Global Information Assurance Certification Paper

GovNet: Creating an Invulnerable Network

SANS Security Essential

GSEC Practical Assignment

Version 1.2f (amended August 13, 2001)

November 25, 2001

Written by:

Maria Astudillo

Mary Washington College / MBUS 511

TABLE OF CONTENTS

INTRODUCTION

Being the most powerful country in the world, the United States has always been the target of many types of attacks. However, no one could imagine that the attacks in our own homeland could be of such magnitude, as it occurred on September 11, 2001. Even if these terrorist attacks "had little impact on critical government and business networks…any future attacks against U.S. companies, which own and operate most of the nation's critical infrastructure systems, may be different" (16). An attack in the nation's Information Technology (IT) infrastructure can cause great damage to the American economy. Concern with the protection of IT infrastructure, the Bush administration is considering the idea of creating a "closed IP network for government agencies" (2). This network would be a private voice and data network based on existing Internet Protocol (IP) technology, and it would have no connectivity with commercial or public networks (10). Such network would be known as the Government Network or GovNet.

By separating the government network from the rest of the Internet, the U.S. Government expects to reduce the threats and vulnerabilities of its IT infrastructure. The assurance level of GovNet is supposed to be extremely high. However, other issues such as the acquisition costs, limitations on management authority and oversight across multiple U.S. Government domains may make it almost impossible to realize it in the near future, without having to make some changes in the original government proposal to implement such network.

This is not the first time that the government has tried to have its networking resources separated from the rest of the world. Agencies such as the Central Intelligence Agency (CIA), and the Department of Defense (DoD) operate on separate classified networks, as well as the Department of Energy, which has some of its laboratories on a private line. The United Stated Army has created its own portal, making it the world's largest intranet, and all government agencies are part of the .MIL or the .GOV top-level domains.

REQUIREMENTS

The U.S. government has requested information for the creation of a network (GovNet) that would serve critical government functions. One of the requirements of such a network is for it to "have commercial-grade voice communication capabilities and the potential for adding video, as well as the ability to support critical government functions" (10), such as space flight and air traffic control. Also, and most important is that the GovNet should be immune from malicious codes and other computer viruses (10). The network would be built using fiber optic and dedicated routers.

In addition, the network would provide not only the highest level of reliability and availability, but also a rapid response time for customer outages. The traffic would be secured using encryption, and it would be able to carry classified information. All components and links should be located in the U.S or Canada, and it would evolve to

ensure that the technology and services are current with commercial services to the maximum extent practical (4).

ADVANTAGES

By creating the government network from scratch, security measures that deny potential attackers an easy access to the system could be implemented from the early stages. This would create a defense in depth strategy that includes the usage of a strong encryption code for network-level traffic from the beginning. Also, from a security standpoint, "physically isolating a network is the single most effective way to improve security" (11) because there will be no gateways to the Internet or other networks. Another advantage of GovNet is based on the fact that the agencies using the network would be able to react in a quicker manner to worm and virus's attacks. Richard Clarke, the new special advisor to the president for cyberspace security, believes that it is because any malicious data would have to be moved between separate computers. This policy, known as "air gap", does not guarantee that the network would not get any viruses or worms. It supports the idea that if infections are to take place in GovNet, it would normally happen a few days later, hopefully after a countermeasure has been found for the source of infection (8).

ISSUES

CONSTRAINTS

The creation of such a network could cost billions of dollars if we take into account the size of the United States government. It would require a great number of labor hours to make it operational. Furthermore, GovNet would not allow its members to have access to the World Wide Web. According to Mark Rasch, a former Justice Department computer crime prosecutor, this would limit its value as a communication tool (15). More than likely, employees who require access to the Internet would have to acquire a second desktop computer completely isolated from GovNet. This would increase the amount of dollars needed for the investment since money would not only be needed to create GovNet, but also to keep the other networks operational.

VULNERABILITIES

Having a network of such size could also make it more vulnerable to social engineering. According to the SANS Institute, social engineering is defined as the process of attacking a network or system by exploiting the people who interact with that system. Computer users are often the weakest link in a network, since human beings are always trying to be helpful. At the same time, users have created a trust relationship among them, the other employees they interact with, and their computers (19). In a network of the size of GovNet, it is going to be harder to identify who is who. The risk of having someone requesting information due to an emergency, representing a higher authority could be a major issue. Identification measures need to be implemented to provide secure access to

the system. However, attackers are always smart enough to find ways to overcome barriers. There is always the possibility of someone willing to sell information for the right price. U.S. enemies have tried for decades to recreate our technology. Even though sometimes they have been unsuccessful in acquiring our best-kept technological secrets, they can still understand them and apply them to some degree. In addition, they have the capability to pay an insider to obtain the information and technology they want. One of the biggest downsides of GovNet is that it may not be able to prevent insider threats. With the network being physically isolated, compromising a host will depend on actually having physical contact with the hardware and software used, which is not impossible if the person doing it is an insider. Keep in mind that around 40 percent of the security breaches come from within the network, and whether or not this is done unintentionally, that is a different story (13).

Another major issue would be accessing the system through a non-secure device. If people are required to have another desktop to access the Web, they could unknowingly download malicious code onto a floppy, and then transfer it to their GovNet terminal. The computer can then be infected, and once the information is shared, it could potentially infect the entire network. On the same token, an infected computer can be switched from the open Net to the secure network, causing viruses and worms to spread into the secure network. An example of this vulnerability is what happened with Melissa virus, which was introduced from the Internet into a closed military network, even though the military network is a closed one (2).

CONTROLLING ACCESS TODAY

SECRET INTERNET PROTOCOL ROUTER NETWORK

The controversy is surrounding the effectiveness of the method used by the government, in actuality, to secure its information. One of the techniques in place today to access data over a secure network belongs to the Department of Defense. The DoD has implemented a Secret Internet Protocol Router Network (SIPRNET). SIPRNET was first implemented on March 3, 1994, and by Spring '95 it was composed of " a collection of 31 backbone routers interconnected by high-speed serial links to serve the long-haul data transport needs of secret-level DoD subscribers" (9). As the SIPRNET name implies, this DoD classified network uses Transmission Control Protocol/ Internet Protocol (TCP/IP) routers and also has many of the same other hardware and software configurations typically found in other TCP/IP commercial networks (14).

The differences between SIPRNET and the rest of the Internet are far more striking than the similarities between the two. First, access to a SIPRNET terminal is restricted to users with a U.S. Government clearance at the SECRET level. The data packets sent using the SIPRNET are encrypted, unlike the majority of Internet traffic. Finally, SIPRNET is a closed structure that uses protected distribution methods, totally opposed to the way the Internet is at present (9).

.MIL AND .GOV DOMAINS

The U.S. Government owns two top-level domains, the .GOV, reserved exclusively for the U.S. Government agencies, and the .MIL, for the U.S. military. These domains represent the range of IP addresses destined to be used by all government IT assets. As such, many agencies within the government and the military started using IP address verification to grant access to other sensitive government/military resources over the Internet. This was an excellent idea, however, distributed denial-of-service attacks, malicious code, and IP spoofing have limited availability of this sites, as well as the quantity and quality of the information presented at these government websites.

PROPOSALS TO INCREASE SECURITY

PHYSICAL NETWORK SEPARATION

One of the main proposals to implement GovNet contemplates the creation of a new network, physically separated from the Internet. This network would be of exclusive use by the government. The advocates of this idea expect that by separating GovNet from the Internet, the government will be able to mitigate threats such as hackers, trojans, viruses, and denial-of-service attacks. Richard Clarke, the cyber-security czar, envisions a "set of departmental and agency "intranets," which use Internet technologies, that would run on leased fiber optic cable instead of passing through routers and switches connected to the Internet" (13). His concern is well founded not only because there has been an increase in the number of functions, concerning the national economy and national security, put on the Internet, but also because of the diverse traffic moving throughout the Internet today. Obviously, the downside to this approach is the total isolation from the rest of the world. This could incite some employees to circumvent the security policies in place, creating network vulnerabilities. For instance, employees may not fully understand the need to remove or at least turn off the modem's auto-answer feature, and be tempted to dial-up an external Internet Service Provider (ISP) to check email or the news.

NON-ROUTABLE IP ADDRESSES

A few people do not agree with the Government's plan of creating a GovNet separate from the Internet, since they believe that it is going to be quite expensive, and think that approach will not solve the problem. One of these people is Ken Watson, who is the director of critical infrastructure protection at Cisco Systems Inc. Mr. Watson recommends using non-routable IP addresses, given that network users cannot see them (18).

Non-routable addresses are used for intra-enterprise connectivity, where there is no intent to directly connect to either the Internet or other enterprises. In this scheme, the different machines connected to this private network use one of the IP addresses in one of the three blocks reserved by the Internet Assigned Numbers Authority (IANA).

The three blocks of non-routable IP addresses are:

10.0.0.0 → 10.255.255.255
172.16.0.0 → 172.31.255.255
192.168.0.0 → 192.168.255.255 (12)

VIRTUAL PRIVATE NETWORKS

Another suggestion being analyzed at this point is the creation of a chain of Virtual Private Networks (VPN) to connect the different governmental agencies, protecting vital government services like the electric power industry and emergency services (7,17). Depending on the style selected, VPNs may or may not use the Internet to sent data. The first type of VPN use leased lines to send data, while the Internet VPNs do not have to use separate circuits to create a secure transmission medium. Instead, Internet-based VPNs offer flexibility by taking advantage of existing Internet infrastructure. They utilize cryptography to share information securely over the Internet, while minimizing the chance of eavesdropping and interference from unauthorized people.

A VPN follows three steps to transfer data securely over the Internet. First, it *encrypts* the information using a security protocol, like IP Security Protocol (IPSec) or Point-to-Point Tunneling Protocol (PPTP). Next, after the data has been encrypted and sent over the Internet, the VPN takes care of *authenticating* the receiving party by applying techniques such as: password authentication, public-key cryptography, bulk encryption algorithms and digital certificates. The last step to complete the data transfer is the *decryption* of the data received through the VPN (5).

CONCLUSION

Cyber crime is increasing. According to The Computer Emergency Response Team Coordination Centre, there have been approximately 35,000 attacks in the first nine months of this year (1). Considering that the U.S. economy and security depend on an elaborate IT infrastructure, new security measures need to be put in place to protect our national interests. Nowadays, industries such as banking, transportation, energy, water, health, and telecommunications among others, access some sort of network in order to do daily business. An attack in any of these systems could cause disruption to activities critical to our economy and national security, causing irreparable losses.

The implementation of a private government network or GovNet seems to be a viable solution to the ever-increasing threats to official government communications. However, designing the system from scratch is going to be very expensive, time consuming, and might not be readily available for implementation in the time required by the General Services Administration (GSA), the acquisition arm of the government.

It might be wise to create a network using a combination of the resources and methods already implemented. By using a leased line with a VPN to encrypt the data before

transmission and then combining it with non-routable IP addresses, the information assurance level would increase. At the same time, the government should deploy more host-based intrusion detection systems to secure every machine on the network.

An investment of such magnitude is not restricted to the hardware and software. It is also important to invest in training the users to reduce the so-called "social engineering", and to create awareness on the importance of keeping the systems updated with the latest software patches. This might be a challenge that managers must overcome if GovNet is to be successful. Keep in mind that "90% of the hacks on government systems occur because people haven't updated the patches on their operating systems or applications" (7). Hackers exploit these vulnerabilities to install back doors to gain access to these compromised systems at a later time.

Having a secure network would require more than using intrusion detection techniques. If GovNet is created, issues such as who would get access to the system, along with the problem of dealing with different government organizations and all the equipment needed for its administration could actually create a recipe for an insecure network (6).

A new network would increase the attention of hackers who would go the extra mile in order to break in. Therefore, we must ensure that GovNet's *integrity* can withstand unlawful entries to network resources. Also, that the network is always *available* during and after an attack, and that there have been no violations in the *confidentiality* of the information residing inside it.

REFERENCES

1. Anderson, Kevin. US plan for secure internet 'flawed'. 22 Oct. 2001
< http://news.bbc.co.uk/hi/english/sci/tech/newsid_1601000/1601823.stm >.

2. Barrett, Randy. ZDNet: Bush Wants Separate Net. 22 Oct. 2001
< http://www.zdnet.com/zdnn/stories/news/0,4586,2818103,00.html >.

3. Greene, Tim . General-purpose VPN hardware suffices for most. 21 Oct. 2001
< http://www.computerworld.com/storyba/0,4125,NAV47_STO58476,00.html>.

4. GSA - Federal Technology Service . Request for Information for a Government Network Designed to Serve Critical Government Functions (GOVNET). 25 Oct. 2001
< http://www.fts.gsa.gov/govnet/govnet.doc >.

5. International Engineering Consortium. IEC: Online Education - Virtual Private Networks (VPNs). 24 Nov. 2001 < http://www.iec.org/online/tutorials/vpn/index.html >.

6. Lemos, Robert. Security experts leery of government Net. 22 Oct. 2001
< http://www.zdnet.com/zdnn/stories/news/0,4586,5098169,00.html?chkpt=zdnnp1tp02 >.

7. - - -. ZDNet: Printer Friendly - Defending America against cyberterrorism. 16 Nov. 2001
< http://www.zdnet.com/filters/printerfriendly/0,6061,2824322-2,00.html >.

8. - - -. ZDNet: Printer Friendly - Net threat: Enemies at the gate. 16 Nov. 2001
< http://www.zdnet.com/filters/printerfriendly/0,6061,5099371-2,00.html >.

9. Pike, John. Secret Internet Protocol Router Network (SIPRNET). 22 Oct. 2001
< http://www.fas.org/irp/program/disseminate/siprnet.htm >.

10. Pruitt, Scarlet. Washington seeks input to build its own Net. 16 Nov. 2001
< http://www.cnn.com/2001/TECH/internet/10/14/gov.net.idg/index.html >.

11. Raikow, David. ZDNet: Printer Friendly - Will our government have its own Internet? 22 Oct. 2001 < http://www.zdnet.com/filters/printerfriendly/0,6061,2818268-79,00.html >.

12. Rekhter, Y., et al. RFC1597 Address Allocation for Private Internets. 24 Nov. 2001
< http://www.faqs.org/rfcs/rfc1597.html >.

13. Reuters, Inc. Cybersecurity czar snubs ID plan, defends Govnet. CNN.com. 16 Nov. 2001. Keyword: GovNet.

14. Seffers, George I. Fit to fight the info war? 24 Nov. 2001
< http://www.fcw.com/fcw/articles/2001/0312/news-iwar-03-12-01.asp>.

15. USATODAY.com. White House seeks government computer network. 22 Oct. 2001
< http://www.usatoday.com/life/cyber/tech/2001/10/10/cybersecurity-supercomputer.htm >.

16. Verton, Dan . Analysts: Insiders may pose security threat. 25 Oct. 2001
< http://www.computerworld.com/itresources/rcstory/0,4167,STO64774_KEY73,00.html >.

17. - -. Feds mull global VPNs for critical services. 21 Oct. 2001
< http://www.computerworld.com/storyba/0,4125,NAV47_STO60804,00.html >.

18. Verton, Dan. Feds consider splitting Net for security. 21 Oct. 2001
< http://www.computerworld.com/storyba/0,4125,NAV47_STO60901,00.html >.

19. Northcutt, Stephen. SANS Security Essentials Version 1.2f (amended August 13, 2001). The SANS Institute, 2001.