Int. J. Information and Computer Security, Vol. 1, No. 1/2, 2007
Original publication at:http://www.inderscience.com/filter.php?aid=12251

Selection of an EAP Authentication Method for a WLAN

Authors: Ali, K M
Owens, T J

Abstract

IEEE 802.1X is a key part of IEEE802.11i. By employing EAP it supports a variety of upper layer authentication methods each with different benefits and drawbacks. Any one of these authentication methods can be the ideal choice for a specific networking environment. The fact that IEEE 802.11i leaves the selection of the most suitable authentication method to system implementers makes the authentication framework more flexible but on the other hand leads to the question of how to select the authentication method that suits an organisation's requirements and specific networking environment. This paper gives an overview of EAP authentication methods and provides a table comparing their properties. It then identifies the crucial factors to be considered when employing EAP authentication methods in WLAN environments. The paper presents algorithms that guide the selection of an EAP-authentication method for a WLAN and demonstrates their application through three examples.

Keywords: IEEE 802.1X, EAP, LEAP, MD5, PEAP, PKI, RADIUS, TLS, TTLS.

1. Introduction

The IEEE 802.1X authentication framework was originally designed for wired networks but due to the flaws and vulnerabilities in the authentication schemes proposed in the original IEEE 802.11 standard, IEEE 802.1X was revised for use on wireless networks. (Shumman and Ran, 2003). IEEE 802.1X is very simple in concept. Its purpose is to implement access control at the point at which a user joins the network. The main point of providing port security is to protect network connections where these connections might be accessible in a non-secure area. The reason why IEEE 802.1X is so appropriate for IEEE 802.11 networks. (Edney, J and Arbaugh, W., 2004) is that the nature of wireless LANs makes almost all links publicly accessible.

IEEE 802.1X divides the network universe into three entities:

1) Supplicant, which wants to join the network.
2) Authenticator, which controls access.
3) Authentication server, which makes authentication decisions.

To accomplish its goals IEEE 802.1X utilises well-known protocols such as EAP and RADIUS. Due to the range of different applications for WLANs, a single authentication method could not be suitable in all cases.

The IEEE 802.11 standard cannot and does not define the upper layer authentication method (by being upper layer the authentication method falls

outside the scope of LAN protocol standards), and instead leaves it to the implementers of the system to decide which authentication method to use.

Given the number of authentication methods that could be supported by EAP, the question arises, which one is the best one to use? There is no simple answer; each method can be an ideal choice for a specific networking environment.

This paper identifies factors upon which the selection decision will depend and based on these factors the paper presents algorithms that guide the selection of the most suitable EAP-authentication method.

The paper is organised as follows: In section 2 an overview is provided of the EAP protocol. In section 3 the most common EAP authentication methods are presented. In section 4 factors to be considered when selecting the most suitable authentication method for a particular WLAN environment are identified. In section 5 algorithms that guide the selection of an EAP authentication method are presented. In section 6 examples of the application of the selection algorithms are provided. In section 7 managerial implications of ensuring the chosen authentication method maintains the required level of protection are discussed. The paper is concluded in section 8.

2. EAP

IEEE 802.1X, which provides an authentication framework, employs extensible authentication protocol (EAP) to support various authentication methods.

EAP is a protocol that defines how to carry out authentication, but it is the EAP methods such as TLS, PEAP, LEAP, TTLS, and so forth that actually determine the answer to the question, are you really who you say you are? in the network authentication process.

EAP is a general protocol for PPP authentication and is built around the challenge/response communication paradigm. (Ma and Cao, 2003). EAP does not select a specific authentication method at the link control phase, but rather postpones this decision until the authentication phase. This allows the authenticator (access point) to request more information before determining the specific authentication method. The EAP authentication process can be summarised as follows:

- The authenticator sends one or more requests to authenticate the supplicant. The request message has a type field to indicate what is being requested.
- The supplicant responds to each request. The type field of the response message must correspond to that of the request message.
- After multiple exchanges of request/response messages, the authenticator ends the authentication phase with a success or failure message.

EAP messages do not have an addressing mechanism and are transmitted as EAPOL protocol between the supplicant and the authenticator, and are carried as a RADIUS attribute between the authenticator and the authentication server (RADIUS) (Mishra and Ho, 2004).

3. EAP Authentication Methods

As mentioned earlier IEEE 802.1X by employing EAP supports a variety of authentication methods with different

benefits and drawbacks. This section provides an overview of the most common EAP authentication methods, and compares their properties and security attributes in table 1.

▪ **MD5:** Message digest 5 (MD5) is a challenge-based unilateral authentication mechanism. As with any other authentication scheme that uses a random challenge combined with a password and hash algorithm, it is open to a dictionary attack. There are three main reasons that MD5 is an inappropriate wireless authentication algorithm:

Firstly, MD5 requires that the user password be stored in a way that lets the authenticator get at the original plain text password. This opens up the possibility of an entity other than the authentication server getting access to the file of passwords.

Secondly, MD5 only authenticates the supplicant. It does nothing to authenticate the authentication server, the RADIUS server. Since wireless is especially vulnerable to impersonation, this is a major problem. Whereas impersonating a dial-up access server on the other end of a phone line is fairly difficult, impersonating a wireless access server just means getting within a couple hundred feet of the supplicant. This lack of mutual authentication is the basic reason why some wireless vendors have chosen not to allow MD5 as an authentication option for WLANs.

Thirdly, MD5 does not create a WEP session key, ideally, immediately after authentication, the wireless client and access point jump into WEP-encrypted communications, which reduces the risks of eavesdropping, impersonation, or data corruption by a hostile attacker. This problem limits its usefulness in the wireless world.

For all these reasons MD5 is not recommended to be used as an authentication method in WLANs.

▪ **LEAP:** LEAP is Cisco's lightweight EAP, which is widely deployed in today's WLANs. (Cisco Systems, 2003).

With this method, the RADIUS server sends an authentication challenge to the client, the client uses a one-way hash of the user-supplied password to fashion a response to the RADIUS server. Using information from its user database, the RADIUS server creates it is own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, enabling the client to authenticate the RADIUS server. After the completion of this process, an EAP success/failure message is sent to the client and both the RADIUS server and the client derive the dynamic WEP key.

LEAP's use of unencrypted challenges and responses does leave it open to online (active) and offline (passive) dictionary attacks. Active dictionary attacks can be prevented using lockout mechanisms available on RADIUS servers to lockout the user after a certain number of invalid login attempts. An offline dictionary attack such as that using a tool that was introduced at Unstrung's live event in New York (Cisco Systems, 2003) is carried out in two phases to uncover the user's password. In the first phase, the attacker captures the challenge/response messages exchanged between the user and the access point. In the second phase, the attacker looks for a password match by computing a list of possible challenge/response messages using a pre-computed dictionary and comparing these messages against the captured challenge/response messages. The attacker uses known

authentication protocol vulnerabilities to reduce the size of the user password dictionary (Cisco Systems, 2004).

Using a strong password policy and periodically expiring passwords significantly reduces an offline attack tools chances of success. Unlike online attacks, offline attacks are not easily detected. With Cisco's LEAP, security keys change dynamically with every communication session, preventing an attacker from collecting the packets required to decode data. (Cisco Systems, 2002).

- TLS: Transport layer security (TLS) protocol is based on SSL v3.0, which is used in most web browsers for secure web transactions. SSL was developed by the Netscape Communications Corporation in 1994 (Cisco Systems, 2003) to secure transactions over the World Wide Web. Soon after, the Internet Engineering Task Force (IETF) began work to develop a standard protocol that provided the same functionality. They used SSL 3.0 as the basis for that work, which became the TLS v1.0 protocol.

TLS provides a very secure mutual authentication protocol that overcomes the shortcomings of the password-based and challenge-based methods.

TLS uses public key certificates to authenticate both the wireless clients and the RADIUS servers by establishing an encrypted TLS session between the two communicating parties.

The TLS protocol is composed of two layers: the TLS record protocol and the TLS handshake protocol (Ma and Cao, 2003).

The TLS record protocol provides connection security that has two basic properties:

1. The connection is private. Symmetric key cryptography is used for data encryption. The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol such as TLS handshake protocol. The record protocol can also be used without encryption.
2. The connection is reliable. The message transport includes a message integrity check using a keyed MAC. Secure hash functions are used for MAC computations. The record protocol can operate without a MAC, but is generally only used in this mode while another protocol uses the record protocol as transport for negotiating security parameters.

While the TLS record protocol is used for encapsulation of various higher level protocols, the TLS handshake protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. The TLS handshake protocol provides connection security that has the following properties:

1. The peer's identity can be identified using symmetric or public key cryptography.
2. The negotiation of the shared secret is secure.
3. The negotiation is reliable in that no attacker can modify the negotiation without being detected by the communicating parties.

EPA-TLS is considered as the best available (security wise) authentication method for WLANs but the main concern with this method is that it requires Public Key Infrastructure (PKI) because it uses a digital certificate to authenticate the server to the client; the server requires the client

to send it a digital certificate if it wishes to authenticate the client.

▪ **TTLS:** To overcome complications associated with the use of PKI in the client, tunnelled transport layer security (TTLS) was developed.

With TTLS, server site certificates are required. As the one of the few currently available tunnelling authentication methods, TTLS is a two step authentication method, in the first step, an asymmetric algorithm based on server keys is used to verify the server's identity and set up a symmetric encryption tunnel.

The second step involves verifying the client's identity by using a second authentication method through the symmetric encryption tunnel for the actual authentication negotiation. The second authentication method used within the tunnel may by an EAP type (often MD5) or a legacy method such as PAP.

The symmetric encryption tunnel of TTLS is used only for protecting the authentication method, therefore, once verified the encryption tunnel collapses and it is up to the client and the server to create a WEP encryption tunnel for on-going data confidentiality.

EAP-TTLS offers strong security during authentication while accommodating existing end-user working methods (user ID/password), thus avoiding the complexities of PKI in the client's site.

▪ **PEAP:** Protected EAP (PEAP) is an authentication type that is designed to allow hybrid authentication. While for server-side authentication PEAP employs PKI, for client-side authentication, PEAP can use any other EAP authentication type. But unlike TTLS, legacy methods are not supported for the client authentication step. There is an EAP-MS CHAP v2 implementation, but this is incompatible with older RADIUS servers that do not provide EAP support. Because PEAP establishes a secure tunnel via server-side authentication, non-mutually authenticating EAP types can be used for client-side authentication. (Cisco Systems, 2002).

PEAP is based on server-side EAP-TLS, and it addresses the manageability and scalability shortcomings of EAP-TLS. Organisations can avoid the issues associated with installing digital certificates on every client machine as required by EAP-TLS and select the method of client authentication that best suits them.

4. Selection factors

This paper provides algorithms that guide the selection of an EAP-authentication method for a WLAN. The first step in achieving this is the identification of factors upon which the selection decision will depend.

Recalling that different authentication methods have different security capabilities, and provide organisations with different levels of protection, the degree of protection provided by different authentication methods is the first factor to be considered.

The level of protection provided by a certain authentication method depends on:

- Authentication method's implementation technique
- Authentication attribute: mutual or unilateral

Recalling that all EAP-authentication methods (except MD5, which is not recommended for WLANs and is therefore not considered) provide mutual authentication, then the decisive factor when comparing the

level of protection provided by different authentication methods will be their implementation technique.

It is very important to understand the difference between the protection level provided by authentication methods and the protection level required by organisations. These are two totally different concepts while the former depends only on the implementation technique used the latter depends on the security risks and possible attacks in a certain environment as well as the business reasons for deploying WLANs.

The vulnerability of a WLAN in a specific environment, that is the security threats and possible attacks in that environment, is the second factor to be considered in the authentication method selection process.

The third factor comes from the fact that the basic pre-requisite to employ any of these methods is the existence of a supportive network infrastructure or the possibility to upgrade it to meet the requirements of the authentication method that is capable of providing the required protection.

A supportive network infrastructure includes all the hardware, software and firmware components required by a certain authentication method. Different authentication methods depending on their implementation technique require different WLAN infrastructure. While the deployment of TLS requires the existence of public key (PKI) infrastructure, LEAP requires Cisco products or Cisco compatible exchange program (CCX) for non-Cisco infrastructure. Clearly, if the existing infrastructure does not support the IEEE 802.1X authentication frame, or upgrading the existing infrastructure to meet the requirements of the authentication frame is unacceptable, there is no point considering the deployment of EAP-authentication methods.

Finally, as with any other such selection procedure, the cost of implementing a particular authentication method cannot be ignored.

The authentication method's implementation cost always includes the cost of any infrastructure upgrade required to implement the method as well as the cost associated with upgrading the knowledge and skills of the users of the WLAN clients to a level that enables them to use the newly implemented authentication method without difficulties.

From the above discussion and the fact that each of the authentication methods is implemented using a different technique (password-based, certificate-based, and tunnelling), the implementation costs of different authentication methods will vary. Not only that but the implementation cost for the same authentication method in different networking environments will be different depending on the existing WLAN infrastructure.

Crucial is the ability of organisations or WLAN customers to meet the implementation cost imposed by the authentication method that can provide them with the desired level of protection. If that is not the case they might still be able to select another authentication method that is compatible with their budget, but it might not be strong enough to provide the desired level of security. Clearly, in cases where the organisation's emphasis is on security there is no point in implementing any authentication method that is not capable of providing the required level of security.

It is obvious that there is a strong relationship between the selection

factors, each of them having a great impact on the other factors and the selection process itself. For example, if the selected authentication method is not supported by the existing WLAN infrastructure, then there is a need to upgrade it, which means additional implementation costs. If an upgrade is unacceptable then the second best authentication method that is supported by the existing infrastructure has to be selected, but it might not be strong enough to provide the desired degree of protection.

The implementation cost can be very high or very low (in some cases the most secure solution can be implemented without any significant cost) depending on the existing infrastructure and the requirements of a particular organisation in terms of the desired level of security.

There are other less important factors, which will not be considered in this paper, such as deployment difficulties, and the complexity of administration and management, etc.

Due to the following facts the selection of the most suitable authentication method is a very difficult process:

- The selection of the most suitable authentication method does not depend on one factor rather it depends on many factors, which are related and contradictory.

- Based on the fact that different authentication methods require different supportive infrastructure, the authentication method's implementation cost will be different for different authentication methods.

- Different authentication methods are vulnerable to different types of security threats and attacks.

- The security level desired by a certain organisation in a specific environment depends not only on the authentication method used but also on the networking environment and the value and importance of the applications and information hosted by the WLAN and the business reasons for deploying WLANs.

5. EAP Method Selection Algorithms

To provide organisations and WLANs customers with the most suitable authentication solution for their security needs and specific networking environments, EAP authentication method selection algorithms have been developed that are presented in this paper.

The reasons that contributed to the need for these algorithms can be summarised as follows:

- IEEE 802 standards do not define the upper layer authentication scheme instead they leave the choice of this scheme to the system implementers.
- The IEEE 802.1X authentication frame supports a variety of authentication methods each with different benefits and drawbacks. Any one of these methods might be an ideal choice in certain environments.
- Due to the range of WLAN applications a single authentication method could not be suitable for all WLANs.
- Different authentication methods have different security capabilities and require different supportive infrastructure.

Firstly, selection algorithms will be developed based on each one of the selection factors identified in the previous section separately and later the main selection algorithm will be constructed by considering all these factors together.

Based on the discussion in the previous section, the selection algorithms will adhere to the following assumptions:

- The selection algorithms must provide organisations with the authentication method that suits their security requirements with the minimum implementation cost.
- The security (protection) level desired by organisations is the most important factor to be considered in the selection process.
- The authentication method's implementation cost is associated with any infrastructure upgrade required.
- If the existing infrastructure supports the implementation of the most secure authentication method there is no other factor to be considered since there will not be any significant additional costs associated with the authentication method's implementation.

The selection of the most suitable authentication method, based only on the provided degree of security, is a one-step process that involves the identification of the degree of protection provided by different authentication methods.

The selection algorithm is shown in Figure 1 and an explanation of how it works follows.

If an organisation's emphasis is on the most secure solution regardless of other factors such as the existing network infrastructure then TLS represents the best available option. However, if the organisation is not prepared for any reason to deal with the complexities associated with the use of digital certificates on the client's sites, or it does not require the level of security provided by TLS, then it has to consider employing one of the tunnelled methods. The most suitable tunnelled method to employ depends on the organisation's approach to authenticating its WLAN clients. Finally, if the organisation does not require the level of security provided by the above-mentioned methods then LEAP is the only available option.

This algorithm is simple and easy to use. However, the problem with this algorithm is that it selects the most secure solution based not on the vulnerabilities of the environment (the desired degree of protection) but on the authentication method's implementation technique (the provided level of protection).

The selection algorithm based only on the security threats is the most important one factor based algorithm because it identifies the desired level of security in a specific networking environment.

The most demanding step of this algorithm is the identification of the security threats. Once these threats and attacks are identified it is quite easy to select the authentication method that is capable of providing the required level of security.

The identification of the desired level of security depends on the security threats, the importance and value of the applications and information hosted by the WLAN, and the business reasons for deploying the WLAN. The selection algorithm is shown in Figure 2 and an explanation of how it works follows.

In networking environments where MITM and dictionary attacks are possible threats then the only available solution is to deploy TLS. However, if the protection needed is only against dictionary attacks then depending on the network infrastructure and implementation cost organisations can select TTLS, PEAP or TLS.

On the other hand, if there is a threat of MITM attacks but not dictionary attacks, then LEAP or TLS must be considered.

In cases where the organisation's emphasis is on hiding its clients' identities then any one of the tunnelled methods must be considered. The most suitable tunnelled method to deploy depends on the organisation's approach to authenticating its clients.

The basic advantage of this algorithm is its ability to identify the authentication method that is capable of securing the network against the identified security threats. However, in some cases the implementation cost may be very high.

The third selection algorithm is based only on the existing network infrastructure, other factors are not considered.

With this algorithm the selection process begins by investigating the existing WLAN infrastructure and then selecting the most secure authentication method that is supported by it. The selection algorithm is shown in Figure 3 and an explanation of how it works follows.

If upgrading the infrastructure to implement an EAP-authentication method is unacceptable then the following decision process applies. If the existing network infrastructure supports IEEE 802.1X and digital certificates are already in use by other applications then TLS would be the ideal choice since it would secure the WLAN with the strongest available authentication method without any additional costs. But if that is not the case and the existing infrastructure only supports server side certificates then based on the approach the organisation adopts to authenticating its WLAN clients, one of the tunnelled methods can be implemented. On the other hand, if the infrastructure supports the IEEE 802.1X authentication framework but does not support the use of digital certificates for either of the communicating parties, then the organisation is left with the last available authentication option, which is LEAP. It is obvious that if there is no 802.1X supportive infrastructure it is pointless to consider the deployment of EAP authentication methods.

The basic advantage of using this algorithm is that it identifies authentication methods that do not require any additional infrastructure expenditure. However, it has a major disadvantage which is its inability to identify in some cases the authentication method that is strong enough to provide the desired level of protection.

This algorithm can be used by organisations with limited financial resources or those that want to keep their existing infrastructure.

In the selection algorithm based on implementation cost, the selection process begins by assessing the budget available for authentication method implementation and then selecting the most secure authentication solution that can be implemented within the available budget. In the selection algorithm shown in Figure 4 the decisive factor is the ability of the organisation to match the implementation costs imposed by the authentication methods. An explanation of how it works follows.

If the authentication method's implementation cost in terms of infrastructure spending is not an issue, then TLS is recommended.

Nevertheless, if the organisation is looking for strong authentication methods without the additional costs that come with the implementation of

client side certificates then tunnelled methods represent an adequate solution. The preference for one of the tunnelled methods compared to the others depends on the organisation's requirements to employ legacy or EAP methods to authenticate WLAN clients.

However, if the organisation is not prepared to employ tunnelled methods or if the network is based on Cisco WLAN infrastructure then LEAP represents the only available option.

The major benefit of using this algorithm comes from its ability to identify the strongest possible authentication method that is compatible with the available budget. However, its disadvantage is that in some cases it might not identify the authentication method that provides the desired level of protection. This algorithm can be used by organisations that want to secure their WLANs within an available budget.

To overcome the shortcomings associated with the one factor based selection algorithms presented in this paper, the main selection algorithm of this paper was developed. This algorithm is constructed by considering all the factors previously addressed together, namely, the provided level of protection, the desired security level, the existing network infrastructure, and the implementation cost. The security level required by an organisation is considered to be the most important factor then the other factors are considered together. In the selection process the following steps must be performed:

1. The desired level of security must be identified.
2. The authentication method that is capable of providing the desired level of security must be identified.
3. The components of the infrastructure that is required to support the implementation of the selected authentication method must be identified.
4. If there is a need to upgrade the infrastructure then the implementation cost must be considered.
5. If the upgrade cost is unacceptable then the next best authentication method must be selected.
6. Repeat steps 3 to 5 until the authentication method that suits the particular environment is obtained.

The process of searching for an authentication method that is compatible with a certain environment is not endless. The number of available authentication methods limits it.

The main selection algorithm begins by investigating the existing network infrastructure and identifying security threats, see Figure 5.

If the organisation's emphasis is on protecting its clients identities then depending on the existing network infrastructure one of the tunnelled methods should be deployed. However, if the emphasis in not on protecting client identities and digital certificates are already in use by other applications then TLS provides the most secure solution.

In environments where protection against dictionary attacks is needed then either TLS or one of the tunnelled methods must be considered. On the other hand, if there is a risk of MITM attacks then depending on the network infrastructure and the implementation cost LEAP or TLS must be employed.

In environments where the threats include both MITM and dictionary attacks, the only available solution is TLS.

The main advantage of this algorithm is that it can, for different organisations in different environments, identify the most suitable authentication methods with the minimum possible additional costs.

6. Examples of the Application of the Selection Algorithms

To demonstrate the applicability of the selection algorithms, in the following, they are applied in three different scenarios with different security requirements and different networking environments, and shown to deliver sensible results.

Example 1

The following scenario was taken from http://www.microsoft.com/india/casestudies/patniwireless.aspx on 09/12/05.

"Patni Computer Systems Limited is a global IT services provider with 2003 revenues of US $251 million. Employing over 7,000 people globally, Patni operates multiple offshore development centers across 6 cities in India and 22 international offices across the Americas, Europe and Asia-Pacific. Patni's senior management is on the move constantly from one meeting to another. To give its managers more flexibility and freedom from wires and being tied to a particular location, the IT team decided to implement a wireless Local Area Network (WLAN)".

"Patni wanted to have network access without the hassle of wires, network ports and multiple logons. At the same time Patni wanted to make sure it would be implementing a solution that did not compromise on security, offered flawless connectivity and ease of manageability".

In late 2003 Patni implemented wireless LAN using the WLAN networking support provided in Windows XP and Windows 2000 Server.

"The solution adopted by Patni was a WLAN Implementation using an ISA Server, Digital Certificates and Group Policies. The IS department at Patni began by upgrading its laptops to wireless compatible technologies. Patni uses access points from Cisco and WLAN adapters from multiple vendors namely Cisco, Intel, 3Com etc".

"During the evaluation phase, Patni worked closely with the Microsoft technical team to understand the implementation process, architecture and built-in security options. Based on the understanding gained, the company implemented the Internet Authentication Server for authenticating client credentials".

"The implementation was carried out completely by the IT team at Patni. Multiple Access Points from Cisco were used to provide the best possible coverage. All access points were configured to authenticate users using the 802.1X / TLS authentication. Internet Authentication Server from Microsoft was used as the RADIUS Server".

Solution Provided by Applying the Selection Algorithms

The fact that Patni implemented Wireless LAN using the WLAN networking Support provided in Windows XP and Windows 2000 Server and the fact that Windows XP and Windows 2000 Server both support TLS which is strongest available authentication method together with Patni's emphasis on strong security will be used as the input data for the selection algorithms.

First, the main selection algorithm will be applied and then the selection

algorithm based on the existing infrastructure.

The most suitable authentication method that will be identified by the selection algorithms must meet Patni's requirements, which are mentioned above (their security needs and networking environment), otherwise the applicability of these algorithms will be questionable.

The applicability of the selection algorithms will be judged by comparing their output, namely, the authentication methods they identify as the most suitable solution, with the authentication method that was selected by Patni. If the selection algorithms identify the same authentication method as that adopted by Patni then this result supports their applicability.

Patni's IT team with the support provided by Microsoft Co. selected EAP-TLS as the best solution for their networking environments and security needs.

The main selection algorithm in its attempt to provide this WLAN with the most suitable authentication method begins by investigating the existing infrastructure, if it is not compatible with IEEE 802.1X (which is not the case with Patni's infrastructure), then there is no point considering employing any of the authentication methods since one of Paatni's main requirements is to employ the authentication method using the wireless network support provided in Windows XP and Windows 2000 Server.

By checking Patni's existing infrastructure it will be found that it does support IEEE 802.1X.

The next step (see the main selection algorithm) is to identify the authentication methods that suit the organisation's security requirements.

At this point the main selection algorithm, based on the fact that both operating systems (Windows XP and Windows 2000 Server) support EAP-TLS, will identify EAP-TLS as the authentication method that best suits this environment.

TLS in this particular case can be implemented without any significant implementation cost and at the same time provide the most secure solution.

In only two steps the main selection algorithm, by identifying TLS as the solution that best suits Patni's requirements, confirms the correctness of the decision made by Microsoft and Patni.

The same result is obtained if the selection algorithm based only on the existing infrastructure is applied.

Example 2

The following scenario was taken from http://store.mtghouse.com/newWeb/cgi bin/case_study_cal_poly_ponoma.asp on 07/12/05.

"The Southern Polytechnic State University, Marietta, Georgia (SPSU) has a student body composed of approximately 3700 students, about one-third of which are non-traditional and attend evening or weekend classes. SPSU has approximately 800 resident students, but the majority of the student body resides off campus. SPSU students, staff and faculty wanted a wireless LAN service and the mobile Internet access it could provide".

"SPSU's Information Technology Division wanted to implement a campus-wide wireless LAN that would augment its existing 802.11 Ethernet wired network. Discussions with SPSU's primary networking hardware vendor, Enterasys Networks, led it to consider 802.1X-based solutions".

Cross-platform support was also a critical need due to a lack of user

platform control that is typical of universities.

"The majority of SPSU's servers and a considerable portion of its clients run the Linux operating system. In addition to Linux support SPSU required security/authentication solutions for Mac OS X and the Microsoft PC operating systems, both in wired and wireless configurations".

"The client solution would have to be a standard 802.1X implementation and interoperable with SPSU's Funk Steel Belted RADIUS running on Solaris and its open LDAP directory on the back end".

"SPSU decided to use EAP-TTLS, a tunnelled EAP method offering especially strong security, but which did not require the resource burden of EAP-TLS. EAP-TTLS offers a comparable level of security without the need to deploy and maintain client certificates".

"Meetinghouse provided a LINUX solution, plus cross-platform support covering Mac OS X and Microsoft operating systems. The AEGIS Client solution is a standard implementation of 802.1X and fully compatible with SPSU's Steel Belted RADIUS server. In addition, it supports the TTLS tunnelled EAP method and mutual authentication".

"SPSU is rolling-out a campus-wide WLAN first covering those areas with highest user demand. SPSU will implement significant coverage in the future. The present deployment indicates it has met its goals for strong security/authentication".

Solution Provided by Applying the Selection Algorithms

To apply the selection algorithms to the case of SPSU its security and networking environment requirements have first to be identified. These are:

1) A secure networking environment.
2) Strong authentication without the need to deploy PKI infrastructure.
3) The authentication method must be supported by Microsoft, Linux, Apple Mackintosh, and other platforms used by the staff and the student body.

The main selection algorithm, after investigating the compatibility of the SPSU network infrastructure with the requirements of IEEE 802.1X and based on the fact that SPSU decided to employ an EAP method that provides strong security, but which does not require the resource burden of EAP-TLS identifies PEAP and TTLS as the best available options. The choice between them depends on SPSU's approach to authenticating its students and staff, in other words whether students and staff machines support only EAP authentication methods or EAP and legacy methods.

It is known that while PEAP supports only EAP methods for client authentication, TTLS in addition to supporting EAP methods also supports legacy methods.

Because various operating systems are used in different machines there is no guarantee that all machines will support EAP. Therefore, the main selection algorithm identifies TTLS as the solution that suits this environment because it is the only available authentication method that supports EAP as well as legacy methods. This means that regardless of the students' machines operating systems students using different platforms can access the network. At the same time, EAP-TTLS without any significant

additional costs offers a strong authentication level that is comparable with the level of security provided by the most secure solution (TLS) without the need to deploy and maintain client certificates.

The selection algorithm in only three steps confirms the correctness of the decision made by the Meetinghouse and SPSU to select EAP-TTLS as the authentication method that best suits the security needs and networking environment of SPSU. EAP-TLLS is also identified if the selection algorithm based on the existing infrastructure is used or if the algorithm based on the upgrade strategy is used.

Example 3

The following scenario was taken from www.Cisco.com on 11/12/05.

Cisco uses its own technology within its corporate network whenever possible. In the case of wireless technology, Cisco employs Cisco Aironet access points using the Cisco Wireless Security Suite to implement Cisco LEAP and pre-standard TKIP for secure authentication and encryption of all WLAN communication. Cisco Secure ACS is used to provide the RADIUS services required for LEAP. To provide some background and an example of a functioning Cisco Secure ACS deployment with Aironet wireless products, a brief discussion follows of how Cisco has implemented Cisco Secure ACS and Aironet products in its network.

"At the Cisco main campus in San Jose, CA buildings are grouped into three segments. Each segment consists of 6 to 19 buildings and all the buildings in the segment are on a common LAN. Each building has six to eight WLAN access points per floor and all the access points in each building are on their own dedicated VLAN. All inter-building and inter-segment network connections use one-gigabyte fiber optic technology. Other Cisco campuses are similarly configured. All wireless connections are designated as secondary network access. Primary network access is through switch ports over wired Ethernet".

"Cisco Secure ACS is used to provide LEAP authentication for the access points, and is configured to use Microsoft Active Directory for external database authentication. One Cisco Secure ACS is deployed for each segment of 6 to 19 buildings. A Cisco LocalDirector content switch is placed before each Cisco Secure ACS for load balancing and failover. All Aironet access points are configured with one RADIUS server and the LocalDirector content switch is used for failover. The LocalDirector is used because of the way the deployed version of access point software handles RADIUS failover. As a result, Cisco is not currently using accounting on its wireless network".

Solution Provided by Applying the Selection Algorithms

LEAP was developed by Cisco mainly to be used on Cisco wireless products as the first commercial and practical EAP authentication solution. Consequently, one of the main problems with LEAP deployment is that it requires a Cisco products based infrastructure, or if it has to be used with non-Cisco products, Cisco compatible exchange program (CCX) must be installed, which means additional costs and additional configuration and management effort.

When it comes to Cisco's WLAN, there is no doubt that Cisco uses its own technology, in other words the infrastructure is Cisco products based.

It is obvious that the selection in this case will be based mainly on the existing infrastructure.

If the selection algorithm based on the existing infrastructure was applied (at the time when Cisco selected LEAP), LEAP will be identified as the best possible solution.

This confirms the applicability of the selection algorithms, but the interesting thing is that if the same algorithm were applied today it would most probably not identify LEAP. It might identify PEAP, which was not developed at the time Cisco implemented LEAP.

After Cisco adopted LEAP as their authentication solution a long time passed before Microsoft PEAP was developed to address security problems associated with LEAP; mainly related to dictionary attacks.

There is no doubt PEAP is better than LEAP and Cisco will probably upgrade its authentication mechanism if it has not yet already done so.

Cisco has developed a new authentication method known as flexible authentication via secure tunnelling (FAST). However, this paper does not address FAST because it is not yet widely deployed.

The above examples demonstrate the efficiency and usefulness of the selection algorithms proposed in this paper.

7. Managerial Implications

Selecting the most suitable authentication method is a big step towards securing a WLAN. But it does not mean the WLAN is secure and the authentication related risks are completely eliminated. In order for the selected authentication method to be effective it must be looked at on an ongoing basis. This means WLAN managers must take further steps and follow well-defined routines that ensure the selected authentication method maintains the required level of protection.

In this section remembering the information security 80/20 rule which is that 80 percent of exploit risks can be effectively reduced using 20 percent of the recommended security procedures and steps (www.8020info.com/principle.html), the most fundamental aspects and best practices of securing WLANs will be identified.

1) Education and Training: To reduce the flaws in WLAN security that can result from human errors and omissions or as the result of users' limited knowledge of WLAN security threats and risks, education and training for all WLAN users and managers is absolutely essential no matter how good and secure the selected upper-layer authentication method is. On the other hand, providing such training or education means additional costs on top of the selected authentication method's implementation costs. Thus, there is trade-off and WLAN managers need to carefully balance the importance of maintaining the required level of security with the ability of WLAN organisations to match these additional expenses.

2) Product Selection: There exists a wide range of authentication solution products, so the question is which ones to select and how to manage the selected products successfully? Bearing in mind the natural tendency towards ease of deployment and management, only Wi-Fi certified products that ensure interoperability should be selected. On the other hand, the right

selection of the required products (hardware, software and firmware) helps to integrate wireless LANs with existing wired networks (www.theregister.co.uk).

3) Site Survey (SS): The SS is a very important factor in the success of the WLAN implementation. A great deal of information can be obtained from a SS, such as the number of APs required, the coverage and bandwidth performance at different locations. Even more important is how the SS information is analyzed to support important implementation issues such as security, interference, etc. (M. Gast, 2005).

In addition to these points there are other issues that should be considered by WLAN managers such as the instructions and recommendations provided by WLAN vendors. (www.wi.fiplanet.com/tutorials/articles.php/985421).

8. Conclusions

This paper provides algorithms for the selection of an EAP authentication method for a WLAN, the effectiveness and efficiency of which have been demonstrated through three examples taken from real scenarios.

Although one factor-based selection algorithms are simple and may turn out to be powerful in some cases, their drawbacks restrict their application to certain environments and specific requirements.

The main selection algorithm of this paper, by considering several selection factors together, addresses shortcomings of one factor-based selection algorithms and is capable of providing the most suitable authentication method for different organisations in different environments with different requirements.

This algorithm guides the authentication method selection process for a specific organisation by identifying the security level desired in that environment as well as investigating the existing network infrastructure and the possibility of upgrading it to meet the requirements imposed by a particular authentication method.

The major advantage of the main selection algorithm is its ability to balance the threat, information value, and costs in the process of the selection of the most suitable authentication method.

The most interesting feature of the algorithms presented in this paper, besides their potential to identify the most suitable solution for an organisation's requirements, is their flexibility and scalability. The algorithms can easily be reconstructed to address selection factors that are not considered in this paper such as deployment difficulties and administration and management effort. Also these algorithms with little modification can accommodate additional authentication methods that are not addressed in this paper

9. References

- Cisco Systems, (2002) 'A Comprehensive Review of 802.11 WLAN Security and the Cisco wireless Security Suite', Cisco Systems Inc, New York, USA.

- Cisco Systems, (2004) 'Cisco Response to Dictionary Attacks', Cisco Systems, Inc, New York, USA.

- Cisco Systems, (2003) 'Cisco SAFE: WLAN Security in Depth', Cisco Systems, Inc, New York, USA.

- Edney, J and Arbaugh, W., (2004) 'Real 802.11 Security: Wi-Fi Protected Access and 802.11i', Addison-Wesley, Boston, USA.

- M. Gast, (2005) '802.11 Wireless Networks; The Definitive Guide, 2nd Edition' O'reilly, USA.

- Ma, Y and Cao, X., (2003), 'How to use EAP-TLS Authentication in PWLAN Environment', *IEEE*, Proceeding of the 2003 International conference on neural networks and signal processing, Volume 2, 14-17 Dec, Pages 1677-1680.

- Mishra, A and Ho, M., (2004) 'Proactive Key Distribution Using Neighbor Graphs', *IEEE wireless communication*, Volume 11, Pages 26-36.

- Shumman, W. and Ran, T., (2003), 'WLAN and it's Security problems', *IEEE*, Proceedings of the 2003 International conference on Parallel and Distributed Computing, Applications and Technologies, Pages 241-245.

- http://store.mtghouse.com/newWeb/cgi-bin/case_study_cal_poly_ponoma.asp 07/12/05.

- http://www.microsoft.com/india/casestudies/patniwireless.aspx 09/12/05.

- www.Cisco.com 11/12/05.

- www.8020info.com/principle.html 21/02/06.

- www.sans.org/resources/errors.php. 23/02/06.

- www.wi.fiplanet.com/tutorials/articles.php/985421. 24/02/06

- www.theregister.co.uk 25/05/05

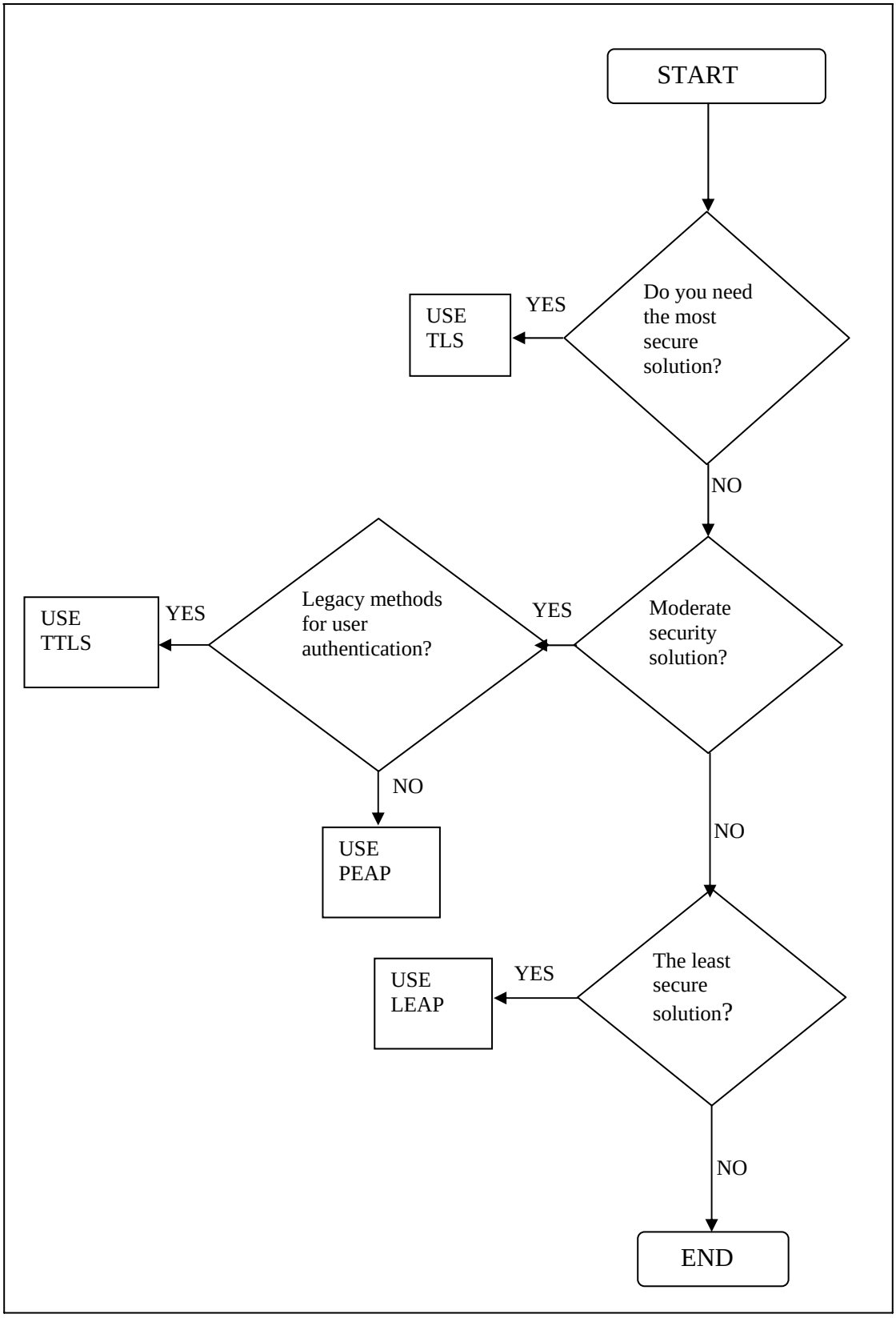


Figure 1: EAP Authentication Method Selection Algorithm Based on Security Level provided

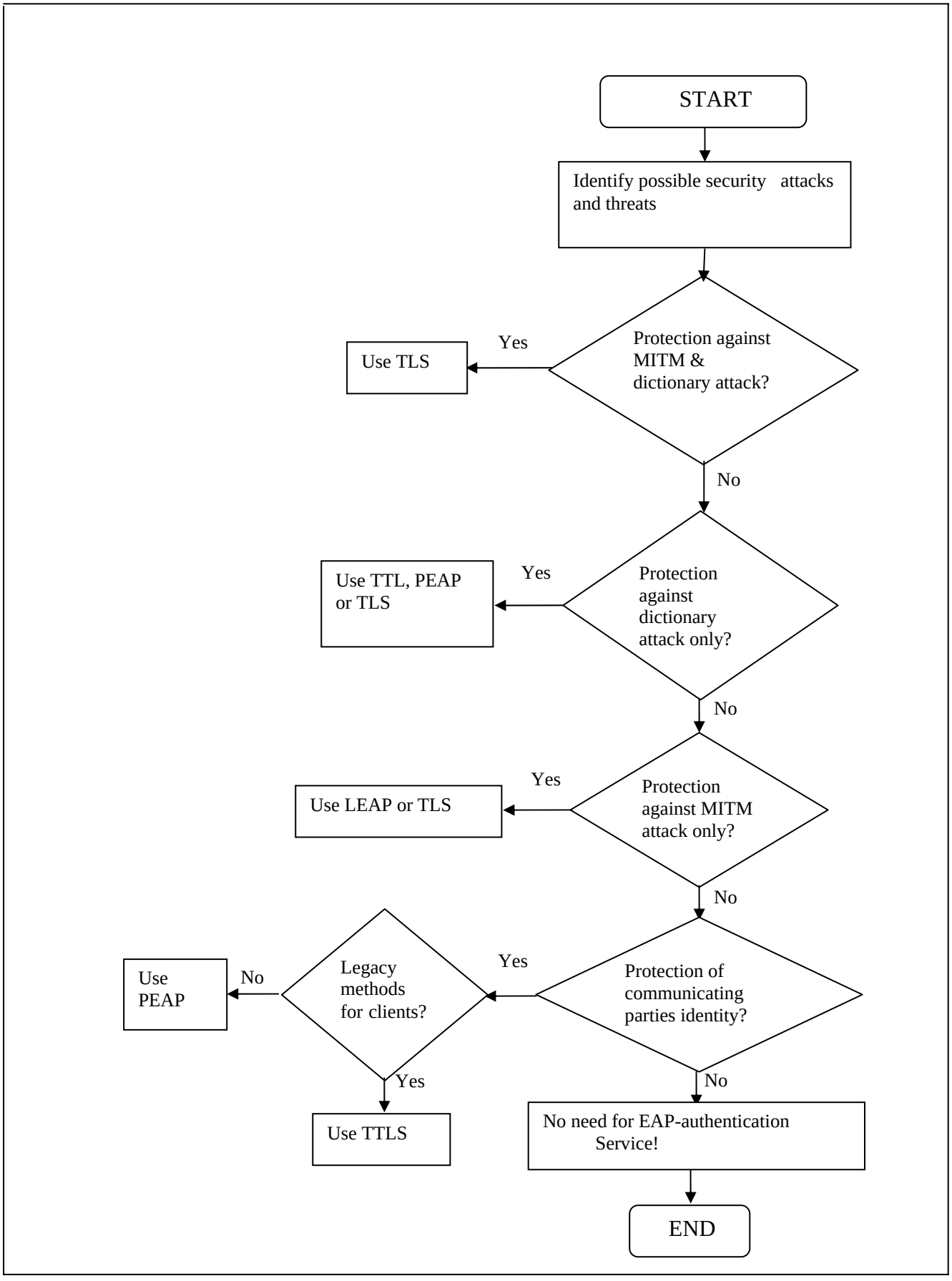


Figure 2: EAP Authentication Method Selection Algorithm Based on Possible Attacks

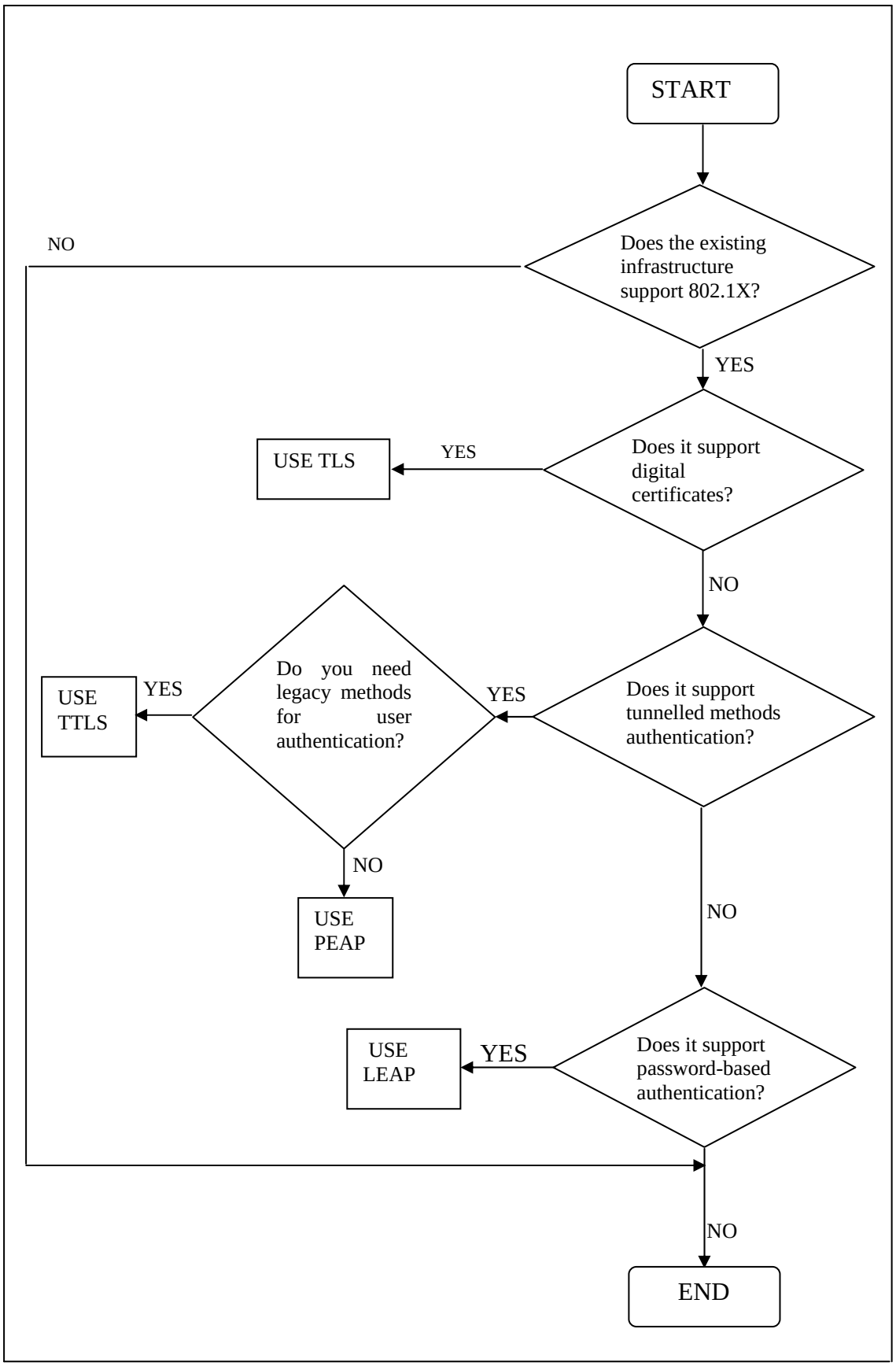


Figure 3: EAP Authentication Method Selection Algorithm Based on Existing Network Infrastructure

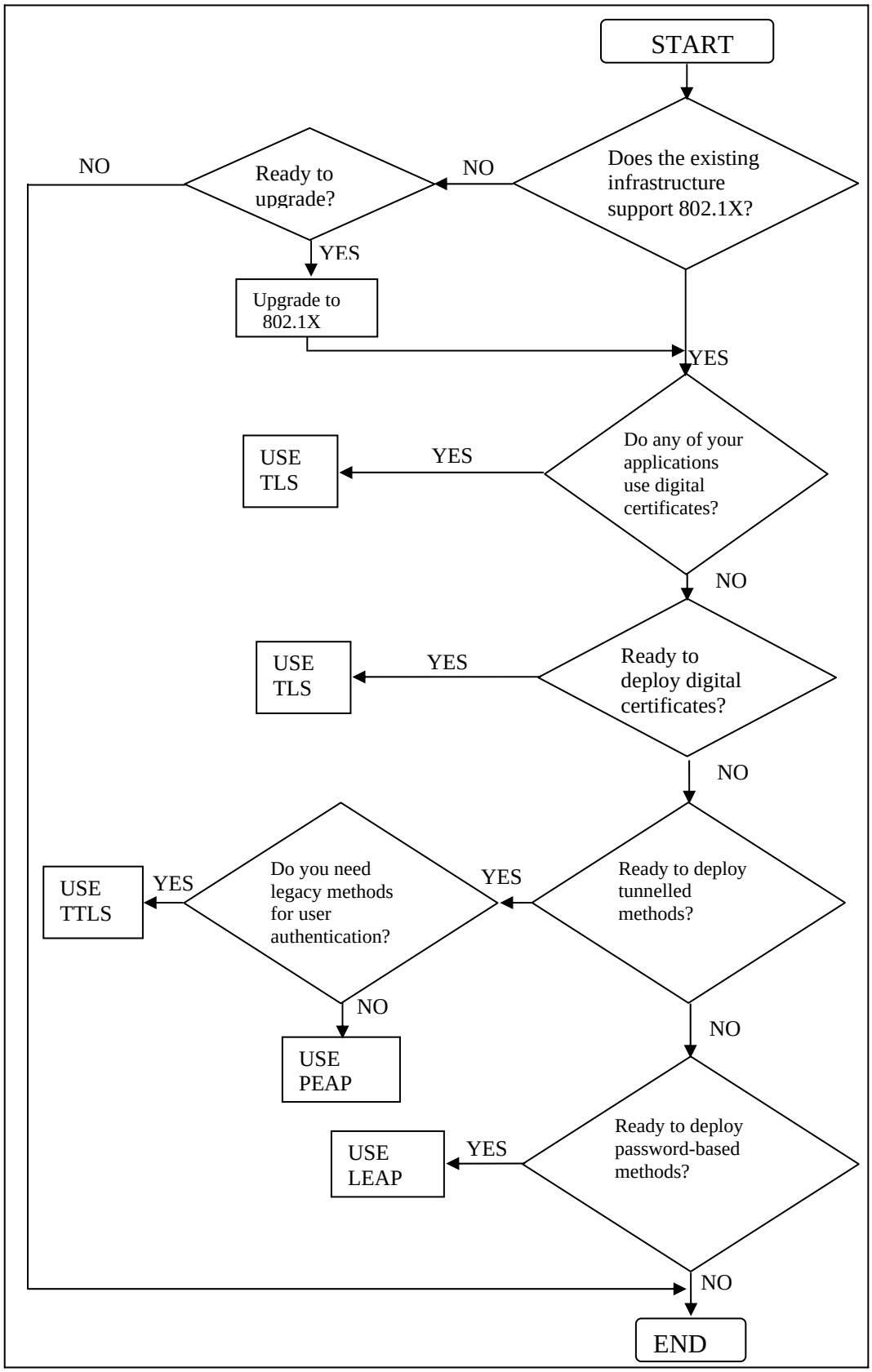
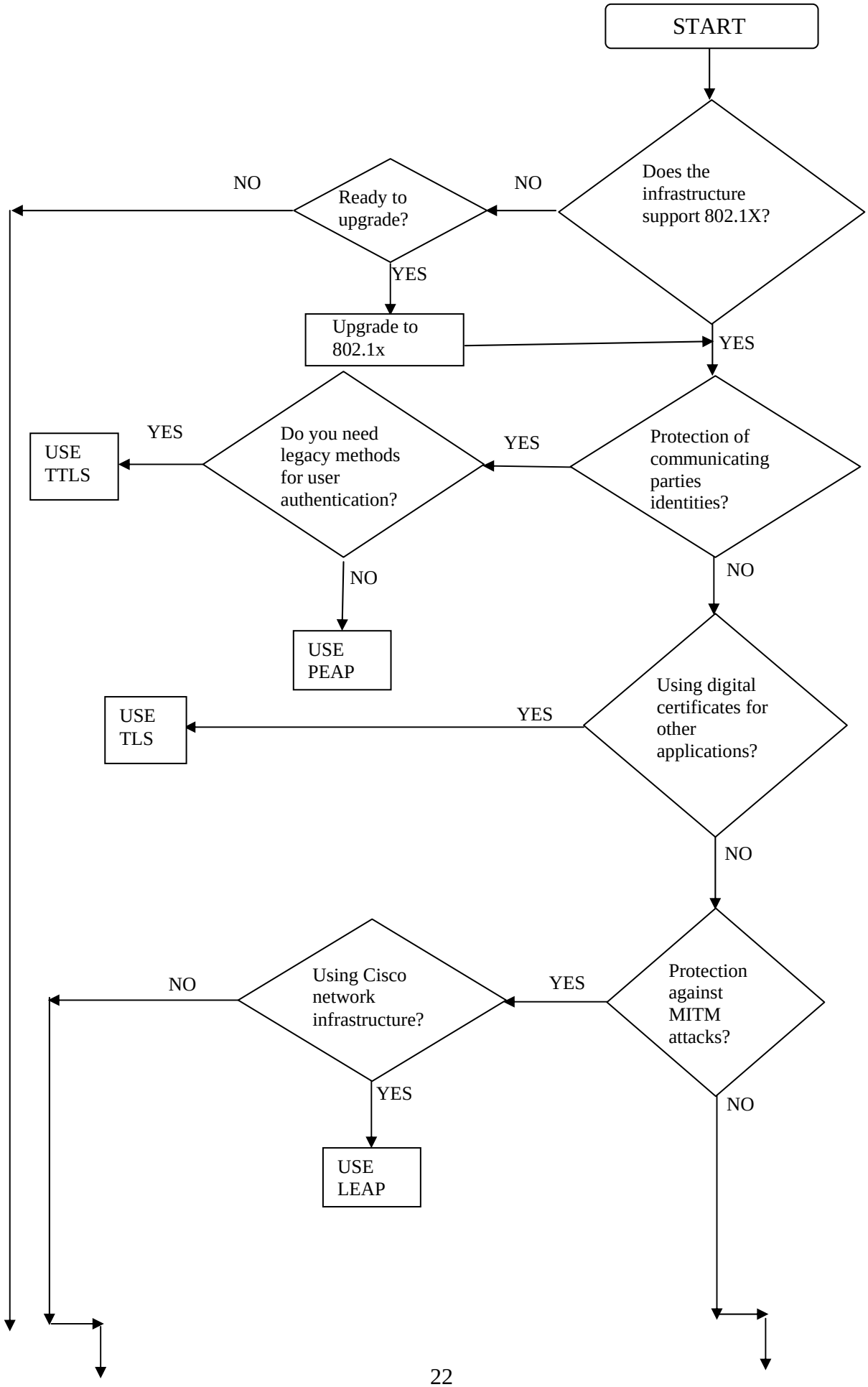


Figure 4: EAP Authentication Method Selection Algorithm Based on Upgrade Strategy


START
Does the infrastructure support 802.1X?
NO
Ready to upgrade?
NO
YES
Upgrade to 802.1x
YES
Protection of communicating parties identities?
YES
Do you need legacy methods for user authentication?
YES
USE TTLS
NO
USE PEAP
NO
Using digital certificates for other applications?
YES
USE TLS
NO
Protection against MITM attacks?
YES
Using Cisco network infrastructure?
NO
YES
USE LEAP
NO

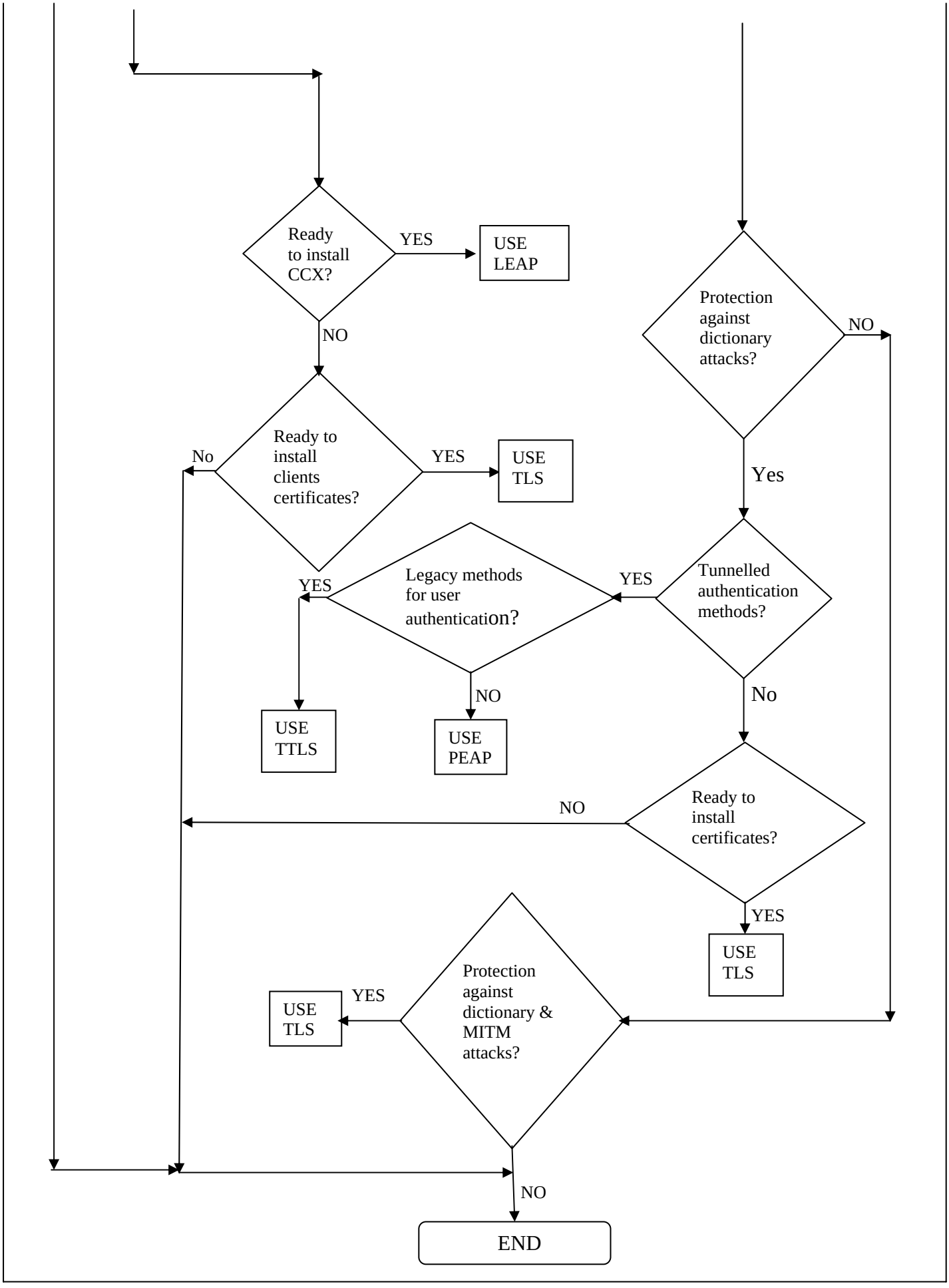


Figure 5: Main Algorithm for EAP Authentication Method Selection

EAP Method / Property	MD5	LEAP	TLS	TTLS	PEAP
Implementation	Challenge Based	Password Based	Certificate Based	Server Side Certificate	Server Side Certificate
Authentication Attributes	Unilateral	Mutual	Mutual	Mutual	Mutual
Deployment Difficulties	Easy	Easy	Hard	Moderate	Moderate
Dynamic Re-keying	No	Yes	Yes	Yes	Yes
Requires Server Certificate	No	No	Yes	Yes	Yes
Requires Client Certificate	No	No	Yes	No	No
Tunnelled	No	No	No	Yes	Yes
WPA Compatible	No	Yes	Yes	Yes	Yes
WLAN Security	Poor	Moderate	Strongest	Strong	Strong
Security Risks	Identity exposed, Dictionary attack, MITM attack.	Identity exposed, Dictionary attack.	Identity exposed.	MITM attack.	MITM attack. Identity hidden in phase2 but potential exposure in Phase1.

Table 1: Properties of EAP Authentication Methods.