Inquiry 1: Algorithm Analysis, Algorithm Correctness, and Distributed Algorithms

Abstract

The three reading for this week focused on algorithms and how to conduct different analysis methods and correctness along with the distributed nature of computer systems in today's environment. It is safe to say that algorithm use helps us understand how a computer operates no matter the programming language. By conducting analysis and verifying the correctness of the algorithm, it has a significant impact on such things as storage and times requirements. The complexity of an algorithm is a function that describes its efficiency regarding the data that is required to process the algorithm. The complexity analysis article looks into different ways such as worse case analysis, asymptotic behavior, and Big-O notation. The second article discusses the formal verification of mathematical algorithms. Since computers are used in safety and critical systems where human life is affected, it is imperative to have a formal process in place to catch any errors in design. Formal verification is the process to mathematically proves the correctness of design on a formal mathematical specification. The three major approaches used in formal verification are a Symbolic simulation, temporal logic model checking, and general them proving. One of the modern theories used is the HOL Light theorem prover. The advantage of using this approach is that it utilizes the underlying pure mathematics, the formalization of floating point operations, proof of exclusion zone properties, relative error computation for rounding, and number theoretic isolation. Since this HOL is programmable, it allows for automation which cuts down on the amount of human interaction and speeds up the verification process. The third article discusses the distributed nature of our computer systems. A distributed system is a series of computers that appear to a single system to the user. It can include anything from computers, processes or processors. Several advantages to distributed systems are economics, speed, inherent distribution, reliability, incremental growth. In this environment, distributed algorithm act as routers within the network. Leader Election, distributed broadcast routing, distributed unicast routing, multicast routing, and parallel algorithms are used to help understand the complexity of a distributed algorithm. In closing, algorithms are the heartbeat of computations within our information systems, and the process is needed to help understand the complexity and resources required.

Inquiry 2: Topics in Computer Science in my company

I work for Sentek Global Inc. which is a consulting company for the Department of the Navy. We provide various Information Technology (IT) services, but the biggest is IT security. As security control assessor, I see all types of hardware/software systems deploying out to the Navy, and I must say I am astonished at the lack of security concepts most of these systems have. Of course working with such a large infrastructure such as the Navy, most of the topics listed I see and deal with routinely. I'm going to touch on the security aspect first and then discuss some of the other topics. Costs seem to be the overwriting reason for not building security into their designs. Of course the proper research on the costs of security by design and trying to provide security after the fact. It horrifies me to think that systems that provide life or death consequences have such little respect for its security posture. I too served in the Navy, and if I knew then what I know now from working in this industry, I would strongly recommend that the Navy push harder for research in cybersecurity. We hear it every day in the news and it still surprisingly taken to lightly until a compromise happens. By then it is too late. Supporting digital democracy starts with understanding the risks involved. The only way to accomplish this is to conduct the research necessary and communicating the risks to people. By doing this, the hope is for the understanding of costs both tangible and intangible. Too many times I see the look how much I saved today vice tomorrow.

Another area where I routinely deal with is the topics of Abundant-data applications, algorithms, and architectures. My job deals with determining risks to a particular architecture of a system. The challenging part to this is new accreditations are coming to us where the development and testing were conducted in a lab environment. Once it comes to me and me evaluate their test data, a risk determination is provided, and authorization to operate (ATO) is granted based on the risk. What tends to happen is once the program or application is installed in its operational environment, modifications are made to the system whether to process or simply needed to work properly, which invalidates the ATO. The challenge lays with duplicating the operational environment with a Navy ship. There is a research sector within the contract to support such techniques, but I have seen it not used within its purpose. Most of the time it is used on site assessments on why something is not working as intended. It is because of the different applications, and architectures available. Not enough funding is provided in the research and development department and ensuring it is used in this aspect.

Areas of emerging technologies for computing hardware, communications and sensing is also and area of conern in my office. As we assess security controls, mitgations and remidations, we constantly find new techonolgies that the programs are using and with little to no information about how these systems are incorarated into the arcittecture. Usally when we collabaratrate to try and come to an understanding for an risk determination, we are left with no altenrnative but to issue a high risk due to lack of communication and informationa about the product. Reasearch and communication at the beginning stage of this accreradaton cycle would of atleast provided and understanding to the security control assesser. It may not have changed the risk but at least we can effectively communicate and provide a meaningful collaration on a way forward to allow an authoriazation to operate with the lowest risk possible. This technology also roles into the large scale networking that I deal with. Something as complex as the nework configuration of the Naby both ship and shore is a dauthing task to try and understand. We usually have about 4 hours to asses and provide a risk dertmiation to the program. As you can probably guess, this process requires a lot of research that we just do not have the time for. We are depended on the program to provide us the nessceccsry information. I could go on on and with just about every task listed inn the assignment but wanted to just mention these in particular because this is were I belive the industry is lacking in research.