Office Action Response – MAGIC BLACK HOLE
Serial No. 88328846

I. Likelihood of Confusion

a. Comparison of Marks

In response to the refusal for likelihood of confusion with respect to the registered mark BLACK HOLE TECHNOLOGY (Reg. No. 5482414), Applicant respectfully disagrees and would like to respond with the following.

In comparison of the two marks, the term "TECHNOLOGY" is disclaimed in the registered mark, and therefore should be given less weight than the dominant portions of the mark. Other than this disclaimed term however, all other portions should be seen as equally weighted and dominant. The examiner claims that:

> "The addition of the term MAGIC to applicant's mark also does not change the commercial impression of the mark because MAGIC acts as an adjective and merely describes the dominant phrase, BLACK HOLE. Thus, it is subservient to the dominant phrase. Therefore, the dominant phrase in applicant's mark is BLACK HOLE."

Applicant respectfully contends that this reasoning is not correct, and is a misinterpretation of the TMEP and associated case law. "MAGIC" in this case is an entirely fanciful and arbitrary term. The Examiner contends that because one use of the term "MAGIC" is an adjective, therefore it is subservient. However, the exact language of the TMEP states: "If the common element of two marks is "weak" in that it is generic, descriptive, or highly suggestive of the named goods or services, it is unlikely that consumers will be confused unless the overall combinations have other commonality."[TMEP1207.01(b)(viii)]. The "weakness" of a term is dependent on its descriptiveness of the goods/services the mark is associated with, rather than the analysis simply determining what parts of speech each term in the overall mark is. In this context "MAGIC" has nothing to do with the goods of computer software, and therefore is a fanciful and arbitrary term in the overall mark "MAGIC BLACK HOLE". "Although there is no mechanical test to select a "dominant" element of a compound word mark, consumers would be more likely to perceive a fanciful or arbitrary term, rather than a descriptive or generic term, as the source-indicating feature of the mark. [TMEP1207.01(b)(viii)] As such, consumers would likely perceive "MAGIC" as a fellow dominant portion of the mark along with BLACK HOLE.

Given the above analysis there must be said to be an appreciable distinction between "MAGIC BLACK HOLE" and "BLACK HOLE TECHNOLGOY" (or even "BLACK HOLE" discounting the disclaimed portion of the registered mark). Further, this fanciful and arbitrary term "MAGIC" will give a clearly distinct commercial impression from "BLACK HOLE TECHNOLGOY". "MAGIC" being something distinct, and usually orthogonal, to "TECHNOLOGY". Therefore, Applicant respectfully contends that the two instant marks are distinct to such a degree that the average consuming public would not be confused by the source identification.

b. Comparison of Goods

In terms of the comparison of goods, Applicant respectfully contends there are appreciable differences here as well. As the Examiner has highlighted, the comparison is between: "Computer software and computer programs, namely, systems and network security software directed to internet security, e-mail management, e-mail filtering, anti-virus, anti-spam, e-mail policy management" (Applicant's goods) and Registration No. 5482414 covers "Computer hardware and software for use in recognizing, identifying, stopping, recording, and tracking cyber hacking attacks to computer networks". While these two goods exist in the field of computer software and cyber security, that is where the similarity ends. Registrant's goods are concerned with the recording and respond to cyber attacks to computer networks. The security of computer networks is something concerns the access of networks, distribution and monitoring of credentials, and monitoring usage of network-accessible resources [EXHIBIT A]. Applicant's goods on the other hand are strictly relating to emails, their management and filtering of unwanted email. As such, these two goods are distinct in their application and their use. This in turn would cause their purchasing public to be different, people looking for network security compared to people looking for email management tools.

In combination, the distinction in marks when all terms are given their necessary weight and dominance, and the distinction in goods, when comparing the two separate areas of technology which each good services (network security vs email management), Applicant contends that there is not an impermissible level of likelihood of confusion as to warrant a refusal. Applicant respectfully requests immediately proceeding to the Principal Register.

II. <u>Entity Clarification</u>

For clarification, Applicant is a Limited Liability Company formed in Canada. Applicant will amend as such accordingly.

III. <u>Amending of Goods</u>

Applicant accepts the amendments as proposed by the Examiner and will amend as such: *Downloaded computer software and computer programs, namely, network security software in the fields of internet security and threat detection, e-mail management, e-mail filtering, anti-virus, anti-spam, e-mail policy management*

IV. <u>44(d) Advisory - Suspension Pending Foreign Application</u>

Applicant informs the Examining Attorney that the corresponding foreign registration in Canada has not yet issued. As such, applicant requests that the U.S. application be suspended until a copy of the foreign registration is available.

EXHIBIT A

WIKIPEDIA

Network security

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: it secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Contents

Network security concept

Network security starts with authentication, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users.[1] Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS)[2] help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wireshark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account.[3]

Communication between two hosts using a network may be encrypted to maintain privacy.

Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.[4]

Security management

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. In order to minimize susceptibility to malicious attacks from external threats to the network, corporations often employ tools which carry out network security verifications (https://ipfabric.io/product/network-security/).

Types of attacks

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movements to find and gain access to assets available via the network.[5]

Types of attacks include:[6]

- Passive
  - Network
    - Wiretapping
    - Port scanner
    - Idle scan
    - Encryption
    - Traffic analysis
- Active:
  - Virus
  - Eavesdropping
  - Data modification
  - Denial-of-service attack
  - DNS spoofing
  - Man in the middle
  - ARP poisoning
  - VLAN hopping
  - Smurf attack
  - Buffer overflow
  - Heap overflow
  - Format string attack
  - SQL injection
  - Phishing
  - Cross-site scripting
  - CSRF
  - Cyber-attack

See also

- Cloud computing security
- Crimeware
- Cyber security standards
- Data loss prevention software
- Greynet
- Identity-based security
- Metasploit Project
- Mobile security
- Netsentron
- Network enclave
- Network Security Toolkit
- TCP Gender Changer
- TCP sequence prediction attack
- TCP sequence prediction attack
- Timeline of computer security hacker history
- Wireless security
- Dynamic secrets
- Low Orbit Ion Cannon
- High Orbit Ion Cannon

References

1. A Role-Based Trusted Network Provides Pervasive Security and Compliance (http://newsroom.cisco.com/dlls/2008/ts_010208b.html?sid=BAC-NewsWire) - interview with Jayshree Ullal, senior VP of Cisco
2. Dave Dittrich, *Network monitoring/Intrusion Detection Systems (IDS)* (http://staff.washington.edu/dittrich/network.html) Archived (https://web.archive.org/web/20060827234520/http://staff.washington.edu/dittrich/network.html) 2006-08-27 at the Wayback Machine, University of Washington.
3. "Dark Reading: Automating Breach Detection For The Way Security Professionals Think" (http://www.darkreading.com/operations/automating-breach-detection-for-the-way-security-professionals-think/a/d-id/1322443). October 1, 2015.
4. " "Honeypots, Honeynets"" (http://www.honeypots.net). Honeypots.net. 2007-05-26. Retrieved 2011-12-09.
5. Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257
6. "BIG-IP logout page" (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf) (PDF). Cnss.gov. 1970-01-01. Retrieved 2018-09-24.

Further reading

- *Case Study: Network Clarity* (http://www.scmagazine.com/case-study-network-clarity/article/324988), SC Magazine 2014
- Cisco. (2011). What is network security?. Retrieved from cisco.com (http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html)
- Security of the Internet (http://www.cert.org/encyc_article/tocencyc.html) (*The Froehlich/Kent Encyclopedia of Telecommunications vol. 15*. Marcel Dekker, New York, 1997, pp. 231–255.)
- *Introduction to Network Security* (http://www.interhack.net/pubs/network-security), Matt Curtin.
- *MPLS, SD-WAN and Network Security'* (http://www.catonetworks.com/blog/mpls-sdwan-and-network-security/)*, Yishay Yovel.*
- *Security Monitoring with Cisco Security MARS* (http://www.ciscopress.com/bookstore/product.asp?isbn=1587052709), Gary Halleen/Greg Kellogg, Cisco Press, Jul. 6, 2007.
- *Self-Defending Networks: The Next Generation of Network Security* (http://www.ciscopress.com/bookstore/product.asp?isbn=1587052539), Duane DeCapite, Cisco Press, Sep. 8, 2006.
- *Security Threat Mitigation and Response: Understanding CS-MARS* (http://www.ciscopress.com/bookstore/product.asp?isbn=1587052601), Dale Tesch/Greg Abelar (http://www.ciscopress.com/authors/bio.asp?a=b411523c-c935-4708-a563-d24de8fcfc71), Cisco Press, Sep. 26, 2006.
- *Securing Your Business with Cisco ASA and PIX Firewalls* (http://www.ciscopress.com/bookstore/product.asp?isbn=1587052148), Greg Abelar (http://www.ciscopress.com/authors/bio.asp?a=b411523c-c935-4708-a563-d24de8fcfc71), Cisco Press, May 27, 2005.
- *Deploying Zone-Based Firewalls* (http://www.ciscopress.com/bookstore/product.asp?isbn=1587053101), Ivan Pepelnjak, Cisco Press, Oct. 5, 2006.

- *Network Security: PRIVATE Communication in a PUBLIC World*, Charlie Kaufman | Radia Perlman | Mike Speciner, Prentice-Hall, 2002. ISBN .
- *Network Infrastructure Security* (https://www.springer.com/computer/communications/book/978-1-4419-0165-1), Angus Wong and Alan Yeung, Springer, 2009.