Open access Journal International Journal of Emerging Trends in Science and Technology

Cyber-Science and Cyber Security

Author
Dr Daruri Venugopal
M.Sc; M.Phil; M.Tech; Ph.D.(Post.Doc.)
Dept. of Computer Scinece & Engineering
Siddhartha Institute of Technology and Sciences
Narapally, Ghatkesar, R.R.Dist.
Email: *Profdarurivg.edu@gmail.com*

Abstract
In Cyber Science cyber-security, anyone can evaluate whether there are underlying fundamental principles that would make it possible to adopt a more scientific approach, identify what is needed in creating a science of cyber-security, and recommend specific ways in which scientific methods can be applied. Our study identified several sub-fields of computer science that are specifically relevant and also provides some recommendations on further developing the Cyber science.
Keywords—*Scientific method ; recommend ; scientific approach*

Introduction

The need to secure computational infrastructure has become significant in all areas including those of relevance to the Cyber Security and the intelligence community. Owing to the level of interconnection and interdependency of modern computing systems, the possibility exists that critical functions can be seriously degraded by exploiting security flaws. While the level of effort expended in securing networks and computers is significant, current approaches in this area overly rely on empiricism and are viewed to have had only limited success.We can examine the theory and practice of cyber security, and we can evaluate whether there are underlying fundamental principles that would make it possible to adopt a more scientific approach, identify what is needed in creating a science of cyber-security, and recommend specific ways in which scientific methods can be applied. The challenge in defining a science of cyber-security derives from the peculiar aspects of the field. The "universe" of cyber-security is an artificially constructed environment that is only weakly tied to the physical universe. Therefore, there are few a priori constraints on either the attackers or the defenders.

Importance of the Cyber science

There are several areas that are traditionally a part of computer science that have contributed in the past to a deeper understanding of cyber-security and where increased future emphasis could bring continued improvement. The field of model checking seems particularly relevant in that one creates a model for the security of a given system or key kernel and then tests the assumptions using a well defined set of possible inputs. While the input space is potentially infinite, the benefit is that specific threats can be modeled.

- The area of cryptography has traditionally focused on provable aspects of secure communication with careful attention paid to the nature of assumptions.

Problem statement

Our current security approaches have had limited success and have become an arms race with our adversaries. In order to achieve security breakthroughs we need a more fundamental understanding of the science of cyber-security. However, we do not even have the fundamental concepts, principles, mathematical constructs, or tools to reliably predict or even measure cyber-security.

" Is there reason to believe the above goals are, in principle, not achievable ?

There is every reason to expect that significant progress can be made toward the above goals. One must first understand the nature of the scientific enterprise for cyber-security and characterize the objects under discussion. There is a great deal of valuable science that can be accomplished if an accepted approach to discourse can be developed. While these primarily technical activities will not in and of themselves "solve" the cyber-security problem given that it has both technical and social aspects, they will significantly aid progress.

Objectives

Our study identified several sub-fields of computer science that are specifically relevant. These include model checking, cryptography, randomization, and type theory. In model checking, one develops a specification of an algorithm and then attempts to validate various assertions about the correctness of that specification under the specific assumptions about the model. Model checking provides a useful and rigorous framework for examining security issues. Cryptography, which examines communication in the presence of an adversary and in which the assumed power of that adversary must be clearly specified is viewed today as a rigorous field, and the approaches pursued in this area hold useful lessons for a future science of cyber-security

Hypothesis

Actions in this universe consist of sequences of changes to binary data, interleaved in time, and having some sort of locations in space. One can speculate as to why mathematics is so effective in explaining physics, but the cyber-world is inherently mathematical. Mathematics is a natural way for reasoning about it and this point of view is a theme that appears repeatedly in this report. Second, cyber-security has good guys and bad guys.

Conclusion & Recommendations

The science seems underdeveloped in reporting experimental results, and consequently in the ability to use them. The research community does not seem to have developed a generally accepted way of reporting empirical studies so that people could reproduce the work and use the results.

There have been lots of reports on the need for R&D for cyber-security. There is universal agreement that more work is needed. We couldn't find anyone who even felt that there is already enough known, and all that is needed is to apply current knowledge. Cyber-security is a problem that may be manageable, but not only is it not solvable, there's no agreement that it is being managed well.

These programs should have a long time horizon and periodic reviews of accomplishments." Centers and programs sponsored by the Department of Defense have several attractive features. First, they give the sponsors access to the best ideas and people. Informal relationships are particularly important in this area.

References

1. T. Alpcan and Bas¸ar T., Network Security: A Decision and Game Theoretic Approach. Cambridge University Press, 2011.
2. Al Bessey, Ken Block, et al., A few billion lines of code later: Using static analysis to find bugs in the real world. software systems. Communications of the ACM, 53, 2010.
3. LeventaButtyan and Jean-Pierre Hubaux, Security and Cooperation inWireless Networks.Cambridge University Press, 2007.

4. Michael R. Clarkson and Fred B. Schneider, Hyperproperties. In CSF 2008: 21st IEEE Computer Security Foundations, Symposium. - Foundation Conference, Pittsburgh, PA, JUN 23-25, 2008.
5. UlfarErlingsson, Low-level software security: Attacks an AudunJosang, Security protocol using spin. Proc. TACAS96, LNCS, 1996.

Author Profile

Prof. Daruri Venugopal received the Bachelors and M.Sc. degrees in Mathematics from Osmania University in 1995 and 1997, respectively. He done his M.Phil Mathematics from Algappa University in the yer 2003. He Done his Doctorate from NITK, Surathakal in the year 2006 in Computer Science Engineering. He done his M.Tech Computer Science Engineering from JRN Deemed University in 2007. Presently he is perusing the Post. Doct.Programme in Computer Scinece Engineering.
Presently working as Professor & Dean of Siddhartha Group of Institutions, Ghatkesar, Hyderabad.