

# Reading a Scientific Article

November 1, 2021

# Chapter 1

## Reading an article

### 1.1 Accessing the article

I chose to read the article on “Comparing anomaly-detection algorithms for keystroke dynamics.” by Kevin S. Killourhy and R. Maxion [1]. There were multiple sources where I found this article available, such as ResearchGate or IEEE explore. Since all of them were the same, choosing which source to use was not important in this case. However, I chose ReasearchGate in order to generate a formatted citation form for this paper.

### 1.2 Publication

This article was published in the Conference Proceeding entitled “International Conference on Dependable Systems and Networks” held in 2009 [2]. Conferences are the most interactive way of presenting and publishing an article. The author, most often, also have some sort of presence at an event where they talk and present their work. In this case, the outreach can also be highly increased and getting more people closely involved in the work is easier. The field of this conference is obviously Computer Science, while it aims more towards, what is specified in the title: “Dependable Systems and Networks”.

I think the choice of this medium of publication is made because maybe the authors aimed for a higher reach and with trying to get the people to understand while talking about their work. At the same time, they also maybe wanted a more open debate on their work, where people could probably start asking questions as well.

### 1.3 Purugganan and Hewitt's technique

Coplete citation: Kevin S. Killourhy and R. Maxion, 29 September 2009, Comparing anomaly-detection algorithms for keystroke dynamics, International Conference on Dependable Systems and Networks (DSN).

Web Link: <https://ieeexplore.ieee.org/document/5270346> (Accessed 31-10-2021)

Keywords: None specified

General subject: The study of keystroke pattern recognition and anomaly detection in such algorithms.

Specific subject: To “collect a keystroke-dynamics data set” and to analyze different classification and detection algorithms with a fair measure of performance in what stands anomaly detection.

Hypothesis: Using anomaly detection algorithms in password typing can reduce the risk of fraudulent attempts to steal accounts.

Methodology: The methodology section is divided into 3 parts: collection of data, detector implementation and evaluation.

Results: The 14 detectors were evaluated using statistical significance. The best rate was obtained by the Manhattan (scaled) detector.

Summary of key points: Password cracking can be detected using anomaly detection algorithms, but the rate of recognition is not yet high enough with any of the 14 evaluated ones, thus it can not be widely used, yet.

Context: This article is directly connected to any password cracking and cyber security researches. In most of the cases, the target of cyber attacks that contain password cracking are individuals, but a lot of in-house password cracking is used in companies as well! This article can be easily contextualized in a day-to-day life by almost anyone nowadays.

Significance: The most important thing about this article is that it proves that there is a lot of possible improvement in his field in the sense of anomaly detection. It proves that this anomaly detection algorithms are still lacking and that they can not be used in practice yet.

Important Figures and/or Tables: Table 2 page 8

## 1.4 References

One article that drew my attention is “Identity authentication based on keystroke latencies” by Rick Joyce and Gopal Gupta. This article, after some inspection seems to be a more in-depth analysis of such algorithms of authentication, which is an interesting topic and closely related to the initial article. [3]

One article that cites this selected article is called “RHU Keystroke: A mobile-based benchmark for keystroke dynamics systems” [4]. This article tries to analyze similar behaviours, however, this time, on a mobile screen with touch sensitivity. This is interesting as the mobile platforms are growing in popularity.

## 1.5 IMRD

Firstly, the article that I initially chose does not necessary follow the IMRD format. There is one reason that this article does not follow this specific format strictly, and that is that sometimes, in these types of articles, more information is needed than what can be categorized in this subsection. A lot of the times, a good background introduction is needed in the field of Computer Science.

At the same time, the article on “Graphs over time: densification laws, shrinking diameters and possible explanations.” also does not implement the same standard strictly. For example, in this article, the main point of difference is the fact that there is also a proposed model section. Articles can vary by their structure according to what they actually represent.

## 1.6 Citations

The article that I have chosen has been cited for 224 times in other papers and for 11 times in patents.

## 1.7 Contribution

The article that I chose contributes to the analysis and development of cyber security, as well as computer science in general, as it proves limitations of specific algorithms.

# References

- [1] K. Killourhy and R. Maxion, “Comparing anomaly-detection algorithms for keystroke dynamics,” 08 2009. doi: 10.1109/DSN.2009.5270346 pp. 125 – 134.
- [2] “International conference on dependable systems and networks (dsn),” 08 2009. doi: 10.1109/dsn15427.2009
- [3] R. Joyce and G. Gupta, “Identity authentication based on keystroke latencies,” *Commun. ACM*, vol. 33, no. 2, p. 168–176, Feb. 1990. doi: 10.1145/75577.75582. [Online]. Available: <https://doi.org/10.1145/75577.75582>
- [4] M. El-Abed, M. Dafer, and R. E. Khayat, “Rhu keystroke: A mobile-based benchmark for keystroke dynamics systems,” in *2014 International Carnahan Conference on Security Technology (ICCST)*, 2014. doi: 10.1109/CCST.2014.6986984 pp. 1–4.