

## Complying with DoT Regulation on Secure Use of WiFi: Less in Letter, More in Spirit

Kaustubh Phanse, Ph.D.  
Wireless Architect

Hemant Chaskar, Ph.D.  
Director, Technology

Pravin Bhagwat, Ph.D.  
CTO

AirTight Networks Pvt. Ltd.

S. No. 7, Pinnac House II, Kothrud, Pune - 411038

The Department of Telecommunications (DoT), Government of India, recently published a regulation (dated February 23, 2009) outlining the procedure for secure use of WiFi. All Internet Service Providers (ISPs)—serving leased line subscribers, home users, and WiFi hotspots in public places—have four months to comply. The DoT regulation comes in the wake of recent events of cyber terrorism in India that exposed how easy it is to misuse unsecured WiFi networks and put national security at stake.

The goal of the DoT regulation is to prevent misuse of WiFi Internet access and to be able to track the perpetrator in case of abuse. To this effect, DoT has instructed ISPs to enforce centralized authentication using LoginID and Password for each user. Organizations subscribing to leased lines have the option to setup and maintain their own centralized authentication and submit proof of compliance to their ISP.

In this article, we discuss why complying with the DoT regulation in letter is not enough to prevent misuse of WiFi. We present complementary measures that can help ISPs and subscribers to comply with the DoT regulation in spirit.

Centralized authentication<sup>1</sup> has long been used in wired networks (e.g., dial-up modems, Ethernet local area networks) to restrict network access to authorized users and to record their network usage. But there is a fundamental difference between wired and WiFi networks. In WiFi, data transmission is unguided and over the air. So a malicious user can bypass the centralized authentication system and misuse WiFi Internet access in several ways. And do it easily without much technical know-how and with off-the-shelf equipment (e.g., laptop) and free software tools available on the Internet.

1. Anyone with a WiFi device in the vicinity of an unsecured WiFi network can eavesdrop on the in-flight data from other users, including sensitive information such as Login ID and Password. A malicious user can use the data to spoof the identity of a legitimate WiFi user, gain unauthorized Internet access, and misuse it.
2. If a legitimate user is already logged into an unsecured WiFi network, a hacker can hijack the session and gain unauthorized Internet access by spoofing the MAC and IP addresses of the authenticated user's device. The hacker does not require Login ID and Password!
3. Use of default settings (e.g., password, SSID) on WiFi access points—those deployed by ISPs or independently by end users—is too common. Information about these default settings is available on the Internet, with which a hacker can gain full control of the access point and misuse it without getting detected.

---

<sup>1</sup> Use of Login ID and Password is one way to implement centralized authentication. For information about other authentication methods, refer to the enclosed Appendix.

4. Despite centralized authentication and wired security measures such as firewalls, unmanaged WiFi devices can open wireless backdoors into enterprise networks. For instance, a “Rogue AP” (an unmanaged WiFi access point attached to the enterprise LAN without administrator’s knowledge) can allow unauthorized users to access the Internet via the enterprise LAN. Even organizations with no official WiFi are equally at risk.
5. Network Address Translation (NAT) is common on WiFi access points. Centralized authentication cannot stop unauthorized users from gaining Internet access through an unsecured NAT AP, nor will it be able to identify the users.
6. A motivated hacker can set up a “honeypot” (a fake WiFi network with the same name or SSID as a neighboring WiFi network). Legitimate users unwittingly connect to the honeypot and leak their credentials. The hacker can then use the stolen credentials to attack the genuine WiFi network and cause havoc.

Before committing a crime, malicious users are unlikely to register their identity with ISPs using a photo ID. They will resort to use of fake photo IDs or even simply, resort to using one of the above means to carry out their mission without leaving a trace. Despite complying with the DoT regulation strictly in letter, ISPs and subscribers may still find themselves at the wrong end of the law.

As a complementary solution, we recommend the following WiFi security best practices. Implementing these guidelines, ISPs and subscribers will be able to truly secure their networks against WiFi misuse, and in turn help DoT will achieve its goal. In fact, if subscribers follow these best practices, ISPs could relax the need for centralized authentication based on Login ID and Password.

1. Any private WiFi network (e.g., enterprises, home users) should be secured with WiFi Protected Access (WPA/WPA2) encryption. WiFi access points should not be left Open (without encryption) and should not use the flawed Wired Equivalent Privacy (WEP) encryption.
2. IEEE 802.1x based central authentication should be used in conjunction with WPA/WPA2. 802.1x authentication is much more secure than Login ID and Password based authentication. For smaller organizations or home subscribers, central authentication is impractical. They should instead use Pre-Shared Key (PSK) based authentication in conjunction with WPA/WPA2. On many access points, this setting is also known as WPA-Personal and WPA2-Personal. For PSK authentication, use a strong passphrase or key that is at least eight characters long and is a combination of alphanumeric and special characters.
3. Do not use factory default or “out of the box” settings on your access points. Change the login and password. Use a strong password that is at least eight characters long and is a combination of alphanumeric and special characters. Change the default SSID to a name that is simple to remember but does not reveal your identity.
4. WiFi hotspots at public places and Guest WiFi access are usually implemented over Open WiFi for ease of use and administration. Here central authentication is necessary. To prevent leakage of sensitive data (e.g., Login and Password), WiFi hotspots should use higher layer security such as secure socket layer (SSL) protocol. For instance, with Web-based authentication, use HTTPS (HTTP with SSL) so that

- when a user authenticates, the Login and Password are sent over a secure connection and cannot be stolen over Open WiFi.
5. Conduct WiFi security audits regularly to avoid gaps in your WiFi security posture and to ensure compliance with the DoT regulation. Consider use of a Wireless Intrusion Prevention System (WIPS) for complete protection against all kinds of wireless threats including unmanaged devices (e.g., Rogue APs). WIPS can also be repurposed as a cost-effective solution for conducting WiFi security audits and submitting DoT regulation compliance reports to your ISP.

In summary, DoT's efforts in ensuring secure use of WiFi are laudable and we see at least two positive outcomes. One it will trigger a nationwide awareness drive about WiFi security. Two it will compel ISPs, enterprises, and end users to take WiFi security seriously. Unless WiFi users implement the suggested WiFi security best practices locally, centralized authentication alone will not serve the purpose DoT is trying to achieve. Bodies such as the Indian Computer Emergency Response Team (CERT-In) and the Data Security Council of India (DSCI) can play an important role in creating awareness about these best practices. ISPs should direct their subscribers to implement the recommended best practices and demand periodic compliance reports. Doing so will allow ISPs to truly secure WiFi Internet access across their subscriber base, while relaxing the stringent requirement of centralized authentication.

## Appendix: Common Authentication Techniques

Authentication is a process of verifying identify of an entity (device or person) at the remote end of a communication link. Authentication methods vary widely based on applications. Described below are common authentication methods used by Internet Service Providers (ISPs).

### PPP Authentication:

PPP (Point to Point Protocol) is widely used protocol to carry IP packets over the serial communication link between the modems at the customer premises called customer premise equipment (CPE) and the ISP POP (Point of Presence). The PPP prescribes initial handshaking during which the two ends of the link can negotiate a common feature set, perform link management functions, and also prescribes formats for framing IP packets over the link.

The PPP (RFC1661) initially provided support for two simple authentication methods (RFC1334) that are still implemented by many ISPs today. The packet link gets established only after successful authentication. The first authentication method is called **PAP** (Password Authentication Protocol) in which the CPE sends the user name and password in clear to the POP until POP acknowledges its receipt. The second method is called **CHAP** in which the POP sends a challenge to the CPE. The CPE prepares response to challenge by cryptographically processing the challenge using the pre-established password. The response is sent to the POP. The POP verifies if the response is correct using the same password. CHAP avoids sending password in clear text over the link.

Note that both PAP and CHAP are typically used to authenticate link termination point at the customer premises. They are typically not used to authenticate end users proper who access the Internet from the customer premises.

However, people thought that PAP and CHAP are relatively weak, because PAP sends password in clear over the link and CHAP cryptographic processing is not strong enough. People demanded support for additional authentication protocols in PPP. To solve this problem, the option of **EAP** (Extensible Authentication Protocol RFC3748) was added in PPP alongside PAP and CHAP. The way EAP is designed, it does not specify any authentication method, but specifies carrier packets for authentication methods. Several authentication methods such as OTP, GTC, smart cards, MSCHAP (Microsoft CHAP) and certificates can used over EAP. EAP is also called as **802.1x**. Due to its flexibility EAP can be also used to authenticate end users proper who access the Internet from the customer premises.

It is common practice that the service provider doesn't want to keep a copy of their user database (usernames, passwords, other credentials etc.) at every POP; they want a central database. The protocol used between the POP and the central database to get permission to allow a dial-in user access to the network is called RADIUS (Remote Access Dial-In User Service).

### Web based Authentication:

In the web based authentication (also called as HTTP authentication), CPE is allowed to establish IP layer connection with the POP, but is not initially allowed to run any application on it. That is, all transport layer ports are closed at the POP for the user. Thereafter there are two methods for authentication – Basic and Digest.

In the Basic authentication, analogous to PAP, username and password are sent in clear to the POP. In Digest authentication, analogous to CHAP, the POP issues challenge to which the CPE has to respond. These authentication transactions take place over HTTP (RFC2068). After successful authentication, the transport layer ports are opened for the user. The authenticated user is later identified at the POP via IP address, cookie etc. Web based authentication is suitable if the POP and the CPE are not connected via serial link, but are connected via routed IP network.

Just as PPP later evolved to incorporate EAP, HTTP based authentications have also evolved to support more advanced methods. For example, HTTPS uses certificate based authentication over HTTP.