# Security of Agrarian Portals

M. Havránek, P. Benda, V. Lohr, Z. Havlíček

Faculty of Economics and Management, Czech University of Life Sciences in Prague, Czech Republic

## Anotace

Tento příspěvek se zabývá hodnocením bezpečnosti agrárních portálů provozovaných v České republice. Zaměřuje se převážně na bezpečnost autentizačního procesu při přístupu ke vzdáleným serverům. Na rozdíl například od aplikací internetového bankovnictví se ukazuje, že bezpečnosti agroportálů není věnována velká pozornost. Avšak i tyto systémy obsahují citlivé údaje, které je nutné adekvátně zabezpečit. Do hodnocení byly zahrnuty portály eAGRI, Portál farmáře, Internet pro chovatele a Agromanual. Pro porovnání výsledků zabezpečení agrárních portálů byly do srovnání také zahrnuty dva nejrozšířenější tuzemské portály – seznam.cz a Datové schránky. Cílem příspěvku je poukázat na nedostatečnou úroveň zabezpečení v souvislosti se správou identit uživatelů a navrhnout opatření pro zvýšení bezpečnosti.

## Klíčová slova

Zabezpečení, autentizace, agrární portály, intranet, metriky, informační systémy.

## Abstract

This paper deals with the safety evaluation of agrarian portals operated in the Czech Republic. It focuses mainly on security authentication process when accessing remote servers. The security of internet banking application has high level but the safety of agrarian portals seems to be very low. However, these systems contain sensitive data that must be adequately secured. The assessment covers "eAGRI" portal, "Portál farmáře" (Farmers portal), "Internet pro chovatele" (Internet for breeders) and "Agromanuál". Two most popular domestic portals – „seznam.cz" and "Datové schránky" (Data boxes) were also included to compare the results of agricultural portals security. The aim of this paper is to point out the lack of security in relation to the management of user identities and suggest measures to improve safety.

## Key words

Security, authentication, agrarian portals, intranet, metrics, information systems.

## Introduction

Since the beginning of mankind, the person in the society or community is in some way identified. In the various forms of human activities and communication with each other, it was necessary to identify the person and thus to distinguish him from one another. In ancient times merchant affirmed the identity with the finger printed in the clay plates to prove identity. Various seals and amulets were also used. In the modern history, the person is identified by hereditary characteristics in conjunction with paper documents that belonged to him. A person is referred to with a number, ID card, passport, etc. Identifying the value of original passports or legitimating securities was relatively low before the invention of photography.

From the perspective of information and communication technologies present trend points to the substantial centralization of data and applications. Original batch processing in the middle of the 20th century did not require verification of identity remote system - access to a computing machine was physically restricted by authorized persons. After the launch of the host-terminal model we can speak about relatively closed system. At the beginning of the 21st century the data were largely moved on server-side. In recent years there has been a shift to applications on the server side. This trend is related to the development of cloud-based applications. Given that these applications need to be accessed remotely, usually through a global network internet, great emphasis is placed on ensuring the authenticity of users accessing „remotely". (Vaněk, 2010), (Vaněk, 2011)

In conjunction with the development of the Internet also in agrarian sector (Šimek, 2008), the individual parts of network are in the hands of private companies and therefore it is not possible to prevent potential interception or alteration of communication, it is necessary to provide sophisticated authentication methods.

### Authentication security

Proof of identity password is the most common method of authentication. While in the early computer networks they were operated locally, or local user authentication to local computers, the risk of misuse of passwords is relatively low. Using passwords were transferred to use also in Internet, where it is no longer possible to rely on the secure transfer of data. Yet already in the initial authentication systems the good habit was to save passwords on the server in a hidden form - preferably in the form of hash. When authenticating, only the password print is being compared and the attacker cannot determine the password itself during the transmission.

Another way of authentication is a challenge -response. It eliminates the risk referred to in the preceding paragraph. It provides two forms of authentication - just determine if the opposite side of the connection is „live" user (presence of natural persons) to avoid robots and machines. The second is the authentication by factor of knowledge.

Authentication certificate is based on the public key infrastructure. This consists of CAs exhibiting certificates of private keys of individual users. Currently, to improve safety, or for the provision of some IT services asymmetric, cryptography is often used. An example of this is the use of electronic signatures, encrypted connections using digital certificates, often used for example in electronic banking. When using asymmetric cryptography, a crucial role is the use of the certificates. Certified keys are used for authentication, encryption and secure communication. Each of the party's secured communication has two keys - one private, the other public. Often, however, not only one but more pairs of keys are used for each subscriber, when various key pairs are used for various purposes. But generally it is vital to keep the private key carefully on the smart card, floppy disk that is protected, on the hard drive with controlled access to the operating system, etc. On the contrary the public key is published. (Brechlerová, 2004 ) A certification authority (CA) performs publication usually in such a way that the public key is stated as on of the entries in the certificate which is an electronic document with exactly given items. One of them is the public key, as well as identification of the signature algorithm, certificate serial number, identification certificate authority that issued the certificate, a place where you can find the certification policy, seniors certificates of the certification path, the period of validity, the next item is the identity of the owner key (common name). For sending signed e – mails, one should have an e-mail address in certificate. There are standards and recommendations, which items should be included in the certificate and the way how to be achieved. Still, there is some speculation as how to fulfill the certificate, respectively which information to place to which field in the certificate, so it is necessary to establish that data were structured in the same way at least in the given area. An example of this problem is the location of identifier of the citizen, replacing the native contact number for the public sector. After consideration I.CA (First Certification Authority) gives this to the name Alternative / Other name and others are likely to respect this fact, otherwise it would complicate development of application that needs this data.

Secure form of authentication provides one-time passwords, a password, which is not possible to carry out using an attack or repeating eavesdropping because the password is usable only once. (RFC2289) It can be easy to implement two-factor authentication, the second factor (for example, after entering the traditional static passwords) is token property to generate the OTP. Most hardware and software tokens does not protect current password, just press the button and look at the display, there is no need to enter your PIN or something like that. OTP is thus complement of the password, not a substitute. (Valasek, 2011) (Hoyer, 2009)

The advantage is that authenticating person requires no special equipment apart from token: one-time password is in the form of 6-8 characters or digits which are necessary just to be copied, direct connection of token to a computer is not necessary. It can therefore authenticate to a foreign computer in an internet cafe etc.

## Materials and methods

Considerable attention is paid to secure logging into portal applications. Unfortunately it focuses mainly on safety of the password and its saving.

The general requirements for secure authentication can meet the following recommendations: (Greer, 1999) (McClure, and others, 2007)

1. Choose strong passwords
2. Passwords should be changed regularly
3. Never save your password
4. For each system you choose a different password
5. Maintain computer and antivirus program updated
6. Do not download and install illegal software

Closer examination reveals that the points 1-4 place significant demands on the user‘s memory and in real life it is almost impossible to faithfully comply with these rules. Regular change of the password in connection with the complexity leads the user to write down the password. But this is in contradiction with point 3. These requirements increase with the number of systems to which the user has accesses. This makes contradictory requirements 3 and 4.

Numbers of systems to which users gain access in the course of life continues to grow and requirements set out in paragraphs 1-4 are almost unreal. Responsibility for imperfect way of security is transferred to a large extent to the user in terms of system operators.

Point 5 is relatively easy to meet when setting your computer and OS correctly. The problem may be requirements for older/unpatched versions of software. This can occur when the software requires discontinued and unpatched software platform.

A simpler situation seems to be at a point 6, where it is up to the user whether he is willing to take the risk with the use of illegal software. But we cannot rule out a hidden installation caused by such a virus or spurious e-mail.

The analysis of agricultural sites was examined security authentication data. The evaluation was based on an analysis of literary sources selected following criteria:

1. The system used to connect and transfer data secure HTTPS
2. The system is secured by DNSSEC domain record
3. The system enables multi-factor authentication (one-time passwords, smart cards)

For comparison, the assessment has also added two dominant Czech portals – Datové schránky and seznam.cz.

For the evaluation of the author attributes metrics designed for secure authentication in information systems. Attributes of selected metrics are not standardized. The author proposes the evaluation in accordance with the available literature. (Vanicek, 2004) (Hayden, 2010) and (Učeň, 2001).

For the safety assessment of selected authentication systems have been designed following attributes of security metrics:

The rate of connection security assessed using an encrypted connection using HTTPS. For appropriate use of HTTPS is important trusted CA that can be trusted worldwide. Supreme HTTPS can be achieved by so-called extended validation when the CA guarantees not only domain ownership, but also belonging to the organization (table 1).

The level of security service assesses the use of DNSSEC security technology. This technology allows detecting a fake DNS entry (table 2). It is therefore an appropriate defense against phishing

| Metric | Connection security |
|---|---|
| Name of metric | Connection security |
| Metric purpose | Encrypted connections make it harder for intercepting communications |
| Method of measurement | Analysis website |
| Metric interpretation | 0 – no HTTPS<br>50 - uses HTTPS with certificate from not trusted CA<br>90- uses HTTPS with certificate issued by trusted CA (without extended validation)<br>100 - uses HTTPS with certificate issued by trusted CA (with extended validation) |
| Source data | Web page, list of CAs and information about certificates from CA |

Source: own processing

Table 1: Connection security metric.

and pharming attacks. The service on the server side has no other options – it is either implemented or not.

| Metric | DNSSEC |
|---|---|
| Name of metric | DNSSEC |
| Metric purpose | The level of protection against spoofing DNS record |
| Method of measurement | DNS query |
| Metric interpretation | 0 – no DNSSEC<br>100 - uses DNSSEC |
| Source data | Register nic.cz |

Source: own processing

Table 2: DNSSEC metric.

Multifactor authentication typically uses other authentication data than a user name and password. Electronic signature (certificate) or one-time password can be used as an additional authentication data. The rate of multi-factor authentication is the ratio between the numbers of authentication factors against the highest number of factors obtained from the evaluation of the options (table 3).

| Metric | Multi-factor authentication |
|---|---|
| Name of metric | Multi-factor authentication |
| Metric purpose | The use of multiple methods of authentication |
| Method of measurement | $X = 100 * \frac{n}{\max(n)}$,<br>where X is rate of multifactor authentication, n = number of authentication methods, max (n) - the highest number of authentication methods in the sample |
| Methods of measurement | Website analysis |
| Metric interpretation | Ratio of multi-factor authentication |
| Source data | Website |

Source: own processing

Table 3: Multi-factor authentication metric.

The weight of metrics is identical. Metrics are therefore normalized to values between 0 and 100. Results will be displayed as a radial diagram.

### Portal eAGRI

Portal "eAGRI" forms the central point of access to information resources of MZ ČR (Ministry of Agriculture). It was originated by merging sites mze.cz, upu.cz (page land offices) and farmar.eu (Portál farmáře). "Portál sítě pro venkov" was also integrated in this system. The portal supports for individual applications SSO, a single sign-on to all components.

Single sign-on is enabled with implementation of LDAP background. In LDAP the user certificate is also possible (table 4).

| *Parameter* | *Result* | *Notes* |
|---|---|---|
| Address | | **https://ilogin.mze.cz/distauth/UI/Login** |
| HTTPS | Yes | Trusted CA, only identity validation |
| DNSSEC | No | |
| Multi-factor authentication | No | |

Source: own processing

Table 4: Results for portal eAGRI.

### Portál farmáře

The user registers into "Portál farmáře" with request for access to the registry of the Ministry of Agriculture. To set up access it is required to submit documents necessary to verify the identity and eligibility of the applicant. User is authenticated to prove the identity (identity card or passport). Eligibility is presented by individual's identity card or passport. For other legal entities according to legal form:

Legal entity - a statement of the basic registers or extract from the commercial register (OR) or other certificate of business from which it is clear who is the legal representative of the company. If the applicant is not the legal representative of the entity, the applicant must submit a certified power of attorney, which is subject to the legal representative referred to in the submission of the statement of the OR or in a certificate of legal status. The power of attorney must be authorized by the applicant access to protected data subject to the Farmer‘s portal (also in the case of authorized natural person) and signature of principal/s must be officially verified (table 5).

| *Parameter* | *Result* | *Notes* |
|---|---|---|
| Address | | **https://www.szif.cz/irj/portal/pf/pf-uvod** |
| HTTPS | Yes | Trusted CA, extended validation |
| DNSSEC | No | |
| Multi-factor authentication | No | |

Source: own processing

Table 5: Results for Portál farmáře.

### Internet pro chovatele

Application "Přístup k datům" (data access) enables data to breeders of dairy cattle, sheep and goat farmers, dairies and milk cooperatives in electronic form. User name and password provides the user with the access to the data that belongs only to him.

Through the application of data access the user can obtain the results of analyses of samples of milk yield control of cattle, sheep and goats in two forms and the results of analyses of samples of milk for monetization. New users acquire access rights through the registration form.

The user name „aaa" and the password „aaa" has concluded in successful authentication during testing when determining where the user is redirected after a failed test - Therefore the user with these credentials already existed in the system. The same situation also occurred during logon of user „bbb" and the password „bbb" (table 6).

| *Parameter* | *Result* | *Notes* |
|---|---|---|
| Address | | http://data.cmsch.cz/login_data.php |
| HTTPS | No | |
| DNSSEC | No | |
| Multi-factor authentication | No | |

Source: own processing

Table 6: Results for Internet pro chovatele.

### Agromanual.cz

"Agromanuál" is a portal dedicated to plant protection products for both gardeners and farmers. When the user registers (through unsecured channel), the password is sent back to the user in plaintext.

The portal is closely bound to Agromanualshop.cz, but the two systems have separate login information. It is necessary to register separately (table 7).

| *Parameter* | *Result* | *Notes* |
|---|---|---|
| Address | | http://data.cmsch.cz/login_data.php |
| HTTPS | No | |
| DNSSEC | No | |
| Multi-factor authentication | No | |

Source: own processing

Table 7: Results for Agromanual.cz.

### Agroweb.cz

This site does not allow registration and login; therefore it was not included in the testing.

### Seznam.cz

One of the most popular Czech portals provides very low security of authentication. Check-in is possible only with username and password. With regard to the number of users and the potential risk of abuse of the accounts the security is rather worrying (table 8).

| *Parameter* | *Result* | *Notes* |
|---|---|---|
| Address | | http://www.seznam.cz |
| HTTPS | Yes | Entry pages uses only HTTP, password is sent over HTTPS |
| DNSSEC | No | |
| Multi-factor authentication | No | |

Source: own processing

Table 8: Results for seznam.cz.

### Datoveschranky.info

Data boxes (right "informační systém datových schránek- ISDS) are operated pursuant to Act No. 300/2008 Coll. Electronic acts and authorized conversion of documents. The main advantage is to ensure the authenticity of users. It is secured by a personal identification during the registration process. If the request is sent electronically, a trusted digital signature is required to sign (table 9).

| *Parameter* | *Result* | *Notes* |
|---|---|---|
| Address | | http://www.mojedatovaschranka.cz |
| HTTPS | Yes | Trusted CA, extended validation |
| DNSSEC | No | |
| Multi-factor authentication | No | Chip card, SMS messages (paid by user, price 3 CZK per message), one-time passwords |

Source: own processing

Table 9: Results for ISDS.

## Results and discussion

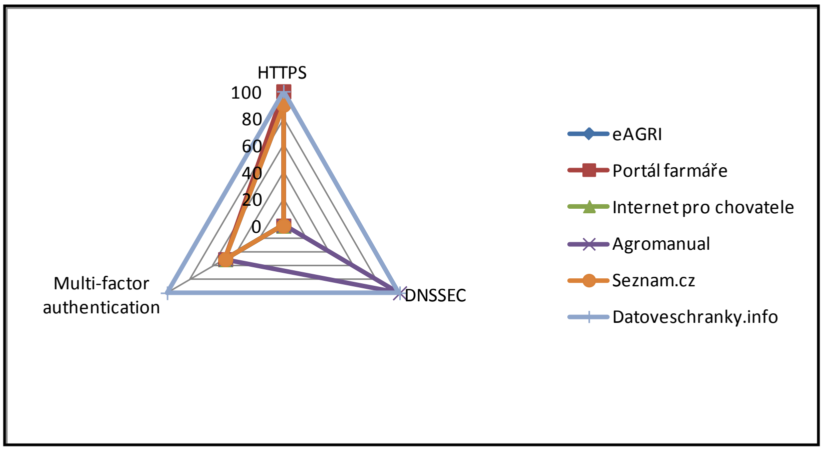
Numeric expression of metrics based on the measurements is shown in Table 10. For clarity, the results are plotted in Graph 1.

Dominance of data boxes is a clear in Graph 1. In terms of security authentication "Datové schránky" reach the highest level of security in all criteria.

| | *HTTPS* | *DNSSEC* | *Multi-factor authentication* |
|---|---|---|---|
| eAGRI | 90 | 0 | 50 |
| Portál farmáře | 100 | 0 | 50 |
| Internet pro chovatele | 0 | 0 | 50 |
| Agromanual | 0 | 100 | 50 |
| Seznam.cz | 90 | 0 | 50 |
| Datoveschranky.info | 100 | 100 | 100 |

Source: own processing

Table 10: Rating authentication security of portals.



Source: own processing

Graph 1: Comparison of security.

“eAGRI” and “Portál farmáře” were evaluated to be the best portals as for the agrarian ones. The same authentication against LDAP as well as protocol HTTPS with a trusted certificate is used by both portals for secure data transfer. What is more “Portál farmáře” make also use of so-called extended validation. This confirms not only certified subject domain’s ownership; it also confirms the identity of that company. Acceding user can thus be sure that the site really belongs to the actual company. During testing authentication data of some users were randomly found in portal “Internet pro chovatele”. These users have the same password as the user name. It is a big security threat.

Apart from agrarian portals the best evaluated are “Datové schránky“ They provide security at a high level. Conversely seznam.cz is evaluated very low in terms of security authentication.

Recommendation for portals (outside “Datové schránky”) is primarily to enable solution that support multi-factor authentication.

The final order for agrarian portals (sorted from best rated) is following:

1. „Portál farmáře“. It uses secure protocol for internet communication, but users can be only authenticated using passwords. In these times the password can be stolen from computer or captured from keyboard. I suggest implementation of DNSSEC and multi-factor authentication.
2. eAGRI. The only difference between „Portál farmáře“ and eAGRI is, that eAGRI doesn‘t use extended validation for certificate. This vulnerability has disadvantage in communication with counterparty, when we cannot guarantee ownership of web address. In other cases it can be acceptable. I suggest implementation of DNSSEC and multi-factor authentication.
3. Agromanual uses from secure techniques only DNSSEC. It is important to ensure, that user opens actually the page, he had requested. But using combination authentication using password

with unsecure connection is highly vulnerable. I suggest implementation of HTTPs and multi-factor authentication.

4. The worst safety had „Internet pro chovatele“, that uses no security techniques. It implicates very high vulnerability of this portal. I suggest implementation of DNSSEC, multi-factor authentication and HTTPs.

The future research will be focused on improving authentication security of agrarian portals. For this reason were in comparison included „Datové schránky“. These are now at the top on security authentication.

## Conclusion

This paper defines metrics for measuring authentication security of web portals. These metrics are then applied to agrarian portals. Detailed results are described in chapter Results and discussion.

Security of some agrarian portals is on very low level and should be increased using some advanced techniques. Also best rated portals offer only single-factor authentication, that is currently rated as low secured. Passwords can be captured via keyloggers or screenlogers. Possible solution is to use one-time passwords system or some OpenID solutions with high authentication security.

*Corresponding author:*
*Ing. Martin Havránek*
*Department of Information Technologies, Faculty of Economics and Management,*
*Czech University of Life Sciences in Prague, Kamýcka 129, Prague 6, 16521, Czech Republic*
*Phone: +420 224 382 045, E-mail: havranek@pef.czu.cz*

## References

[1] Brechlerová, D. Certifikáty jako základ e-podpisu, autentizace i šifrování. Ekonomické a informační systémy v praxi. [Online] 12, 2004. [Accessed: 25. 8 2011.] available at: http://www.systemonline.cz/clanky/certifikaty-jako-zaklad-e-podpisu-autentizace-i-sifrovani.htm.

[2] CZ.NIC. Statistiky CZ. NIC. [Online] [Accessed: 5. 6 2013.] available at: https://stats.nic.cz/.

[3] CZ.NIC. Statistiky. [Online] [Accessed: 30. 11 2011.] available at: http://www.nic.cz/stats/.

[4] Doseděl, T. Počítačová bezpečnost a ochrana dat, Brno, Computer Press, 2004, ISBN 9788025101063.

[5] Doucek, P., Novák, L. , Svatá, V. 2008, Řízení bezpečnosti informací, Prague: Professional Publishing, 2008, ISBN 978-80-86946-88-7.

[6] Greer, T. Intranety. Brno, Computer Press, 1999, ISBN 80-7226-135-5.

[7] Hayden, L. IT Security Metrics. McGraw-Hill, 2010, ISBN: 978-0-07-171340-5.

[8] Hoyer, P. OTP and Challenge/Response algorithms for financial and e-government identity assurance. [author of the book] Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider, ISSE 2008, Securing Electronic Business Processes, Wiesbaden, Vieweg+Teubner, 2009.

[9] Hung, T. Troy H. A brief Sony password analysis, Troy Hunt‘s Blog. [Online] [Accessed: 26. Aug 2011.] available at: http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html.

[10] McClure, S., Scambray, J., Kurtz, G. Hacking bez záhad. Prague, Grada, 2007. ISBN 978-80-247-1502-5.

[11] NIC.CZ. CZ.NIC - O DNSSEC. [Online] [Accessed: 30. 11 2011.] available at: http://www.dnssec.cz.

[12] Pour, J. Informační systémy a technologie. Prague, University of Economics and Management, 2006, ISBN 80-86730-03-4.

[13] RFC2289. RFC 2289. A One-Time Password System, RFC Editor. [Online] [Accessed: 2. 9 2011.] available at: http://www.rfc-editor.org/rfc/rfc2289.txt.

[14] Šimek, P., Vaněk, J., Jarolímek, J. Information and communication technologies and multifunctional agri-food systems in the Czech Republic, Plant, Soil and Environment, 2008, Vol. 54, No. 12, p. 547-551. ISSN: 1214-1178.

[15] Učeň, P. Metriky v informatice. Prague, Grada Publishing, 2001, ISBN 80-247-0080-8.

[16] Valášek, M. Hesla na jedno použití. Lupa.cz - server about Czech internet. [Online] 15. 12 2011. [Accessed: 15. 12 2011.] available at: http://www.lupa.cz/clanky/hesla-na-jedno-pouziti/.

[17] Vaněk, J., Kánská, E., Jarolímek, J., Šimek, P. State and evaluation of information and communication technologies development in agricultural enterprises in Czech Republic, Plant, Soil and Environment, 2010, Vol. 56, No. 3, p. 143-147, ISSN: 1214-1178.

[18] Vaněk, J., Jarolímek, J., Vogeltanzová, T. Information and Communication Technologies for Regional Development in the Czech Republic – Broadband Connectivity in Rural Areas. AGRIS on-line Papers in Economics and Informatics, 2011, Vol. III, No. 3, p. 67-76, ISSN: 1804-1930.

[19] Vaníček, J. Měření a hodnocení jakosti informačních systémů. Prague, CULS FEM, 2004. ISBN 80-213-1206-8.