamil

Rahul Balamurugan

Project Mentors: Dr. Hussein Alnuweiri

Mr. Salah Hessien

Submission Date: 17/10/2019

"An Aggie does not lie, cheat, or steal, or tolerate those who do."

TABLE OF CONTENTS

Page

Introduction

Building Automation Systems (BAS) that use the BACnet (Building Automation Control network) protocol need security improvement because they are currently entirely unencrypted and highly vulnerable to malicious cyber-attacks. Therefore, to protect the building utilization data, employees' privacy and safety, there is an urgent need to work towards threat detection and prevention in BACnet systems. This report discusses the results of a survey with multiple foci- the need for security in unencrypted IP-based BAS, cyber-physical security features that customers believe they need/don't need, what information the audience believes could be obtained from a hacked BAS, how someone could possibly go about getting access to BAS controls, and finally, their opinions on the intrusion of privacy due to data collection for security purposes. The audience for the survey was multifaceted- including subject experts, Building Service operators, BACnet users (via User Forums), Building Automation companies, and the general public (potential users of BAS). From the survey, we wanted to get an idea of what attacks and devices we would need to model to emulate a real BACnet system, and what features our anomaly detection algorithm would need to have to appeal to a wider customer base. Additionally, we wanted to find out how feasible automated detection of cyber-physical threats was in the eyes of experts in the field.

The responses we got from the survey helped to determine the direction of development of our intrusion detection system. The responses will also help us to improve our presentations and explanations for this project and any future projects that we participate in. From the responses we also aim to improve our marketing skills to sell/develop our ideas and for the public to recognize the importance of security in BAS.

Methodology

Target Audience:

The methods used in the project are surveys aimed towards two different audiences. One for the general public assuming no/partial knowledge of security on Building Automation Systems. The other (Technical survey) is for the representatives of companies, professors or any individuals who have knowledge about Building Automation Systems and BACnet. The survey forms sent to the companies were sent to individuals with prior knowledge of BACnet security and their input will be needed on how to improve BACnet security. We also reached out to people in online BACnet community forums, specifically The BACnet Institute and the BACnet Protocol Stack/Discussion on sourceforge.net.

Survey Form Distribution:

For the general audience survey, we reached out through social media platforms such as Instagram and WhatsApp with the dual objectives of both filling out the forms and urging people to educate themselves on BAS security. As the reach of this method was very large, we could not estimate the number of responses in the limited timeframe we had. At the end of the survey, we had 51 responses to this form. The links to the survey form were sent through WhatsApp groups and posts on Instagram.

For the individuals with prior knowledge on BACnet we sent links to the more technical questionnaire through emails and created relevant discussion threads on the above-mentioned online forums.

Additionally, the links to the survey were distributed to a few professionals in the technology and cyber-security sectors via WhatsApp. The estimated reach of the technical survey was more than 15 people, with the uncertainty in upper bounds due to the links being shared on the community forums. At the end of the survey, we received only 6 responses to this questionnaire. This was quite a letdown, as this survey was of higher priority than the other due to the experience and technical knowledge of the respondents. However, each of the responses were insightful and actually helped us refine the survey.

Questionnaire Setup:

For investigating our customer needs, we formulated questions to narrow down our focus on the issues that customers would want to resolve on BACnet systems. We wanted to target a wide range of audience and we designed two separate surveys- one targeting the general audience and the other targeting professionals and experts in the BACnet systems. For both surveys, we set up a combination of yes/no, agree/disagree, and open-ended questions. Yes/no questions were asked with the aim of getting a quantitative reasoning of certain aspects of our project while gathering data such as the percentage of BACnet users among the respondents. On the other hand, the aim of open-ended questions was to get interesting and insightful opinions on questions with no fixed answers. This in turn could allow us to identify aspects of the project we've ignored or help us avoid pitfalls. We also used multiple choice and checklist types of questions for the objective information we wanted, with the aim of helping us make decisions on certain project specifications.

We decided to use Google Forms to create our survey questionnaires as it allows for greater collaborative effort and was enough to organize the small amount of data we expected to be able to collect. Though the question options available were simplistic and did not allow much freedom to target non-standard data, for the purpose of this survey, Google Forms was an adequate choice. Both the questionnaires are appended at the end of this document. The rationale behind the questions and the results we got from the survey are discussed in the following section.

Customer needs analysis

The results of our survey were very mixed, with general trends being quite difficult to confirm. This was especially the case for the general survey. The main reason for this state was lacking the large number of responses needed for conclusive results and the relatively higher average number of options per question which only compounded the issue. However, many interesting points came up in the survey responses due to the spaces left for open-ended answers. The results have been presented and analyzed below in detail.

Audience diversity:

One of the main objectives of this survey was to gather the opinions of people from a wide range of backgrounds. This was mostly achieved as we were able to see a great variety in the responses for "What is your profession?" which happened to be the first query in both survey forms. In the case of the general survey, most of the respondents were from an engineering background (45 of 51), of which 67% were students and the rest were professionals. Two other respondents were a doctor and a graphic designer.

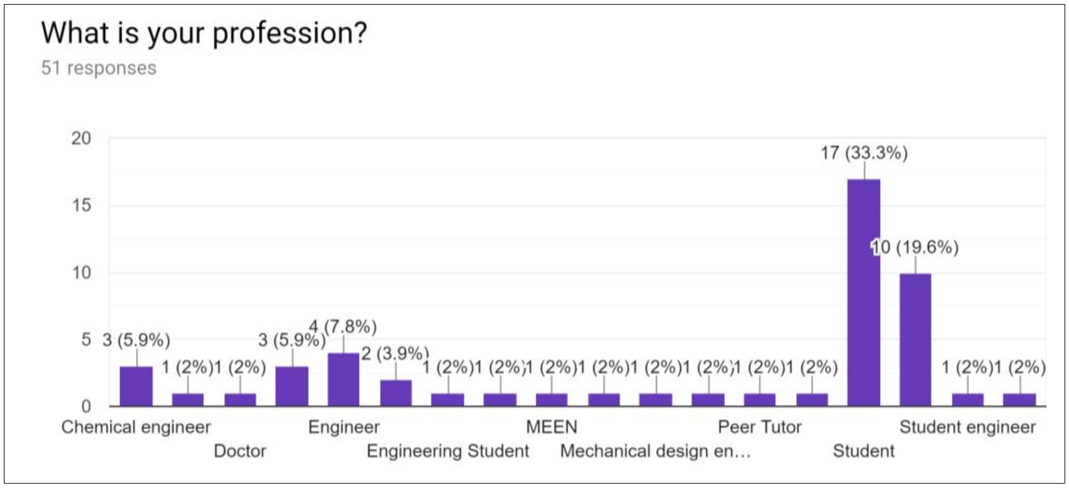

Figure 1

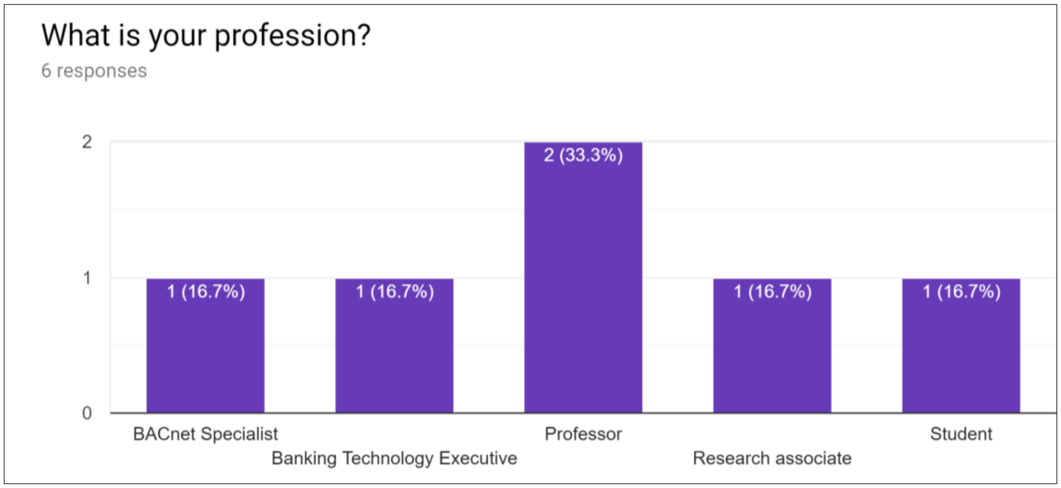

Figure 2

In the technical survey too, we managed to achieve the goal of diversity in respondent background as can be seen in the chart (figure 2) above. Correlating the profession of the respondent to their responses led to some interesting relations, mainly involved with how serious they believed the need for security measures in BACnet systems was.

BAS User Percentage:

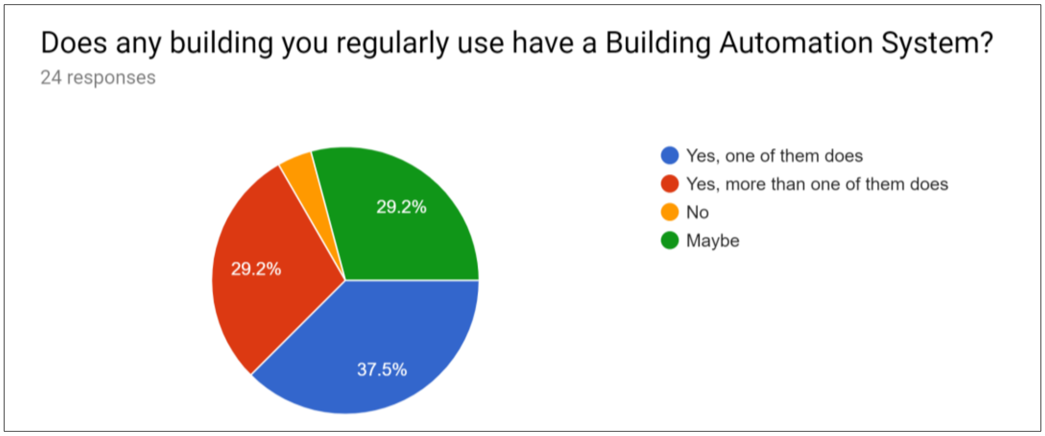

Figure 3

We expected that the number of people who use BAS, i.e., work, study, or live in automated buildings among the general public to be significant. This was validated in the response to the second question in the general survey, shown below. From the results, around 67% of the respondents to the question definitely used one or more buildings with a BAS and only ~4% definitely did not. The rest were unsure. This result indicates that potentially 96% of the respondents interacted with a BAS on a regular basis, which in turn validates a key assumption of our project about the penetration of Building Automation Systems.

Necessity/Urgency of our project:

The potential of our project was validated by both an expert in the cyber-security field and our Faculty Advisor. However, we wanted to get a quantitative understanding of the necessity and/or urgency of this project. For that reason, we asked for the general public's opinion on the need for security in Building Automation Systems as well as the experts' opinion of the severity of the need for security measures. The more technical question was set as a scale of 0-10, with 10 being extremely urgent whereas the general question was of the Yes/No type.

As expected, the majority (96%) of general respondents replied that there was a need for development in BAS security (figure 4). This could be interpreted as the result of higher awareness of the need for cyber-security in connected environments among the general public, i.e., a result borne more of common sense than experience.

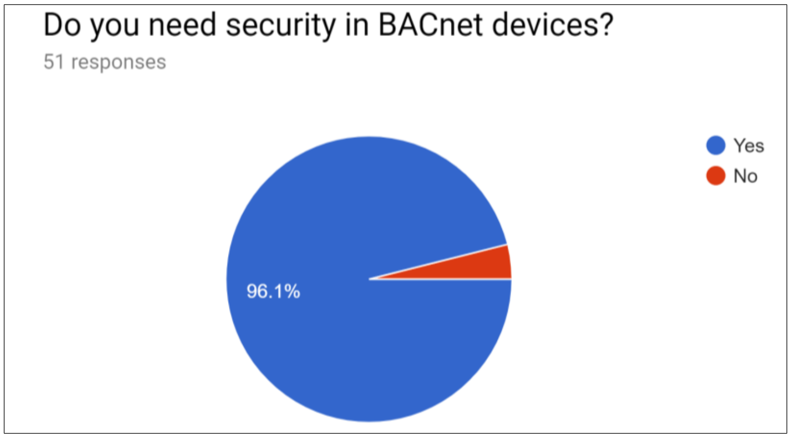

Figure 4

Similarly, for the technical survey, the trend of the responses (figure 5) was towards the higher end of the scale. But surprisingly enough, the results were not all 9 or 10 on the scale and were quite spread out between 5 and 10. Although this may have been due to the subjective nature of the question and the low number of responses, this may indicate that the issue of cybersecurity is important, but not as urgent as we originally felt it was. On the other hand, the people who answered 9 on the scale to this question were either researchers or BACnet specialists, who are the ones most invested in this field and hence naturally form the meat of our customer base.

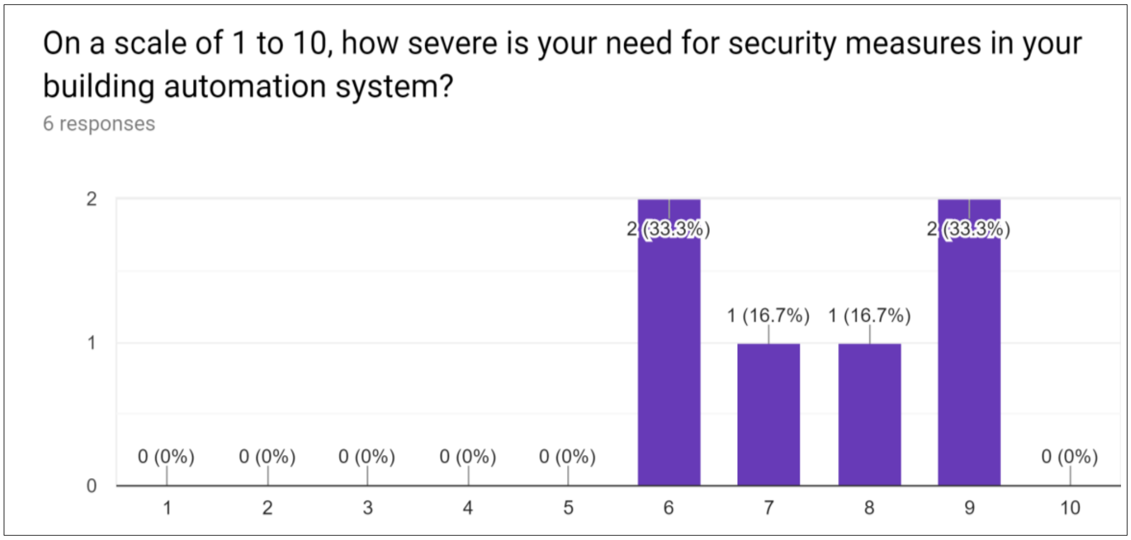

Figure 5

Sensors to model in project:

The question of what BACnet devices to model in our proposed emulation of a real-time BACnet system to run the machine learning algorithm on was something we urgently needed an answer to. As the services to model were decided already, we aimed to get an idea of what sensors were necessary by posing the question to the experts via the technical survey.

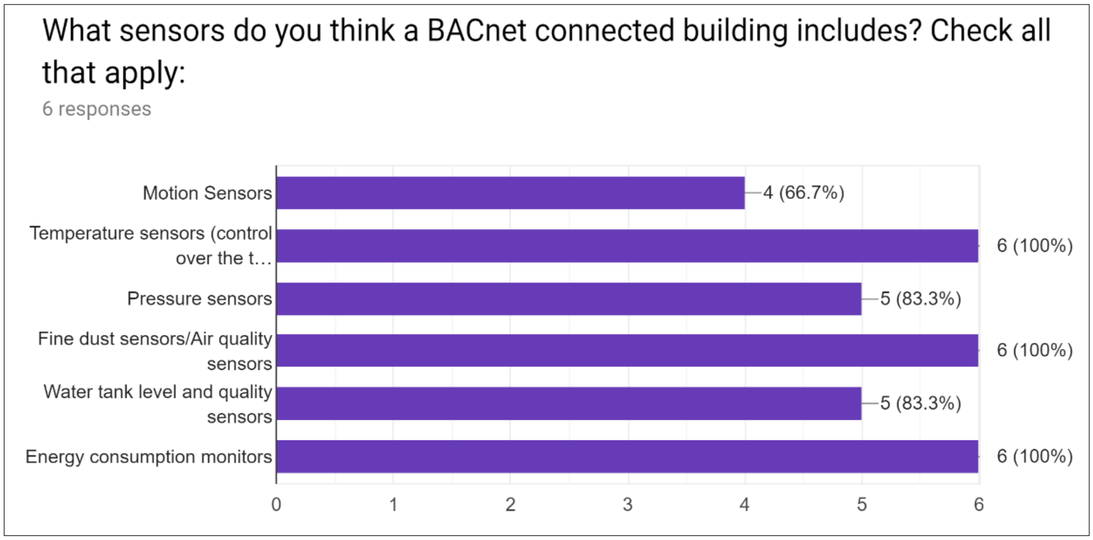

Figure 6

The responses (above, figure 6) showed that all of the given options could be used; and as the small number of responses made it impossible to conclude the trend, we could interpret it as having free reign to choose between the options given. None of the respondents added their own options as allowed by the ‘other…’ checkbox, which could indicate that our selection was satisfactorily exhaustive.

Attacks to model in project:

The other modeling requirement of our project is the synthesis of attacks on the emulated BACnet system. To that end, we asked the technical survey respondents about the attack they think a BACnet would most likely face. Of the responses (figure 7), 50% were of the opinion that Man-in-the-middle attacks were the most common one. We took this result into consideration and are planning to generate attacks with probabilities in accordance with the distribution of the results below, setting aside the custom answer of ‘all kinds of cyber-attacks.

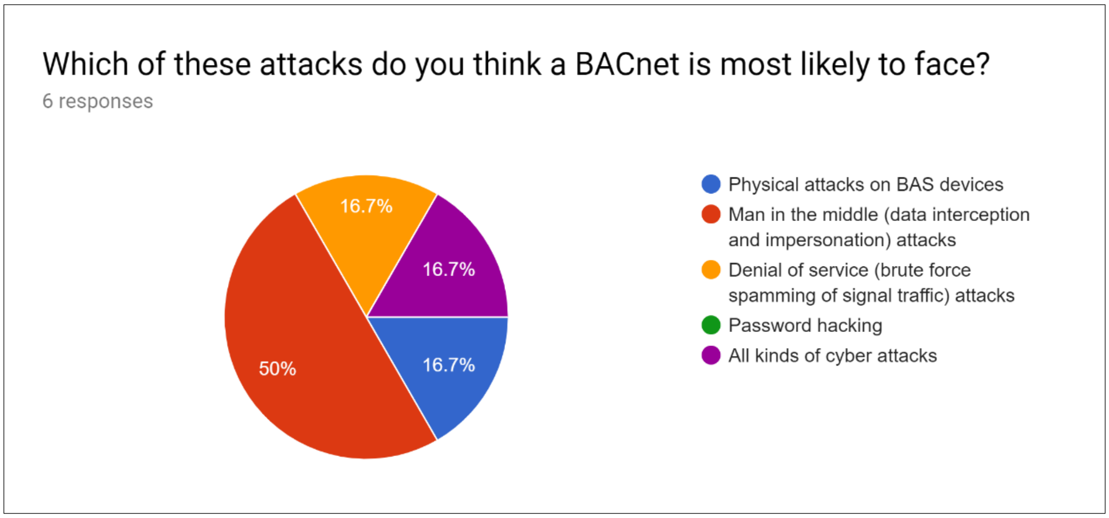

Figure 7

BAS Security Features:

Regular security features are a given in any private or critical software, and BAS is no exception. However, all the communication on BAS networks are unencrypted even as of today, making for highly vulnerable systems. From [1], the available security measures for BAS were found- which were then used as the options to a question asked on the technical survey in addition to a few other options we thought of. In the question the respondents were asked to select the currently available security features in Building Automation Systems according to their knowledge of the same from a checklist. The results are given below.

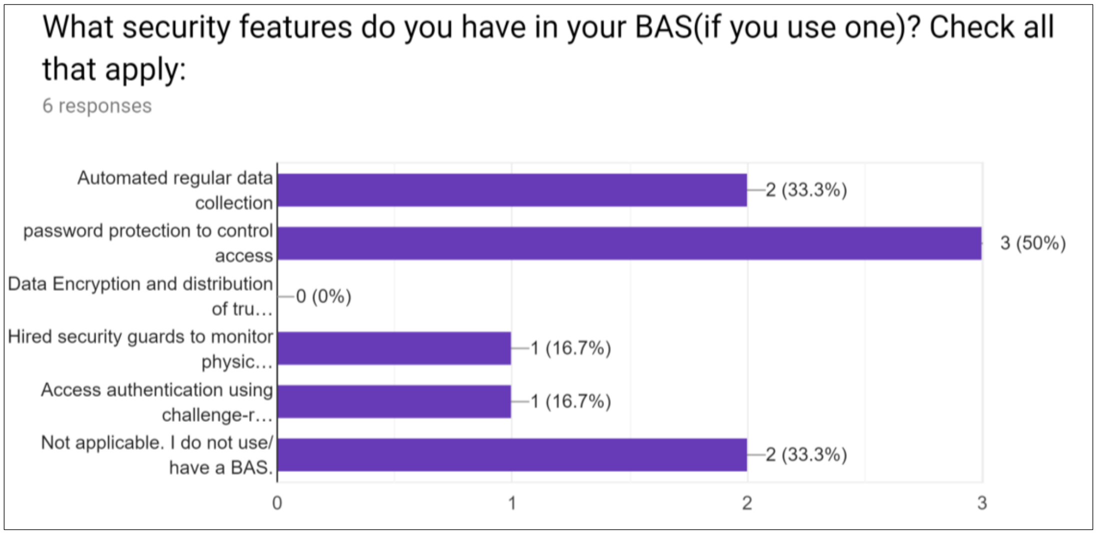

Figure 8

Further, the respondents were asked to check off the security features they would like to see in a BAS. The most popular picks for this question were ‘data encryption and distribution of trusted keys’ (50%), ‘automated regular data collection’ (33.3%), and ‘password protection to control access’ (33.3%). This result helped us improve on our design of anomaly detection software- not the functional aspects, but the access protection and authentication parts. The full chart is given below.

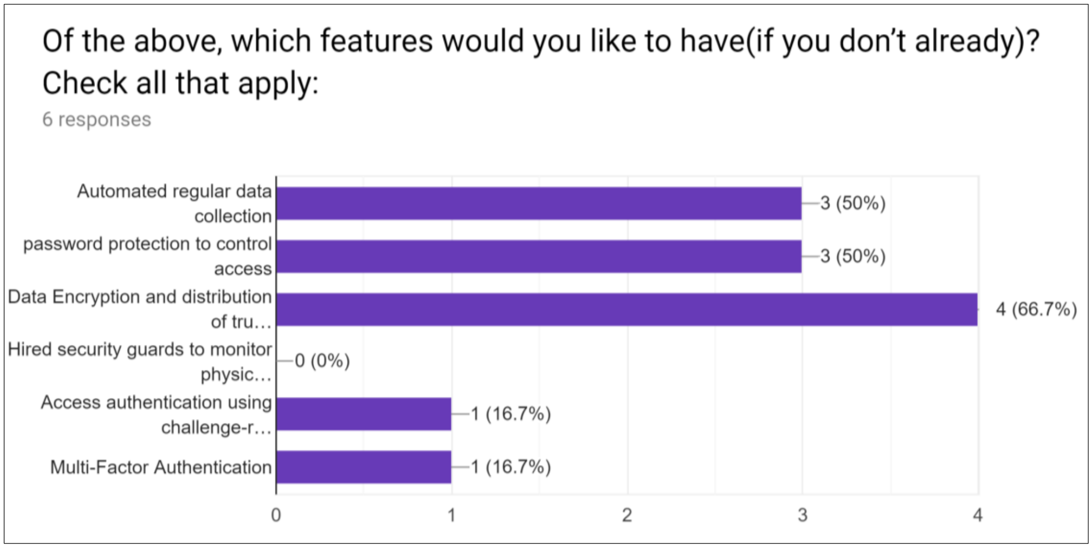

Figure 9

There were quite a few opinions regarding frequent authentication and other complicated identity verification methods. The same Yes/No question regarding the necessity of authentication every time one connects to a BAS was asked in both general and technical survey forms. Responses to the general questionnaire were ~80% 'Yes' selections (figure 10), which may indicate the willingness or capacity of the regular user to bear with tighter (or more frequent) authentication mechanisms to improve security. An example would be the adoption of the two-factor authentication by the TAMU system which most students got used to as a matter of fact. A similar percentage of responses to the technical survey form (figure 11) could be a matter of coincidence but is more likely to be due to the trend of grudgingly accepting tighter authentication methods being common to all Connected people.

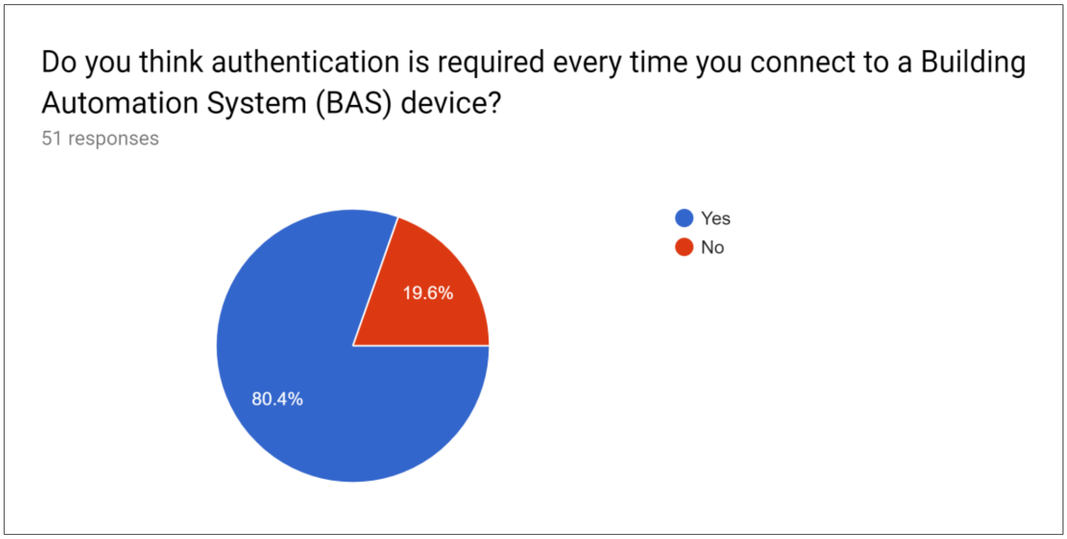

Figure 10

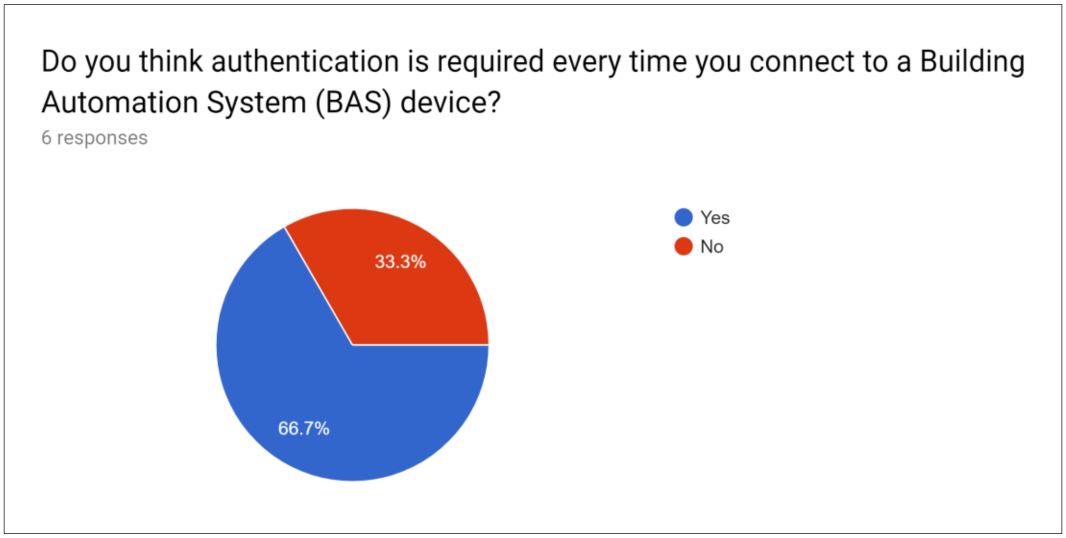

Figure 11

On the topic of BAS security features, the respondents to the technical survey were additionally asked to mention features they would rather not have in a BAS. It was expected that a certain number of responses would mention authentication mechanisms; but due to the small response pool, only one person (a professor) mentioned that they would not like overly complicated authentication mechanisms. Another respondent raised concern over potential security breaches due to the over-collection of data for security purposes. This last point will surely be added to the list of things to look out for in our anomaly detection program, i.e., to avoid over-collecting data.

Opinion on Data Collection:

Data collection, being what it is, is a topic of contention many companies which depend on analytics such as Google and AWS (Amazon Web Services) have to face in many of their applications [3]. The breach of privacy that is entailed by any data collection method rears its head even in the case of our proposed anomaly detector, as we plan to use machine learning (naturally with a lot of collected data) to implement it. We asked both the general public and the narrower technical audience about their opinions on data collection in order to prevent cyber-attacks on BAS networks. The responses have been summarized in the charts below:

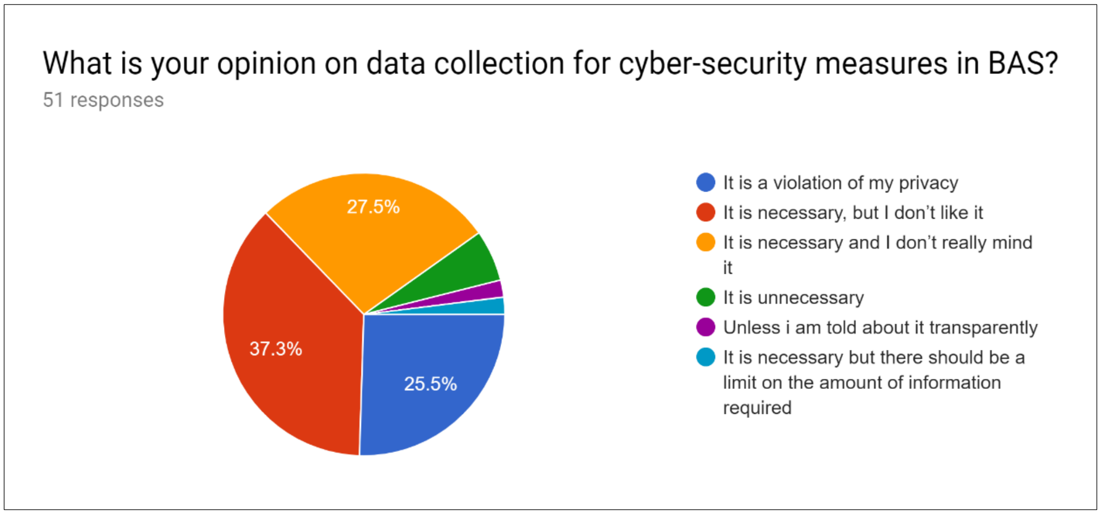

Figure 12

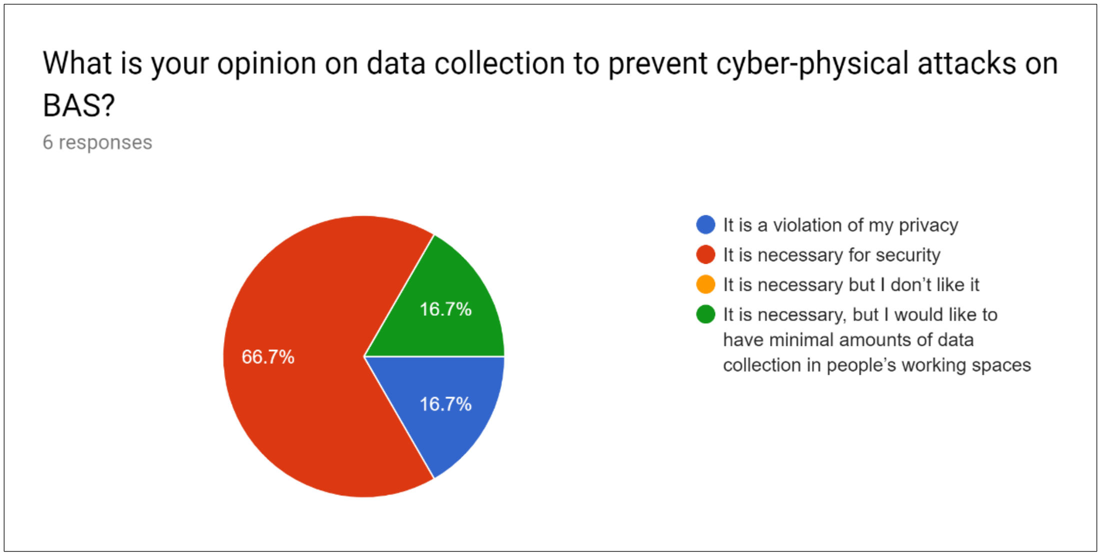

Figure 13

The general opinion on the subject (figure 12) was near equally divided between "it is a violation of my privacy" and "it's necessary, and I don't mind it" (~25%), and "It is necessary, but I don't like it." (37%). The mixed response was in fact more positive than we hoped, as we believed that the public opinion on data collection was overwhelmingly negative.

On the other hand, more than 80% of the respondents to the technical survey form (figure13) responded that data collection was necessary for network security, of which 1/3rd opined that they'd prefer lesser amounts of data collection from individual workspaces/living spaces.

From an intruder's perspective:

As a point of interest, we wanted to know the opinion of the public on the kind of information would be at risk if someone were to hack a BAS. The question, "what would you do if you received access to a BACnet device?", being an open-ended one, got a wide range of answers from the general respondents (in figure 14 below). Answers ranged from accessing banking credentials, exams (because we sent the survey to university students), locating specific individuals, obtaining or granting access to restricted areas. All of these answers are very probable as demonstrated by the Target attack in 2013 where hackers managed to obtain credentials of customers through the cash registers [2].

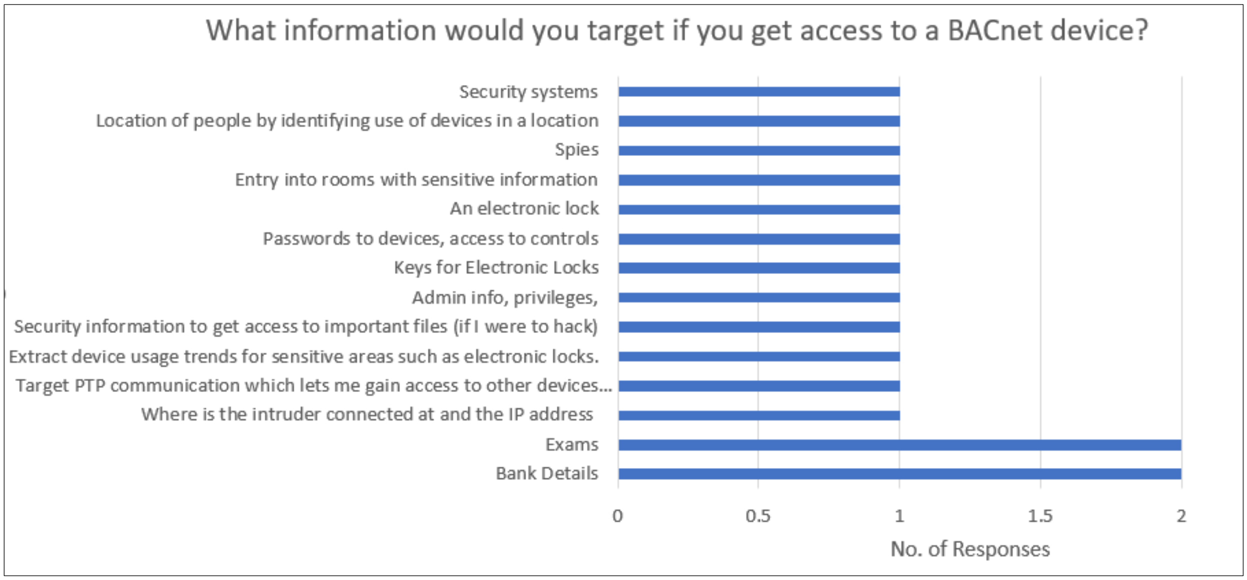

Figure 14

A similar question was asked on the technical survey form, "What information do you think can be obtained from hacking into Building Automation Systems?" The difference between this and the previous being that the answer was more objective here, as the respondents were assumed to have the necessary background to understand the given options and answer to the best of their knowledge. From the responses (figure 15, below) it could be seen that the IP addresses of the BAS devices were the most sought-after piece of information. This was in line with our expectations as gaining the IP address of the devices on an unencrypted (as it is still in most BAS) network would mean being able to access the information in the remaining options as well with the exception of personal information.

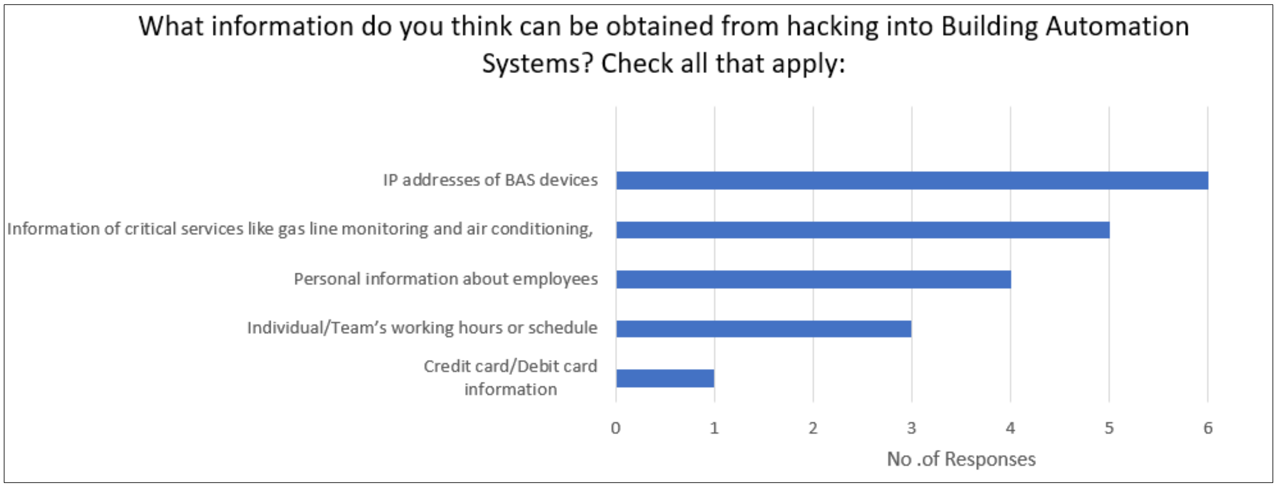

Figure 15

Additional Comments:

At the end of the technical survey, the respondents were asked to provide their opinion on BAS security and/or the survey itself. The responses were:

1. "For the question 'What security features do you have in your BAS (if you use one)?', A respondent replied that "you should provide also the alternative answer: Not applicable (since some users might not have access or possess such a BAS)."

2. "Password Change notification periodically will be an added advantage"

3. "An interesting survey with insightful questions. BAS is emerging as a crucial security space and is only getting better with the advancements in the areas of related technology and data analytics mechanisms"

The first response led to an improvement in the survey form, and the second could perhaps be added to the list of security features in a BAS. The opinion expressed by the third response was simply a validation of our project in general, received with thanks.

Evaluation of assignment

From the responses of the general survey, we found out that the public realizes the importance of security in buildings and therefore supports the goal of our project to detect anomalies in network traffic. The majority of the public also believe that the buildings they go to school, work or live have building automation systems. This shows the versatility of BACnet protocol and we aim to implement this model using 4 towers (raspberry pi stacks) which could represent university buildings, apartments, company buildings, hospitals etc. simply by varying the modelled sensors, services and traffic patterns. The responses from the general survey also showed that the public believe that BACnet devices need security. This shows that the public is aware of the danger in these devices being vulnerable to attackers and which in turn makes us develop BACnet devices to be secure and require authentication to access these devices. However, from the technical survey we received responses that they would rather not have too many authentication procedures as this could become too cumbersome, and also to avoid collecting too much data. Thus, a middle ground solution would be to allow multiple levels of access with general users having only a single authentication upon connection and those with higher authority to access the control layer having to go through stricter authentication mechanisms. Therefore, any breach in the building can potentially be a breach of trust through one of the buildings' employees. We also wanted to know how the public would react to data being used for cyber security purposes. With data collection being a sensitive topic currently, almost 1/4th of the responses believe that it is a violation of their privacy. This result was useful is helping us decide the level of data collection we should undertake.

Regarding the veracity of the results themselves, it has to be mentioned that this survey would have been served much better by larger numbers. It can be assumed that there is uncertainty in data measurement in the case of objective questions. However, since we based our observations and analysis on the general trends rather than concrete numbers, the probability of us making erroneous inferences should be much lower. If the number of responses had been in the range of 500-1000, this survey could have been a tool to assess the state of BAS security and public awareness regarding the same.

Conclusion

Overall, we learnt a lot from the market needs analysis to cater our project towards the public. Although the technical survey's response count was minimal and not enough to guarantee a fair representation of our audience (aim was 20+ responses), the responses were very informative and helpful in developing our project. From the respondents of the general survey, we managed to obtain 51 responses and many of them did not fully complete the survey. Through social media we received some responses that they were not able to understand what the survey was about and so they left some questions blank. This is partly our fault as we should seek to improve the presentation of our project. We researched into the topic and made the questionnaire with the assumption that our audience would capture the main idea behind our project. In the future, we hope to provide an extensive explanation of key terms and phrases of our project so that our audience can have a fair grasp of the concepts before diving into answering the survey questions.

For the most part, we captured a general yet extensive viewpoint of our audience that'll help us in honing our presentation content and focus on monitoring certain information that prove essential to a customer.

References

[1] Granzer, Wolfgang & Praus, Friedrich & Kastner, Wolfgang. (2010). Security in Building Automation Systems. Industrial Electronics, IEEE Transactions on. 57. 3622 - 3630. 10.1109/TIE.2009.2036033.

[2] Krebsonsecurity.com. (2019). *Target Hackers Broke in Via HVAC Company — Krebs on Security*. [online] Available at: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/ [Accessed 15 Oct. 2019].

Appendix I

BACnet Survey Form

Building Automation Systems (BAS) are softwares that can connect and automate relevant devices/sensors like a/c vents, electronic locks, lighting, supply lines and other utilities in a building. Of these systems, the BACnet (Building Automation Control network) is a widely used standard protocol for BAS systems. BACnet is preferred because it employs basic encryption methods as compared to most others which are completely in clear text, but it is still very vulnerable to cyber and physical attacks.

Our project is to identify/detect hackers who have gained access to the Building Automation Systems by implementing data collection and machine learning on the BACnet protocol.

Please help us understand the general opinion on BAS security by taking a few minutes of your time to complete this survey. Thank you.

* Required

1. **What is your profession?** *

   ____

2. **Does any building you regularly use have a Building Automation System?**
   Mark only one oval.

   ○ Yes, one of them does
   ○ Yes, more than one of them does
   ○ No
   ○ Maybe

3. **Why do you think BACnet systems are important?**
   Check all that apply.

   □ To allow for interoperable (compatible communication without restrictions) communications between devices
   □ To detect hackers in a Building Management System
   □ To improve the automation capabilities of Building Management Systems

4. **Do you need security in BACnet devices?**
   Mark only one oval.

   ○ Yes
   ○ No
   ○ Other: ________________________________

5. **Do you think authentication is required every time you connect to a Building Automation System (BAS) device?**
   Mark only one oval.

   ○ Yes
   ○ No

6. **Are automated detection of threats on BACnet systems a feasible option?**

Mark only one oval.

○ Yes

○ No

○ Other: ______________________________

7. **What information would you target if you get access to a BACnet device?**

____

8. **What is your opinion on data collection for cyber-security measures in BAS?**

Mark only one oval.

○ It is a violation of my privacy

○ It is necessary, but I don’t like it

○ It is necessary and I don’t really mind it

○ It is unnecessary

○ Other: ______________________________

Appendix II

BACnet survey

Building Automation Systems (BAS) are softwares that can connect and automate relevant devices like a/c vents, electronic locks, lighting, supply lines and other utilities in a building. Of these systems, the BACnet (Building Automation Control network) is a widely used standard which provides a wide platform for network integration and supports a wide selection of devices. It is preferred because it uses some basic encryption methods as compared to most other BAS which do not, but the BACnet is still very vulnerable to cyber and physical attacks. This is especially the case as the number of BAS networks is increasing these days.

Our project is aimed at implementing data collection and machine learning to teach a software how to detect attacks or threats on a BACnet system.

Please help us understand the general opinion on BAS security by taking a few minutes of your time to complete this survey. Thank you.

1. **What is your profession?**

2. **Do you think authentication is required every time you connect to a Building Automation System (BAS) device?**

   Mark only one oval.

   ○ Yes
   ○ No

3. **What information do you think can be obtained from hacking into Building Automation Systems? Check all that apply:**

   Check all that apply.

   □ Credit card/Debit card information
   □ Personal information about employees
   □ Individual/Team’s working hours or schedule
   □ Information of critical services like gas line monitoring and air conditioning
   □ IP addresses of BAS devices
   □ Other:

4. **What sensors do you think a BACnet connected building includes? Check all that apply:**
Check all that apply.

□ Motion Sensors
□ Temperature sensors (control over the temperature of a room instead of one central Air Conditioner)
□ Pressure sensors
□ Fine dust sensors/Air quality sensors
□ Water tank level and quality sensors
□ Energy consumption monitors
□ Other: ______________________________

5. **Which of these attacks do you think a BACnet is most likely to face?**
Mark only one oval.

○ Physical attacks on BAS devices
○ Man in the middle (data interception and impersonation) attacks
○ Denial of service (brute force spamming of signal traffic) attacks
○ Password hacking
○ Other: ______________________________

6. **What security features do you have in your BAS(if you use one)? Check all that apply:**
Check all that apply.

□ Automated regular data collection
□ password protection to control access
□ Data Encryption and distribution of trusted keys
□ Hired security guards to monitor physical activity around BAS devices
□ Access authentication using challenge-response mechanism
□ Not applicable. I do not use/have a BAS.

7. **Of the above, which features would you like to have(if you don’t already)? Check all that apply:**
Check all that apply.

□ Automated regular data collection
□ password protection to control access
□ Data Encryption and distribution of trusted keys
□ Hired security guards to monitor physical activity around BAS devices
□ Access authentication using challenge-response mechanism
□ Other: ______________________________

8. **What would you like Building Automation Systems to not include?**

9. **Are automated detection of threats on BACnet systems a feasible option?**
Mark only one oval.

○ Strongly disagree
○ Disagree
○ Neutral
○ Strongly agree
○ Agree

10. **What is your opinion on data collection to prevent cyber-physical attacks on BAS?**
Mark only one oval.

○ It is a violation of my privacy
○ It is necessary for security
○ It is necessary but I don’t like it
○ It is necessary, but I would like to have minimal amounts of data collection in people’s working spaces

11. **On a scale of 1 to 10, how severe is your need for security measures in your building automation system?**
Mark only one oval.

	1	2	3	4	5	6	7	8	9	10	
Not really necessary	○	○	○	○	○	○	○	○	○	○	We need it right now

12. **Thanks for giving this survey your time. We appreciate your opinions and would like to hear your thoughts on this survey and/or on BACnet (BAS) security in general. Please do tell us here:**