Emerging cybersecurity technologies and essay

ASSIGN BUSTER

This is extremely important because most of our national power grid suppliers are privately owned. This paper will further analyze the subjectivity technologies of today as well as the technologies coming down the pipeline, and the policies that guide the United States against malicious threats to national security.

Subjectivity Technology Technology in the right hands can be a very beautiful thing, but that very same technology in the wrong hands or the hands of those seeking to cause harm can be very dangerous.

Some of the most common subjectivity cosmologies that exist today include: Intrusion detection systems, Intrusion prevention systems, Encryption, and Firewalls for network protection, as well as, biometric measures like fingerprint scans for access control. These technologies offer a baseline of security protection against the most common threats. Intrusion detection and prevention systems monitor traffic/ logs either on the individual host or on the network in real time looking for signatures of common attacks or anomalies that will trigger an alarm either of an attack in motion or an attack that has already occurred.

Firewalls monitor network traffic in real time and either allows or denies certain traffic into or out of the network based on the type of firewall and the rules they are programmed to follow.

Firewalls are a very important baseline in system infrastructure and design. Encryption is one of the most important technologies of subjectivity designed to protect the confidentiality of data. Encryption uses a complex mathematical formula and a key which randomizes and creates a coded or

encrypted message. Only the party that the message or data is originally intended for can read in plain text by using he appropriate key to decrypt the data.

Some encryption algorithms such as AES (Advanced Encryption Standard) are very complex and with the strongest computers on earth may still take a lifetime to break. Biometric measures such as fingerprint scans, hand topology, palm scans, retina scans, iris scans, etc.

Are very controversial with regard to individual civil rights. Biometric measures are also a very strong technology for the protection of physical access and physical security access control with classified facilities. Most forms of biometric security are very expensive to implement and maintain, UT also a stronger form of security and harder for criminals to copy or break.

The federal government has devoted more money now to research and development Of security technologies than ever before. DARPA (Defense Advanced Research Projects Agency) reported that the funds devoted to this cause for the fiscal year of 201 2 were well over $200 million dollars (Hoover, 2011) which was a 70% increase from the year before.

If new technologies are going to continue to defend our national security they must be able to defend against the more sophisticated, dynamic, asymmetrical threats that we errantly see emerging.

Asymmetric threats are attacks that seek to exploit new vulnerabilities and the art of surprise to take advantage of an opponent. “ Terrorists will often exploit new vulnerabilities in cyberspace to engage in asymmetrical warfare.

” (Nee, 2008) Advanced persistent threats are another type of dynamic sophisticated threats that we see often in attacks.

Advanced persistent threats are attacks from hackers and cyber criminals considered “ advanced” because of the methods they employ and the nature of the threats themselves commonly deployed by State actors (Tankard, 2011).

These attacks are often well funded and very well planned out to increase the percentage of success for the attacker. Features of New Technology Some of the new subjectivity technologies include remote agent technology, prioritize research & development, and real-time forensic analysis. Remote agent technology was designed to combat the problem of latency with network monitoring. Regular compliance log audits and patches use to be sufficient in the past, but not anymore with more sophisticated and dynamic threats.

Remote agents can conduct centralized remote security sets on a network through a secure SSL connection checking availability and performance of monitored resources.

(MUMS, 201 2) The remote agent can then report the results back to a centralized system. Remote agents offer many positive features including conducting the tests without passing non- secure protocols through the firewall setup to protect the network, as well as, a low amount of overhead processing power and manpower to perform the frequent tests.

In my current role as a network security engineer, we use a tool called Nations to monitor our production servers and their traffic. This Nations Monitoring tool provides us many types of useful data including disk usage, CPU load, etc.

And reports to the central Nations server where we can analyze the data quickly and often can predict major issues before they OCCUr. Another new technology that must be discussed is real-time forensic analysis. Real-time forensic analysis allows analysts to reproduce a situation or incident in real-time in order to determine the cause of an intrusion or the source and quickly triage the situation.

With this continuous real-time analysis all packets are captured and copied to provide an image of all critical areas on he network. Dealing with latency, time consumption, and a high percentage of false positives and false negatives continues to plague the security professional with the current forensic tools available. Another issue that we encounter when using the standard " post incident" forensic analysis tools is the breaking Of network connections and dismounting encrypted disks, which causes a loss of critical volatile data.

By analyzing active systems in real-time we eliminate some of this risk.

Foreperson is a real-time forensic analysis tool that is designed to capture, store, and analyze data on active networks. This LOL has been designed to not only capture and analyze, but to do so without intruding or tainting the data on the machine for presentation in a courtroom. (7) Role of Federal Government in Development The federal government plays a vital role in the

development of subjectivity technologies and their implementation through policy.

Agencies like DoD, NSA, DISH, IONIAN, and many more lead the charge in the battle for cyber supremacy and national protection.

Although many of these top agencies have classified budgets in regards to their research and development, we know that they tip the scales into the billions of dollars. As mentioned in the introduction to this paper, cooperative interaction between agencies and information sharing between federal agencies and private organizations is a key to developing technologies and mitigating the risk of espionage's, hacking, and destruction of our critical national power grid. As a tool for collaboration, the NSA uses many programs but often employs Sacra's. 1) Sacra's are Cooperative Research and Development Agreements.

These agreements create cohesiveness between the NSA, companies, and other organizations to create development Sacra's do not operate on strict requirement standards, therefore they are very flexible which also contributes to the development of technology. When talking about Sacra's we discover that often times they are initiated in order to pass technologies from Federal R labs to private sector companies to increase international economic competitiveness, as well as, bolster security initiatives. 8) Like the National Security Agency, the Department of Homeland Security also has many programs devoted to research and development and information sharing. The Department of Homeland Security has something called the Science and Technology Directorate which focuses on emerging security

areas and threats such as Advanced Persistent Threats, cybernetics's, and Moving Target defenses.

Federal Acquisition Regulation regulates the amount and type of cohesive partnerships federal agencies Can engage in through contracting with private companies.

NSA uses both FAR cooperation as well as Sacra's. DISH participates in partnerships to the extent that FAR regulation allows. " DISH has the added benefit, based on language in the Homeland Security Act and Homeland Security Presidential Directive 7 (HSRP-7), to collaborate with industry sectors to ascertain the hypervelocity needs of those sectors.

" (9) Federal Government: Positive or Negative? The federal government involvement in the development of technology and information sharing with the private sector is overall a positive.