A Password-Based authentication and Key Agreement Protocol for Wireless LAN Based on Elliptic Curve and Digital Signature

Article *in* International Journal of Computer Science and Information Security, · October 2011

CITATIONS
0

READS
49

3 authors, including:

Saed Rezayi
University of Oregon
6 PUBLICATIONS **11** CITATIONS

SEE PROFILE

A Password-Based authentication and Key Agreement Protocol for Wireless LAN Based on Elliptic Curve and Digital Signature

Saed Rezayi
Department of Electrical Engineering
Amir kabir University of Tehran
Tehran, Iran
saed.rezaei@aut.ac.ir

Mona Sotoodeh
Department of Applied Mathematics
Science and Research Azad University
Tehran, Iran
m.sotoodeh@srbiau.ac.ir

Hojjat Esmaili
Department of Computer Engineering
Sharif University of Tehran
hojjat.esmaili@gmail.com

***Abstract*—Password-based authentication protocols are the strongest among all methods which has been proposed through the period that wireless networks have been rapidly growing, and no perfect scheme has been provided for this sensitive technology. The biggest drawback of strong password protocols is IPR (Intellectual Properties Right); hence they have not become standard; SPEKE, SRP, Snapi and AuthA for instance. In this paper we propose a user-friendly, easy to deploy and PKI-free protocol to provide authentication in WLAN. We utilize elliptic curve and digital signature to improve AMP (Authentication via Memorable Password) and apply it for wireless networks as AMP is not patented and strong enough to secure WLAN against almost all possible known attacks.**

Keywords—WLAN, Password-Based Authentication, AMP, Elliptic Curve, Digital Signature.

I. INTRODUCTION

IEEE 802.11 standard was presented in 1997 and as it is becoming more and more prevalent, security in such networks is becoming a challenging issue and is in great demand. Since wireless standard was introduced, a multitude of protocols and RFCs have been proposed to provide authentication mechanism for entities in a WLAN but a few of them have the chance to become a standard regardless of their strengths.

Apart from this, first password-based key exchange protocol, LGSN [1], was introduced in 1989 and many protocols have followed it. In 1992 first verifier-based protocol, A-EKE [2], presented which was one variant of EKE [3] (Encrypted Key Exchange) a symmetric cryptographic authentication and key agreement scheme. Verifier-based means that client possesses a password while server stores its verifier rather than the password. Next attempt to improve password-based protocols was AKE which unlike EKE was based on asymmetric cryptography; SRP [4] and AMP [5] for instance. These protocols need nothing but a password which is a memorable quantity, hence they are simpler and cheaper to deploy compared with PKI-based schemes. Elliptic curve cryptosystem [6, 7] as a powerful mathematical tool has been applied in cryptography in recent years [8, 9, 10]. The security of Elliptic Curve cryptography relies on the discrete logarithm problem (DLP) over the points on an elliptic curve, whereas the hardness of the RSA [11] public-key encryption and signature is based on integer factorization problem. In cryptography, these problems are used over finite fields in number theory [12].

In this paper elliptic curve cryptosystem is combined with AMP to produce a stronger authentication protocol. To complete the authentication process, any mutually agreeable method can be used to verify that their keys match; the security of the resulting protocol is obviously dependent on the choice of this method. For this part we choose the Elliptic Curve analogue of the Digital Signature Algorithm or ECDSA [13] for short.

The remainder of this paper is organized as follows. In section 2 we give a review about authentication and key agreement concept and requirements in wireless LANs. A brief mathematical background of elliptic curve over finite field is presented in section 3. In section 4 our protocol is proposed. Section 5 describes the security and performance analysis of the proposed protocol. Finally, in section 6 the conclusion and future work is provided.

II. WLAN AUTHENTICATION REQUIERMENTS

Authentication is one of five key issues in network security [14] and it verifies users to be who they say they are. Public Key Infrastructure (PKI [15]) is one of the ways to ensure authentication through digital certificates but not only is highly costly and complicated to implement but also it has risks [16]. Thus, a strong password-based method is the primary choice.

The requirements for authentication in wireless networks, regardless of type of method, are categorized as follows. Since EAP [17] is a common framework in

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

wireless security we refer to this standard to gain some points of it.

A. EAP mandatory requirements specified in [17].

- During authentication, a *strong master session key* must be generated.
- The method which is used for wireless networks must provide *mutual authentication*.
- An authentication method must be *resistant to online and offline dictionary attacks.*
- An authentication method must *protect against man-in-the-middle and replay attacks*.

B. Other requirements related to applicability [18].

- Authentication in wireless networks must achieve *flexibility* in order to adapt to the many different profiles. Authentication also needs to be flexible to suit the different security requirements.
- Authentication model in a WLAN should be *scalable*. Scalability in authentication refers to the ability to adapt from small to large (and vice versa) wireless networks and the capacity to support heavy authentication loads.
- It is valuable for an authentication protocol to be *efficient*. Efficiency within an authentication model is a measure of the costs required to manage computation, communication and storage.
- *Ease of implementation* is another crucial issue because authentication is a burden on administrators' shoulders.

In addition there are some desirable characteristics of a key establishment protocol. Key establishment is a process or protocol whereby a shared secret becomes available to two or more parties, for subsequent cryptographic use. Key establishment is subdivided into key transport and key agreement. A key transport protocol or mechanism is a key establishment technique where one party creates or otherwise obtains a secret value, and securely transfers it to the other(s). While a key agreement protocol or mechanism is a key establishment technique in which a shared secret is derived by two (or more) parties as a function of information contributed by, or associated with, each of these, (ideally) such that no party can predetermine the resulting value [19]. In this paper we are dealing with a key agreement protocol.

C. Requirements of a secure key agreement protocol

- *Perfect forward secrecy* which means that revealing the password to an attacker does not help him obtain the session keys of past sessions.
- A protocol is said to be *resistant to a known-key attack* if compromise of past session keys does not allow a passive adversary to compromise future session keys.
- *Zero-knowledge password proof* means that a party A who knows a password, makes a counterpart B convinced that A is who knows the password without revealing any information about the password itself.

III. MATHEMATICAL BACKGROUND

In this section we briefly discuss about elliptic curve over finite fields, digital signature based on elliptic curve and AMP algorithm.

A. Finite Fields

Let p be a prime number. The finite field F_p, called a prime field, is comprised of the set of integers $\{0,1,2,\dots,p-1\}$ with the following arithmetic operations

- Addition: if $a, b \in F_p$, then $a + b = r$, where r is the reminder when $a + b$ is divided by p and $0 \le r \le p-1$. This is known as addition modulo p.
- Multiplication: if $a, b \in F_p$, then $a.b = s$, where s is the reminder when $a.b$ is divided by p and $0 \le s \le p-1$. This is known as multiplication modulo p.
- Inversion: if a is a non-zero element in F_p, the inverse of a modulo p, denoted a^{-1}, is the unique integer $c \in F_p$ for which $a.c = 1$.

B. Elliptic Curve

Let $p > 3$ be an odd prime. An elliptic curve E defined over F_p is an equation of the form

$$y^2 = x^3 + ax + b \qquad (1)$$

Where $a, b \in F_p$ and $4a^3 + 27b^2 \not\equiv 0 \ (mod\ p)$. The set $E(F_p)$ consists of all points (x, y) with $x, y \in F_p$ which satisfies the equation (1), together with a single element denoted $\mathcal{O}$ and called the *point at infinity*.

There is a rule, called the chord-and-tangent rule, for adding two points on an elliptic curve to give a third elliptic curve point. The following algebraic formulas for the sum of two points and the double of a point can be obtained from this rule (for more details refer to [12]).

- For all $P \in E(F_p)$, $P + \mathcal{O} = \mathcal{O} + P = P$
- If $P = (x, y) \in E(F_p)$, then $(x, y) + (x, -y) = \mathcal{O}$. the point $(x, -y)$ is denoted by $-P$ and is called the negative of P.
- Let $P = (x_1, y_1) \in E(F_p)$ and $Q = (x_2, y_2) \in E(F_p)$, where $P \neq \pm Q$. Then $P + Q = (x_3, y_3)$, where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Let $P = (x_1, y_1) \in E(F_p)$. Then $2P = (x_3, y_3)$ where

$$x_3 = \left(\frac{3{x_1}^2 + a}{2y_1}\right)^2 - 2x_1$$

$$y_3 = \left(\frac{3{x_1}^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

Observe that the addition of two elliptic curve points in $E(F_p)$ requires a few arithmetic operations (addition, subtraction, multiplication, and inversion) in the underlying field.

In many ways elliptic curves are natural analogs of multiplicative groups of fields in Discrete Logarithm Problem (DLP). But they have the advantage that one has more flexibility in choosing an elliptic curve than a finite field. Besides, since the ECDLP appears to be significantly harder than the DLP, the strength-per-key-bit is substantially greater in elliptic curve systems than in conventional discrete logarithm systems. Thus, smaller parameters can be used in ECC than with DL systems but with equivalent levels of security. The advantages that can be gained from smaller parameters include speed (faster computations) and smaller keys. These advantages are especially important in environments where processing power, storage space, bandwidth, or power consumption is constrained like WLANs.

C. AMP

AMP is considered as strong and secure password based authentication and key agreement protocol and is based on asymmetric cryptosystem, in addition, it provides password file protection against server file compromise. Security of AMP is based on two familiar hard problems which are believed infeasible to solve in polynomial time. One is Discrete Logarithm Problem; given a prime p, a generator g of a multiplicative group $\mathcal{Z}_p$, and an element $g^x \in \mathcal{Z}_p$, find the integer $x \in [0,\ p-2]$. The other is Diffie-Hellman Problem [20]; given a prime p, a generator g of a multiplicative group $\mathcal{Z}_p$, and elements $g^x,\ g^y \in \mathcal{Z}_p$, find $g^{xy} \in \mathcal{Z}_p$.

The following notation is used to describe this algorithm according to [13].

id	Entity identification
π	A's password
τ	Password salt
x	A's private key randomly selected from $\mathcal{Z}_p$
y	B's private key randomly selected from $\mathcal{Z}_p$
g	A generator of $\mathcal{Z}_p$ selected by A
$h_i()$	Secure hash functions

AMP^n four pass protocol:

$A\ (id,\pi)$		$B\ (id, g^\pi)$
$x \in \mathcal{Z}_p$		
$G_1 = g^x$	$\xrightarrow{id, g^x}$	
		fetch (id,π)
		$y \in \mathcal{Z}_p$
$w = (x+\pi)^{-1}x$	$\xleftarrow{g^{(x+\pi)y}}$	$G_2 = (G_1 g^\pi)^y$
$\alpha = (G_2)^w$		$\beta = (G_1)^y$
$\mathcal{K}_1 = h_1(\alpha)$		$\mathcal{K}_2 = h_1(\beta)$
$\mathcal{H}_{11} = h_2(G_1, \mathcal{K}_1)$	$\xrightarrow{\mathcal{H}_{11}}$	$\mathcal{H}_{12} = h_2(G_1, \mathcal{K}_2)$
		verify $\mathcal{H}_{11} = \mathcal{H}_{12}$
$\mathcal{H}_{21} = h_3(G_2, \mathcal{K}_1)$	$\xrightarrow{\mathcal{H}_{22}}$	$\mathcal{H}_{22} = h_3(G_2, \mathcal{K}_2)$
verify $\mathcal{H}_{21} = \mathcal{H}_{22}$		

If instead of password, its verifier was stored in server, it would be resistant against server impersonation attack; but we just presented AMP naked in this section. For other variants of AMP refer to [6]. Note that A and B agree on g^{xy}.

D. ECDSA

ECDSA is the elliptic curve variant of DSA which is digital signature mechanism which provides a high level of assurance. There are three main phases in this algorithm; key pair generation, signature generation and signature validation.

Key generation: each entity does the following for domain parameter and associated key pair generation.

1. Select coefficients a and b from F_p verifiably at random. Let E be the curve $y^2 = x^3 + ax + b$.
2. Compute $N = \#E(F_q)$ and verify that N is divisible by a large prime n ($n > 2^{160}$ and $n > 4\sqrt{p}$).
3. Select a random or pseudorandom integer d in the interval $[1, n-1]$.
4. Compute $Q = dG$.
5. The public key is Q; the private key is d.

To assure that a set $D = (p, a, b, G, n)$ of EC domain parameters is valid see [13].

Signature generation: to sign a message m, an entity A with domain parameters D and associated key pair (d, Q) does the following.

1. Select a random or pseudorandom integer k in the interval $[1, n-1]$.
2. Compute $kG = (x_1, y_1)$ and put $r = x_1 \ mod\ n$ if $r = 0$ go to step 1.
3. Compute $e = H(m)$ where H is a strong one way hash function is.
4. Compute $s = k^{-1}(e + dr)\ mod\ n$. If $s = 0$ go to step 1.
5. A's signature for the message m is (r, s).

Signature validation: to verify A's signature on m, B obtains an authentic copy of A's domain parameters D and associated public key Q.

1. Compute $e = H(m)$.
2. Compute $w = s^{-1}\ mod\ n$.
3. Compute $u_1 = ew\ mod\ n$ and $u_2 = rw\ mod\ n$
4. Compute $X = u_1 G + u_2 Q$
5. If $X = \mathcal{O}$, then reject the signature. Otherwise, compute x-coordinnate of X; x_2.
6. Accept the signature if and only if $r = x_2$.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VI. PROPOSED PROTOCOL

In this section we present our method to improve AMP scheme. As previously mentioned we combine AMP with Elliptic Curve, since smaller parameters can be used in ECC compared with RSA. Besides, the level of latency is quite high in RSA as compared to ECC for the same level of security and for the same type of operations; sign, verification, encryption and decryption. In [21] a key establishment protocol was tested by both ECC and RSA and the latency in millisecond measured as a performance parameters. It is seen from Fig. 1 that RSA has at least four times greater latency than ECC.

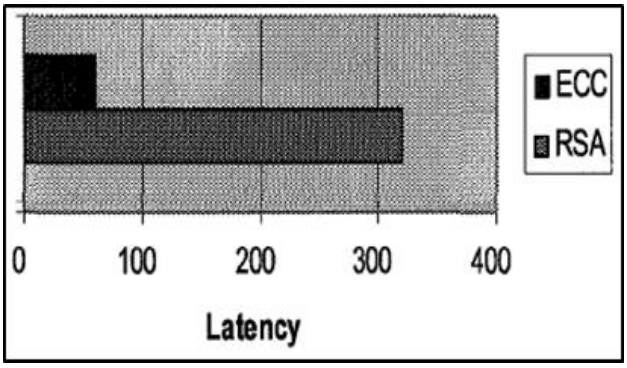

Figure 1: Latency: ECC vs. RSA

Furthermore, for the two last steps, we utilize ECDSA which is a high secure signing method than hash functions. Before running the protocol, entity A chooses an elliptic curve $(\text{i.e. } E(F_p) \text{ over } F_p)$, and then he randomly selects a large prime G from F_p. Moreover (d, Q) is his key pair. We assume that A and B securely shared password π. See section 2 for parameter selection. The rest of the protocol is illustrated as follows.

$A\ (id,\pi)$		$B\ (id, g^{\pi})$
$x \in F_p$		
$X = xG = (x_1, y_1)$	$\xrightarrow{Q,id,X,G}$	
$r = x_1$		*fetch* (id,π)
		$y \in F_p$
$w = (x+\pi)^{-1}$	$\overset{Y}{\leftarrow}$	$Y = y(X + \pi G)$
$S = xwY$		$S = yX$
$e = h(S)$		
$s = x^{-1}(e + dr)$	$\overset{s,r}{\rightarrow}$	$h(S) = e$
		$z = s^{-1}$
		$u_1 = ez\ , u_2 = rz$
		$u_1G + u_2Q = (x_2, y_2)$
		verify $r = x_2$

A randomly selects x from F_p and computes $X = xG = (x_1, y_1)$ and puts $r = x_1$. He sends $X, G,\ Q$ (his public key) and his id to B

1. Upon receiving A's id, B fetches A's password according to received id and randomly selects y, computes $Y = y(X + \pi Q)$, and sends it to A.
2. A computes $w = (x+\pi)^{-1}$ and obtains the session key as follows.

$$\begin{aligned} S = xwY &= x(x+\pi)^{-1}y(X + \pi Q) \\ &= x(x+\pi)^{-1}y(xG + \pi G) \\ &= x(x+\pi)^{-1}y(x+\pi)G = xyG \end{aligned}$$

He signs it as described in section 3.4, and sends (r, s) as digital signature.

3. B also computes the session key as follows.
$S = yX = xyG$
And verifies the validity of digital signature as below,
$z = s^{-1}$
$$= x(e + dr)^{-1}$$
$$\Rightarrow u_1 = ex(e + dr)^{-1}\ ,\ u_2 = rx(e + dr)^{-1}$$
To $r = x_2$ get satisfied following equation must be true:
$$u_1G + u_2Q = xG$$
$$u_1G + u_2Q = ex(e + dr)^{-1}G + rx(e + dr)^{-1}Q$$
$$Q = dG \xrightarrow{yields} (e + dr)^{-1}(e + rd)xG = xG$$

V. SECURITY AND PERFORMANCE ANALYSIS

A. *Security Analysis*

We claim that our proposed protocol is secure enough to be used in sensitive Wireless LANs and protect these networks against well-known attacks. Because the security of the authentication model depends on the security of the individual protocols in the model; AMP and ECDSA, besides more flexible and stronger cryptosystem is applied to make it applicable in WLANs. In addition to generating strong session key and providing mutual authentication, following properties are presented to prove our protocol strength.

Perfect Forward Secrecy: our protocol provides perfect forward secrecy (as AMP and other strong password based protocols do) via Diffie-Hellman problem and DLP and due to the complicacy of these problems. Because even if an adversary eavesdrops π, he cannot obtain old session keys because the session key is formed by random numbers, x and y, generated by both entities which are not available and obtainable.

Man in the Middle Attack: this attack is infeasible because an attacker does not know the password π. Assume he is in the middle of traffic exchange and A, B have no idea about this. He gets A's information but does not send them to B, instead, he stores them and selects a large prime from F_p, let k, then he computes $K = kG$ and sends it to B. B computes $Y = y(K + \pi G)$ and sends it to A. on the way, attacker grabs Y and sends it to A, but A and B shared session key, S, does not match due to wrong digital signature which A produced.

Dictionary Attack: offline dictionary attack is not feasible because an adversary, who guesses the password π, has to solve DLP problem to find y in equation $Y = y(X + \pi G)$ and obtains S. Online dictionary attack is also

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

not applicable because the entity A is never asked for password.

Replay Attack: is negligible because *X* should include an ephemeral parameter of A while *Y* should include ephemeral parameters of both parties of the session. Finding those parameters corresponds to solving the discrete logarithm problem.

Zero Knowledge Password Proof: this property is provided since no information about password is exchanged between two parties.

Known-Key Attack: our protocol resists this attack since session keys are generated by random values which are irrelevant in different runs of protocol.

B. Performance Analysis

Flexibility: our protocol is based on AMP, and AMP has several variants for various functional considerations. So it can implemented in every scenarios; wired or wireless. For example, as we mentioned, one variant of AMP is secure against password-file compromise attack whereas another is useful for situations where are very restricted and A, B are allowed to send only one message.

Scalability: since AMP has light constraints and is easy to generalize and because of its low management costs and low administrative overhead unlike PKI, our proposed protocol is highly scalable.

Efficiency: AMP is the most efficient protocol among the existing verifier-based protocols regarding several factors such as the number of protocol steps, large message blocks and exponentiations [6]. Hence a generalization of AMP on elliptic curve is very useful for further efficiency in space and speed.

Ease of Implementation: due to all reasons provided in this sub-section and since our protocol does not need any particular Infrastructure, it can be implemented easily.

VI. CONCLUSION AND FUTURE WORK

In this work we proposed a password-based authentication and key agreement protocol based on elliptic curve for WLAN. In fact we modified AMP and applied ECDSA digital signature standard to amplify the security of AMP since elliptic curve cryptosystem is stronger and more flexible. Further, we showed that our protocol has all parameters related to security and applicability. Besides, it satisfies all mandatory requirements of EAP.

For future work a key management scheme can be designed and placed in layering model to manage and refresh keys for preventing cryptanalysis attacks. Besides, this protocol can be implemented in OPNET simulator to gain advantages from more statistical parameters and it can be compared with other authentication protocols using OPNET.

REFRENCES

[1] M. Lomas, L. Gong, J. Saltzer, and R. Needham, "Reducing risks from poorly chosen keys," *ACM Symposium on Operating System Principles*, 1989, pp.14-18.

[2] S. Bellovin and M. Merritt, "Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password-file compromise," *Proceedings of the 1st ACM Conference on Computer and Communications Security*, 1993, pp. 244-250.

[3] S. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," *Proc. IEEE Comp. Society Symp. on Research in Security and Privacy*, 1992, pp. 72-84.

[4] T. Wu, "Secure remote password protocol," *Internet Society Symposium on Network and Distributed System Security*, 1998.

[5] T. Kwon, "Authentication and key agreement via memorable passwords," *In Proceedings of the ISOC Network and Distributed System Security (NDSS)*, 2001.

[6] V. Miller, "Uses of elliptic curves in cryptography", *Advances in Cryptology, Lecture Notes in Computer Science, Springer-Verlag*, 1986, pp. 417-426.

[7] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, 1987, pp. 203-209.

[8] C. Tang, and D. O. Wu, "An Efficient Mobile Authentication Scheme for wireless networks," *IEEE Transactions on Wireless Communications, Vol. 7, No. 4*, 2008, pp. 1408-1416.

[9] H. Zhu, and T. Liu, "A Robust and Efficient Password-authenticated key agreement scheme without verification table Based on elliptic curve cryptosystem," *International Conference on Computational Aspects of Social Networks*, 2010, pp. 74-77.

[10] K. R. Pillai, and M. P. Sebastian, "Elliptic Curve based Authenticated Session Key Establishment Protocol for High Security Applications in Constrained Network Environment," *International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3*, 2010, pp. 144-156.

[11] R Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Crypto-systems," *Communications of the ACM, Vol. 21, No. 2*, 1978.

[12] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd edition, Springer-Verlag, 1994.

[13] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security, Vol. 1, No. 1*, 2001 pp. 36-63.

[14] W. Peterson, and C. Scott, *Tactical Perimeter Defense*, Security Certified Program, LLC, 2007.

[15] R. Housley, and T. Polk, *Planning for PKI*, John Wiley & Sons, New York, 2001.

[16] C. Ellison, and B. Schneier, "Ten Risks of PKI: What You Are not Being Told about Public Key Infrastructure," Computer Security Journal, Vol. 17, No. 1, 2000.

[17] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlsonand, and H. Levkowetz, RFC 3748 "Extensible Authentication Protocol (EAP)," June 2004 [Online]. Available: http://tools.ietf.org/html/rfc3748.

[18] H. H. Ngo, "Dynamic Group-Based Authentication in Wireless Networks," Ph.D. dissertation, Dept. Information Technology, Univ. Monash, 2010.

[19] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, 1st edition, CRC Press, 1996.

[20] W. Diffie, and M. E. Hellman, "New Directions in Cryptography," *IEEE Transaction on Information Theory, Vol.22, No. 6*, 1996, pp. 644-654.

[21] V. Sethi, and B. Thuraisingham, "A Comparative Study of A Key Agreement Protocol Based on ECC and RSA," Department of Computer Science, The University of Texas at Dallas, Tech. Rep. UTDCS-60-06, Nov. 2006.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500