Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Aging protocols that could incapacitate the Internet

Prof. Bharate L.M.[1], Prof. Patil P.S.[2], Prof. Joshi A.S.[3] Prof. Mane S.M.[4]

[1,3,4] Assistant Professor, Department of CSE, VVPIET, Solapur
[2]Assistant Professor, Department of CSE, BIT, Barshi.

Abstract--The biggest threat to the Internet is the fact that it was never really designed. For e.g., the BGP protocol is used by Internet routers to exchange information about changes to the Internet's network topologies. However, it also is among the most fundamentally broken; as Internet routing information can be poisoned with bogus routing information. Instead, it evolved in fits and start, thanks to various protocols that have been cobbled together to fulfill the needs of the moment. Few of protocols from them were designed with security in mind. or if they were sported no more than was needed to keep out a nosy neighbor, not a malicious attacker. The result is a welter of aging protocols susceptible to exploit on an Internet scale. Here are six Internet protocols that could stand to be replaced sooner rather than later or are (mercifully) on the way out.
Keywords-- Aging protocols, Secure Sockets Layer, Internet Protocol, domain name system, SMTP.

I. INTRODUCTION

The biggest threat to the Internet is that it evolved over time with various protocols, there are very few of which are designed with security in mind. For example, the BGP protocol is used by Internet routers to exchange information about changes to the Internet's network topology. However, it is also among the most fundamentally broken, as Internet routing information could be poisoned with bogus routing information. One of email's underlying protocols is SMTP, which has no inherent protection due to its origins in a time when cyber attacks were not common. Meanwhile, a warning for domain name system (DNS) security was sounded in 2008 when a massive flaw in the protocol's design was discovered. That spurred work on DNSSEC, a protection extension for DNS, as a way to keep fake data from being inserted into DNS servers. though, DNSSEC needs to be implemented to work in the first place.

NTP keeps the clocks of computers around the world in sync, but it is a product of an age in which safety measures was not a top precedence, making it possible to use the mechanics of the protocol, in grouping with a fleet of compromised computers, to launch denial-of-service attacks. Meanwhile, Internet Protocol (IP) version 4 is fast running out of Web address space, and the only key is a migration to IPv6.
Secure Sockets Layer (SSL) has had a replacement for years, but only now are Internet organizations replacing it.

II. BGP: BORDER GATEWAY PROTOCOL

BGP is used by Internet routers to exchange information about changes to the Internet’s network topology, making it one of the oldest and most vital Internet protocols. It’s also among the most

basically broken down, built at a time when Internet peering was based on little more than mutual faith. With a little work, Internet routing information can be poisoned with bogus routing information, also called as BGP spoofing.

Such spoofing has happened before, many times. The resulting failure is usually obvious enough that it's detected and corrected in small measure, but it offers enough of a window for an attacker to do horrible damage. Worst of all, the problem is essentially unfixable as it presently stands. As Dave Rand of Trend Micro explained to Larry Seltzer, no central authority can be used to verify whether a particular address belongs to a particular network. And because BGP is such a preliminary protocol, there's no replacing it in the small term. At least the Core Infrastructure plan has put "fixing BGP" on its to-do list. BGP is also used by Internet Service Providers (ISPs) to direct traffic between services around the world. BGP, simply put, is the backbone of the Internet. The crisis, however, is that it's easy to trick this routing protocol into sending information where it should not go. For security-sensitive information, that is terrible.

And, because BGP is the almost literal backbone of the Internet, it's very hard to replace or even fix. It's akin to "Highway Star" Gillian rear-ending people on the road—simple to do, damaging and complex to prove malicious intent. It's also quite familiar.

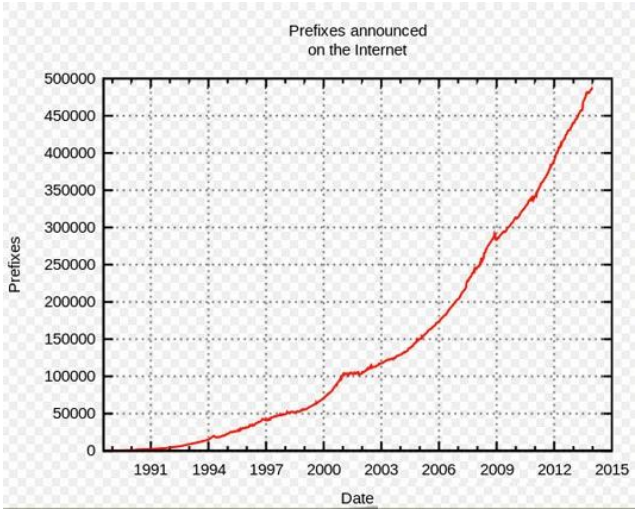

Fig. 1 Prefixes announced on the Internet.

III. SMTP: SIMPLE MAIL TRANSFER PROTOCOL

Our second aging standard is the Simple Mail Transfer Protocol (SMTP). SMTP is used to send and receive email. actually, that's all it does. It was first established in 1982, when the Internet was in its early life and the idea of bad actors seemed far-fetched by its creators (the first iteration of SMTP lacked any type of security). present iterations of SMTP do have security fundamentals, like domain verification to make sure the mail is sent to the intended server and vice versa, but these aren't mandatory for the protocol. That makes it unimportant for hackers to send a malicious email or make their spamming operations unknown. It's as if our Gillian character could speed by people so rapidly, or kick up so much dirt, that no one would be able to identify him.
Despite myriad initiatives launched over the years to destroy it off, email remains in wide use, along with one of its fundamental protocols, SMTP. SMTP's biggest problem, as put in an email by Steve Hultquist; chief evangelist at network analytics firm Red Seal, is that it has no inherent security due to its origins in more innocent days: "SMTP was conceived as a simple way to transfer email

between users on the Internet when it was young and before the protocol architects had recognized the threat of terrible actors."Over time, various bolt-ons for SMTP have been developed to tighten its security. head among them is reverse DNS checking to ensure the sender is in fact who they claim to be. But the protocols themselves don't mandate that kind of security; it's a matter of who bothers to apply them. All it takes is one mail gateway that doesn't perform due diligence with incoming email to blow the game for everybody. Maybe Inbox will be able to show a way out of the email muddle, but don't hold your breath.

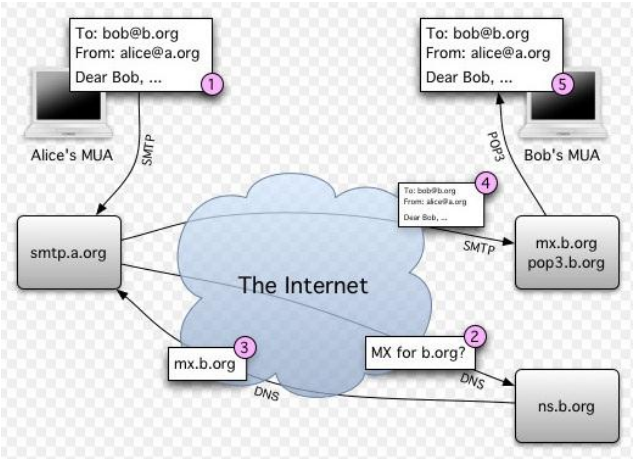

Fig. 2 simple mail transfer on internet.

IV. DNS: DOMAIN NAME SYSTEM

This protocol, like BGP and others, has protection issues. With DNS, it's pretty serious: hackers, for a time could easily insert fake data into DNS servers, allow them to interrupt user and application requests. moreover, DNS names can be used to implement a phishing attack—a type of attack hackers use to trick you into giving up responsive information. A phishing attack through the DNS allows a hacker's website to pose as a legal site, like UPS.com, through similar domain names, like USP.com.So how can you protect yourself from these clear, aging vulnerabilities? Sadly, there is little you can really do. setting up each of these issues is tricky because so many legacy systems-—older systems built with these protocols in mind—would break if any were to go offline. While you only cannot fix these problems.

Because the Internet protocol that translates IP addresses into domain names is so foundational to the way the Internet works, it is a ordinary attack, due to flaw in the protocol and security weaknesses in the software that discover it. The Iranian Cyber Army outright took over the DNS servers for Twitter's domain, and the Syrian Electronic Army hijack the New York Times' domain registration account. A wake-up call for DNS security was sounded in 2008 when security researcher Dan Kaminsky unearthed a massive flaw in the protocol's design. That spur work on DNSSEC, a security addition for DNS, as a way to keep fake data from being inserted into DNS servers. But DNSSEC wants to be implemented to work in the first place. poorer, it can impact the performance of a DNS server under heavy load and could even be used to launch denial-of-service indication attacks. The cure may not be as bad as the bug, but it's clearly a work in progress.

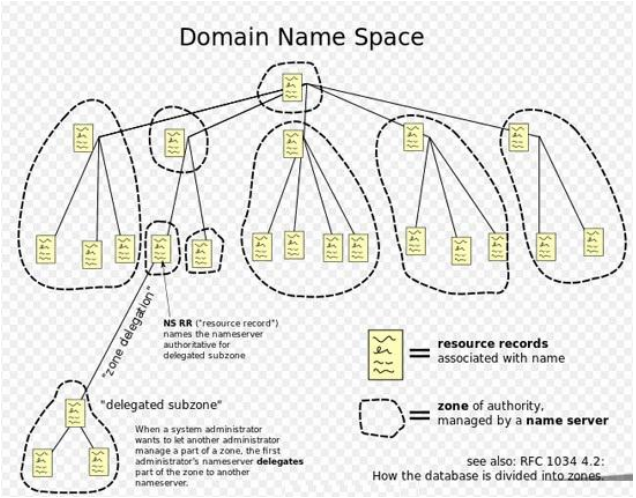

Fig. 3 Domain name space.

V. NTP: NETWORK TIME PROTOCOL

NTP's noble purpose is to keep the clocks of computers around the world in sync, from whole server farms to simple desktops.

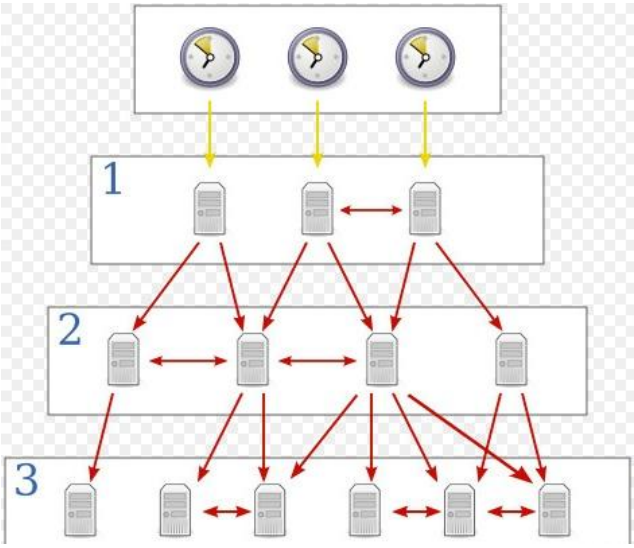

Fig.4 Network Time Protocol.

But it, too, is a product of an age in which security wasn't a top precedence. That made it feasible to use the mechanics of the protocol, in combination with a fleet of compromised computers, to launch denial-of-service attacks. Fortunately, good work is being done to ensure that NTP servers are patched against such exploits and have been set up properly from the beginning to keep the attacks from occurrence. But nothing says future exploit of NTP are not feasible, especially given the lack of scrutiny over the protocol and its implementations in the past.

VI. IPV4: INTERNET PROTOCOL

Despite all the clever dodges to work around the depletion of the IPv4 address space, no one denies the days of IPv4 allocations -- even for big names like Microsoft -- are fast upcoming to an end. The

only workable long-term solution has been known for years: Migrate to IPv6.IPv6 is making good headway in new technology markets such as the mobile globe, where IPv6 is broadly used for 4G networks. For everybody else, the obstacles in the way of moving to IPv6 are seemingly nonstop. Simple inertia is a big one: Many won't upgrade unless they are compulsory to Qualified IPv6 expertise remains insufficient, according to California IPv6 Task Force co chair Ed Horley, and the NIST is troubled that attackers are poised to pounce the minute the switches are thrown. Then over again, no one said altering the fundamental infrastructure of the Internet would be easy

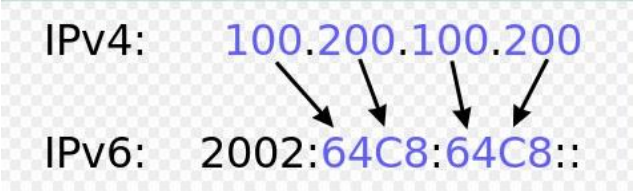

Fig. 4 Internet Protocol.

VII. SSL: SECURE SOCKETS LAYER

As a rule of thumb, the elder a protocol, the more likely it is to be broken in some way -- and the more urgently it needs to be replaced with a descendant. Secure Sockets Layer has had a substitution for years, but only now are we getting around to ditching SSL, mainly because disaster struck.SSL was designed to provide cryptographic protection for application-layer connections like HTTP, but its last open revision was in 1996. A alternate protocol, Transport Layer Security appeared three years afterward, and its widely used 1.2 version landed in 2008. But SSL itself remains in use, in big part as a backward-compatibility evaluated. Consequently, all major browsers have continued to support SSL even if it's used in only 0.3 percent of the communication conducted today (according to Mozilla).

Now we have as good an incentive to ditch SSL altogether as there could be: The infamous POODLE attack, for which the best improvement measure is to get rid of SSL -- period. Mozilla and Google are now doing that, meaning any enterprise that used SSL internally for whatever reason also require to ditch it, stat. Maybe backward compatibility isn't all it's cracked up to be.

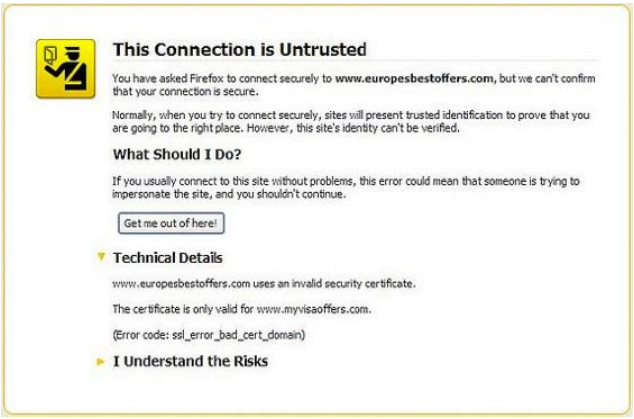

Fig.4 Network Time Protocol.

VIII. CONCLUSION

In sum, network security is always a big issue. Network attacks just reflect various problems in the existing network architecture and protocol organization. We just categorize them and list some possible ways to deal with them. From Border Gateway Protocol to Secure Sockets Layer, several Internet protocols are no match for today's malicious hackers and should be replaced.

REFERENCES

[1] Caicedo, C. E. , J. B. Joshi, and D. Tuladhar, 2009. IPv6 Security Challenges, IEEE Computers, 42(2):36-42.
[2] Atul Kant Kaushik, and R C Joshi, 2010. "Network Forensic System for ICMP Attacks" International Journal of Computer Applications;2(3):14–21.
[3] Daniel L. lough, David, C. lee., Scott F. Midkiff, Nathaniel J. Davis IV, and Phillip E. Benchoff,1998.The Next Generation of the Internet: "Aspects of the IPv6", IEEE Network, 12(1):28-33.
[4] Saleh, A. M. , and J. M. Simmons, 2011. Technology & architecture to enable the explosive growth of the internet-IEEE Communications Magazine.
[5] Ugo Fiore & Francesco Palmieri. Enhanced security strategies for MPLS signaling; -Journal of Networks;2[5], 2007
[6] Douligeris C, D. Serpanos, Serpanos, D. 2007.IP Security (IPSec) . IEEE Book: Network Security: Current Status and Future directions;65 – 82.
[7] Behrouz A. Forouzan. "TCP/IP Protocol Suite"; third edition. :- Publication-Tata McGraw Hill[2003]
[8] Hiromi, R.; Yoshifuji, H., "Problems on IPv4-IPv6 n/w transition",- Proceeding of the International Symposium on Applications and the Internet Workshop;Saint 2005.
[9] S. Kent. 1989. Comments on security problems in the TCP/IP suite. ACM SIGCOMM Computer Communication Review;19[3] 10-19
[10] Goth, G. 2012. The End of IPv4 is Nearly Here in 2014, IEEE Internet Computing; 16(2) 7-11.
[11] W. R. Stevens, TCP/IP Illustrated Volume-1 –The Protocols; Addison-Wesley-1994
[12] S. M. Bellovin, "Security Problems in the TCP/IP Protocols"; Computer Communications analysis, Volume-19, No. 2, pp. 32-48, April 1989.
[13] Krsul, C. L. Schuba, I.V. Kuhn, Makus G. E.H. Spafford, D. Zamboni, A. Sundaram, Analysis of a Denial of Service Attack on TCP.
[14] CERT, 'TCP SYN Flooding and IP Spoofing Attack';- Carnegie Mellon University.
[15] D. E. Comer, Internetworking with TCP/IP: Volume- I Principles, Protocols & Architecture, Prentice Hall.
[16] S. Cheung, K. N. Levitt, C. Ko, "Intrusion Detection for Network Infrastructures"; IEEE Symposium on Security & Privacy, Oakland, CA[May 1995]

BIOGRAPHIES

Prof. Bharate L.M. is Asst. Professor at VVPIET, Solapur. His qualifications include B.E.(CSE), M.Tech(SE).He have a rich industrial as well as teaching experience in the areas of Data Communication and Computer Networks, Information Security; Web Technology. His research interests include Computer Networks and Network Security..

Prof. Patil P.S. is Asst. Professor at BIT, Barshi. Her qualifications include B.E.(CSE), M.Tech(SE). She have a rich industrial as well as teaching experience in the areas of s/w Engineering, Data Communication and Computer n/w & Security. Her research interests include Computer Networks and Network Security.

Prof. Joshi A.S. is Asst. Professor at VVPIET, Solapur. His qualifications include B.E.(CSE), M.E(CN). He has a rich industrial as well as teaching experience in the areas of Data Structure, Data Communication and Computer Networks & Security. His research interests include Computer Networks and Network Security.

Prof. Mane S.M. is Asst. Professor at VVPIET, Solapur. His qualifications include B.E.(CSE), M.E(CSE). He has a rich teaching experience in the areas of Data Communication and Computer Networks & Security. His research interests include Computer Networks.

