Certain cybersecurity: the impossible dream

Kaled Aljebur, Mostfa Albdair, Ron Addie, *Member, IEEE,*

***Abstract*—The abstract goes here.**

I. Introduction

One of the most important themes in the history of the philosophy of science, initiated by David Hume, has been the difficulty of inductive reasoning, i.e., how are we able to infer facts from observations. Karl Popper's "solution" to this problem is that the scientific method is really about trying to find evidence *against* a hypothesis, and when such evidence cannot be found, despite our best efforts, this can be regarded as strong evidence *for* the hypothesis. Popper's resolution was, and remains, quite influential.

However, this debate has not ceased since Popper's contribution. Other key contributions were made by Kuhn, and xx, but there is still no universally accepted resolution.

However, more pragmatically, this question is also addressed by statistics. Furthermore, statistics has quantitative procedures.

Even so, statistics also has some really difficult foundational issues that are not just theoretical. Fundamentally, statistical reasoning relies on assumptions, just like deductive reasoning. In particular, we have to adopt a model. Naive practitioners (and that is the vast majority, esp given that most of them are not actually educated in statistics), like to believe that it is satisfactory to pick a standard statistical method and apply it. This is, after all, what they are taught to do. In fact, not behaving this way is regarded by most users of statistics as unorthodox, and unsound.

So, statistics is really the modern form of inductive reasoning, and it is certainly a lot better defined than the philosophical concept of inductive reasoning.

But, what about deductive reasoning?

The "default" viewpoint is that we only use this in mathematics, or perhaps for going from one set of assumptions to another. But cybersecurity, and especially public key cryptography, and also block-chain techniques, seem to suggest that we can effectively use deductive reasoning about the real world.

In cybersecurity, the essential problem is to prove that something is impossible. (You could call it "the impossible dream", i.e. not dreaming about achieving something impossible, but rather dreaming that we can make something not wanted impossible). This is, in general, difficult. However, here is a simple example of how deductive reasoning can easily achieve it.

Suppose I ask you to draw a right-angle triangle, on a flat surface, with sides of length 3, 4, and 6. (Yes: 6). The right answer to such a request is to say: "No, I can't do that. It is impossible.". You can show this by deductive reasoning. But the statement is about a real-world event: drawing a triangle. This has nothin to do with the precision of the measurements. The inaccuracy can be quantified. Even an approximately 3,4,6 right-triangle is impossible. There are events, even with approximate measurements, which can be proved to be impossible. Granted, the impossibility of non-pythagorean triangles doesn't seem to help a lot in cybersecurity, but what if we can entangle real world events in mathematically precise statements in such a way that the events themselves become impossible?

We can, and already do this, using similar reasoning to the above, concluding that certain cybersecurity events can't happen: this is what is happening when certificates are used, and digital signatures. Conventional wisdom, from the background of science, statistics, and experimental methods, strongly suggests that certainty of this sort is impossible. But the triangle shows that the problem is not with deducing impossibility. Deducing impossibility is possible! But can we employ such deductions?

I think we are already doing so, and there will be a lot more such deductions in the near future.

This demo file is intended to serve as a "starter file" for IEEE journal papers produced under LATEX using IEEEtran.cls version 1.6b and later. May all your publication endeavors be successful.

mds
November 18, 2002

A. Subsection Heading Here

Subsection text here.

1) Subsubsection Heading Here: Subsubsection text here.

II. Conclusion

The conclusion goes here.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

Appendix two text goes here.

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LATEX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.