Metrics for ICS device security

Harikrishnan Manikandan 4613201
Harm Grifioen 4303598
Hans Schouten 4314891
Lars van de Kamp 4501829

Introduction

ICS devices have been around for a very long time, controlling some of the most critical infrastructure in the world. However, due to the uprise of the internet, people realized how beneficial it would be to connect the devices to the web for remote control and monitoring, thereby drastically reducing costs. By doing this, the devices became exposed to a whole new area of threats that were not present before. The devices were not designed to be connected to the web in a safe manner. It is therefore vital to measure how secure the critical infrastructure is, and what can be done in order to improve it. This document will give an overview of different metrics that can be used in order to measure this security.

The security issue at hand

Industrial Control Systems are part of critical infrastructure that companies, and society as a whole, heavily rely on. When access to these systems is granted to the wrong people, this could lead to large disruptions in everyday life. The Shodan ICS [Shodan ICS] dataset lists numerous Industrial Control Systems that are publicly accessible via the internet. Even when these are password protected, the systems should not be accessible from anywhere else in the world other than on-site or from specific control rooms. In addition, using password bruteforcing or exploitation of vulnerabilities in the firmware any publicly accessible Industrial Control System could get compromised. The high impact that the underlying infrastructure makes on civilization as a whole, makes the analysis crucial to fortify the defenses around the globe.

Ideal metrics for security decision makers

An ideal framework for security decision makers should take into account the:

1. Controls
2. Vulnerabilities
3. Incidents
4. (Prevented) losses.

Metrics on network hygiene indicate whether the appropriate configurations and controls are in place (aspect 1). Furthermore, these metrics are complemented with metrics on the level of software patching, attempting to fix current vulnerabilities (2). Besides the opportunities to attack a system, also the incentives to do so should be taken into account. Therefore, incident metrics are used to consider the entire threat landscape by mapping the attacks that did actually occur, or are most likely to occur using incident data like the Shodan ICS datasets (3). Finally, metrics need to be defined with regards to the losses and prevented losses (4). Both occurred and prevented incidents should be analyzed and quantified in such a way that the cost benefit analysis becomes clear due to the use of the chosen security policy.

In addition to the four pillars mentioned above, a metric needs to clearly resemble the level of security to all involved stakeholders. Everyone, ranging from a maintenance employee all the way to c level executives should be able to grasp the situation regarding the security infrastructure. By allowing all individuals to understand the situation, topics such as renewed investments or policy changes are more easily discussed. It provides context to the current situation, that in turn could validate new rounds of funding whereas originally it could have been seen as having low intrinsic value and thus a low return on investment. These discussions can generate consensus throughout the organization, highlighting the costs and benefits of security programs, thus helping security decision makers in doing their job.

Metrics used in practice

The US National Security Agency (NSA) constructed a framework for measuring ICS security, focussing on the potential impact and loss relating to possible attack scenarios [NSA, 2010]. The first step is to create an accurate map reflecting all networked assets and the digital communication links that connect them. The next step is to perform a loss assessment which aims to identify actions that can be performed by an adversary via unauthorized access to the device. In the final step, the potential loss are determined based on the achievable malicious actions combined with the expected frequency of such incidents. Their framework offers a cost-benefit analysis approach which will allow organisations to prioritize their defensive efforts by identifying network security improvements that provide the greatest benefit for a given cost.

Boyer and McQueen define a set of seven ideal-based metrics for Industrial Control Systems [Boyer McQueen, 2008]. Each ideal is associated with an abstract dimension of security and represents a system condition at a given point in time. In a perfectly secure system, all ideals are satisfied. When attempting to assess a complete ICS system in every possible dimension, an overarching measure is computed based on the individual metrics defined for each ideal.

Metrics that can be designed from the dataset

In this section, we define different metrics for the dataset in order to measure security. In order to define the metrics, we first have to define what a metric is. We have taken the following definition of a metric:

> *“Metrics allow us to measure attributes and behaviors of interest. A meter, for example, is a metric that allows us to measure length, while the number of defects per shipment is a metric that allows us to measure quality.” [Cyber Threat Metrics, 2012]*

Following this definition, version number itself is not a metric, but the number of vulnerabilities known for a certain version number is.

Number of publicly accessible devices over time. This shows improvements or declines in security of the different types of ICS. In addition, it could also reflect the interest third parties have in specific industries.
Update frequency. Using the version number and the timestamps, a metric can be created for the update frequency of the devices. The lower the update frequency, the more susceptible the device is against existing and future exploits.

The number of firmware vulnerabilities. By cross-referencing the current version numbers with a list of known vulnerabilities for specific versions [CVE Details], the score of the most critical vulnerability can be used as a metric defining the lack of security in a specific system.

Manufacturer. The manufacturer of the device can also be taken into account. This can be cross-referenced with a list of ‘vulnerable’ manufacturers, those who originate from a certain country or have a poor reputation. The vulnerabilities known per manufacturer will be the metric of this trust score per manufacturer.

The number of accessible devices per location. While the dataset only shows publicly accessible devices, this might still be a useful metric to see which locations are most vulnerable to attacks. These area’s will have a higher attack vector than other areas, which need to be combined into a likelihood score per location.

The number of accessible devices per organization (type). Another highly influential factor is the type of organization that is behind the specific accessible system. Certain high profile institutions might be more attractive targets due to their larger potential impact on society. Therefore, industry that belongs to an instance could indicate the likelihood of being targeted and thus the number of incidents and perhaps even the number of known vulnerabilities that are known. The high-profile nature of a system, could lead to more time being invested in finding vulnerabilities and exploiting these since there is also a larger return when successful.

Other valuable metrics not directly visible in the data:

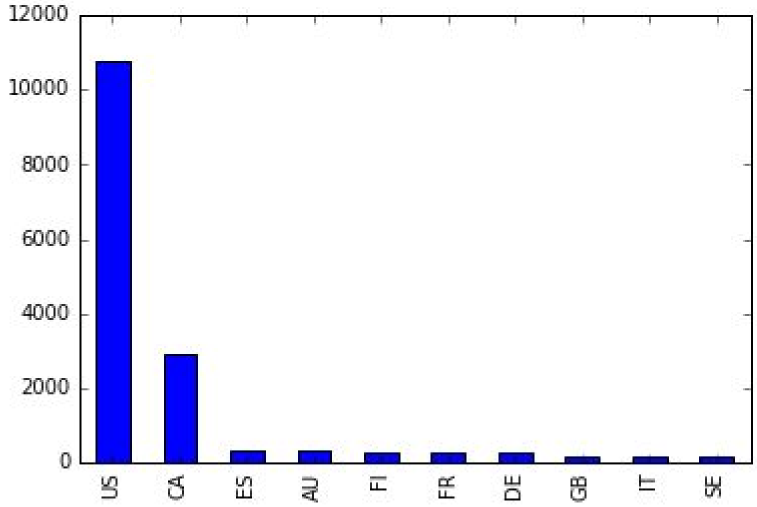
1. Ensure basic infrastructure for protection with a list of mandatory checks, adding the present mechanisms to a total protection score.
2. The checks should include verifying if the latest software patches has been installed, at least in critical infrastructure. The time to update can be of great importance when compared to the released update frequencies.
3. Each company should assess its security infrastructure by employing security firms to perform penetration tests. The amount and severity of vulnerabilities have to be recorded and the aggregated risk of all its vulnerabilities is assigned to the company. The risk factors of the vulnerabilities have to be incremented each time the same vulnerability appears in successive audits.
4. A list of attacks on relevant infrastructure has to be maintained and the losses that might have been incurred by the organization if it had been attacked has to be assessed based on the scale of the organization and amount of its customers impacted. This amount aggregated over the top certain percentage of the attacks gives an estimation of the amount of money saved by the company. Any attacks from

which the company couldn't have protected itself against has to be assessed again and the estimated damage must be subtracted from the above amount.

Metric evaluation

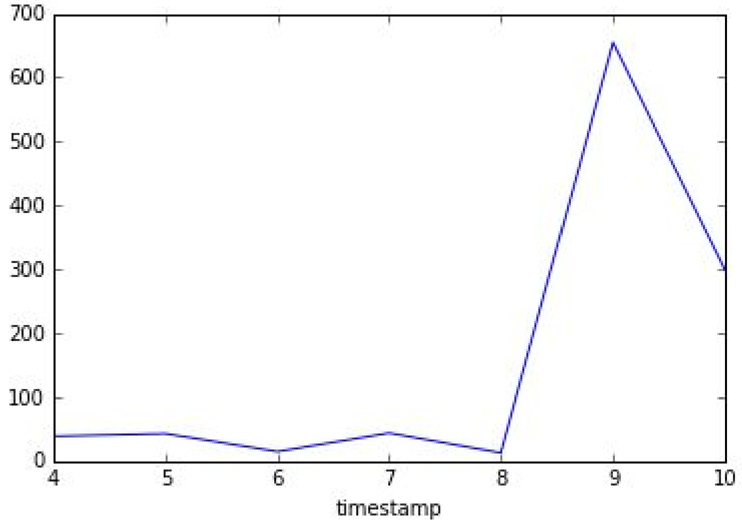
The metrics suggested in the above section will be evaluated along with the information contained in the dataset to discuss their efficacy and viability in this section.

The number of accessible devices per location.
A metric of number of publicly accessible ICS per country can be used as a score to assess threat level per region. This isn't a deterministic indicator as there are many reasons why some countries are more susceptible than others. A graph of the publicly accessible devices per top 10 countries is shown below:

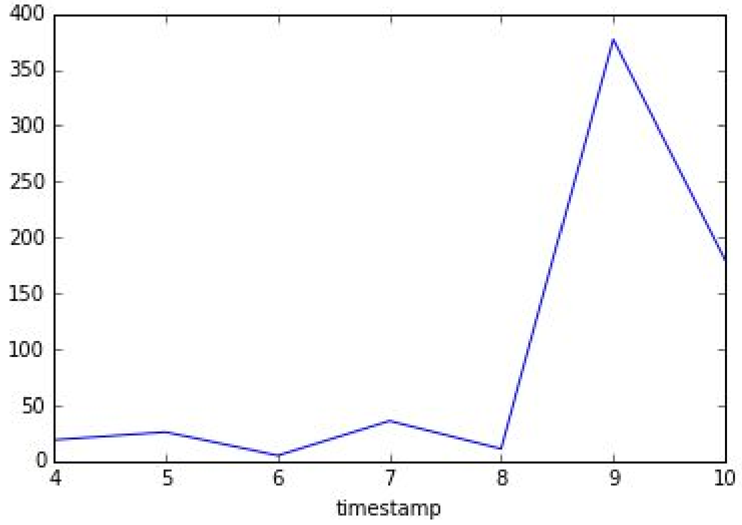


This data should be normalized over the number of people living in each country, since larger countries would probably have more companies and more ICS.

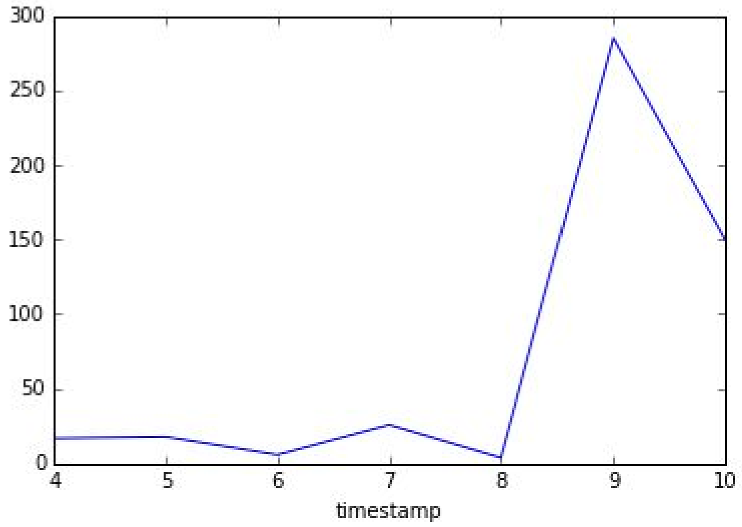
Number of publicly accessible devices over time.
The number of publicly accessible devices per company over a period of time must also be computed and maintained for any general trends across the sector. The number of publicly accessible devices added each month per organisation are shown in the figures below. As we can see, the same trend appears throughout the different organizations. The last plot shows the overall trend containing all instances.



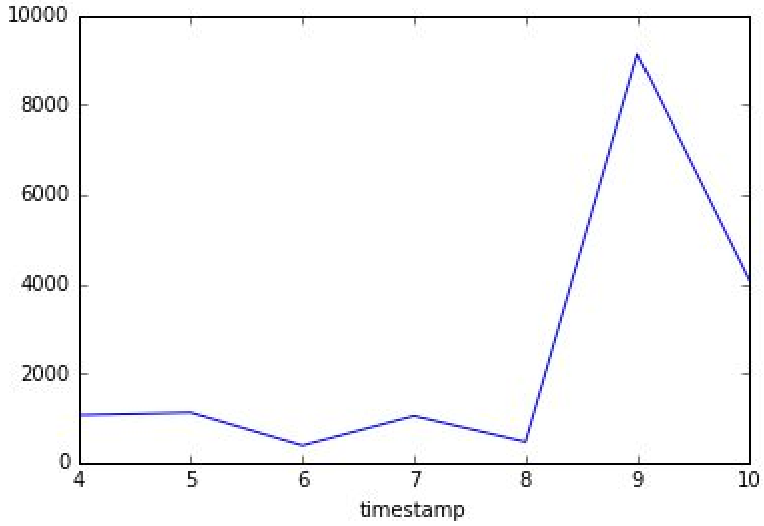
AT&T Internet Services



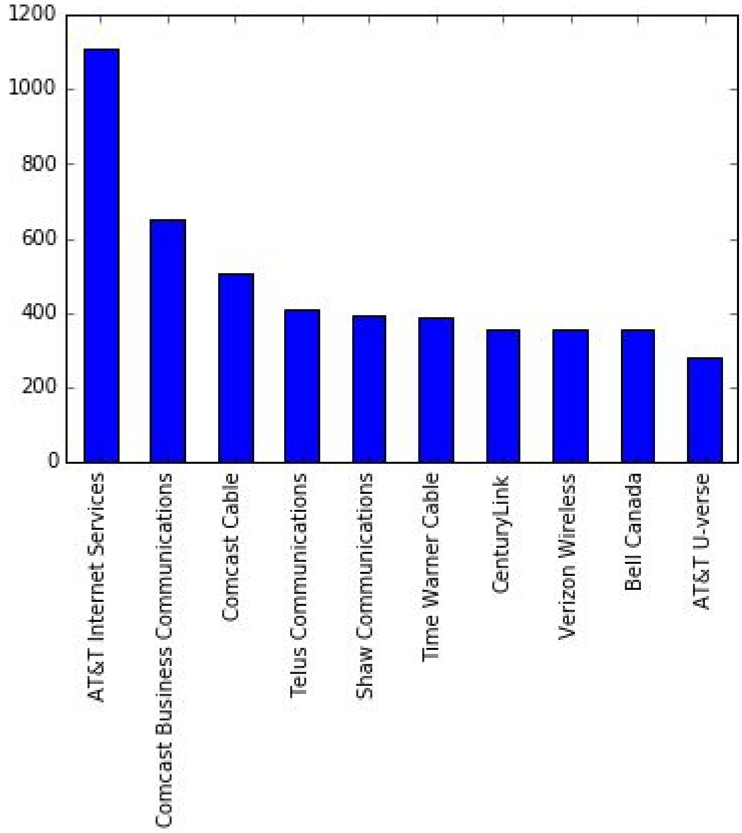
Comcast Business Communications



Comcast Cable

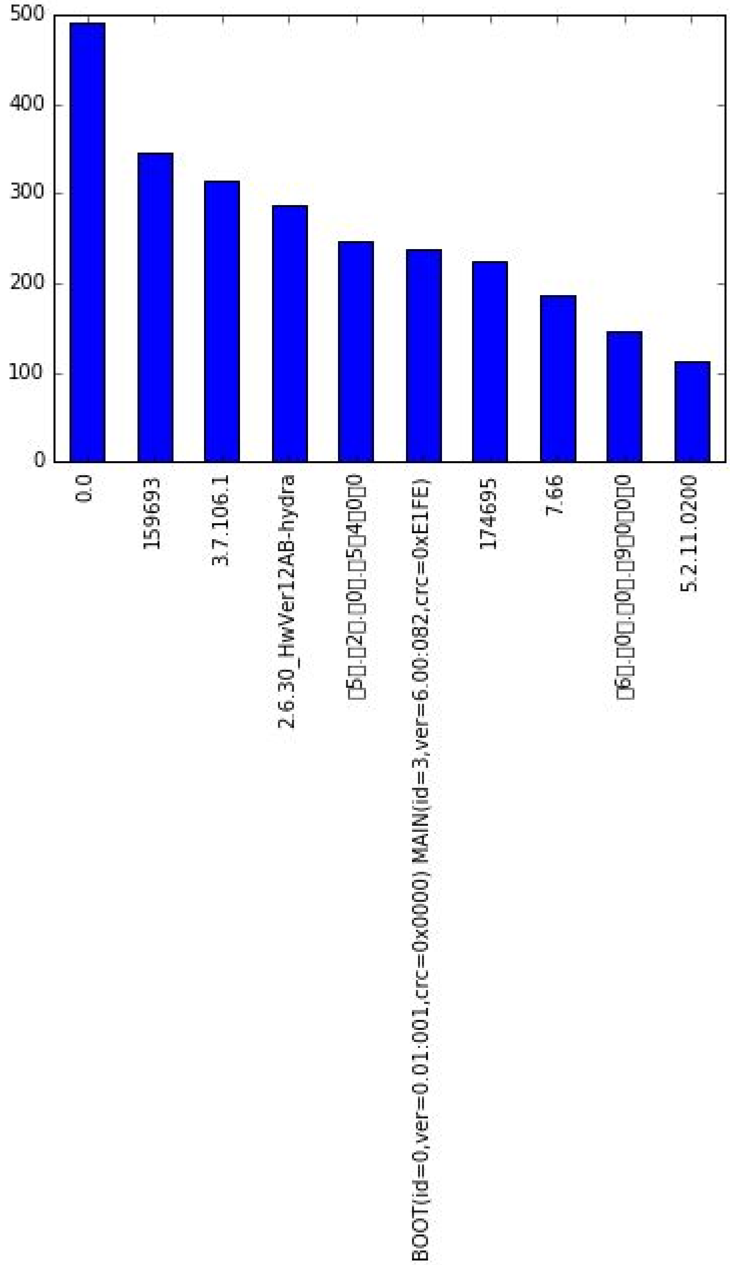


The number of accessible devices per organization (type).
The highest number of entries in the “bacnet.json” dataset. Do note that the higher the number of accessible devices does not automatically imply poorer security levels, as this could also be due to a larger company size. These need to be normalized to company size, to paint a more accurate picture.



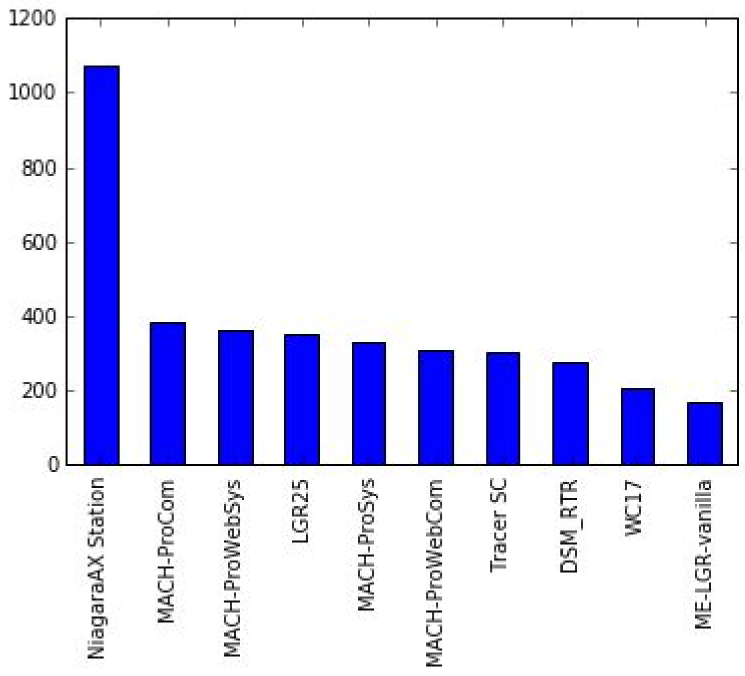
The number of firmware vulnerabilities & Update frequency.

The version numbers are hard to track as most of the entries are empty while very few of the rest have valuable information. It seems that the data does not provide us with the needed insights to validate these metrics. The 10 most frequent version numbers are shown below:



Manufacturer

The product and manufacturer information is also hard to track since most of the entries do not have this field filled out. The list of top 10 most frequent products are shown below:



Conclusion

Even though several variables are lacking in the dataset, some of our metrics can still be derived. The location, time-series, and organization analysis have shown potential to indicate the security of a system. The manufacturer metric is partially affected by missing data, but could prove to still be useful as the top 10 does allow us to see predominant manufacturers in the industry. Here, the available data could function as a sample that can indicate the distribution. Hopefully, our metrics will improve the understanding of the different security situations and help society in better protecting its critical infrastructure for many years to come.

References

National Security Agency (NSA). (2010). A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)
https://scadahacker.com/library/Documents/Assessment_Guidance/NSA%20-%20Framework%20for%20Assessing%20and%20Improving%20Security%20Posture%20of%20ICS.pdf

Boyer and McQueen. (2008). Ideal Based Cyber Security Technical Metrics for Control Systems
https://inldigitallibrary.inl.gov/sites/sti/sti/3884735.pdf

Shodan map of publicly accessible Industrial Control Systems
https://icsmap.shodan.io/

Mateski et al. (2012). Cyber Threat Metrics
https://fas.org/irp/eprint/metrics.pdf

CVE Details. Current CVSS Score Distribution For All Vulnerabilities
http://www.cvedetails.com/