Volume 2, Issue 1, January 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Improving the more security in data transmission by using dynamic key And router updating techniques

Dr.R.Seshadri
Prof & Director of university computer center
S.V.University, Tirupati, India

Prof.N..Penchalaiah
Department of Computer Science Engineering
ASCET, Gudur, India

Abstract—**Now days the wireless networks are facing a gigantic problem of network security. Even though there are some kinds of algorithms[4][5] and methods to rise above this obscurity, there is something that is left unsatisfied yet, such as data transfer with a great safekeeping and fortification, to put off the hackers from information thieving and modification, to salvage the data from various viruses etc., Here now we will make out some problems that occurred for the period of information transmitting viz. Service and performance constraints, Unauthorized use of service, solutions[12] to those problems, MAC Spoofing[7] and Session Hijacking, Traffic analysis and Eavesdropping, Higher level attacks, Rogue access points, SMTP[3] session hijacking, Operating system bugs, different types of security methods like Treat base stations as un trusted, Setting up a virtual private network(VPN)[6] and some of the other important methods are also discussed in this paper.**

***Keywords*— TKIP, EAP, PEAP, WEP, VPN, VLAN, WPA**

I. INTRODUCTION

Generally there are a few concepts that are used frequently when discussing security options. These issues need to be addressed when sensitive information is transferred over the internet via web, email or wireless applications. These **key concepts** are:

II. AUTHENTICATION

Authentication[6] is the process of proving one's identity to another individual or system component. The more secure the method of authentication, the more confident you can be that individuals who interact with the system are who they claim to be. A common method of authentication is the username/password challenge. This method is only secured if the password is chosen wisely and if the password is not made accessible to others.

There are different protocols [3] used in the authentication, they are*:*

A. TKIP(Temporal Key Integrity Protocol)

This stands for temporal key integrity protocol[3], and the acronym is pronounced as fee-kip, this is part of the IEEE 802.11i standard. TKIP implements per-packet key mixing with a re-keying system and also provides a message integrity check. These avoid the problems of WEP.

B. EAP(Extensible Authentication Protocol)

The WPA[6][7] improvement over the IEEE 802.1x, standards already improved the authentications for accesses of wireless of wired LANs. In addition to this, extra measures such as the extensible authentication protocol[6], have initiated an even greater amount of security, this as EAP uses a central authentications server.

EAP Versions: EAP-MSCHAPv2, EAP-FAST

C. PEAP(Protected Extensible Authentication Protocol)

This stands for protected Extensible Authentication Protocol[3][6], this protocols allows for a secure transport of

data, passwords, and encryption keys without the need of a certificate server. This was developed by CISCO, Microsoft, and RSA security.

III. CONFIDENTIALITY

Confidentiality is achieved through encryption. Encryption is the process of protecting information from unintended recipients. It therefore provides privacy and is often used in conjunction with authentication to hide user identity information (such as user name/pw)

IV. INTEGRITY

Integrity of info is every bit as important as authentication and confidentiality when securely transferring information between two parties. Data integrity is preserved with digital signatures. These are a mechanism used to verify that a piece of information as come from a secure recognized by the system and has not been modified by an unrecognized or unauthorized party. Digital certificates can be used with a digital signing algorithm to verify the integrity of documents

V. NON-REPUDIATION

This is the acknowledgement that a contract/ debt are legally enforceable. Without the benefit of face to face interaction, notarization or signed hard copies and receipts, employing a secure means of authentication, signing and encrypting[4]. Information is vital for any secure application. A properly implemented digital security model does more than just empower individuals with the ability to safely communicate private info across a network. It is also enables reliable and legally binding audits. Authentication[6], confidentiality and integrity are the key concepts of the non repudiation.

VI. TYPES OF SECURITY PROBLEMS

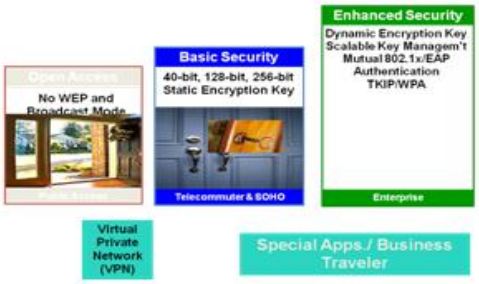


Fig. 1. Basic Wireless Security Profiles

A. *Easy access*

Wireless LANs are easy to find. Strictly speaking, this is not a security threat. All wireless networks need to announce their existence so potential clients can link up and use the services provided by the network. 802.11 require that networks periodically announce their existence to the world with special frames called Beacons.

However, the information needed to join a network is also the information needed to launch an attack on a network. Beacon frames are not processed by any privacy functions, which mean that your 802.11 network and its parameters are available for anybody with an 802.11 card. "War drivers" have used high-gain antennas and software to log the appearance of Beacon frames and associate them with a geographic location using GPS.

Short of moving into heavily-shielded office space that does not allow RF signals to escape, there is no solution for this problem. The best you can do is to mitigate the risk by using strong access control and encryption solutions to prevent a wireless network from being used as an easy entry point into the network. Deploy access points outside firewalls, and protect sensitive traffic with VPNs.

B. *Unauthorized use of service*

Several war drivers have published results indicating that a clear majority of access points are put in service with only minimal modifications to their default configuration. Nearly all of the access points running with default configurations have not activated WEP (Wired Equivalent Privacy) nor have a default key used by all the vendor's products out of the box. Without WEP[6][7], network access is usually there for the taking.

Two problems can result from such open access. In addition to bandwidth charges for unauthorized use, legal problems may result. Unauthorized users may not necessarily obey your service provider's terms of service, and it may take only one spammer to cause your ISP to revoke your connectivity.

Whether unauthorized use is a problem depends on the objectives of the service. For corporate users extending wired networks, access to wireless networks must be as tightly controlled as for the existing wired network. Strong authentication is a must before access is granted to the network.

C. *Service and performance constraints*

Wireless LANs have limited transmission capacity. Networks based on 802.11b have a bit rate of 11 Mbps, and networks based on the newer 802.11a technology have bit rates up to 54 Mbps. This capacity is shared between all the users associated with an access point. Due to MAC-layer overhead, the actual effective throughput tops out at roughly

half of the nominal bit rate. It is not hard to imagine how local area

Radio capacity can be overwhelmed in several ways. It can be swamped by traffic coming in from the wired network at a rate greater than the radio channel can handle. If an attacker were to launch a ping flood from a Fast Ethernet segment, it could easily overwhelm the capacity of an access point. Depending on the deployment scenario, it might even be possible to overwhelm several access points by using a broadcast address as the destination of the ping flood.

Attackers could also inject traffic into the radio network without being attached to a wireless access point. The 802.11 MAC is designed to allow multiple networks to share the same space and radio channel. Attackers wishing to take out the wireless network could send their own traffic on the same radio channel, and the target network would accommodate the new traffic as best it could use the CSMA/CA mechanisms in the standard.

Large traffic loads need not be maliciously generated, either, as any network engineer can tell you. Large file transfers or complex client/server systems may transfer large amounts of data over the network to assist users with their jobs. If enough users start pulling vast tracts of data through the same access point, network access may resemble sucking molasses through a straw north of the Arctic Circle in January.

Addressing performance problems starts with monitoring and discovering them. Many access points will report statistics via SNMP, but not with the level of detail required to make sense of end-user performance complaints. Wireless network analyzers can report on the signal quality and network health at a single location, but tools designed for wireless network administrators are only beginning to emerge.

D. MAC Spoofing and Session Hijacking

802.11 networks do not authenticate frames. Every frame has a source address, but there is no guarantee that the station sending the frame actually put the frame "in the air." Just as on traditional Ethernet networks, there is no protection against forgery of frame source addresses. Attackers can use spoofed frames to redirect traffic and corrupt ARP tables. At a much simpler level, attackers can observe the MAC addresses of stations in use on the network and adopt those addresses for malicious transmissions. To prevent this class of attacks, user authentication mechanisms are being developed for 802.11 networks. By requiring authentication by potential users, unauthorized users can be kept from accessing the network. (Denial of service attacks will still be possible, though, because nothing can keep attackers from having access to the radio layer.

Attackers can use spoofed frames in active attacks as well. In addition to hijacking sessions, attackers can exploit the lack of authentication of access points. Access points are identified by their broadcasts of Beacon frames. Any station that claims to be an access point and broadcasts the right service set identifier (SSID, also commonly called a network name) will appear to be part of an authorized network. Attackers can, however, easily pretend to be an access point because nothing in 802.11 requires an access point to prove it really is an access point. At that point, the attacker could potentially steal credentials and use them to gain access to the network through a man-in-the-middle (MITM) attack.

Using methods based on TLS, access points will need to prove their identity before clients provide authentication credentials, and credentials are protected by strong cryptography for transmission over the air.

E. Higher level attacks

Previously in the Series Once an attacker gains access to a wireless network, it can serve as a launch point for attacks on other systems. Many networks have a hard outer shell composed of perimeter security devices that are carefully configured and meticulously monitored. Inside the shell, though, is a soft, vulnerable (and tasty?)Center.

F. Rogue access points

Easy access to wireless LANs is coupled with easy deployment. When combined, these two characteristics can cause headaches for network administrators. Any user can run to a nearby computer store, purchase an access point, and connect it to the corporate network without authorization. Many access points are now priced well within the signing authority of even the most junior managers. Departments may also be able to roll out their own wireless LANs without authorization from the powers that be.

"Rogue" access points deployed by end users pose great security risks. End users are not security experts, and may not be aware of the risks posed by wireless LANs. Most existing small deployments mapped by war drivers do not enable the security features on products, and many access points have had only minimal changes made to the default settings. It is hard to believe that end users within a large corporation will do much better.

G. Traffic analysis and Eavesdropping

802.11 provide no protection against attacks that passively observe traffic. The main risk is that 802.11 do not provide a way to secure data in transit against eavesdropping. Frame headers are always "in the clear" and are visible to anybody with a wireless network analyzer. Security against eavesdropping was supposed to be provided by the much-maligned Wired Equivalent Privacy specification. A great deal has been written about the flaws in WEP[8]. It protects only the initial association with the network and user data frames. Management and control frames are not encrypted or authenticated by WEP[8], leaving an attacker wide latitude to disrupt transmissions with spoofed frames. Early WEP implementations are vulnerable to cracking by tools such as Air Snort and WE Crack, but the latest firmware releases from most vendors eliminate all known attacks. The latest products go one step farther and use key management protocols to change the WEP key every 15 minutes. Even the busiest wireless LAN does not generate enough data for known attacks to recover the key in 15 minutes.

Whether you rely on WEP solely, or layer stronger cryptographic solutions on top of it is largely a question of risk management. The latest product releases have no known vulnerabilities. While that is some comfort, the same claim could have been made in July 2001 before release of the current generation of WEP-cracking tools. If your wireless LAN is being used for sensitive data, WEP may very well be insufficient for your needs. Strong cryptographic solutions like SSH, SSL, and IPSec were designed to transmit data securely over public channels and have proven resistant to attack over many years, and will almost certainly provide a higher level of security.

1) *Application backdoors :* Some programs have special features that allow for remote access. Others contain bugs that provide a backdoor, or hidden access, that provides some level of control of the program.
2) *SMTP session hijacking :* SMTP[is the most common method of Sending e-mail over the Internet . By gaining access to a list of e- mail Addresses , a person can send unsolicited junk e-mail (spam) to thousands of users . This is done quite often by redirecting the e-mail through the SMTP[3] server of an unsuspecting host , making the actual sender of the spam difficult to trace.
3) *Operating system bugs:* Like applications , some operating systems Have backdoors . Others provide remote access with insufficient security controls or have bugs that an experienced hacker can take advantage of .
4) *Denial of service :* You have probably heard this phrase used in news reports on the attacks on major Web sites . This type of attack is nearly Impossible to counter. What happens is that the hacker sends a request to the server to connect to it . When the server responds with an acknowledgement and tries to establish a session , it cannot find the system that made the request . By inundating a server with these unanswerable session requests a hacker causes the server to slow to a crawl or eventually crash.
5) *E-mail bombs:* An e-mail bomb is usually a personal attack. Someone sends you the same e-mail hundreds or thousands of times until your e-mail system cannot accept any more messages.
6) *Viruses:* Probably the most well-known threat is computer viruses. A virus is a small program that can copy itself to other computers. This way it can spread quickly from one system to the next. Viruses range from harmless messages to erasing all of your data.
7) *Spam:* Typically harmless but always annoying, spam is the electronic equivalent of junk mail. Spam can be dangerous though. Quite often it contains links to Web sites. Be careful of clicking on these because you may accidentally accept a cookie that provides a backdoor to your computer.
8) *Redirect bombs :*Hackers can use ICMP to change (redirect) the Path information takes by sending it to a different router . This is one of the ways that a denial of service attack is set up.

H. SOLUTIONS

Algorithms for security in wireless networks:

1) Encryption algorithm

Generally speaking, an encryption[4] and P (plain text) +R (pseudo random bit) = C(cipher)-----(1).

P (plain text) = C (cipher) - R (pseudo random bit) ---(2)[12].

The evolution of cipher system stems from

Traditional linear, mechanical, simple Substitution and shifting stream cipher to Nonlinear electrical, software block cipher and Till today's public key cipher. All of the above Cipher systems, linear stream cipher is the Simplest and easy to be implemented. Its characteristic is that the generated pseudo random bits possess recursive and superposition property. Each bit in the sequence has close correlation. Even when some bits have been damaged or jammed, we still can recover the bit stream by recursive and superposition criterion. As to the nonlinear stream cipher and public key

Cipher[4] system, when their data has been attacked, the only way for recovering the pseudo random bit sequence is to check the preset key table. Block cipher system is implemented based on substitution, permutation and shifting by using software to replace the hardware system. For public key, it is a high security ciphering system, especially for triple DES, which is still unbreakable until now because its key length is over.

2) Spread spectrum

Most of the telecommunication and satellite communication systems used spread spectrum[12] techniques for increasing the capability of data security and anti-noise and jamming [lO][ll]. Since the data has been spread, its recovery rate has also been raised. For example, if we transmitted a "l", only when we receive a "1" then we can claim that it is correct. But if we spread a "1" three times such as "1117', then we receive "0 1 l", " 10 1 ", "1 1 O", or " 1 1 1 ",we can recover the original right data "1" by means of majority or maximum likelihood theorem[12]. In recent years, the spread spectrum technique has been applied for watermarking. However, the only one approach is direct spreading. Here, we propose two new processing methods. One is called block spread spectrum which is based on block processing. The other is called duplicate spreading whose characteristic is performing duplication. By using the block and duplicate spreading, we can increase the information quantity of embedded data by reducing the embedding[10] capacity. As the embedded data information increases, the recovery capability is also raised.

3) Resolving problems

There are many options that organizations can do today to put proper security protection around their wireless strategy and technology, A 128-bit WEP[8] key is usually entered as a string of 26 hexadecimal characters. 26 digits of four bits each gives 104 bits; adding the 24-bit IV produces the complete 128-bit WEP key. Most devices also allow the user to enter it as 13 ASCII characters. A 256-bit WEP system is available from some vendors. As with the other WEP-variants 24 bits of that is for the IV, leaving 232 bits for actual protection. These 232 bits are typically entered as 58 hexadecimal characters. ((58 × 4 bits =) 232 bits) + 24 IV bits = 256-bit WEP key.Hence we can provide more secure to the data by 256 bits of that for the IV, and providing dynamic key to the data instead of public key. If WEP-based security is the only option available on your router, it's time to upgrade. Newer routers will likely have WPA-based encryption on several different levels. The normal variations are WPA and WPA2. Beyond that, there's two different types of authentication; TKIP[3] (as mentioned above) as well as "AES," which is a newer and more secure method. AES and TKIP are the algorithms used during the sending and receiving of packets via the network. AES is more advanced and provides a higher level of protection. TKIP was really only developed to provide an "interim" solution until something better could be developed, which was eventually AES. Most routers that use WPA [6][7]are setup to use TKIP[3] by default, so simply logging into your router and changing the setting to AES can a make a world of difference.

The only way to crack WPA[8], as mentioned above, is to sniff out the password associated with the "handshake" authentication [6]process, and if this password is extremely complicated, it will be almost impossible to crack. The only downside to this high-level of security is the fact that it will slow down the overall speed of your network, but in the long-run, it's well worth it.

4) Wireless security policy and architecture design

Organization need to develop a wireless security policy to define what not allowed with wireless technology. From a holistic view, the wireless net work should be designed with the proper architecture to minimize risk. Because of wireless leakage, one of the first principles to basic field coverage is to only to provide coverage for the areas that you want to have access.

5) Wireless policy issues

Policy needs to dictate permitted services and usage i.e., what types of connections are permitted? Wireless access is often binary. I.e. full net work access or no network access-roles potentially need to be created for. (Scanner vs.ful LAN access), One needs a means of identifying enforcing wireless access policies Policy needs to indicate how access will be controlled…i.e., time of the day. Policy requirements dictate that all access needs to be logged Use complains and standards enforcements. Centralized control of security policies Wireless management Wireless intrusion alert issues Process to update client software levels

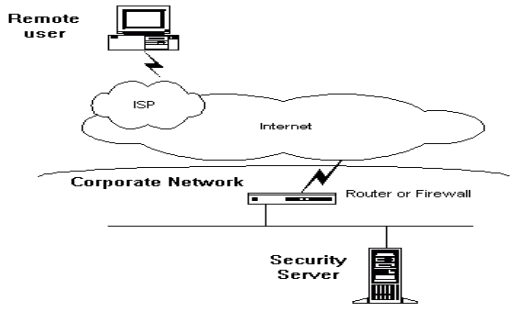
6) Intrusion detection polices

Treat base stations as un trusted From the network security architecture, the base stations should be evaluated and determined if it should be treated as an un-trusted device and need to be quarantined before the wireless clients can gain access to the internal network.

Setting up a virtual private network(VPN) It is generally agreed upon that only way to ensure a secure WLAN is to make it a VPN .VPN adds encryption and authentication. This makes a WLAN as usable as a wired LAN.

A virtual private network (VPN) is a way to use a public telecommunication infrastructure , such as the Internet , to provide remote offices or individual users with secure access to their organization's network. A virtual private network[1] can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities , but at a much lower cost. Implementation of network security by VPN.

Step 1. - The remote user dials into their local ISP and logs into the ISP's network as usual.



Step 2- When connectivity to the corporate network is desired, the user initiates a tunnel request to the destination Security server on the corporate network. The security server authenticates the user and creates the other end of tunnel.

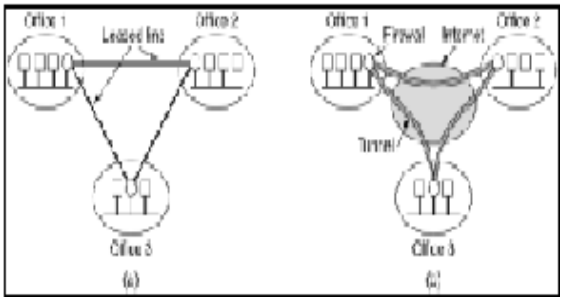


Fig : a) A leased line private network

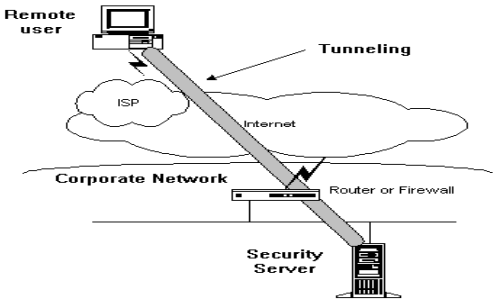
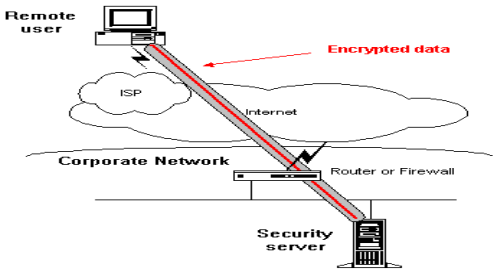
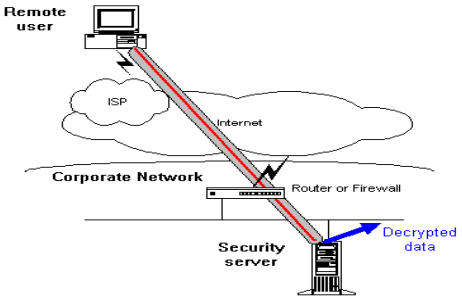


Fig: b) A virtual private network

Step 3. - The user then sends data through the tunnel which encrypted by the VPN[1] software before being sent over the ISP connection.

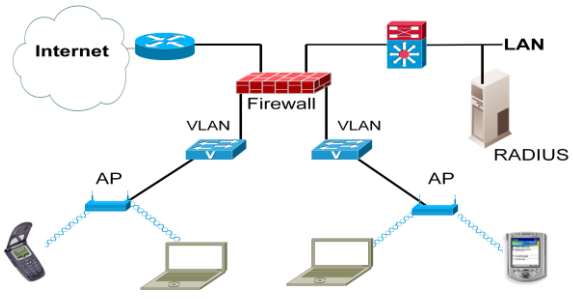


Step 4 - The destination Security server receives the encrypted data and decrypts. The Security server then forwards the decrypted data packets onto the corporate network. Any information sent back to the Remote user is also encrypted before being sent over the Internet.



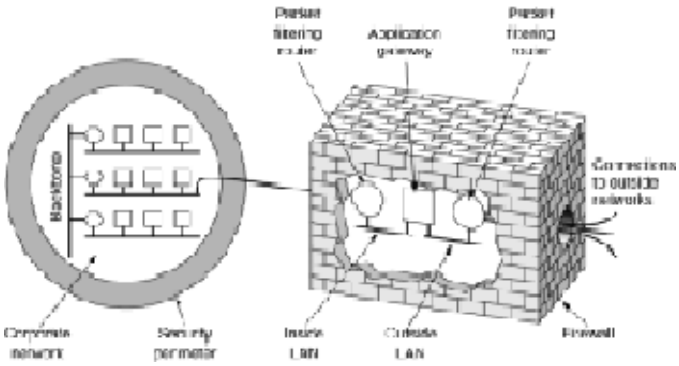
7) Firewall

A firewall[1] provides a strong barrier between your private network and the Internet. You can set firewalls to restrict the number of open ports, what type of packets are passed through and which protocols are allowed through . You should already have a good firewall in place before you implement a VPN, but a firewall can also be used to terminate the VPN sessions.



A firewall is different from antivirus software, but the two of them work together to help protect your computer. You might say that a firewall guards the windows and doors against strangers or unwanted programs trying to get in,

while an antivirus program protects against viruses or other security threats that can try to sneak in through the front door.



8) About VLAN

A virtual local area network, virtual LAN or VLAN[1], is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch. VLAN[1] membership can be configured through software instead of physically relocating devices or connections.

VLAN Benefits:

- Increased performance
- Improved manageability
- Network tuning and simplification of software configurations
- Physical topology independence
- Increased security options

Limitations of VLAN:

- Broadcast limitations
- Device limitations
- Port constraints

9) MAC address filtering

Some access point has the ability to filter only trusted MAC address[1]. The idea is that there is a central department, which the only department is allowed to hand out network access. Then, AP's are configured to only accept connections from a closed set of net work cards should be uniquely identifiable by their MAC address, this is done by maintaining a list of allowed MAC address. All connections from other MAC address are then disallowed.

10) Securing the wireless net works

- Ensure that all unused ports are closed.
- Enforce the rule of least access
- Ensure insurance and authentications standards are created and enforced
- Use strong encryption
- Use dynamic keys in WEP.

VII. CONCLUSION

Wireless LAN security is a work in progress. The protocols are evolving to meet the needs of serious users. Until the protocols have proven themselve , the best course of action for net work engineers Is to assume that the link layer offers no security. Treat wireless stations as you would treat an unknown user asking for access to net work resources over an un-trusted network. Polices and resources developed for remote dial up users may be helpful because of the similarity between a wireless stations and a dial up client. Both are unknown users who must be authenticated before network access is granted, and the use of an UN trusted network means that strong encryption (IPSec,SSlorSSH) should be required.

Meanwhile, the wireless LAN market is one of the few in the telecom arena that is growing, so vendors need to address security if they want to participate. For organization that can handle the extra demands on processing power and network traffic over head involved, virtual private probably offer the most robust security since the wireless side of the network become an integral part of the overall enterprise security infrastructure.

REFERENCES

[1] Arbaugh, W., Mishra, A., .An Initial Security Analysis of the 802.1X Standard.,

[2] R.T. Morris, 1985. *A Weakness in the 4.2BSD Unix TC P/IP Software*. Computing & Science Technical Report No.117, AT&T BellLaboratories, Murray Hill, New Jersey

COMPUTER NETWORKS--ANDREW S. TENAUNBAUM

[3].S.M. Bellovin. *Security Problems in the TCP/IP Protocol Suite*. Computer Communication Review, Vol. 19, No. 2, pp.32-48,April1989.

[4] R.L.Rives.the RC4 Encryption algorithm. RSA Data security, Inc., Mar. 12, 1992

[5] J.Walkers,"overview of 802011 security",

[6] Aboba, B., Simon, D., .PPP EAP TLS Authentication

Protocol,. IETF RFC 2716,

[7] Funk, P., Blake-Wilson, S., .EAP Tunneled TLS Authentication Protocol (EAP-TTLS),.

[8] Walker, Jesse, "Unsafe at any Key Size: an analysis of the WEP encapsulation, November 2000 "

[9] E. Koch and J. Zhao, “Embeddingrobust labels into images for copyright protection,” *Technical report,FRA WHOFER Institute for ComputerGraphics*, Darmstadt, Germany, 1994.

[10] D.CopperSmith , "Fast evolution of algorithms in fields of characteristic row", IEEE Transactions on Information Theory, 30 (1984), 587-594.

[11] J. Pollard. Monte Carlo Methods for Index Computation (mod p).Mathematics of Computation, 32:918-924, 1978.

[12] Stallings, W. Cryptography and Network Security. Prentice Hall, 2003.

[13]. D.Boneh and X. Boyen, Secure Identity Based Encryption Without Random Oracles, extended abstract in Proceedings of CRYPTO '04, LNC 3152, Springer-Verlag, 2004.

AUTHORS

Dr.R.Seshadri Working as Professor & Director, University Computer Centre, Sri Venkateswara University, Tirupati. He was completed his PhD in S.V.University in 1998 in the field of “ Simulation Modeling & Compression of E.C.G. Data Signals (Data compression Techniques) Electronics & Communication Engg.”. He has richest of knowledge in Research field, he is guiding 10 Ph.D in Fulltime as well as Part time. He has vast experience in teaching of 26 years. He published 10 national and international conferences and 18 papers published different Journals.

Prof.N.Penchalaiah Research Scholar in SV University, Tirupati and Working as Professor in CSE Dept,ASCET,Gudur. He was completed his M.Tech in Sathyabama University in 2006. He has 11 years of teaching experience. He guided PG & UG Projects. He published 2 National Conferences and 8 Inter National Journals.