Security of medical data transfer and storage in Internet. Cryptography, antiviral security and electronic signature problems, which must be solved in nearest Future in practical context

Piotr Kasztelowicz, Marek Czubenko, Iwona Zięba

The informatical revolution in computer age, which gives significant benefit in transfer of medical information requests to pay still more attention for aspect of network security. All known advantages of network technologies - first of all simplicity of copying, multiplication and sending information to many individuals can be also dangerous, if illegal, not permitted persons get access to medical data bases. Internet is assumed to be as especially “anarchic” medium, therefore in order to use it in professional work any security principles should be bewared. In our presentation we will try to find the optimal security solution in organisational and technological aspects for any medical network. In our opinion the harmonious co-operation between users, medical authorities and network administrators is core of the success.

Organisational and Legal regulations

The Law in many countries takes into considerations the legal problem associated with computer and network. Especially specific regulations concerning new technologies in context of Internet publications should be created - the law for authors – copyrights. In medicine it seems more important to avoid transporting and spreading computing viruses, hacking including illegal information capturing from broken servers and destroying servers as well as other network components. In our opinion except general used legal principles a local regulation code should be created and requested for use. Authorities, who will use Internet for professional medical information transfer can in this situation, if any code exists, keep in their hands important instruments to secure this network - including violations other networks attempted from host computers working in their local area network. But the general principles of privacy, confidentiality, which are important, established by long term tradition met in the network, should be honoured to avoid anybody feeling to be investigated by network administrators. Strong careful controls are not necessary, here it seems to be recommended more education activity to learn network users, how to avoid possible complications and what is allowed to do in their network activity. We advise to pay more attention for the network, where students work, because more attempts of codes violations seem to be there. The following elements should be included into the proposed regulations::

- Principles of usage PC-computers connected to network
- Principles of creating, storing and protecting account password to data, servers and services
- Principles which way and who will be informed about network accidents and damage or problems and how many time need to be to react on such signals. Existing of helpdesk for users is very desirable.
- Instruments for network and institutional authorities, operators including administrators of whole network and detailed network services (for instance discussing list moderators). Here any special services can posses their separate regulations
- Network security systems and regulation, how punish attempts of it abuse. What kinds of proofs should be collected before removing a user from network in such cases.

- Principles to avoid publishing and spreading inappropriate information (propagated sexual violation, racism, other illegal information, permanent, not accepted by institution serving network) to remove it form servers
- Principles of accessing and staying in rooms, where are placed computers and other network elements.

Such a code should be supported in prepared form with information about the principles. The potential users should be informed about important elements of it (and accept them, by signing acceptation form)– for instance “yellow notebook” with important phone numbers to call helpdesk, with important addresses, emails and principles. Some of it information and text of code can be placed on web. Such regulation remains a “Highway Code” for individuals surfing through cyberspace, but it should not be too restrictive. Such code should not stop the transfer in network by its too restrictive nature but regulate it the appropriate way If too many restrictive code is established, then, very often and any time it’s broken by all. This same we will emphase, we know the administrators anytime tend to create restrictive regulations, because there are comfortable for their work. We will recommend to avoid restrictive codes, because only rational and acceptable ones, are efficient in purpose to persuade proper behaviour using the network as well as condemning the unacceptable, abusive activity.

How every user should guard and protect his network and computer account?

Passwords

This is simple true, every individual using computer connected to the network should defend himself against abusive behaviour of other local users and strangers just the way he does with his own home. It is also impossible to guard system, computers, network and data putting even with a big effort of network administrator, if users don’t take care of security. The basic tool to secure an account to network is the password. It’ s clear, that if an access to mailbox is possible from any place of net to give each user easy to access mail independently from actual stay-place in any moment, the password is one security tool only to guard mailbox from non permitted access. Therefore users should be educated, how they should manage their passwords. Some network administrators use systems, that automatically generate passwords and force to use them by all users after a given time forcing to change them. In our opinion this method normally is too restrictive – it seems better to teach users to manage themselves single-time passwords system (skey), which can be suggested, if a person must login into system from particularly unsafe place. The aware of this problem in aspect of password should pay attention to:

- avoid to set a password containing simple and known phrases or data, which are characteristic for him or his family (name of wife, date of birth of daughter, registration number of user’s car)
- password should be difficult to break it and it should contain minimum eight characters including at least: one letter, one digit and one special character (*,&,@,#...)

The user should know, he must not give his account to network and password to other persons and to write down password the way, that it can not be simple captured. Network administrator has an important role to educate all, how crucial to network security significance in Internet plays appropriate password protection.

Secure data interchange

During transfer data often must flow a long distance passing through many intermediate servers and networks. This can be simple imagined, information can be captured, if anyone intentionally will get access to it. Although such an activity has criminal character, but the responsibility, if access to this data can follow to break a medical confidentiality and as result undermining position of our organisation: hospital or others. As we have said, all advantages of Internet to copy and resent many data in short time used dishonestly, can give many disaster (as be relevant if used honestly and properly). The most important method to avoid it is to promote safe network behaviour. The first step of it is to determine which data can be transferred free and which can be accessed only by permitted persons. The next step is to establish a secure way of transfer professional and confidential data. After reading Eysenbach interesting series of papers about them (confidentiality and medical Internet) we'll propose distinguish these three confidentiality levels:

- free – the information are completely free. There are no access limitation for access to it. There is permission to copy it to others or cite.
- professional – this is form of limited access to information, which give permission to get it. if conditions of subscription has been met. The user will be asked to read the code, fill in a form to get access, sometimes to pay a fee. This same level can have the information on net, which seemingly are totally free, but copyright or permission to resent it has been not allowed. Here should be distinguished intentional permission as very important not to t violate the network etiquette and privacy. Intentional permission is like the principle of opened door with inscription, who can go in. This limited access and ability to copy or resent a data for specified persons or under condition by anybody after checking each person, if established rules have been met. The author assumes that all the people are honest and intentions of all visitors are good. This also does not give a permission to break it. If anybody tries to abuse it – his activity is then classified to be intrusive and the consequences can be suffered. Eysenbach gives more examples of such intrusive behaviour, other than spams, scams and frauds has been also widely described on net.
- confidential – the information are especially protected and can be read by permitted individuals only. It has respect to a large extent of telemedicine, where information about a patient has being transferred through net.

The important to promote programs using secure protocols to communicate with others, particularly, if confidential post or other form of data interchange is planned. So instead telnet ssh is good alternative, similarly to copy files secure-ftp is better than standard ftp. Gradually administrated by us web-services will be equipped with SSL . This standard has been already included to electronic banking, and thus seems to be quite safe, because no serious crashes has been here described. This should be part of education, which will increase awareness of medical professionals using internet in professional contacts.

Access control systems – the most important tools of server administrator

Control access is most often used and typical to assure a higher degree of security of server. This tool can specify the host, which can be permitted to connect to any given port of our server and to accept particular services and reject access from the places, which we can consider to be suspicious of hacking our server. Our team has good experience with this method and introducing it to all service can effective protect a medical server from destroying. Additionally information about every attempt to connect with server are written to logs, what enables to identify host, where those attempts have been performed from. Below we include examples of such records.

An example of unpermitted access to server Dorota to ftp, connection has been refused:

```
Apr 30 04:04:50 dorota ftpd[4829]: refused connect from aoquir9.uab.es
May  1 12:41:56 dorota ftpd[11703]: refused connect from 80.116.10.96
May  1 14:11:43 dorota ftpd[13365]: refused connect from
ip3e83d888.speed.planet.nl
```

A like previous example to server Sun to telnet port:

```
May   3  13:39:49  sun  telnet:  tcpserver:  deny  1636  :212.51.193.152:23
host226-pool6211052.interbusiness.it:62.110.52.226:root:4099
```

Here was foiled attempt to retrieve by intruder records from domain names server from Sun. DNS is an important service for all networks, therefore information including such data should be primarily secured

```
2002-04-18 10:35:29.592013500 tcpserver: status: 0/40
2002-04-22 12:28:36.740827500 tcpserver: status: 1/40
2002-04-22 12:28:36.758824500 tcpserver: pid 7240 from 216.23.92.170
2002-04-22  12:28:36.758842500  tcpserver:  deny  7240  0:212.51.193.152:53
:216.23.92.170::1897
```

Including an access control system due to some consequences for normal users of server. If any user will get access to any important service from untypical, free not known place, a server can reject it. Each time, if we will change this place ourselves, we must give this information about new address to network administrator to allow access. We have been assumed, that with this system are secured the most important or potentially “vulnerable” services. We also let to access from every host to mailbox to give possibility to read and send mail regardless of stay place. Additional problem is, how react on such abusive activity, if has been proved by record in server’s logs? Usually we apply to contact with network administrator of server, which such attempt has been performed from, but very often no effect has been met. It seems to be helpful to create Work Group affiliated at Polish Medical Internet Society for this institutional activity. The co-operation between users, network administrator and medical staff including known authorities first of all to perceive problem and later to help with authoritative position and international contacts to stop it, can be desirable. The destroying of important server by hackers can cause many problems and need long time to rebuild system and resources.

Antiviral security

Computing viruses in last years periodically attack computing systems and software. They are significant source of problems, losses of profits in commercial system and damages in attacked computers. Paradoxically, other than in case of hacking, viruses very seldom destroy internet servers but are only transferred through to Windows workstations, where the devastation is done.. The UNIX operating systems working on servers usually are not damaged by most met viruses. So it is a situation of existing a target place, which will be attacked – workstation and transit servers, which are blind to transfer it. There are two principles to avoid consequences of viral infections. First - to avoid infection. Most often the viruses contains executable file send with email as attachments or present in software originated from unproven source. Thus we have a simple principle – to avoid to activate potentially received viruses with email

- it should be avoided to open attachments, and installing it on disks when obtained from unknown persons or from persons, who are us known, but from content of mail body (information) don’t follow, that this person will send us such file. The peoples, who send binaries as attachments should inform about it in message body and inform, from which sources originates a file and which with antiviral software has been checked
- it should be used to send normal email message body only simple text mode, do not use RTF or www form. This can secure of pinning the virus itself to email messages. Simple text mode messages are not able to transfer viruses.
- There should be avoided to use email software on workstation to connect with mailservers, which has known “bad opinion” as viruses transferplaces. We highly recommend Pegasus-Mail or Eudora (including useful Eudora-Light) as free, proven and safe.

It is necessary to use on our computer connected to Internet at least two antiviral software – one from this two with function of activity monitoring.

Antiviral scanners installed on server

A new way to protect our computer against infection is to install antiviral scanner on mail server. We have written, that viruses usually do not damage an UNIX server, but these servers – particularly mail servers contribute to spread viruses. The idea is to remove virus before it reaches the target place – work station. The scanners installed on mail servers protect many users not only to get email containing such a virus but to send a virus to other peoples from our computer as well. In our servers we will gradually install this high effective protection tool. An example of efficiency to stop popular Romeo & Juliet virus has been shown below. This is testing post sent to one of authors of this presentation. The mail has been not delivered:

```
Date: 16 Sep 2001 16:05:40 -0000
From: postmaster@lodz.ptkardio.pl
To: pekasz@am.torun.pl
Subject: VIRUS IN YOUR MAIL TO Piotr.Kasztelowicz@lodz.ptkardio.pl

                   V I R U S  A L E R T

  Our viruschecker found a VIRUS in your email to
"Piotr.Kasztelowicz@lodz.ptkardio.pl".
           We stopped delivery of this email!

    Now it is on you to check your system for viruses

  For further information about this viruschecker see:
               http://amavis.org/
        AMaViS - A Mail Virus Scanner, licenced GPL



For your reference, here are the headers from your email:

------------------------- BEGIN HEADERS -----------------------------
Received: (qmail 24861 invoked from network); 16 Sep 2001 16:05:37 -0000
Received: from dorota.am.torun.pl (root@158.75.16.66)
  by 212.51.193.152 with SMTP; 16 Sep 2001 16:05:37 -0000
Received: from dorota.am.torun.pl (dorota.am.torun.pl [158.75.16.66])
```

```
        by dorota.am.torun.pl (8.9.3+Sun/8.9.3) with ESMTP id SAA04318
        for <Piotr.Kasztelowicz@lodz.ptkardio.pl>; Sun, 16 Sep 2001
18:15:06 +0200 (MET DST)
Date: Sun, 16 Sep 2001 18:15:05 +0200 (MET DST)
From: Piotr Kasztelowicz <pekasz@am.torun.pl>
To: <Piotr.Kasztelowicz@lodz.ptkardio.pl>
Subject: ,,... (fwd)
Message-ID: <Pine.GSO.4.31.0109161814440.4316-102000@dorota.am.torun.pl>
MIME-Version: 1.0
Content-Type: MULTIPART/Mixed; BOUNDARY="----
=_NextPart_000_001D_01C04A9A.F06454A0"
-------------------------- END HEADERS ------------------------------
```

In logs of server the more detailed information about virus has been written:

```
Now it is on you to check your system for viruses
Originally bin/qmail-local -- alias /var/qmail/alias Piotr.Kasztelowicz -
Piotr.Kasztelowicz
lodz.ptkardio.pl pekasz@am.torun.pl ./Mailbox
The mail has been stored as /var/virusmails/alias/virus-20010916-24862
xxxxxxxxxxxxxxxxxxSun Sep 16 18:05:38 MET DST 2001xxxxxxxxxxxxxxxxxxxxxxx
qmail-local (0.2.1) called -- alias /var/qmail/alias Piotr.Kasztelowicz -
Piotr.Kasztelowicz
lodz.ptkardio.pl pekasz@am.torun.pl ./Mailbox
FROM: pekasz@am.torun.pl
TO: Piotr.Kasztelowicz@lodz.ptkardio.pl
maxlevel: 0
Contents of /var/tmp/qmail-local24862/unpacked
.:
total 86
drwx------   3 alias    nofiles      512 Sep 16 18:05 .
drwx------   3 alias    nofiles      512 Sep 16 18:05 ..
-rw-------   1 alias    nofiles      242 Sep 16 18:05 1000656338.24879-
0.sun
drwx------   2 alias    nofiles      512 Sep 16 18:05 SFX
-rw-------   1 alias    nofiles     6360 Sep 16 18:05 xjuliet.chm
-rw-------   1 alias    nofiles    34304 Sep 16 18:05 xromeo.exe

./SFX:
total 0
drwx------   2 alias    nofiles      512 Sep 16 18:05 .
drwx------   3 alias    nofiles      512 Sep 16 18:05 ..
H+BEDV AntiVir scanstatus0 is: 0
Mcafee scanstatus1 is: 0
Dr. Solomon (old) scanstatus2 is: 0
Dr. Solomon (new) scanstatus3 is: 0
Sophos Sweep scanstatus4 is: 0
NAI Virus Scan 4.x scanstatus5 is: 0
KasperskyLab AVP scanstatus6 is: 0
KasperskyLab AVPDaemonClient scantatus7 is: 0
F-Secure Antivirus scanstatus8 is: 0
Trend Micro FileScanner scanstatus9 is: 0
CyberSoft vfind scanstatus10 is: 0
CAI InoculateIT (inocucmd) scanstatus11 is: 100

Virus FOUND Sent notification to virusalert
```

We do not consider another area of network activity - potentially dangerous- web surfing. Very similar manner we can infect our computer (workstation) surfing through websites. Clicking an icon or button we may transfer a piece of program code onto our computer and activate it. This is also a typical scenario of getting infected. Here the situation is much more complicated, than in case of mail transfer. Of course one can find packages containing antiviral protection function against viruses coming via www. But any mean websurfer will not use them, because the efficiency of his web browser decreases significantly. We suppose, the only way is to educate users. What is important – there is no particular group of topics of infected websites. One can infect a computer visiting sexual oriented websites as well as religious ones. It is also an element of war, like in case of Israel-Palestinian conflict.

Electronic signature

The idea is based upon Ph. Zimmerman concept named "Pretty Good Privacy" (PGP), who create system of pair keys enabling signing and encrypting electronic documents and files. The electronic signature is generated and allow to identify author of electronic documents including binary files with the help of created by sender or in case encrypting of information sender and recipient keys. In pair of keys one named secret should be accessible for the owner only. The public is necessary for its owner identification and should be shared for the people whom its owner will send any document.

- Secret key is provided to encrypt information with public key of recipient and should be kept secretly by its owner. Decryption is performed with the help of public key of sender and secret key of recipient. Similarly nobody other is allowed to decrypt
- Public key should be shared with others, whom any document will be send to identify its author. Generally this key is used to sign documents. One should copy this key only from credible sources to have trust, this key is not fabricated and false. In future apart from already used trusting systems and ability to add to keys signatures confirming its origin certification system is been planned. This will be based on legal regulation and certifying institutions will take governmental rights.

Now, it is used three known software system to deal with electronic signature and keys. We use for MS-Windows platform PGP 7.x.x and for UNIX GnuPG actually in version 1.0.7. The compatibility of these two systems has been achieved – keys can be interchanged and signatures can be decrypted through both systems, what is important, because software differences at the end could be significant obstacle in mutual communication.

Below we will present example of public key written by GnuPG in version 1.0.4 yet:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.0.4 (SunOS)
Comment: For info see http://www.gnupg.org

 mQGiBDpU6zYRBADG3EmYOWIfZQeg8pcsJjDkvRK5RFDIEK3wGOMPGidIJ318n4ee
xQF4BJZAo/nIkiaKi3mUDD9qJBuwXB7Dm0+WBD/RovGcHNDsNJZGLA5XE3AQUjMa
NmDluSf/vq3lSOsGGmWm1ZiX/+qb4wrZNv+1nnbESAM2MvZklThgsAOfpwCgy6Gj
BYlG0qwregGWIq2mLdqXoRcEAKqBlPgRyfbbcmKLl9qQrcraeAsTFAQf9JYkVnzs
co4/GoWW3g3QGfhfbHqgmhRvhceU01iVYwUbPwo8ijshcgGth2TbMc6Eu0XInfS6
o3Eh7MdAGqJOXMj6jlgVr3lxaLogRxy2C/3hiYQ3hTIQVtBDN3bkNohuH6fUgTHQ
y1Q4A/422X/5fk2tsU4tSuzmzERSsX/3LQJQ1rNp0oD4t8TDD+63c4bf+TSwO9FT
91uuqeCTk/4a5TsLtZa5AvrPxevvScZf4+NvFMB5Y0j5WIPcUh8tuz+WOIUvXgtO
3KhduLLWKFBrVUZ0SWsW5YYbrw9NZbZ8SEpN1VzDvCh6sGQS6rQwUGlvdHIgS2Fz
enRlbG93aWN6IChwZWthc3opIDxwZWthc3pAYW0udG9ydW4ucGw+iFcEExECABcF
AjpU6zYFCwcKAwQDFQMCAxYCAQIXgAAKCRBdOHPy8+7YrxTJAKClzp37Qw7Fdnyg
VjXL+B+FQCquIwCdEy9KkL/n2rUA1Yyg0FWD43jFSFe0PFBpb3RyIEthc3p0ZWxv
d2ljeiAocGVrYXN6KSA8UGlvdHIuS2FzenRlbG93aWN6QGFtLnRvcnVuLnBsPohX
BBMRAgAXBQI6XMl6BQsHCgMEAxUDAgMWAgECF4AACgkQXThz8vPu2K9r0gCghgk3
PDpkf314abypPNOerM9YubIAoMRmvKcDYQE1MKNl62IbCOb66vO+uQENBDpU69MQ
BADaARDwJib9ls/ghnwYAEVXxVZ1Y8Of5F+w96yAJElXXbDjA00oS3iq7j1Z5su0
O1qvCLfZs8EBCWqXNG/Co0Zvr3xss68mvLofsA4FVJEjxrZEc9Qqqm/RUMy3sqig
```

```
whTLxGDymntb5Hze8gazI4rxp+hWVKkoTtNds/uV1i+efwADBwQAk29GZ8aaqA8F
7FKtcIjBq+WrHc+XZDsJRFz0lAwP3tHcD5Zvzl/UdZjq5U3n9T9zYLfR3iZdGY5u
sjaMeRgglxIbTOZPkgVAUXM9OD5pTdV1RsUrQoTv3LN9bPFGpN3D8QWTN6gvzDxN
miA4QFc8FQQHp9xr1vVmnoBrX7HUIDyIRgQYEQIABgUCOlTr0wAKCRBdOHPy8+7Y
r1cgAJ9E1oJHSptidiU8Bw5s5oKMRJanHACgyMMkGU89aspVrpWLhq0IvOVwXck==gvP/
 -----END PGP PUBLIC KEY BLOCK-----
```

The key’s body is present between sections “begin PGP key block” and “end PGP public bock”

An example of email including electronic signature looks: like this:

```
From: Piotr Kasztelowicz <pekasz@lodz.ptkardio.pl>
To: <pekasz@am.torun.pl>
Content-Length: 391

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

To jest przesylka z elektronicznym podpisem

- ---
Piotr Kasztelowicz                 <Piotr.Kasztelowicz@lodz.ptkardio.pl>
[http://www.am.torun.pl/~pekasz]
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.7 (SunOS)

iD8DBQE81xt6XThz8vPu2K8RAjbZAJ0ZbwHn/RAkJTyCVHRbTQAJV7TxHgCgmWDm
yiZXjoFVq1w7iRGnQ1Jqhf8=
=rwq9
-----END PGP SIGNATURE-----
```

The electronic PGP signature is visible between two described “begin” and “end” lines. The next step is to verify signature. We must prior to it retrieve public key of sender of this mail. After verifying we are informed, if the signature is good, that this letter is really written by this concrete person and its body was not changed by others before arrival to our mailbox.

Here is an example of such verification of this email. As shown – the signature is good. All is in this example ok.

```
Date: Tue, 7 May 2002 02:10:21 +0200 (MET DST)
From: Piotr Kasztelowicz <pekasz@lodz.ptkardio.pl>
To: pekasz@am.torun.pl
Subject: przesylka z elektronicznym podpisem

To jest przesylka z elektronicznym podpisem

---

Piotr Kasztelowicz                 <Piotr.Kasztelowicz@lodz.ptkardio.pl>
[http://www.am.torun.pl/~pekasz]

------------ Output from gpg ------------
gpg: please see http://www.gnupg.org/faq.html for more information
gpg: Signature made Tue May 07 02:10:34 2002 MET DST using DSA key ID F3EED8AF
gpg: Good signature from "Piotr Kasztelowicz (pekasz)
<Piotr.Kasztelowicz@am.torun.pl>"
gpg:                 aka "Piotr Kasztelowicz (pekasz) <pekasz@am.torun.pl>"
```

Possibility to sign electronic documents and encrypting tools shall become in future crucial for progress of new communication technologies in medicine, banking sector, e-commerce and other. There are not common opinion yet, how in future should be performed key certification process, but the first certification world agencies have been already created. To accustom medical professional to key using one year ago we are established key server – ***http://sun.lodz.ptkardio.pl:11371*** on server of Lodz Branch of Polish Cardiac Society. Here can be stored the public keys of physicians, which can be retrieved as well as send to server by each network user using PGP 7.x..x (for Microsoft Windows) interface.

In conclusion we'll present the importance of "safe network behaviour" . Answering the question – " problems, which must be solved in nearest Future in practical context" the most important seem to be

- Establishing common security standards for medical network community based on simple but proven rules and software
- Educating medical professional s the "safe network behaviour"
- Installing antiviral scanners on mail servers and using antiviral software on work stations
- Creating legal codes to guard network and systems against abusive activity
- Still monitoring and interchanging information about potential security problems and methods to solve it.