IT-Security for Meteorological Measuring Networks

Dipl.-Ing. Gerhard Pevny, Logotronic GmbH, Phorusgasse 8, 1040 Vienna, Austria
Tel: +43/1/5872971-14, E-mail: gerhard.pevny@logotronic.co.at

Mag. Roland Potzmann, ZAMG - Zentralanstalt für Meteorologie und Geodynamik,
Hohe Warte 38, 1191 Vienna, Austria,
Tel: +43/1/36026-2706, Fax: +43/1/36026-2720, E-mail: roland.potzmann@zamg.ac.at

ABSTRACT

Everyone knows today about Internet hacker attacks against public and private institutions. Enormous financial losses and the breakdown of important services are the consequence of these incidents. Today measuring networks, also meteorological networks and hydrological networks, are using increasingly the Internet for their data transfer and become therefore more and more vulnerable to hacker attacks.
The TAWES network is the national synoptic and climatological measuring network of Austria. The existing network performed well for more that 10 years, but the fast developments in communication technology are now addressed by a project, that ZAMG and Logotronic have started about 1 1/2 years ago. The project target is to to upgrade the existing TAWES network in order to integrate the following additional features:

- Best possible IT-security
- Total accessibility to all components of the network via Internet
- Preparation for the Internet of Things (IoT)
- On network level deployment of only well established Internet standards
- Long lifetime although using latest technology from fast changing markets
- Test of Internet access over satellite as an highly available backup data path

Detailed technical studies and technical developments led to an actually ongoing test operation integrating some updated TAWES stations, central servers and maintenance PCs in routine operation. The test system is limited regarding the number of measuring stations but it is already offering the full functionality of the finally planned system.

Motivation for the project

Everyone knows today about Internet hacker attacks against public and private institutions. Enormous financial losses and the breakdown of important services are the consequence of these incidents. Today measuring networks, also meteorological networks and hydrological networks, are using increasingly the Internet for their data transfer and become therefore more and more vulnerable to hacker attacks. Please imagine the case, that your meteorological measuring network becomes a victim of such Internet criminals and you have a stop of service for some days and maybe days or weeks of labour time to overcome the situation....
In the year 2005 the Austrian meteorological institute ZAMG launched an international tender for supply and installation of a new version of the national Austrian meteorological measuring network, called TAWES network. The contract for the turnkey supply went to an Austrian consortium where Logotronic was responsible for the delivery of all measuring equipment. In the meantime nearly 300 automatic weather stations are installed all over Austria and the network is performing well.

Fig, 1: TAWES station Pitztal Glacier - Weatherstation in a high alpine environment

Nevertheless time is changing and the technical requirements for measuring networks are changing, too. ZAMG and Logotronic considered some facts which needed investigation in order to have different technical updates of the existing system

- Best possible IT-security for all measuring stations, servers, maintenance PCs, etc Of course ZAMG has a perfect IT-department, responsible also for IT-security, but measuring networks are still something different to standard IT components.

- Full Internet communication using the most advanced technologies
  Up to now the TAWES network communication is based on special telephone landlines with high availability and GPRS mobile radio. Integration of the latest standards in communication technology is necessary in order to have fast Internet available (LTE or fast wired Internet connections). The Internet should be used for all communications, but without reduction in the reliability of the communication. Redundant communication paths must be existing at all measuring stations.

- Internet of Things - IoT
  Integration of new sensor technology, especially related to the so called Internet of Things - IoT, where every member in the network has Internet access. We think, that in the near future maybe meteorological sensors will have standardized interfaces to the Internet. For actual dataloggersl communication over Internet has already become the standard. There is also the idea to integrate actual sensors with different interfaces, like RS485, SDI-12, etc) in the new system by developing the necessary interface modules to Internet standards.

- Deployment of standard products in order to reach long system lifetime
  Another goal was to reach a maximum of independence from propriatory, mostly manufacturer standards, because we see such a dependency as a limiting factor of system lifetime. As near at the sensors as possible all communication within the network is translated into well proven and mature Internet standards, where lots of products are available from the shelf and at least compatible products will be available in the future.

- Independence of Internet providers and cell-phone providers
  All Internet providers offer also some options for IT-security, like VPNs, special firewalls, etc. We think, that IT-security is such an important matter, that it should not be sourced-out. In most cases these services are not completely documented and work as "black box". To create the infrastructure in-house brings on one hand complete transparency about the technical details as well as independence of special services of Internet providers.

- There was also some progress in the development of Internet communication over satellites. The old system of telephone landlines with high availabilty could be replaced by new Internet connectivity via satellite.

Beside all of this new functionality it should only be an update of the existing and well working system, not a replacement. The plan was to develop a "Network on Measuring

Station Level" and to connect all local TAWES station networks together with the central servers to a big austrian-wide LAN with total communication and all options for access to the system components.
This system upgrades will lead the way to a completely new level of measuring network performance, based on the exisiting components, extended by some smart high tech components. In Austria maybe this network will be called TAWES V2.

Basic technical reqirements

In order to fullfill these extensiv expectations we have defined some basic technical requirements.

- We use only published and well proven Internet standards for all items. No propriatory software and no propriatory protocols will be used on network level.

- An old problem in using modern technology, especially Internet communication technology for meteorological and hydrological measuring networks are the different time scales in this two areas. In Internet communication technology 2 years are eternity, for meteorological measuring networks a period of two years is maybe the time necessary for installation and putting it into operation with expected another 20 years of operation. We are facing this problem by avoiding any network-wide dependency of special hardware and software. Especially we defined as a rule to separate as much as possible hardware and software functionalities. As an example you can buy Internet routers as a black-box, integrating both hardware and special software in one module. If the producer decides to change some important features, maybe you start from scratch. We use for TAWES V2 freely available open source software and install this software on standard hardware, available from the shelf. So we can change hardware and software independently.

- Use of open-source software
  Open-source software projects in many cases reach an unbelievable high level of technical maturity. Because there is a big voluntary team working on the particular modules and frequently also brilliant technicians are part of these development teams Such products are mostly superior to solutions of single manufacturers regarding lifetime and technical perfection.Take as examples for such open-source freeware projects the LINUX operating system or the Apache-Web server.

Basics of IT-Security

There are some basic threads for components communicating over the Internet. The new TAWES V2 IT-security system has to consider the following aspects:

1. Authenticity
   On every communication it must be absolutely shure, that you are communicating

with the right partner and not with a fake. This leads to high sophisticated authentication of the partners on each communication.

2. Confidentiality
   No unauthorized person nor machine can read your information. This leads to safe, encrypted data transfers.

3. Integrity
   The communication procedures must guarantee, that the same data is received as it is sent, without the possibility for faking the message contents.

4. Viruses, trojans, malware
   Each communication partner has to be protected by state-of-the-art firewalls with as least options for intrusion as possible.

Technical solution TAWES V2

Fortunately all of these requirements were already addressed and solved in the Internet community, but according to our knowledge not in suffient scale in meteorological and hydrological measuring networks. The challenge of our project is the adaption of this already existing standards for our networks. The following part of the presentation will descibe the actually developed technical solution.

VPN -Virtual Private Network

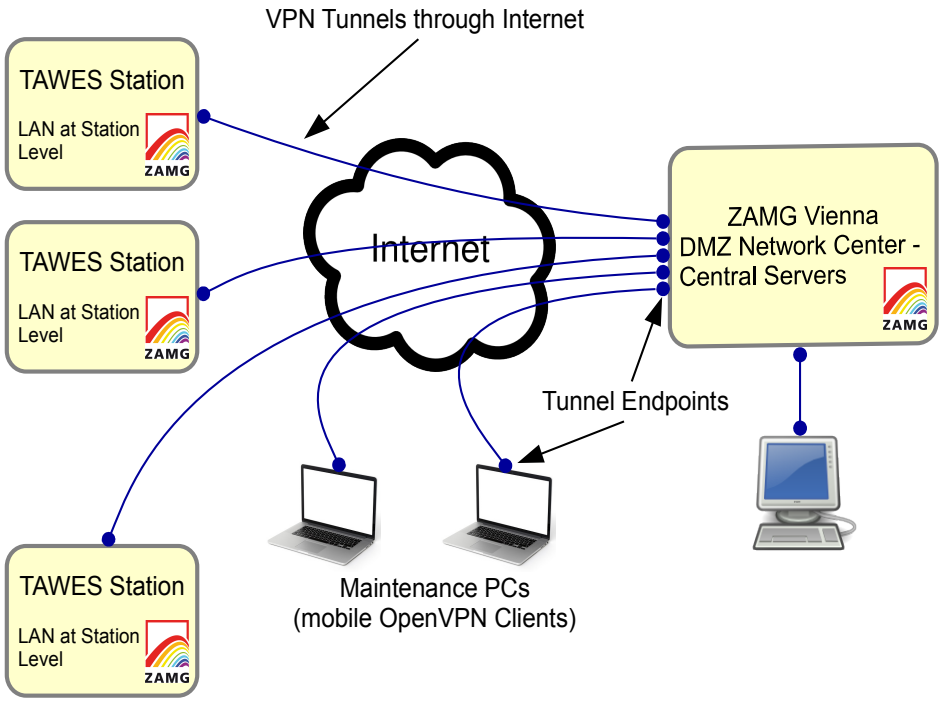

Fig. 2: VPN Tunnels

The basis of the TAWES V2 system are so called virtual private networks (VPN).

Wikipedia:
"A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network."

If you translate this into measuring networks it means, that you have direct access over the VPN to all measuring stations, servers, etc as if they are in your local network. You don´t care about the physical location of the station nor about the particular path of communication. You just type-in the IP-address or the url of the station and you have access.

The participants in the TAWES V2 network actually are:

- Automatic weather stations

- Network center with servers
- Maintenance PCs or tablets

In the future it will be possible to easily extend this endpoints by adding other intelligent units.

- Video cameras
- Intelligent sensors
- .....

Tunnels through the Internet

With the help of VPN software tools it is possible to create so called tunnels through the Internet. That means, that between two endpoints in the network we have a protected, encrypted path for communication. Only the participants in the VPN can use the tunnel for communication. There are some few standards available for the creation of such VPNs respective Internet-tunnels. We studied intensively the two standards

- IPsec
- OpenVPN

Both systems are well established, worldwide used standards and implemented on a big variety of systems. They are independent from hardware and operating systems. Both systems are widly implemented in routers from different manufacturers and also in all actually used operating systems like Windows, LINUX, iOS, Android, ... So it is easily possible to use an Internet router at the measuring station, another router at the network center, and to connect with a Windows-maintenance PC to the VPN. After detailed studies we decided to use both VPN-systems for the operation of TAWES V2.

IPsec offers perfect security for point to point data transfers. We are actually using IPsec for all routine data transfers from the measuring stations to the network center.
OpenVPN offers especially the option to create multi-member networks with all access options between the network-members, also mobile clients. We are using this type of VPN for maintenance access. After a maintenance PC is connected to the VPN it has access to all components of the network. Actually not used, but possible, is the communication between measuring stations. The result of this concept is the separation of routine data transfer and

maintenance access into two different, logically completely separated VPNs. For each VPN the access rules, firewall rules, etc can be defined completely separated.

Authentication
Everyone who wants to connect to the VPN has to authenticate itself, both human beeings, weather stations and servers. For this purpose every unit gets a so called digital certificate. A certificate can be compared to an ID card, which is checked thoroughly before a connection to the VPN is granted. In the network center we installed a small software tool for the creation and administration of new certificates. Certificates are superior to other authentication systems like i.e. password systems.. Some advantages of certificates:

- One certificate per user, no sharing of passwords
- Easy administration and installtion of certificates at measuring stations, maintenance PCs etc.
- Certificates have a limited validity. This feature can be used to grants access for users for a limited period of time for i.e. timely limited research projects
- If a certificate becomes dubious if i.e. a maintenance PC gets lost within minutes the certificate can be revocated network-wide by use of central revocation lists.

For TAWES V2 we are actually using cerificates according to the X.509 standard.

Confidentiality, data integrity
Both IPsec and OpenVPN have high sophisticated encryption systems which should be absolutely safe according to the actual state-of-the-art. The same standards are actually used also for high security systems like bank communications and nearly all professional wide-area communication.

Viruses, trojans, malware
VPNs have no option to protect against malware. But by use of state-of-the-art firewalls the access to central servers or measuring stations can be limited to only VPN connections or at least to very few other "holes" in the firewall. Our strategy in TAWES V2 is to close the measuring stations nearly completely against all communication initiated from outside the station and from outside the VPN. The only allowed communication to and from a measuring station is the communication through the tunnel. All other access attempts will be refused by the firewall.

Data transfer protocols
Not directly connected with IT-security, but also important is the fact, that TAWES V2 is only using well established Internet protocols for all communication.

- Routine data transfer is done by an veteran Internet standard, the ftp-protocol (file transfer protocol),
- Access to the components at the measuring station for configuration and maintenence purposes is done by html, the language of the Web-browsers.

- Time synchronization of all components by NTP (Network Time Protocol)
- The access to the stations is done by symbolic names (urls - Unifrom Resource Locator). To resolve these names TAWES V2 is using DNS standard (Domain Name Service)

Hardware upgrade

We decided to use in TAWES V2 a special Internet gateway unit, consisting of a well established open-source freeware together with a standard processor board from the shelf based on a LINUX-like operating system. The applied software integrates all necessary functions like VPNs, firewall, etc in one software package. The hardware offers relatively low power consumption at 12VDC and a wide operating temperature range and is therefore perfectly suited for applications at remote sites. Since harware and firmware are separated we can at any time choose a different hardware platform, if the actual one maybe is not available any more. Addionally the firmware package is available in open-source, can be compiled by ourselfes and is available from different sources.

Conclusion and actual state of the project

The project started about 1 1/2 years ago and actually we have some few stations in a routine test-operation. These stations have the standard TAWES sensor suite and are additionally equipped with video-camera. Some employees at ZAMG have maintenance access to the measuring network using OpenVPN. At the same time we are testing at these sites satellite communication. One station is equipped with Inmarsat-BGAN M2M satellite transceiver, a second one with a similar system from Thuraya. Both satellite paths go in the network centre not via terrestrial lines, but also via satellite communication, using Eutelsat´s TooWay technology. This test operation is planned for about 6 months.