SME_and_PR Material for TETRADYN and CADS Use

CUBIT and Cyber Net Security and Net Health

Topic:
The connection between CUBIT Core Logic with Cyber Net Security and Net Health

Article:

Our need to think more virally, more biologically, for our information security and cyber defense, and a way to apply something from the biomedical domain to the cyber domain. We need to learn from the primal and basic life forms, and how we deal with threats in the biological space, in order to attain and sustain health and wellness in the cyber space.

In general, our society's approach to treatment of cyber network security and incidents of attack is not that much different from that towards infectious diseases such as influenza, salmonella, e.coli, and others. Most people and most institutions operate not on principles of wellness maintenance and preventive medicine but on reaction to and treatment of symptoms. This may be termed an "allopathic" response technology, or philosophy, or psychology, and it is one that can be very expensive and even fatal in the long run. It is often a practical and short-term economical way to "get by" and deal with problems if and only if they arise and hit you in the face. Or stomach, or heart, or online credit system, or customer database, or government website.

There have been many variations of cyber network attacks over the years and almost as many motivations and purposes underlying their origins. What we see definitively in recent years and months is an accelerating maturation of techniques and organization among the attackers. While sporadic prankster-hackers still abound and will never be eradicated entirely, the fact is simple and unmistakeable that attackers are more sophisticated in purpose, motivation, method and discipline. Many attacks bear the mark of state-based plans intended to disrupt (or to test-feel the defenses for a later disruption) some critical aspect of another nation's financial, military, healthcare, or energy infrastructures. Other attacks bear the marks of organized but quasi-non-state terrorist organizations. By far, however, many have signs of being the work and the toolkits of organized criminal groups who are using the penetrations, disruptions, and espionage activities to simply and very effectively gain capital by stealing it from or otherwise cheating their victims.

Here is simply one recent article, this from BBC World News (July 14, 2009; http://news.bbc.co.uk/2/hi/technology/8149034.stm). In it, Maggie Shiels writes, "Cyber crooks are increasingly operating like successful businesses, deploying the same tools legitimate companies use to boost their profits." She points out what network developers such as Cisco are saying and doing, and what people who are deep in the world of anti-virus protection, computer and network security, and internet-crime law enforcement are saying and doing about a problem that has changed before our eyes in a matter of a few years.

As Cisco spokesman Patrick Peterson stated, "Capitalism is a powerful force and these criminal types are collaborating with one another and sharing resources, renting out botnets and forming alliances." Utilizing off-the-shelf spyware and web-based services that can check performance on

a given user's PC, the criminals organizing attacks are actually able, through their enhanced economic means and alliances among each other, able to test out how well a piece of malware is performing and to then make improvements on the viral or worm software in order to better defeat protective measures in place on the PCs of individuals or corporations.

Cybercrime is big business, organized business, and it is getting to be, more and more, all about big and organized profiteering. Meanwhile, most of the world and most organizations, both in the private corporate sector and particularly within government agencies and bureaucracies, are bogged down in what is not even good, old-fashioned allopathic medicine. What's been going on in the name of cyber network security and defense has been mostly a process of waiting to be mugged and then hoping to have a policeman nearby to go running after the criminal down the darkened alley, without much knowledge of the streets, the profile of the mugger, or the nature of who's who in the neighborhood as far as friend or foe.

We can learn a lot from biology and in particular microbiology that can help us to build a better immune system, and it is exactly that which we need to have, to have more of, and to concentrate our energies upon. I am referring to how our bodies work with their immune systems in order to provide effective filters and defenses against intruders that will generally turn our bodies into simply food, or a factory, for the benefit of the new competing species (bacteria, virus, parasite, etc.). We can also gain from using tools and resources, including some fundamental methodologies and architectures, that have been designed and tested in a variety of operational environments, for responding to dispositions, threats, outbreaks, and even widespread epidemics or pandemics in the biological space. Here I am speaking about infectious diseases, like influenza and also food-borne or community-based diseases such as salmonella, e.coli, norovirus, or MRSA, and new approaches that are very network-intensive, community-focused, and adaptive/responsive, such as:

CUBIT (Coordinated Biothreat Intervention and Treatment) - and within it -
CRAIDO (Community Rapid Response Diagnostics for Infectious Disease Outbreaks)
VSRB (Virtual Sample Repository Bank).

Let's examine what goes on when we are starting to deal with a new outbreak of a biological agent such as a new strain of influenza. Let's consider both the natural responses and countermeasures and those invented and assisted by human science and engineering. The body's immune system, with or without some prior assistance from the outside (e.g., a vaccination) is engaged in a constant exercise of anomaly and intrusion detection on multiple scales all of which have to do ultimately with pattern matching and fitting among molecules. Regardless of the intrusion, whether it is a wood splinter or a thorn from a rosebush, or a population of bacteria or viruses on the move, there is a basic process underlying all of the body's immune system and the other systems working together, and her we should carefully and perpetually note that there are, in fact, no such "individual" or separate "systems" but only one whole, one body, and that it is we in our desire to classify, separate, and categorize, who have come up with "immune," "nervous," "cardiovascular," "sensory" systems and all of our beautiful, useful, but often fundamentally misleading language and logic.

This basic process is one of engagement, contact, and recognition. "What is it and what do I do with it?" – and all on a very fundamental level of macromolecules (and quite a few small ones, too!). Molecular reactions are what drive T-cells to do their "work," and molecular reactions drive blood vessel dilation and blood plasma density alteration to help move both cells of certain

types as well as different nutrients to the source of some particular kinds of molecular interactions that on a vastly different scale of logic are measured as "redness" or "pain." All of this involves many small parts inside the body that are working in different ways to answer questions about the relationship of the new object (e.g., antigen, virus, bacterium, transfused blood cells from another human) with the home organism, the "self."

I am emphasizing the point about anomaly detection here because it is so important for both biological health and cyber network health. When something is detected as being in the "does not belong here" category, then and only then can the host organism – the body, or the computer system/network – begin to do something, to engage some algorithm, be it tried and true or purely an experimental guess in the dark, for dealing appropriately with the intruder. If the determination is made, by mistake, that X is part of the home team and belongs where it is, to be not only allowed to do its own thing but also sustained and aided, by nutrients, and by protection through that body's own defenses against other agents, then the intruder has a total "free hand." We see this left and right in biology and in computers and networks. It's called disease, and in extreme cases, beyond the point of any return to health, it is called death.

In fighting something in the biomedical space like a viral outbreak, epidemic, or full-scale pandemic, we know that what often matters are the changes that can occur, via gene sequences controlling the entire makeup and behavior of the intruder organism, which will render our defenses inert or at least weakened. We have our immune systems, and the enhancements from vaccinations and specialized medications, for instance. We also have antibiotic and other medications plus dietary regimes that can influence our body's ability to support its immune system and even to directly remove the cause of the infection. In the most severe cases there can be surgery, or radiation treatment, and somewhere in the middle are preemptive techniques that include cleansing of the gastrointestinal tract with emetics and diuretics. All of these are supportive measures to assist the basis physiological system, the operating system of the body, not to replace it, because to fix the problem means to work with and through that operating system, not apart from it. Anything else is guaranteed system termination, death. Now particularly those methods that are centered upon specific vaccines and medications, these depend for their effectiveness very much upon what are those particular gene sequences. This is so because from the gene sequence we can know about the metabolism, the 1-2-3-4 step by step behaviors, of the microorganisms we are trying to reduce and eliminate from the body.

We have many tools that are good for analysis, tracking, predicting, and responding, and some are relatively new ones, like those that comprise the CUBIT Suite of sensing and testing, bioprotection, and in particular, realtime mobile, ad hoc, multiplexed diagnostics and reporting. CUBIT is something conceived and designed for biothreats in mind, biopathogens and biomedical conditions and dispositions. But it is admirably and powerfully adaptive to the problem of cyber network security, defense and countermeasures against the precise types of new attacks that are dominating in today's internet-intensive world.

Shifting now to the cyber networks, let's consider what it means to start applying the biological model of defense, and tools like CUBIT, to the problems we see today. Bear in mind and never forget that the new and evolving genre of attacks are coming from highly organized, well-funded, and indeed rich operators that are starting to get the upper hand over the "body" of the internet. What we have is akin to a patient who is getting sick with the flu, they are definitely feeling some of the symptoms. However, they don't realize how strongly they have been hit by the particular flu bug and that they are at risk of a very serious if not fatal situation. It is our aim naturally in the biomedical sphere with CUBIT Suite and other technologies to help the individuals and the

populations At risk from biological threats such as viral epidemics. However, we also see that we can do something in the cyber sphere by applying some of the same tools – the logics, not the physical implementations, of course.

The CUBIT paradigm for detection and tracking of the behavior of new strains, new mutations of some pathogen, in terms of its pragmatic public health goals of mitigating the spread of dangerous infectious diseases once there are outbreaks into the population, may be summarized as follows:

- Sample and measure the agents that are producing the illness aiming to identify and classify according to known specific strains and to set aside those that appear to be changing in the observable population. Seek the variances, the disturbances, that are suspect mutations.
- Observe (quantify) mutations within infected members of the population and associate those mutations with known or suspected changes in the epidemiological and pathogenic attributes of the organism. (In other words, is this mutation becoming more or less like a form that has known effects or can be suspected, on the basis of prior knowledge and hypotheses, to have certain types of effects; e.g., more lethal, less lethal, more virulent action in the respiratory system or less so, more easily transmissible from human to human or less so, and specifically, at the roots, more likely to produce x or y or z amino acid sequence or not.)
- Collect and associate metadata concerning the geographic and demographic data surrounding the mutation cases. This is for the purpose of identifying better what may be related factors in the etymology of the mutated strain and also in the epidemiology going forward in time. Some of this metadata will include information about the social associations (home, school, work, church, club, sport) of the infected individuals and about the environment (animals, livestock, chemicals, general health and diet of the person, the family, the community). All of this is of value to both researchers and responders (i.e., health care providers for the individual and the community as a whole).
- Identify and prioritize new targets (pinpointed individuals and regions) for appropriate increases or decreases) in deployment of resources (vaccines, medications, hospitalization resources). Determine where the projected effects of a more virulent pathogen strain are likeliest to be occurring and spreading, and adjust the resource and logistic plans accordingly.
- In parallel, by managing control and access to samples of the identified mutant or suspect-mutant strains, aid and enhance the process of research and extended clinical validation by making certain samples (and the data thereabout) more readily available to labs and researchers who are capable and working on gene sequencing and new metabolic behaviors of the organism.

How can we best apply this paradigm and, if possible, some of the actual tools, at least those of a mathematical and computational nature, to being effective new measures in the battle against the cyber attack epidemic and, at this point in time, pandemic? We can do so by thinking of the functions that are performed by different agents of attack within a cyber network and how these can be mapped to the functions in a biopathogen attack, an epidemic or pandemic, and then determining how the functions of a CUBIT approach can be executed against these cyber pathogens using essentially a CUBIT-like solution, but one that is not working with the exact same software nor with physical bioassays, PCR or any other form of biosensing and diagnostic process, yet with detectors, sensors, and recognizers of a slightly different “construction.”

Let us reconsider the same basic bullet points as above, but now in the context of a cyber attack that involves any number and variety of viruses, bots, and mechanisms designed to disrupt and/or in some fashion take control of individual computers including servers, to do some task that serves the attacker and not the owner of the computer or network. Remember that in advance, we do not know these details, and we cannot presuppose anything about motivation or purpose, just as in the biological situation we cannot presuppose a particular virus, bacteria, or some other medical condition unrelated to microorganisms.

Thus, our CUBIT Cyber Attack process entails:

- Sample and measure the --
  agents (anomalies indicative of some intrusion, denial of service pre-overload (amplified requests and hits), uncharacteristic statistics of origin, packet type, URL, originating DNS, IP, etc.)
  that are producing the illness (network/server/computer disturbance and performance irregularities)
  aiming to identify and classify according to known specific strains (varieties of attack and style of known or implicit code)
  and to set aside those that appear to be changing in the observable population (i.e., different from prior types of cyber attack).
  Seek the variances, the disturbances, that are suspect mutations (seek indicators of new operators, new perpetrator organizations, new alliances among cyber-criminals and cyber-gangs).

- Observe (quantify) --
  mutations that appear to be taking place in the methods by which the attack is being propagated, particularly giving attention to evidence of changes in the "handshaking" interface between a malware bot, for instance, and a target computer or its human operator. This is in a way like looking for a change in an RNA or DNA sequence that can indicate a change in some known protein production that in turn will be an indicator of characteristic changes in the mechanism by which the invasive organism (e.g., virus, bacteria) can defeat the immune system of the host organism. Here we are looking for the ways in which the malware can defeat an "immune system" in place, through the combination of anti-viral software, operator intelligence and education, and other countermeasures.
- Collect and associate metadata concerning the geographic and demographic data surrounding the cases of infection and the evident cases of mutations. As in the biological domain, the objectives here are essentially twofold: first, to learn more accurately about who is affected, what is the extent of the infection, and what part of a network needs to be "treated" (including by quarantine if necessary), and second, to learn more about the extent and "vector" of any changed forms and where they may be directed next.
- Identify and prioritize new targets (pinpointed individuals and regions) for appropriate increases or decreases) in deployment of protective and "allopathic" resources. Determine where the projected effects of a new :"strain" of the cyber attack agent are likeliest to be occurring and spreading, and adjust the resource and logistic plans accordingly.
- Take measures or actively seek new information that will aid and enhance the process of research and corrective response by making certain samples of the cyber infestation

(and the data thereabout) more readily available to labs and researchers who are capable and working on those particular types of attack agents.

Clearly, there are to date some things that are missing in the world of cyber network security and countermeasures that are much more developed in clinical medicine. Consider just the technologies of gene sequencing, and the pattern matching capabilities brought about by polymerase chain reaction (PCR) techniques. This is an important part of CUBIT in the biomedical domain, so one must ask the question, "What is there that can be a CUBIT type of method to apply to the "genetic" study of cyber organisms?" This leads immediately to a more critical question, "Is the analogy stretched too far and is what we seek a bit out of the realm of either possibility or at least similarity?"

Our claim is that there is such a method, and that we do remain within the realm of achievable applied science and engineering when we claim that we can develop CUBIT-like approaches to the infectious diseases of the internet and web. In an ironic way, there is something very much like PCR in our proposed adaptation and solution. It simply does not involve the amplification (replication) of any long molecular chains.

Our analogy to PCR is based upon the notion that there is a set of attributes that can be described for the behavior of any given cyber attack agent. These define exactly what it does within a target (host, victim) system. What actions are performed against what parts of the operating system and/or specific applications? What digital actions are executed which result in changes to dynamic memory, to something stored on a hard drive, etc.? The more we can specify the attributes of the attacker, the more we know about both its limits (constraints) of action, and the more we know that, then the more we know about its particular "shape" as a functioning agent.

This is comparable to a situation of learning more and more simple facts about how some piece of simple machinery operates. We learn that some thing, some "it," has the ability to make abrasive marks on the interior surfaces of a box-shaped room. Some of these are more intensive marks and gouges into the surface of the room's four walls. All of the marks have the same characteristic in terms of a clockwise motion of the object, whatever it is, that traverses and gouges into the wall surfaces. With the placement of some sensors, we further discover that there is a fixed sequence of hit-skip-hit-skip-hit-skip-hit-skip that is measurable and it is constant.

Eventually we come to the conclusion, in this jaded and contrived example, that there is a spinning rotor, located off-center in the room, and attached to it is a steel-rod arm, and attached to that, a heavy hammer-like object. It turns out that we have the motor turning, and it is rotating an assembly that is responsible for the marks, the impact noise, and the variable-depth gouges. Until we can gather enough information about the entire system of box, motor, and rotary assembly, we are ignorant of not only "facts" but hypotheses. As soon as we have enough information, however, we can rapidly turn the hypothesis into a testable one, do some experimental verification, and then perhaps even repair the system so that the hammerhead is either never hitting the walls, or hitting them with a uniform force – whatsoever that we deem to be desirable.

Let's go back to the cyber attacks. We can create replicas of what we know or at least conjecture (with some evidence) to be the step-by-step behavior of our attacking agents. We can, in fact, create thousands and millions of them, just in the snap of our fingers, because we can generate arrays in our computers (those that are not infected, of course!). We can then do our own version of a gene-sequence matching exercise, on a vastly parallelized scale, in order to see what types of phenomena, what sequences of behavior, appear to follow, to emerge, from the actions of our

projected and suspected bot agents in our model of a host organism (network, intranet, internet). At some point we may be collecting enough information about consequence-type behavior that we can begin to compare these consequence patterns with what we observe in the current outbreak world, or in outbreaks from the past. We can begin to identify better the likely properties that can give us knowledge about what to do next in order to treat an attack in progress and also to track it back to its origin and hopefully with aid for those forces charged with stopping and circumventing the person or persons responsible for the malware attack.

We are a long way from having something like a real time PCR instrument that can whip out an accurate diagnosis of influenza strain within less than two hours. We are far away from having anything that can be used with such relative ease and speed. However, we are in a better position to fight back both defensively and offensively, once we have an architecture for analysis that also has built into it a mechanism to construct expected, next-move or look-ahead consequences. This is part of the value of taking the concepts of PCR and gene sequencing, and the model of infectious disease medicine in general, and starting to see how the problem of cyber attacks is not so different from the problem of an influenza outbreak, not only in the epidemiology of both situations but in the forensics and the development of therapeutics including vaccines.

A CUBIT system for cyber network attacks has not yet been built. It is a subject of active research within our group, and we do believe we are getting closer to refining some field-testable mechanisms. These are software, in fact they could even be termed “bots” in their own right. We look to do with software agents exactly what we have spelled out above in some bullet lists. Sampling, quantifying and measuring, metadata acquisition, prioritization, and expanding the outreach-sharing of information with other centers of cyber network defense activity. This brings us to the point raised in the very beginning of this memorandum, namely, about the need to be more biological in behavior, more viral in fact. The software agents in this CUBIT approach are called Binars and they are designed to act very much like an invasive microorganism, going deep into data structures and memories and being a lot like a cell-penetrating virus. What they do depends in great part upon the “genetic code” uncovered for the malware phenomena being investigated. But their objective is to replicate functions, in a controlled environment, in such a way that the computational immune system, the resources of the network and individual computers, can be itself adjusted, modified, “tweaked” by agents that function like viruses but are not foreign organisms at all but part of the normal body.

When the “organism” (computer, network, etc.) starts generating mutations in its own defense, then it is starting to “fight fire with fire” and make some headway. These mutations may be restricted, of course, to certain computers and subnets, but the fact is that they will be acting not simply as allopathic deterrents to the real attacking cyber-organisms but as microorganisms in their own right, building data structures and interdependencies that will begin to block resource-takeover by the cyber-attackers, going for the same behavioral niche with their own organisms. Now how is this going to actually “heal” the system? Won’t it simply replace one virus population with another and still snuff out (or significantly cripple) the attacked system (network) with something slightly different and indeed “home grown?”

The difference lies in the matter of control. The binars that work for the CUBIT-Cyber main driver are not really taking over and away any resources. They are, after all very virtual within what is itself virtual world. They know how to do their job as virtual T-cells and then to simply disappear into the “ether.”

We are only in the beginning, not only we as a group pursuing the CUBIT paradigm, but as a society, learning what are these new micro-ethereal organisms and how they work. We are capable for getting an upper hand over these kinds of infectious diseases as well as the ones that are made of proteins, nucleic acides, lipids, cellulose, and other molecules in the dance-theater of Vita Primitiva. The sooner we play around with more variety and gene-mixing on our part, the sooner we will be developing better immunities to the attacks coming our way from so many new sources.

Author:

Martin Dudziak, PhD
Chief Scientist, TETRADYN Corporation
http://tetradyn.com
Chattanooga, TN
757-847-5511
202-415-7295