An overview on the security technological levels in the Italian Smart Cities

Vita Santa Barletta[1], Paolo Buono[1], Danilo Caivano[1], Giovanni Dimauro[1] and Antonio Pontrelli[2]

[1] *Department of Computer Science, University of Bari Aldo Moro, Via Orabona 4, 70125, Bari, Italy*
[2] *Exprivia S.p.a., Molfetta, Italy*

Abstract

A Smart City is a multidimensional entity based on Information and Communication Technologies (ICT) and intelligent (smart) use of urban infrastructures for improving the quality of life of its citizens. The management of such technologies and services for the citizens requires addressing adequately the security. The goal of this research work is to analyze existing potentially vulnerable devices in Smart Cities, in order to understand the security level of the city, and thus provide support for a secure management of the city. An analysis on 5 Italian Smart Cities was performed, each one was evaluated on different technological layers: Network and Infrastructure, Sensors, Service Delivery Platform, Application and Services. The results show that currently there are potentially vulnerable devices across different technological levels that compromise security and privacy of smart services offered to citizens. The development of a Smart City requires the implementation of security controls, in order to reduce the possibility for attackers to exploit existing vulnerabilities in the analyzed devices.

Keywords

Security Smart City, Security IoT, Privacy by Design, Secure Project Management

1. Introduction

A Smart City integrates physical, digital and human systems to deliver a sustainable, prosperous and inclusive future for its citizens [1]. In order to improve economic and political efficiency and enable social, cultural, and urban development, the smart city must include a networked infrastructure. Specific goals are: the business development and social inclusion of urban residents in public services; high-tech and creative industries in long-term urban growth; attention to social and relational capital in urban development; social and environmental sustainability [2].

The services of a smart city aim to improve the quality of life of the citizen in different domain sectors. An example is related to digital accounts, that citizens use anywhere and anytime in services that require the users' identity. Any service that accesses and provides sensitive data may ask the identity of the user to prevent data leaks or improper access to such data. Digital accounts are used to access such services [3]. A smart city has more services, since the intelligence of a city is implemented through the deployment of devices, sensors, infrastructures that connect objects and people through services in various areas. From a conceptual point of view, a Smart City can be organized on a bi-dimensional model where one (horizontal) dimension represents the four overlapping technological layers: network and infrastructure, sensors, service delivery platform, application and services; a second (vertical) dimension includes the application domains: people, energy, economy, mobility, living, environment, planning, government.

The increase in connectivity in an enabling factor to be smarter, but this increases the possibilities for cyber attacks and consequently the vulnerability. In order to reduce security threats and incidents,

Proceedings ITASEC 2021, April 7-9, 2021, Italy
EMAIL: vita.barletta@uniba.it (A. 1); paolo.buono@uniba.it (A. 2); danilo.caivano@uniba.it (A. 3); giovanni.dimauro@uniba.it (A. 4); antonio.pontrelli@exprivia.com (A. 5)
ORCID: 0000-0002-0163-6786 (A. 1); 0000-0002-1421-3686 (A. 2); 0000-0001-5719-7447 (A. 3); 0000-0002-4120-5876 (A. 4)
© 2020 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-2940/paper42.pdf

the Smart City should identify threats timely, define and adjust strategies and activities [5]. In order to meet these needs this work analyzed 5 Italian Smart Cities, seeking for vulnerable devices that may become access points for cyber-attacks on the city. An overview of the technological levels of the security of Italian Smart Cities is the first step to plan correctly actions and implement infrastructures.

The paper is organized as follows: Section 2 discusses related works; Section 3 briefly presents the Smart City Integrated Model; Section 4 describes the performed analysis; Section 5 reports results of the analysis; Section 6 performs a discussion about initial findings of this work; Section 7 highlights limits and threats of the work; Section 8 concludes the paper.

2. Related Works

Smart city involves technological, economic and social improvement fueled by technologies based on sensors, big data, open data, new connectivity ways and information exchange [6]. Therefore, smart city security is essential to incorporate the technologies into smart city cyber infrastructure and to improve the conditions of life for its citizens [7]. For instance, in the mobility domain the diffusion of embedded and portable communication devices on modern vehicles entails new security risks since in-vehicle communication protocols are still insecure and vulnerable to attack [8].

Integrity, authenticity, confidentiality and availability are important security requirements in the different domains of the smart city to guarantee the availability of services and, consequently, the connectivity of the city and the citizens [9]. IoT plays a pivotal role within the infrastructure of smart cities as it provides the network architecture responsible for gathering and processing data from distributed sensors and smart devices [10]. The data generated by unprotected smart city infrastructure such as parking garages, or surveillance feeds provide cyber attackers with an ample amount of targeted personal information that can potentially be exploited for fraudulent transactions and identity theft or in some cases obtain control/access to such devices [11]. Therefore, the complexity of smart city [12,13] impacts significantly on security (i.e., illegal access to information) and privacy within smart cities seems to disappear considerably, digital citizens are more and more instrumented with data available about their location and activities [14]. This requires the development of a comprehensive model of security intelligent city management [15], just think of the residents of some buildings in the city of Lappeenranta, who in November 2016 risked freezing to death inside their own homes at the hands of a group of hackers who, by launching a DDoS attack on the central heating system, blocked its operation, knocking out the boilers connected to the network.

Smart Cities, if not properly designed and carefully administered [16], can become insecure infrastructures, exposing public governance to the risk of cyberterrorism attacks [17]. Thus keeping in mind the security and privacy challenges associated with the smart city, this research work aims to report an overview of the security technological levels in Italian smart cities in order to provide the necessary guidelines to be able to safely manage such cities and especially to be able to apply preventive security measures.

3. The Smart City Integrated Model

A Smart City can monitor and integrate functionality of critical infrastructure like roads, tunnels, airways, waterways, railways, communication power supply, etc., control maintenance activities and can help in optimizing the resources while keeping an eye on the security issues as well [18]. Smart city security has become one of the important issues in cyber security [7] and it is necessary to protect every dimension on which a smart city develops its smart services [19].

Generally, a conceptual approach to a smart city includes 6 dimensions [20]: people, government, economy, mobility, environment and living that play a key role in the design of a smart city strategy [21]. However, considering the concept of Smart Sustainable Cities [22] it is necessary to rethink how to construct and manage cities with the help of technologies [23]. An analysis of different definitions [24], models and approaches allow us to conceptually organize a smart city based on a two-dimensional integrated model, as depicted in Fig. 1: horizontal dimension and vertical dimension [3,4].

The *Horizontal* dimension represents a set of four overlapping technological layers: Network and Infrastructure (telecommunication, mobility, energy and environment); Sensors, to collect big data from connected objects in the city; Service Delivery Platform, to elaborate and enhance the big data generated by the other layers; Application and Services which represents the interface with the end users. The *Vertical* dimension includes the application domains in a Smart City: People, Energy, Economy, Mobility, Living, Environment, Planning, Government.

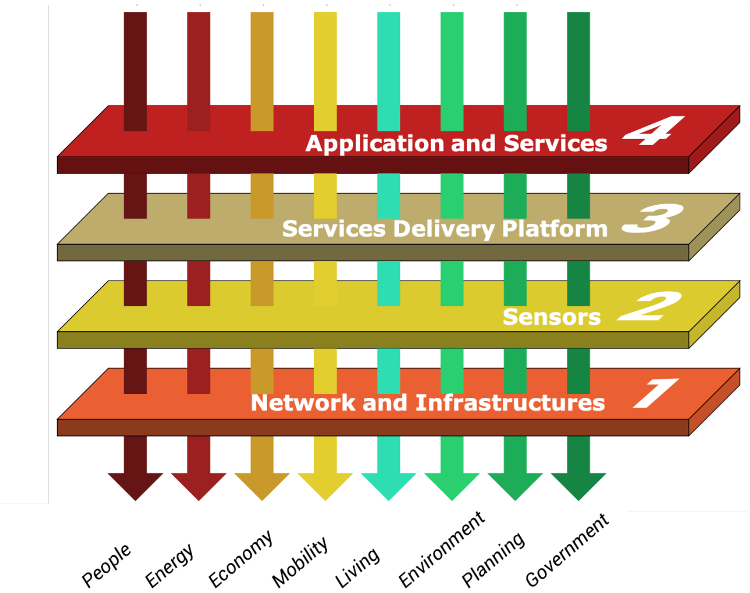
Application and Services 4
Services Delivery Platform 3
Sensors 2
Network and Infrastructures 1
People
Energy
Economy
Mobility
Living
Environment
Planning
Government

Figure 1: The interaction between and Technological Layers (Horizontal) and Application Domains (Vertical)

4. Analysis of Smart Cities Security

The research goal we address is to analyze existing potentially vulnerable devices in Smart Cities, in order to understand the security level of the city, and thus provide support for a secure management of the city. To this aim, we carried out an analysis on Internet-connected devices available in Shodan [25], a search engine that scans the Internet IPs to look for available services. Such services are detected by parsing banners, which are essentially text that allow for identifying login interfaces or certain service characteristics [26]. Therefore, Shodan help to calculate if a target is legitimate or an actual honeypot i.e., an application of deception technique, designed to gather information about the motives and tactics of attackers [27]. It uses a machine learning algorithm that was ported to all of the crawlers in the Shodan network.

The Shodan crawlers continuously update the database in real-time, so that each query returns up-to-date information. The basic algorithm used by crawlers is [28]:

1. Generate a random IPv4 address
2. Generate a random port to test from the list of ports known by Shodan
3. Check the random IPv4 address on the random port and grab a banner
4. Goto 1

Shodan has been used in different research works with the goal of identifying potentially vulnerable IoT devices, an example is [29] whose authors selected a set of search terms to retrieve vulnerable IoT devices with Shodan API and analyze the risk level. In [30], many SCADA devices and webcams were identified using Shodan and with the aim of answering the following questions: “Can Shodan be used for large scale vulnerability analysis on emerging threats? Can Real System exposure and vulnerabilities be verified or quantified?”. Genge et al. expanded the features exposed by Shodan with advanced vulnerability assessment capabilities embedded into a novel tool called Shodan-based vulnerability assessment tool (ShoVAT) [31]. Taking into account the results obtained by such research works the use of Shodan is identified as a good search engine for potentially insecure IoT devices within smart cities.

The research goal and questions have been defined according to the Goal-Question-Metrics paradigm [32,33] as follows:

Research Goal: Analyze Internet connected devices with the aim of characterizing them from a cyber security point of view in the context of Smart City technological layers.

Research Question (RQ): Which are the potentially vulnerable devices according to the horizontal dimension of the model?

Metric: Vulnerable devices (VD): Given a Horizontal Dimension i (HDi), VD(HDi) is equal to the number of IP ports exposed to the Internet for that dimension.

Table 1

Project Distribution

Smart City	#IoT devices
Rome	185.867
Milan	66.276
Turin	45.570
Bari	15.947
Naples	2.498
Total	***316.158***

Selection of the experimental sample. In accordance with the previous research work that investigated the need of Smart Program Management in the smart cities [4] the Italian scenario was selected. In Figure 2 is reported the distribution of webcam in Italy. We selected the 5 cities having the most of webcams for our analysis. These cities are Rome, Milan, Turin, Bari, Naples.

Data Collection. Shodan collects data mostly on web servers (ports 80, 8080, 443, 8443), FTP (port 21), SSH (port 22), Telnet (port 23), SNMP (port 161), IMAP (ports 143, or 993), SMTP (port 25), SIP (port 5060) and Real Time Streaming Protocol (RTSP, port 554). The data collected for each selected device were: City, TCP Port, IoT protocol (e.g., webcam, FTP, industrial devices).

Data Analysis. This step consisted in activities required to produce the analysis, such as data cleaning, data formatting, charts creation.

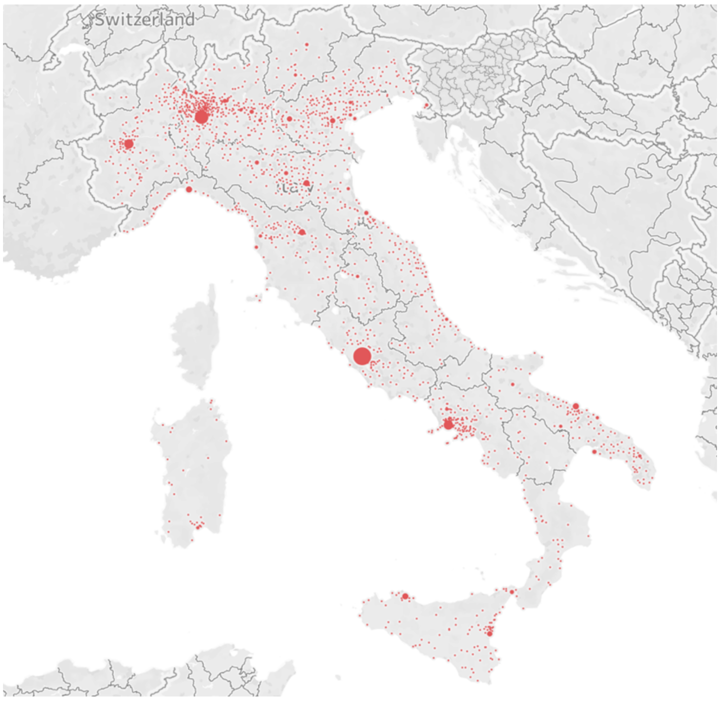

Figure 2: Distribution of webcam in Italy (January 2021)

5. Results

As shown in Table 1, the experimental sample was composed of 5 smart cities and a total of 316.158 devices distributed in the Italian territory.

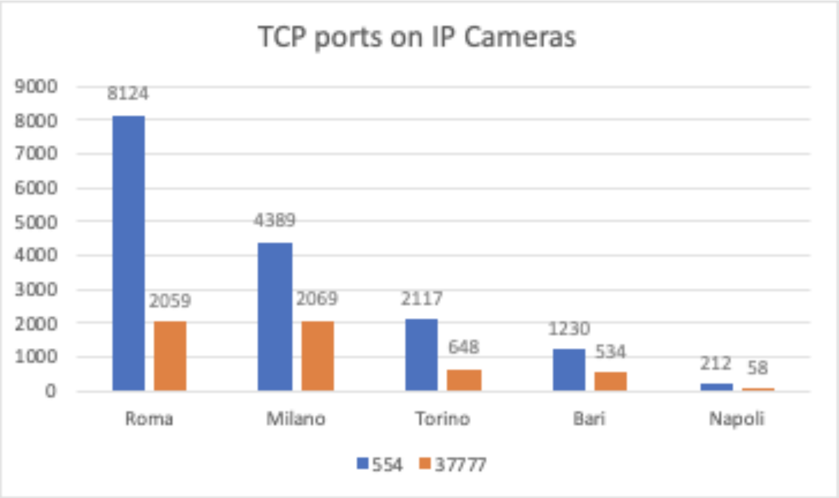

Figure 3: Distribution of webcam in Italy in January 2021

As visible in Figure 3, Rome has the most IP cameras in the considered sample, most of them use 554 port. Even if Milan use half of the IP cameras compared to Rome, the number of IP cameras that use the 37777 port is almost the same. Since the 554 port is considered less secure, we can infer that in Milan more secure webcams are adopted.

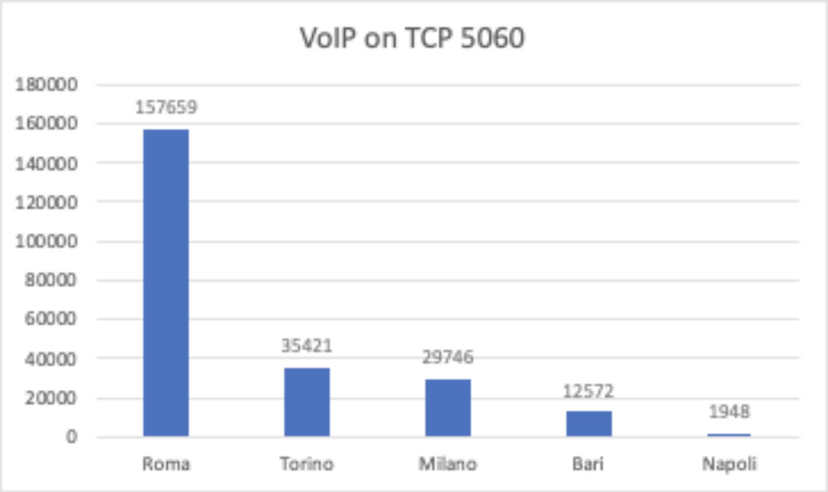

Figure 4: Distribution of devices using VoIP protocol on 5060 TCP port

Figure 4 shows the number of devices that use VoIP on 5060 port. Compared to the previous chart, Rome has the most of devices connected to Internet, but Turin is the second Smart City that use VoIP on 5060 port. This reveals a general tendency to use more voice services in Turin than in Milan, and less webcam.

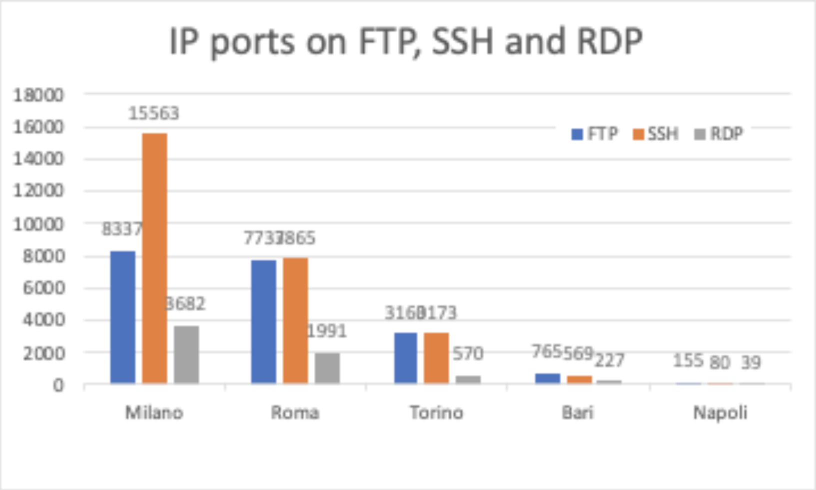

Figure 5: Distribution of devices using FTP, SSH and RDP protocols

Figure 5 reports the use of IP ports for three different services that are used to connect remotely to a device. The data are ordered by the total amount of such services. It is visible that in Milan, more than other cities, such services are used. The analysis reveals that Milan contains the highest number of IP ports in the different protocols. We can see that SSH protocol in Milan is much more used than FTP, revealing more usage of SSH connections that typically are made using terminals. Moreover, in Rome, the number of FTP is almost the same as SSH connections.

Figure 6 reports the number of TCP ports used by industrial devices, ordered by TCP port and, for each port all 5 cities of the sample are reported, ordered by the number of devices. Port 20000 contains the highest number of devices, and then 102, 1911, and the others follows. It is very visible that Milan has the highest number of TCP ports. This reveals a high traffic through industrial devices, which also reveals the industrial soul of the city, that is projected to innovation and progress. Turin is the second city in the use of industrial devices, which is not surprising, considering the industrial history of this city. What is surprising is Rome, on the port 20000. Such ports are more used on SCADA systems, which are intended for monitoring and controlling distributed industrial systems. It is reasonable to think that being a bigger city than Turin, Rome has the highest number of such systems and thus uses more devices that use 20000 TCP port.

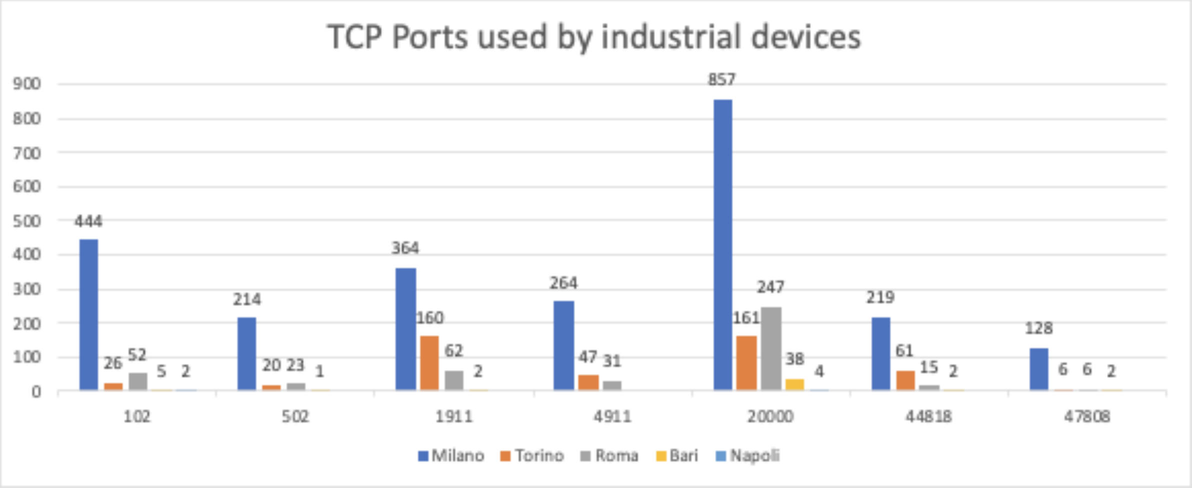

Figure 6: Distribution of devices using TCP Ports

6. Discussions

We have collected data about existing IoT devices in Italy in January 2021 using the Shodan search engine. We have defined a bi-dimensional model to perform our analysis, it considers a horizontal dimension that is composed of four layers (see. Section 3); the vertical dimension considers 8 different domains. We focused on the horizontal dimension that is composed of the layers: 1) Network and Infrastructure; 2) Sensor; 3) Service Delivery Platform; 4) Application and Services. From the analysis of such IoT devices, disaggregated by port, protocol and city we derived some assumption that we are going to discuss here according to the research question reported in Section 4: Which are the potentially vulnerable devices according to the horizontal dimension of the model?

We observed that most of the devices focus on layer 1) and 4) that means most of the threats may come from exploiting vulnerabilities on VoIP, FTP, SSH and RDP, TCP ports on IP Cameras (level 4) and on industrial devices (level 1). While this may be obvious, it is interesting to analyze the different distribution in different cities, according to the various services and devices.

The cities with the highest number of IoT devices are Rome, Milan and Turin. The different distribution of devices reveals the different city organization in terms of technological infrastructure and services to the citizens.

Regarding the level 1) of the model, Rome is the city with the highest number of IP webcams, which reveals more control on security on the streets and public spaces. This is reasonable, if we consider that Rome is a Capital and also a very touristic city. Rome has the highest number of devices that use VoIP protocol, followed by Turin and then Milan, this is a bit surprising because Milan is a European city very oriented to business, so it would have been reasonable to find Milan in the first place. In any case this information has to be considered in the protection against cyber-attack.

Regarding the level 4) of the model we see as Milan emerges with the very high presence of ports used for remote connection, file exchange, and remote control in industrial contexts. Indeed, FTP, SSH and RDP are mainly present in Milan, followed by Rome with around a half of the devices found in Milan. This is in accordance with the TCP ports used in industrial contexts, such as SCADA systems or PLC remote control of industrial settings (such as trains, airports). Milan in general is followed by Turin in terms of number of devices that regard the layer 4), but there is an exception related to port 20000 which is used typically for distributed systems to monitor and control trains, buses, airports, and the likes. Rome actually has more infrastructure than Turin, this means that Rome is more exposed than Turin in terms of security in the layer 4).

7. Limitations and Threats to Validity

In order to provide the reader with all the elements for evaluating the presented results, possible experimental threats to validity, consistency, magnitude of the results and transferability are analyzed below. Threats to *validity*, internal validity, or credibility, is related to the extent that the results match the meanings and knowledge constructed in the investigated context.

To increase credibility in the study, we tried to achieve maximum variation collecting data from IoT devices to different smart cities. We selected the top 5 Smart Cities that have the highest number of webcams in the first round of analysis and then focused on the analysis across all the IoT devices obtained for different cities. *Consistency* refers to whether the researchers did not make any inference that cannot be supported by the data. To increase consistency, we performed all data analysis in groups. The analysis was performed by one researcher and reviewed by all the other researchers. Member checking was also used to check the consistency of our interpretations. Inconsistencies among researchers were resolved in consensus meetings. We used the Framework Method to enhance the consistency of data analysis among the researchers [34]. Finally, regarding the *magnitude of the results*, in this work 316.158 IoT devices from 5 Italian smart cities were analyzed and this represents a limit as the sample size is lower than the total number of Internet connected devices. Furthermore, the selected devices are not worldwide and refer only to Italian Smart Cities.

Therefore, we do not claim generalization of our results to a large population in a positivist perspective. Instead, we believe that the analysis carried out by a search engine such as Shodan on potentially vulnerable devices connected to the network is a good starting point to have a vision on the

Security Smart Cities. The use of a common search engine supported good analytical generalization increasing the potential of *transferability* [35] of the findings to other contexts.

8. Conclusions

The research work presents an overview on the security technological levels in the Italian Smart Cities. An analysis on Internet-connected devices available in Shodan was carried out in order to achieve our goal, i.e., understand the security levels of the cities, and thus provide support for a management that includes security. We analyzed 316.158 IoT devices from 5 Italian smart cities and the results obtained show that the most vulnerable devices focus on Infrastructure and Network (layer 1) and Application and Services (Layer 4). This represents a first step of our research that aims to investigate the impact of security in a complex context such as Smart Cities. We are planning to perform a more extended analysis on all Italian cities.

The results of the vulnerability study can be better presented by mapping services to specific risk levels. This type of metric could be useful to derive a final vulnerability risk level of the smart city. The presentation of the overview of the data can benefit from specific visualizations [36] that are capable to show data in little space and give to the observer an immediate overview. This will lead also to another positive outcome, if the visualization shows immediately the data, it can be used real-time to allow the user to see data instantly. This will then lead to a successive step, that is to represent the evolution of data over time.

9. References

[1] British Standards Institution. (2014). Smart Cities—Vocabulary. Last accessed on 12 February 2021, http://shop.bsigroup.com/ upload/PASs/Free-Download/PAS180.pdf.

[2] Trend Micro. (2017). Securing Smart Cities: Moving Toward Utopia with Security in Mind. Last accessed on 12 February 2021, https://documents.trendmicro.com/assets/wp/wp-securing-smart-cities.pdf

[3] Baldassarre, M. T., Santa Barletta, V., Caivano, D. (2018). Smart Program Management in a Smart City. In 2018 AEIT International Annual Conference (pp.1–6). https://doi.org/10.23919/AEIT.2018.8577379

[4] Barletta, V.S.; Caivano, D.; Dimauro, G.; Nannavecchia, A.; Scalera, M. Managing a Smart City Integrated Model through Smart Program Management. Appl. Sci. 2020, 10, 714. https://doi.org/10.3390/app10020714

[5] Baldassarre, M.T., Barletta, V.S., Caivano, D., Raguseo, D., Scalera, M., Teaching cyber security: The hack-space Integrated model (2019), CEUR Workshop Proceedings, 2315, ISSN: 16130073

[6] Gretzel, U., Werthner, H., Koo, C., & Lamsfus, C. (2015). Conceptual foundations for understanding smart tourism ecosystems. Computers in Human Behavior, 50, 558–563. https://doi.org/10.1016/j.chb.2015.03.043

[7] Ralko, Shawn and Kumar, Sathish, "Smart City Security" (2016). KSU Proceedings on Cybersecurity Education, Research and Practice. 10. Last accessed on 12 February 2021, https://digitalcommons.kennesaw.edu/ccerp/2016/Academic/10

[8] Barletta, V.S.; Caivano, D.; Nannavecchia, A.; Scalera, M. Intrusion Detection for in-Vehicle Communication Networks: An Unsupervised Kohonen SOM Approach. Future Internet 2020, 12, 119. https://doi.org/10.3390/fi12070119

[9] ENISA. (2015). Cyber security for Smart Cities. An architecture model for public transport. Last accessed on 12 February 2021, www.enisa.europa.eu

[10] Ismagilova, E., Hughes, L., Rana, N.P. et al. Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework. Inf Syst Front (2020). https://doi.org/10.1007/s10796-020-10044-1

[11] Rambus. Smart Cities: Threat and Countermeasures. Last accessed on 12 February 2021, https://www.rambus.com/iot/smart-cities/

[12] Baldassarre, M.T.; Barletta, V.; Caivano, D.; Scalera, M. Integrating security and privacy in software development. Softw. Qual. J. 2020, 1–32. https://doi.org/10.1007/s11219-020-09501-6

[13] Baldassarre M.T., Barletta V.S., Caivano D., Scalera M. (2019) Privacy Oriented Software Development. In: Piattini M., Rupino da Cunha P., García Rodríguez de Guzmán I., Pérez-Castillo R. (eds) Quality of Information and Communications Technology. QUATIC 2019. Communications in Computer and Information Science, vol 1010. Springer, Cham. https://doi.org/10.1007/978-3-030-29238-6_2

[14] Adel S. Elmaghraby, Michael M. Losavio. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of Advanced Research, Volume 5, Issue 4, 2014, pp. 491-497, ISSN 2090-1232, https://doi.org/10.1016/j.jare.2014.02.006.

[15] Kaźmierczak, J., Loska, A., Kučera, M., & Abashidze, I. (2018). Technical Infrastructure of "Smart City": Needs of Integrating Various Management Tasks. https://doi.org/10.13140/RG.2.2.28936.52489

[16] Batty, M. (2013). Big data, smart cities and city planning. Dialogues in Human Geography, 3(3), 274–279.

[17] Chatterjee S, Kar AK, Dwivedi YK, Kizgin, H. (2019). Prevention of cybercrimes in smart cities of India: from a citizen's perspective. Information Technology & People. 32(5): 1153-1183. https://doi.org/10.1108/ITP-05-2018-0251

[18] Sujata Joshi, Saksham Saxena, Tanvi Godbole, Shreya (2016). Developing Smart Cities: An Integrated Framework. Procedia Computer Science, Volume 93, 2016, pp. 902-909, ISSN 1877-0509. https://doi.org/10.1016/j.procs.2016.07.258.

[19] Kumar, S.A., Vealey, T., Srivastava, H. (2016). Security in Internet of Things: Challenges, Solutions and Future Direction. 2016 49th Hawaii International Conference on System Sciences (HICSS). Pages 5772-5781.

[20] Anthopoulos, L., Janssen, M., & Weerakkody, V. (2019). A Unified Smart City Model (USCM) for smart city conceptualization and benchmarking. In Smart Cities and Smart Spaces: Concepts, Methodologies, Tools, and Applications (pp. 247–264). IGI Global.

[21] Angelidou, M. (2014). Smart city policies: A spatial approach. Cities, 41, S3–S11. https://doi.org/10.1016/j.cities.2014.06.007

[22] Höjer, M., & Wangel, J. (2015). Smart Sustainable Cities: Definition and Challenges. In L. M. Hilty & B. Aebischer (Eds.), ICT Innovations for Sustainability (pp. 333–349). Cham: Springer International Publishing.

[23] Giffinger, R., & Gudrun, H. (2010). Smart cities ranking: an effective instrument for the positioning of the cities? ACE: Architecture, City and Environment, 4(12), 7–26.

[24] Baldassarre, M., Piattini, M., Pino, F.J., & Visaggio, G. (2009). Comparing ISO/IEC 12207 and CMMI-DEV: Towards a mapping of ISO/IEC 15504-7. 2009 ICSE Workshop on Software Quality, 59-64. doi: 10.1109/WOSQ.2009.5071558

[25] Shodan, https://www.shodan.io/ Last accessed on 12 February 2021

[26] Fernández-Caramés, T.M.; Fraga-Lamas, P. Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases. Sensors 2020, 20, 3048. https://doi.org/10.3390/s20113048

[27] Rae, J. S., Chowdhury, M. M., Jochen, M. Internet of Things Device Hardening Using Shodan.io and ShoVAT: A Survey, 2019 IEEE International Conference on Electro Information Technology (EIT), 2019, pp. 379-385, doi: 10.1109/EIT.2019.8834072.

[28] Matherly, J. Complete Guide to Shodan. Collect. Analyze. Visualize. Make Internet Intelligence Work for You. Available online: https://www.amazon.com/Complete-Guide-Shodan-Visualize-Intelligence-ebook/dp/B01CDIU880. Last accessed on 12 February 2021

[29] Williams, R., McMahon, E., Samtani, S., Patton, M., Chen, H. Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI), 2017, pp. 179-181, doi: 10.1109/ISI.2017.8004904.

[30] Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., Chen, H. Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT). 2014 IEEE Joint Intelligence and Security Informatics Conference, 2014, pp. 232-235, doi: 10.1109/JISIC.2014.43.

[31] Genge, B.; Enăchescu, C. ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services. Secur. Commun. Netw. 2015, 9, 2696–2714

[32] Ardimento, P.; Baldassarre, M.T.; Caivano, D.; Visaggio, G. Multiview Framework for Goal Oriented Measurement Plan Design. In Product Focused Software Process Improvement; PROFES 2004. Lecture Notes in Computer Science; Bomarius, F., Iida, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3009.

[33] Caivano, D., Fernandez-Ropero, M., Pérez-Castillo, R., Piattini, M., Scalera, M. Artifact-based vs. human-perceived understandability and modifiability of refactored business processes: An experiment. 2018. J. Syst. Softw. 144, 143–164. https://doi.org/10.1016/j.jss.2018.06.026.

[34] Gale, N.K., Heath, G., Cameron, E., Rashid, S., Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. BMC Medical Research Methodology 13, 117. https://doi.org/10.1186/1471-2288-13-117

[35] Merriam, B. S., Tidell E. J. (2015). Qualitative Research: A Guide to Design and Implementation. 4th Edition. Jossey-Bass, San Francisco. ISBN: 978-1-119-00361-8ir

[36] Buono P., Costabile M., Legretto A., Marra P. (2021) An Experience on Cooperative Development of Interactive Visualizations for the Analysis of Urban Data. In: Reis T., Bornschlegl M.X., Angelini M., Hemmje M.L. (eds) Advanced Visual Interfaces. Supporting Artificial Intelligence and Big Data Applications. AVI-BDA 2020, ITAVIS 2020. Lecture Notes in Computer Science, vol 12585. Springer, Cham. https://doi.org/10.1007/978-3-030-68007-7_11