Mitigating Higher Ed Cyber Attacks

Gary Rogers
Professor
Palm Beach State College
4200 S Congress Ave
Lake Worth, FL 33461
rogersgs@palmbeachstate.edu

Tina Ashford
Professor of Information Technology
Middle Georgia State College
100 College Station Drive
Macon, GA 31206
tashford@mga.edu

Abstract:

In this presentation we will discuss the many and varied cyber attacks that have recently occurred in the higher ed community. We will discuss the perpetrators, the victims, the impact and how these institutions have evolved to meet this threat.

Mitigation techniques and defense strategies will be covered as will a discussion of effective security policies.

"Most major U.S. companies have been under siege from hackers over the last 18 months".[1] **- Former Homeland Security Secretary Janet Napolitano**

Introduction

Cyberattacks are conducted across the globe on a daily basis. An article in The New York Times reported there has been a 17-fold increase in computer attacks on American infrastructure between 2009 and 2011. In fact, the newspaper indicates there are millions of hacking attempts weekly. "The attacks are increasing exponentially, and so is the sophistication, and I think it's outpaced our ability to re-

1 Retrieved January 22, 2015. http://www.usatoday.com/story/tech/columnist/komando/2013/09/06/cyberattack-hackers-syrian-electronic-army/2757833/

spond," Rodney J. Petersen, head of the cybersecurity program at Educause, told the *Times*. Educause is a nonprofit alliance of schools and technology companies. [2]

Many of these attacks are finding their way into the institutions of higher education. Universities often become high targets for these attacks because they are involved with the research or development of new drugs, computer innovations and technology equipment. Gaining access to these secrets would turn valuable profits for outsider markets. This type of hacking is considered industrial espionage or cyber theft of trade secrets. Most universities acknowledge there are numerous breaches of information and report even when they do find out about the breach of security, it is often much later than the initial attack. Once detected, they often cannot tell what, if any information was compromised.

The cause for concern relates to the high number of attacks that go unnoticed until the damage has occurred. Industrial, government and private sectors are targets for this type of attack; however, colleges and universities have seen a major rise from cyberattacks. According to the news website, *United Press International,* many United States research universities have a history of receiving cyber-attacks that increase daily. These attacks are thought to come from China and are possibly linked to their military, who is their most frequent hacker.

According to Bill Mellon of the University of Wisconsin, "We get 90,000 to 100,000 attempts per day, from China alone, to penetrate our system"[3]. Two recent events of cyber-attacks occurred at the University of Delaware, and Stanford University. The University of Delaware cyber-attack resulted in a data breach of approximately 72,000 current and past employees, including student employees. The Stanford University cyber-attack damages are undetermined, but are still under investigation. The cyber-attacks at both universities occurred in July, 2013. The University of Delaware has provided information on their website regarding their incident. It details what occurred, how it happened, and actions to take if you were a victim of the breach. In addition, the University of Delaware is offering free credit monitoring services. In the case of Stanford University's breach, it is yet undetermined whether personal information was exposed. In addition, it has not determined the extent of the damages. In both cases, the universities provided information as quickly as possible. The responsible party for the cyber-attack on the University of Delaware has not yet been determined. In the case of Stanford University, a hacker with the handle "Ag3nt47" is claiming responsibility for the attack in the form of a tweet. His justification for the attack was simply to show the university their information was not

---

2 Retrieved January 21, 2015. http://www.allgov.com/usa/ca/news/unusual-news/stanford-hit-by-hacker-who-claims-to-have-grabbed-entire-it-database-130726?news=850671

3 Retrieved January 21, 2015 http://www.upi.com/Top_News/US/2013/07/17/US-research-universities-increasingly-targeted-by-cyberattacks/26641374065244/

properly protected. He further expressed that instead of gouging the students for more money, they should concentrate more on protecting their information. [4] Stanford University has yet to confirm the extent of the intrusion. It appears that an information technology worker doing routine checks discovered the possibility of a problem. Stanford security officials believe the records were actually stolen a few days earlier. Stanford promptly notified the FBI and secured assistance from outside security consultants to help assess and mitigate the damage.

After the investigation, it appears the cause of the attack was an exploited web-based security flaw. Web-based types of attack are very difficult to defend, however, Shape Security announced on January 21, 2014 a new way to defend against web-based cyberattacks. Their product, ShapeShifter (https://www.shapesecurity.com) is a network security appliance that disables malware, bots and other scripted attacks trying to interact with your web applications. The ShapeShifter uses a new polymorphic code technique to defend against attacks. Malware has used this type of polymorphism for years to invade machines. Derek Smith, CEO of Shape Security stated, "The ShapeShifter focuses on deflection, not detection. Rather than guessing about traffic and trying to intercept specific attacks based on signatures or heuristics, we allow websites to simply disable the automation that makes these attacks possible."

The NY Times article, 'Universities Face a Rising Barrage of Cyberattacks', emphasized,

> "Information officers say they have also learned the hard way that when a software publisher like Oracle or Microsoft announces that it has discovered a security vulnerability and has developed a "patch" to correct it, systems need to apply the patch right away. As soon as such a hole is disclosed, hacker groups begin designing programs to take advantage of it, hoping to release new attacks before people and organizations get around to installing the patch"[5].

Kaspersky Lab[6], one of the fastest growing IT security vendors in the world believes nearly half of the cyberattacks in 2013 originated from the US and Russia. They have many times noted that locating the

---

4 Retrieved January 21, 2015. http://www.allgov.com/usa/ca/news/unusual-news/stanford-hit-by-hacker-who-claims-to-have-grabbed-entire-it-database-130726?news=850671

5 Retrieved January 22. 2015. http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=0

6 Retrieved January 21, 2015.

country of origin where the attacks originate is difficult since the hackers are finding new and innovative ways to move their initial attack launches to new locations. Both Cornel University, and the University of Wisconsin claim these types of attacks appear to be synonymous with having personal data or intellectual property stolen.

The speed at which information travels today also makes it difficult for IT professionals to keep personal information secure. This personal information includes data as diverse as social security numbers to marriage status to medical data. The basic structure of the Internet confuses things as well. The anonymity of the Internet makes it extremely difficult to ascertain where the attacks originate. Middle points such as Internet Service Providers or even homeowners whose routers are unknowingly used make it nearly impossible to effectively track perpetrators. Tracy B. Mitrano reflects, "while the largest number of attacks appeared to have originated in China, hackers have become adept at bouncing their work around the world. Officials do not know whether the hackers are private or governmental."[7] Of course, the Chinese government vehemently disagrees that the attacks have a Chinese origin. Overall, the increase of cyber-attacks on universities, government entities, and in the private sector, will continue to challenge our institutions in keeping information secure.[8] Even the notorious Edward Snowden agrees that cyberattacks occur regularly. Of course, he indicates it is U.S. hackers that attack Chinese universities.[9]

---

http://www.allgov.com/usa/ca/news/unusual-news/stanford-hit-by-hacker-who-claims-to-have-grabbed-entire-it-database-130726?news=850671

7 Retrieved January 22, 2015. http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=0

8 Retrieved January 22, 2015. http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=0

9 Retrieved January 21, 2015. http://www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked-china-universities-mobile-phones-snowden-tells-china-press/

It is an unfortunate reality that higher education institutions will continue to question how secure their networks are to possible attacks. After all, it is easier to attempt to detect cyberattacks than to defend. Attackers design and focus their attack at an apparent weak point, whereas universities must defend against a wide array of *possible* attacks. Administrators at many universities recognize the challenges of trying to keep information safe and secure while still allowing the free flow and sharing of information that make universities great. While businesses can tighten and restrict their networks to a high level, university networks needs to have their systems more open and accessible to students, faculty and staff. The additional need for the free flow of ideas among professors is critical for the advancement of new ideas. For these reasons, and a myriad of others, university systems and networks are more problematic to properly secure. Cyberattacks will most likely continue to rise until this delicate balance can be addressed.

One cyberattack incident in particular occurred not long ago against John Hopkins University's Applied Physics Laboratory (APL). The physics lab was working on classified research for the Department of Defense and NASA when they were attacked. The incident resulted in a leak of information. The lab immediately took its networks offline until the issue could be contained. These types of attacks are designed to skillfully target and obtain innovative technologies in infancy stages that could be developed by other interested and capable parties. Unfortunately, the hackers in this incident were not caught due to the university's concerns of further information being stolen. They made a rash decision to simply pull their networks offline instead of trying to identify the source. Parting words by APL spokeswoman Mary Worth noted, "*…the Web site had been victimized in the past by smaller attacks, but this recent one was the most significant incident to date."*[10]

To see the extent of the different types of attacks possible, one has only to review Dartmouth College. Dartmouth College is a private institution that was founded in 1769. It has a total undergraduate enrollment of 4,193. It is located in Hanover, N.H.[11] A devastating cyberattack occurred in 2004 at Dartmouth College. According to the Dartmouth Undergraduate Journal of Science[12], "Late on

---

10 Retrieved January 22, 2015. http://weblogs.baltimoresun.com/news/technology/2009/06/johns_hopkins_applied_physics.html

11 January 22, 2015. http://colleges.usnews.rankingsandreviews.com/best-colleges/dartmouth-college-2573

12 Retrieved January 22, 2015. Dartmouth Undergraduate Journal of Science. http://dujs.dartmouth.edu/fall-2009/cyber-attacks-on-the-dartmouth-college-network#.UuAaX7TTmUk

Wednesday, July 24th, 2004, an attacker gained access to eight servers at Dartmouth College including machines storing sensitive information. Dartmouth IT staff discovered and corrected the breach within 48-hours, but not before the attacker was able to deploy file sharing software on to the compromised machines and possibly access the sensitive data... Adam Goldstein, IT Security Engineer for Dartmouth's Computer Services lists five things attackers typically want to do on our network: 1) run websites to host spam links or malware 2) access sensitive data 3) run spam engines 4) use machines as proxies for other attacks 5) obtain full system access for other purposes. To achieve these nefarious ends, attackers typically target systems with out-of-date patches or incorrect configurations or they attempt to "trick" users into running malicious code or revealing sensitive information. I" The article mentioned China hackers as the individuals to blame.

Another cyber-attack at Dartmouth was an SQL Password Cracking Attack. It appears an attacker targeted several MySQL servers on a single network in an apparent brute force password cracking attempt. A question arose as to how they became aware of the network attack. It has yet to be determined since the attacker was never captured. Then again, a simple tool such as Nmap could find the network and its configuration for him/her. Nmap, short for "Network Mapper", is a free and open source utility for network discovery and security auditing. It is common for systems and network administrators to utilize it for network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets to discover what computers are present on a network, what services (application name and version) those systems are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other attributes. It was designed to rapidly scan large networks, but works fine against single computers, whether servers or workstations. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X.[13] On Dartmouth's network, as many others, several servers were running an outdated version of MySQL. Updates to close known vulnerabilities of this software were not applied. Once an attacker used nmap to ascertain the application name and version, it was simple to determine whether the latest updates had been applied. Since they were not, this left the system vulnerable to attack. This is not actually an indictment against Dartmouth since it is nearly impossible for many IT departments to get all their work done and so "mundane" tasks such as applying updates rarely get done "later" or not at all. "Fighting daily fires", meaning addressing users' immediate cries for assistance, must take priority.

Over the years, a number of phishing attacks targeted Dartmouth. According to DUJS, [14] "In February 2008, a spammer sent a forged, fraudulent message "from" info@dartmouth.edu to 1,000 Dartmouth addresses requesting their network passwords. Twenty people replied to the email, and only some of those actually released their passwords." DJUS (2013) says the people who released their passwords

13 http://nmap.org/

14 Retrieved January 22, 2015. Dartmouth Undergraduate Journal of Science. http://dujs.dartmouth.edu/fall-2009/cyber-attacks-on-the-dartmouth-college-network#.UuAaX7TTmUk

were all teachers and other staff members. A possible mitigation for this problem is to provide effective training in this arena to both new and current employees. Many universities such as Columbia University, for example, conduct at least yearly clinics on password protection.[15]

Another type of attack making its way to campuses are those that originate from the inside. They are usually not attempts to compromise the stability of the systems, but rather they are attempts at stealing information stored within the computers. The attacks are not from professional sources, so the art of espionage is not at issue. Attackers of this type take down the systems with denial of service attacks, then hack, change or steal information from the main areas. Often times they are not noticed or detected for some time. As Cisco stated in their February 2013 report, 85% of the malware attacks go unnoticed for two or more weeks.[16] At the university level, a student or resident is often the culprit for enacting threats of this type usually for personal gain or bragging rights.

Most attackers are never apprehended, let alone identified. It is difficult, and in some cases impossible, to accurately identify the source of the attack and link it to a personal system or address with full certainty. There is also a severe shortage of laws to convict parties guilty of cyberattacks. It is rare to find a lawyer and jury that even understands the logistics of networks infrastructure and then comprehends the cyber-attacks at a prosecutable level.
Attacks like those mentioned above cause major concern with our country's ability to defend its own vital information. The fact hackers are gaining access to universities working on confidential research projects for government departments tasked with keeping the information secure, is disturbing and begs attention. There are files stored on servers all over the United States that contain sensitive information or gathered intelligence that could compromise lives. The rise in hacking on companies and educational institutions requires government focus to recognize and develop secure methods for regulating traffic on the Internet. Network security teams are finding it increasingly difficult to keep up with the evolving tactics used by savvy hackers today.

Oklahoma University is becoming an example of developing procedures to guard and protect against cyberattacks[17]. They have taken a very proactive approach to cybersecurity. Members of the staff at OU recognize the fact that multiple attacks occur daily and inevitably the possibility exists that any decent to large sized organization will probably be attacked at one point or another. It is clear that the university realizes these challenges and actively works to defend its sensitive material while still allow-

---

15 Retrieved January 30, 2015 http://cuit.columbia.edu/cuit/security-awareness-training

16 Retrieved February 4, 2015 http://www.cisco.com/web/AP/asiapac/academy/Archive/News_Feb.shtml

17 http://www.ou.edu

ing the students and faculty the ability for a free flow of ideas. The director of the IT Forensics department at OU is working to take measures to develop levels of security that need to be implemented and put in place. Some of the research conducted at OU is confidential and requires security. Multiple attacks in the past ranged from simple probes to direct target hacking. They too note, China has developed a reputation for attempting to steal military and business secrets from the United States. "Many of the attacks come from IP addresses in China…Although that doesn't necessarily mean the attacks themselves originate in China, the nation has developed a reputation for attempting to steal military and business secrets from the United States. "[18] Their primary focus is not in catching the perpetrator. It is, however, in learning to protect their research and sensitive information. In addition, any classified research is no longer housed on the university's network. These are just some steps taken toward a safe network.

Fortunately, there seems to be more awareness for the need of increased security for these network infrastructures if they are to continue to allow sharing of information. Recent funding for programs to fight cyber security is making its way to new programs, curriculums and degrees on college campuses. The Bureau of Labor statistics boasts a 22% increase in cyber security jobs by 2020. IBM recently developed cyber security curriculum and programs to share with several universities across the country.[19] Carnegie Mellon, George Washington University, Penn State and others have received federal funding for scholarships, books, curriculum and programs to support their Cybersecurity programs Apparently the rise in cyberattacks has not gone unnoticed by those tasked with ensuring overall safety.

The U.S. is slowly making some headway on these challenges. October 4, 2013, the U.S. brought criminal action against 13 individuals for DDoS (Distributed Denial of Service) attacks. The individuals caught were members of a group called 'Anonymous' who allegedly tried to launch cyber-attacks against government, law firms, individuals, financial institutions and others. Organizations targeted included MasterCard, Visa, the British Recorded Music Industry, the Ministry of Sound, and the International Federation of the Phonographic Industry. All thirteen individuals were caught and plead guilty to "conspiracy to intentionally cause damage to a protected computer" . [20]

---

18 Retrieved February 4, 2015 http://newsok.com/as-cyberattacks-increase-universities-in-oklahoma-look-to-strike-a-balance-between-openness-and-security/article/3868617

19 Retrieved February 3, 2015 http://www-03.ibm.com/press/us/en/pressrelease/42479.wss

20 Retrieved January 22, 2015 http://www.pcworld.com/article/2052360/us-indicts-13-anonymous-members-for-ddos-attacks.html

Research into further development and implementation of defensive measures is necessary to combat and prosecute cybercrime. Attacking cybercrime is a moving target, and thus must be addressed in an ongoing fashion. As mentioned, it starts with a plan of action and awareness.
Here are a few universities that have taken a proactive stance against cyberattacks

1. **Utilize shared resources needed for cybersecurity to help reduce costs.**
   a. Bucknell University, Susquehanna University and Franklin & Marshall College brought their expertise together and then shared the resources needed to protect their information.
2. **Be innovative.**
   a. A team of researchers at North Carolina State University has written an algorithm that can detect cyberattacks on a network based on the program they wrote.
3. **Make a commitment**.
   a. Indiana University created a $2 million initiative to invite and encourage colleges and universities to band together in fighting the war on cyberattacks.
4. **Commit necessary funding.**
   a. Double your resources as did the University of California, Berkley. They recognized with the huge increase in cyberattacks, their need for additional resources would be critical. They doubled their cyber security budget from last year.

It seems universities and colleges recognize the need for more detection and protection measures if they are to protect information. They are starting to band together to explore new ideas and develop systems for protecting and ensuring our systems continue to hold information secure while allowing ease of access and sharing of ideas.

Login IDs and passwords

It is typical for users to enter their username and password in order to authorize a computer for one year. A problem is that an attacker could get around this quite easily. So, why do it? Well, it does provide a certain level of security, and in combination with other procedures/policies, true security could be found. A problem is that many users may think this is "enough security". Of course, it isn't.

Wireless Networks

Also, many universities use both encrypted and unencrypted wireless networks. Central Washington University, for example, has both an encrypted network (cwu-wpa) and an unencrypted one (cwu-guest), the latter typically used for guests. The first network uses WPA, a basically non-yet-broken encryption protocol. A problem is that many students do not bother to sign onto the encrypted network by going to the appropriate campus office. So, anyone within range of the wireless network can employ software such as Wireshark to gather any sensitive information such as logon ids/passwords, etc.

NFS

It is very common for organizations such as Dartmouth to utilize the Network File System (NFS) protocol throughout. Basically, this allows users to access their home directory from any computer.

Many organizations and colleges use IP rules to authenticate the clients. If someone can gain physical access to the network, an attacker can change certain settings to gain full access. Why? The server will assume that user so-and-so has been properly authenticated when it communicates with any machine with an IP it recognizes as "valid", possibly including the computer of an attacker as well. The catch is that once here, the attacker can view, modify, delete, and create files as if they were any user.

Do mitigations exist? Yes, modern, updated, versions of NFS use Kerberos technology. Microsoft offers a superb explanation of how Kerberos operates. "Kerberos Version 5 is standard on all versions of Windows 2000 and ensures the highest level of security to network resources. The Kerberos protocol name is based on the three- headed dog figure from Greek mythology known as Kerberos. The three heads of Kerberos comprise the Key Distribution Center (KDC), the client user and the server with the desired service to access. The KDC is installed as part of the domain controller and performs two service functions: the Authentication Service (AS) and the Ticket-Granting Service (TGS). Three exchanges are involved when the client initially accesses a server resource:

1. AS Exchange
2. TGS Exchange
3. Client/Server (CS) Exchange

Let's take a closer look at this exchange process and its component parts.

AS Exchange

When initially logging on to a network, users must negotiate access by providing a log-in name and password in order to be verified by the AS portion of a KDC within their domain. The KDC has access to Active Directory user account information. Once successfully authenticated, the user is granted a Ticket to Get Tickets (TGT) that is valid for the local domain. The TGT has a default lifetime of 10 hours and may be renewed throughout the user's log-on session without requiring the user to re-enter his password. The TGT is cached on the local machine in volatile memory space and used to request sessions with services throughout the network. The following is a discussion of the TGT retrieval process.

Example AS Administration

To begin the AS exchange process, the AS request identifies the client to the KDC in plain text. If pre-authentication is enabled, a time stamp will be encrypted using the user's password hash as an encryption key. If the KDC reads a valid time when using the user's password hash (stored in the Active Directory) to decrypt the time stamp, the KDC knows that request isn't a replay of a previous request. The pre-authentication feature may be disabled for specific users in order to support some applications that don't support the security feature. Access the user account from the Active Directory users and the computers will snap-in and select the account tab. From the account options: slide window, check mark the "Do not require Kerberos" pre-authentication option (Figure 1).

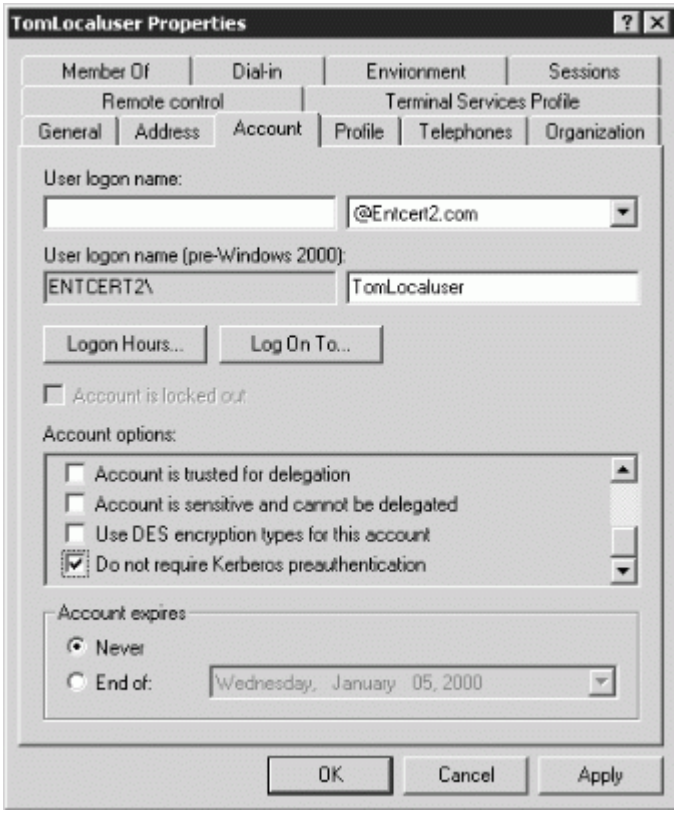

Figure 1: Disable Kerberos Pre-authentication

If the KDC approves the client's request for a TGT, the reply (referred to as the AS reply) will include two sections: a TGT encrypted with a key that only the KDC (TGS) can decrypt and a session key encrypted with the user's password hash to handle future communications with the KDC. Because the client system cannot read the TGT contents, it must blindly present the ticket to the TGS for service tickets. The TGT includes time to live parameters, authorization data, a session key to use when communicating with the client and the client's name.

TGS Exchange

The user presents the TGT to the TGS portion of the KDC when desiring access to a server service. The TGS on the KDC authenticates the user's TGT and creates a ticket and session key for both the cli-

ent and the remote server. This information, known as the service ticket, is then cached locally on the client machine.

The TGS receives the client's TGT and reads it using its own key. If the TGS approves of the client's request, a service ticket is generated for both the client and the target server. The client reads its portion using the TGS session key retrieved earlier from the AS reply. The client presents the server portion of the TGS reply to the target server in the client/server exchange coming next.

Client/Server Exchange

Once the client user has the client/server service ticket, he can establish the session with the server service. The server can decrypt the information coming indirectly from the TGS using its own long-term key with the KDC. The service ticket is then used to authenticate the client user and establish a service session between the server and client. After the ticket's lifetime is exceeded, the service ticket must be renewed to use the service.

Client/Server Exchange Detail

The client blindly passes the server portion of the service ticket to the server in the client/server request to establish a client/server session. If mutual authentication is enabled, the target server returns a time stamp encrypted using the service ticket session key. If the time stamp decrypts correctly, not only has the client authenticated himself to the server, but the server also has authenticated itself to the client. The target server never has to directly communicate with the KDC. This reduces downtime and pressure on the KDC.

Further Clarification of the Log-in Process

A TGT and a service ticket are needed to access services on remote computers, but they are also required to successfully log on to a local system. When the log-on window appears, password encryption using a one-way hash algorithm occurs immediately and negotiations commence with the KDC for a valid TGT and service ticket. The process is the same as accessing a remote service. An access token is created for the user containing all security groups to which they belong. This access token is attached to the user's log-on session and is subsequently inherited by any process or application the user starts.

Referral Tickets

The AS and TGS functions are separate within the KDC. This permits the user to use the TGT obtained from an AS in his domain to obtain service tickets from a TGS in other domains. This is accomplished through referral tickets.

Once a trust has been established between two domains, referral tickets can be granted to clients requesting authorization for services in other domains. When there is a trust established between the two domains, an inter-domain key based on the trust password becomes available for authenticating KDC functions. This can best be explained by example of a user/client seeking services in another domain. As illustrated in Figure 3, a user client in Entcert1.com requests authority for a server in Entcert2.com. He utilizes referral tickets. The process is as follows:

1. The client contacts its domain KDC TGS using a TGT. The KDC recognizes a request for a session with a foreign domain server and responds by returning a referral ticket for the KDC in the foreign domain.

2. The client contacts the KDC of the foreign domain with the referral ticket. This ticket is encrypted with the inter-domain key. Given that the decryption works, the TGS service for the foreign domain returns a service ticket for the server service in Entcert2.com.

3. The client performs the client/server exchange with the server and begins the user session with the service.

When more domains are involved, the referral process extends and involves the transitive properties between Windows 2000 domains. Maintaining individual two-way trusts between all domains creates a complex administrative nightmare. The use of Kerberos transitive domains cuts down on inter-domain administration. This can best be explained by example of a user/client seeking services in another domain. As illustrated in Figure 11-4, Entcert1.com has a trust relationship with Entcert2.com. Entcert2.com has a trust relationship with Entcert3.com. There is no trust between Entcert1.com and Entcert3.com. A client from Entcert1.com accessing a service on a server in Entcert3.com would obtain a service ticket through the following steps (the numbers appearing in Figure 4 correspond to the following numbered explanations):

1. Use the TGS service in Entcert1.com to obtain a referral ticket for a KDC in Entcert2.com.

2. Use the referral ticket with the TGS service on the KDC in Entcert2.com and obtain a referral for Entcert3.com.

3. Use the second referral ticket with the TGS service on the KDC for Entcert3.com and obtain a service ticket for the server in Entcert3.com.

4. Use the Client/Server Exchange to open a session with the service in Entcert3.com.

Delegation with Forwarding and Proxy

Some server services require access to a second server, such as a back-end database. In order to establish a session with the second server, the primary server must be authenticated on behalf of the client's user account and authority level. This is common in a three-tier client/server model. This activity is commonly accomplished with proxy or forwarding authentication."[21]

Student Enrollment Applications

21 Retrieved March 12, 2015 Kerberos Explained. http://technet.microsoft.com/en-us/library/bb742516.aspx

Many colleges use student information systems. Some names of these include Banner, Canvas, and so on. These are central cogs in the college process for students, administrators and even faculty. Students/administrators/faculty typically use these systems to pay for/enroll/change courses, enter/change/access grades, access housing assignments, change contact information and a myriad of other functions. This, of course, makes this an attractive target for attackers. These applications contain their own vulnerabilities as any application software does. Are they always kept updated? Are they fully secure? Have they been previously penetrated? And so on.

Mitigations

Universities should use, at a minimum, a signature based intrusion prevention system (IPS), and an anomaly based IPS system. Intrusion detection/prevention systems "are security tools that, like other measures such as antivirus software, firewalls and access control schemes, are intended to strengthen the security of information and communication systems".[22]

The third system, Snort, provides detection of possible attacks which have circumvented the prevention systems.

Palo Alto Systems, an important purveyor of network security hardware and software provides what an IPs is in a thorough and yet clear manner.[23] "An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine. Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application.

Prevention

The IPS often sits directly behind the firewall and it provides a complementary layer of analysis that negatively selects for dangerous content. Unlike its predecessor the Intrusion Detection System (IDS)—which is a passive system that scans traffic and reports back on threats—the IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network. Specifically, these actions include:

- Sending an alarm to the administrator (as would be seen in an IDS)
- Dropping the malicious packets

---

22 "Anomaly-based network intrusion detection: Techniques, systems and challenges", P. Garcıa-Teodoro, J.Dıaz-Verdejo, G. Macia Fernandez, E.Vazquez. Computers & Security 28 (2009) 18–2.

23 Retrieved March 12, 2015 https://www.paloaltonetworks.com/resources/learning-center/what-is-an-intrusion-prevention-system-ips.html

- Blocking traffic from the source address
- Resetting the connection

As an inline security component, the IPS must work efficiently to avoid degrading network performance. It must also work fast because exploits can happen in near real-time. The IPS must also detect and respond accurately, so as to eliminate threats and false positives (legitimate packets misread as threats).

Detection

The IPS has a number of detection methods for finding exploits, but signature-based detection and statistical anomaly-based detection are the two dominant mechanisms.

Signature-based detection is based on a dictionary of uniquely identifiable patterns (or signatures) in the code of each exploit. As an exploit is discovered, its signature is recorded and stored in a continuously growing dictionary of signatures. Signature detection for IPS breaks down into two types:

- **Exploit-facing** signatures identify individual exploits by triggering on the unique patterns of a particular exploit attempt. The IPS can identify specific exploits by finding a match with an exploit-facing signature in the traffic stream
- **Vulnerability-facing** signatures are broader signatures that target the underlying vulnerability in the system that is being targeted. These signatures allow networks to be protected from variants of an exploit that may not have been directly observed in the wild, but also raise the risk of false-positives.

Statistical anomaly detection takes samples of network traffic at random and compares them to a pre-calculated baseline performance level. When the sample of network traffic activity is outside the parameters of baseline performance, the IPS takes action to handle the situation."

It is crucial this software, much like virus software, gets routinely updated against attack definitions. In addition, campus administrators need to configure this software to properly block the network traffic, or, depending upon need, simply get the software to generate an alert according to these attack definitions. These attacks are typically numerous. Andreas Bohman, the Chief Security Officer for Central Washington University, indicates that the university gets "attacks" many thousands of times a month.

The noted anti-virus vendor, McAfee describes this issue in this manner.[24] "Simply put, anomaly-based intrusion detection triggers an alarm on the IDS when some type of unusual behavior occurs on your network. This would include any event, state, content, or behavior that is considered to be abnormal by a pre-defined standard. Anything that deviates from this baseline of "normal" behavior will be flagged and logged as anomalous.

---

24 Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection, Fengmin Gong, McAfee Systems, https://secure.mcafee.com/japan/products/pdf/Deciphering_Detection_Techniques-Anomaly-Based_Detection_WP_en.pdf

"Normal" behavior can be programmed into the system based on offline learning and research or the system can learn the "normal" behavior online while processing the network traffic.
Some examples of anomalous behavior include:
• HTTP traffic on a non-standard port, say port 53 (protocol anomaly)
• Backdoor service on well-known standard port, e.g., peer-to-peer file sharing using Gnutella on port 80 (protocol anomaly and statistical anomaly)
• A segment of binary code in a user password (application anomaly)
• Too much UDP compared to TCP traffic (statistical anomaly)
• A greater number of bytes coming from an HTTP browser than are going to it (application and statistical anomaly)

Anomaly-Based vs. Signature-Based

What ís the Difference?

When a network is being monitored for potential security incidents, an IDS can implement anomaly and/or signature-based intrusion detection. There are advantages and disadvantages to each method. The best-fortified network uses the two methods together to provide the maximum defense for the network infrastructure.

A signature generally refers to a set of conditions that characterizes the direct manifestation of intrusion activities in terms of packet headers and payload content. Historically, the signature-based method has been the more common of the two methods when looking for suspicious or malicious activity on the network. This method relies on its database of attack signatures and when one or more of these signatures match what ís observed in the live traffic, in the case of a NIDS, an alarm is triggered and the event is logged for further investigation. Signature-based intrusion detection is only as good as its database.

If a signature is not in the database, the IDS will not catch the attack. This is obviously a drawback when you consider that hackers spend a great deal of their time crafting attacks designed to fool signature-based systems.

Anomaly-based intrusion detection, on the other hand, takes a more generalized approach when looking for and detecting threats to your network. When an event falls outside baseline parameters, it is flagged and logged. The behavior is a characterization of the state of the protected system, which is both reflective of the system health and sensitive to attacks. In this context, an anomaly-based method of intrusion detection has the potential to detect new or unknown attacks. Like the signature-based method, however, anomaly-based intrusion detection also relies on information that tells it what is normal and what is not. This is called a profile, and it is key to an effective anomaly-based intrusion detection system.

The Profile

For anomaly-based intrusion detection to be effective, it must have a robust profile that characterizes normal behavior. The target could be a host/IP address, VLAN or physical LAN segment. A profile consists of a comprehensive list of parameters and values that are specifically geared to the target being

monitored. A robust profile must be stable and consistent in tracking the normal behavior of the target environment. An effective anomaly profile must also be sensitive to occurrences of any events that are deemed to be security concerns. Constructing an effective profile involves gathering information on behavior and activity currently considered acceptable on your network. Profiles can vary in complexity from a couple of simple thresholds to comprehensive content characterizations to multi-variable distributions." These systems can be effective. Over the past decade many anomaly-detection techniques have been proposed and/or deployed to provide early warnings of cyber-attacks due to this success.[25] Dartmouth's anomaly IPS system blocked almost 20,000 attacks in 2009 alone.[26]

Spam filtering technology

Many universities utilize several layers of spam filters in order to identify and drop suspicious email. One such software product is Precise Mail. This tool is used by universities as diverse as Rutgers on the East Coast to Central Washington University on the West Coast. This tool allows end-users to:

1. Have control over how they want their external, non-CWU, mail processed, with more or less being sent to GroupWise, the email platform.

2. Add entries on their Allow list so expected mail goes straight to GroupWise, without getting hung up in Precise Mail.[27]

Precise Mail Anti-Spam Gateway can do any of the following things with a message it determines to be spam:
• The message can be discarded
• The message can be quarantined
• The message can have X-PMAS headers added to it
• The message can have its subject line modified and be delivered.[28]

---

25 Undermining an Anomaly-Based Intrusion Detection System Using Common Exploits, Kymie M.C. Tan, Kevin S. Killourhy, and Roy A. Maxion. http://www.cs.cmu.edu/afs/cs.cmu.edu/user/maxion/www/pubs/TanKillourhyMaxion02.pdf

26 Retrieved January 22, 2015 http://dujs.dartmouth.edu/fall-2009/cyber-attacks-on-the-dartmouth-college-network#.UuAWSbTTmUk

27 Retrieved January 22, 2015 https://www.cwu.edu/campus-notices/spam-filtering-here-cwu

28 "PreciseMail Anti-Spam Gateway User's Guide http://sebsits.rutgers.edu/pmas_users_guide.pdf

Server and Workstation Systems

This category fits into the standard anti-virus software environment familiar to most of us. Each institution uses its own preferred software suites. Arguably, any of the more effective products will serve well. For example, servers should execute local firewalls and anti-virus software from vendors such as McAfee or Symantec, or a myriad of others. And then there are products such as LanDesk. LanDesk keeps Windows computers up-to-date with patches. LANDesk is an asset management software system used to remotely inventory and manage desktop computers. It has the ability to report on installed software and hardware, allow remote assistance, and install operating system security patches.[29] Also, it is necessary to provide an early-warning of data compromises on Unix servers. Open Source Tripwire software is such an example. Tripwire is a security and data integrity tool useful for monitoring and alerting on specific file change(s) on a range of systems.[30] Finally, some servers also use log monitoring tools like Logwatch, LogLogic, Snort or Splunk to detect suspicious anomalies in server logs. There is also a wealth of antispyware and anti-malware products that should be installed and executed and kept up to date such as MalawareBytes.[31]

Workstation Systems

Universities, of course, are able to maintain control over university-owned systems such as administrative servers, desktops, laptops, tablets, etc. However, control over non-university owned systems is less sure. LanDesk can be tasked to update workstations under college control. Recent malware such as the Conficker worm have left Dartmouth systems relatively untouched (see "Malware" for details) suggesting that the College's compulsory update practices work well. It is also wise to have a current acceptable use policy. An example can be found at http://www.cwu.edu/its/acceptable-and-ethical-use-policy by Central Washington University in Ellensburg, Washington. Copyright infringement rules should also be posted and students/staff/faculty sign an acknowledgement of abeyance. An example of one such policy can be found at http://www.cwu.edu/its/intellectual-property-copyright-infringement

---

29 Retrieved March 12, 2015 http://www.american.edu/oit/software/LANDesk-FAQ.cfm#whatis

30 Retrieved March 12, 2015 http://sourceforge.net/projects/tripwire/

31 Retrieved March 12, 2015 https://www.malwarebytes.org/enterprise/

Conclusion

It is clear that cyberattackers will continue to be active. A problem exists In that they are both prolific and increasing in the complexity of their attacks. This, of course, means that academic institutions must correspondingly be both proactive and effective in dealing with this threat. There is a definite need to continually employ the latest mitigation strategies and products and continue to be vigilant. Open source products can be used whenever possible to control costs but more effective products such as Splunk may need to be purchased and effectively deployed and upgraded as time progresses. Above all, institutions of higher education must continue user training so that these users can be yet another defense to cyberattacks.