



INFORMATION SECURITY IN INTELLIGENT TRANSPORT SYSTEMS

Ivan Dolnák

ivan.dolnak@fsi.utc.sk

*University of Žilina, Faculty of Special Engineering,
Department of Technical Sciences and Informatics, 1. mája 32, 010 26 Žilina,
Slovak Republic*

Key words: *CONNECT, information security, intelligent transport systems, virtual private networks*

Abstract: This article describes conditions of intelligent transport systems formation and adverts on omission of information security elements in their architecture. It also adverts on absence on information security in intelligent transport system developed intro-project CONNECT which uses public telecommunication environment for data transfer.

INTRODUCTION

Traffic congestions in road transport became global problem. It's result of increased number of road users, urbanization, population growth and changes in population density. Congestion reduces utilization of the transportation infrastructure and increases e. g. amount of accidents, fuel consumption, air pollution and travel time.

Beginning this problems is in the 1920s (Wikipedia, 2006b) when started migration of population from the sparsely populated rural areas and the densely packed urban areas into suburbs. The industrial economy replaced the agricultural economy leading the population to move from rural locations into urban centers. At the same time, motorization was causing expansion of cities. Suburbs provided a reasonable compromise between population density and access to a wide variety of employment, goods and services that were available in the densely populated urban centers. Further, suburbs can be built quickly, supporting a rapid transition from a rural/agricultural economy to an industrial/urban economy.

INTELLIGENT TRANSPORT SYSTEMS

Increasing interest in intelligent transport systems (ITS) comes as result of the above-mentioned evolution and present problems in road transport. The most important advantages of ITS are in increasing utilization of the transportation infrastructure and the safety of roads users without additional traffic infrastructure expansion. Intelligent transport systems can be also helpful during evacuation in crisis situation conditions. It also decrease financial charges, has positive impact on environment and increases filling citizens demands.

Using new information and communication technologies the cardinal assume is in applying innovative applications for solution present problems in transportation. Intelligent transport systems use progressive technologies and apply them in traffic process with aim to create innovative solutions for increasing complex quality.

Intelligent transport systems role could be especially in:

- minimalization of traffic congestions;
- increasing the safety of road users;
- decreasing degradation of the public transport;
- decreasing negative consequences on environment;
- increasing competition and utilization in transport.

Intelligent transport systems otherwise offer solutions to these problems but their massive employment still obstruct differences in look on advantages and disadvantages of these systems, massive differences in individual interests and of course, large investment charges.

Intelligent transport system can be imagined as complex distributed information system. It consists of particular information subsystems which are connected together in telecommunication environment. The term information subsystem means single-purpose information system used for collecting and executing one and the same kind of information. Final concept of intelligent transport system offers ability to get information on arbitrary place and in arbitrary time. Intelligent transport systems can automatically find information, execute and transfer them to the right place when they are needed.

Part of an intelligent transport systems conception is optimal telecommunication environment design. It has to be fulfilled requirements on speed, security and availability of information. This definition has to be also connected to definition of particular information systems interfaces which have important impact to these requirements. The goal is to create intelligent transport system in which the transactions with information are running in real time and according to predetermined conditions.

Intelligent transport systems could not cover only one kind of transport (e. g. road transport). It is also necessary to take a look to coverage other kinds of transport in the future. It is difficult to create intelligent transport system and assure optimal data transfer, because it has to be segmented.

INFORMATION SECURITY

The term information security deals with several different trust aspects of information. Information security is not confined to computer systems, nor to information in an electronic or machine-readable form. It applies to all aspects of safeguarding or protecting information or data, in whatever form.

Most definitions of information security tend to focus, sometimes exclusively, on protection electronic data from unauthorized use. In fact it is a common misconception, or misunderstanding, that information security is synonymous with computer security, in any of its guises. Computer and network security, information technology security, information systems security, information and communications technology security, each of these has a different emphasis, but the common concern is the security of information in some form (electronic in these cases). These all are subsets of information security. Conversely, information security covers not just information but all infrastructures – systems, technologies, services, processes, etc., including computers, voice and data networks, etc.

It is an important point that information security is, inherently and necessarily, neither hermetic nor watertight nor perfectible. No one can ever eradicate all risk of improper or capricious use of any information. The level of information security sought in any particular situation should be commensurate with the value of the information and the loss, financial or otherwise, that might accrue from improper use.

Three widely accepted elements of information security are:

- confidentiality;
- integrity;
- availability;
- accountability.

Historically, up to about 1990, confidentiality was the most important element of information security, followed by integrity, and then availability. By 2001, changing use and expectation patterns had moved availability to the top of most versions of this priority list. The first goal of modern information security has, in effect, become to ensure that systems are predictably dependable in the face of all sorts of malice, and particularly in the face of denial of service attacks.

PROJECT CONNECT

Activities in Central and Eastern European area in field of intelligent transport systems are covered by the project CONNECT (co-ordination and stimulation of innovative ITS activities in Central and Eastern European countries), which works as co-operation among public authorities, road administrations and traffic information service providers. Partners from Austria, Czech Republic, Germany, Hungary, Italy, Poland, Slovakia and Slovenia are working together to improve cross-border traffic and transport through implementing harmonised and synchronised ITS applications on the high level road network in this area.

Project CONNECT amends the six existing TEMPO projects (ARTS, CENTRICO, CORVETTE, SERTI, STREETWISE and VIKING) to the Central and Eastern European countries to ensure co-ordinated traffic management and control as well as high quality traveler information services on most important east-west road-corridors (including Pan-European corridors II, III, IV, V, VII and X) in an enlarged Europe. Project CONNECT started formally in May 2004 with its first phase focusing on studies, feasibility studies and first pilot projects and demonstrations.

In Slovak Republic project CONNECT share:

- ITS Slovakia
- Ministry of Transport, Posts and Telecommunications of the Slovak Republic
- The Transport Research Institute
- The Research Institute of Posts and Telecommunications
- University of Žilina.

CONNECT objectives are:

- integration of the new EU members in ongoing European initiatives;
- stimulation of the co-operation between the CONNECT partners and the existing projects of the TEMPO programme and related working groups (e. g. TMC Forum, DATEX2 Technical Committee);
- fostering cross-border co-ordination of strategies, systems and services (e. g. Traffic Management Plans);
- optimization of the use of road capacity by implementing innovative cross-border ITS applications;
- stimulation of investments in (national) ITS infrastructure;
- improving the safety of road users;
- improving the efficiency of traffic flows and tackling congestions by harmonized cross-border traffic management and control strategies;
- reducing the travel time of road users by providing them with accurate, timely and relevant information as well as by providing cross-border services (e. g. RDS-TMC, web-based services);
- fostering urban/interurban interfaces to ensure fluent traffic flows between the high level and the connecting road network;
- launching projects to foster the “interconnect ability” of transport modes to achieve intermodal/multimodal door-to-door services;
- improving of interoperability among national EFC systems at least to achieve basic pre-conditions for interoperable road user charging;
- harmonization of national system architectures to avoid new borders among the CONNECT member states as result of non-interoperable national telematics systems.

VIRTUAL PRIVATE NETWORKS

Amount of security incidents in the field of informatics still increases and is absolutely normal, that also increase investments to the information security. It doesn't increase only amount of attacks, but also their quality. Today's attacks are more sophisticated and combine different methods.

Nowadays, when the intelligent transport systems are developed, important problem is their information security. These systems are characterized by their new conception, especially their users mobility. Get the appropriate level of information security in this distributed environment is more complicated. It is faded classic concept of information security. Problem is first in using public telecommunication environment which is not secure in the present.

In project CONNECT are still missing solutions of information security in intelligent transport systems. By this time it maybe wasn't necessary. Experiences with large projects (e. g. GSM) but demonstrate that is really necessary to implement it in first phases of development.

In public telecommunication environment are urgent these elements of information security:

- confidentiality;
- integrity;
- accountability.

Availability of these elements in public telecommunication environment, especially in communication among mobile users and centralized systems, can we get for example by applying virtual private network technology. This technology is well known in classic computer networks.

Virtual private network (VPN) (Přibyl, 2006) is private communication network in which is possible communicate secure. It has important place in information security because it can be used for secure data transfer in public and also not secure networks. By the VPN is possible to create secure connection also with insecure protocols.

Applying VPN decreasing financial charges on connection because with VPN we haven't to build own and expensive non public networks. VPN is good scalable and is smart to build them as well as for one user. Of course, this is not possible in real world. It doesn't depend on geographical location, because it's not important where the user is located. He's always secure connected. VPN technology simplifies network topology, their administration and also speed of connection.

VPN has also own limits in transmission across public telecommunication networks. This can be sometimes problem and than organizations have to build private telecommunication networks, but VPN are good solutions. It covers all elements of information security and is technology which offers interesting alternative against private networks.

CONCLUSION

Designers of intelligent transport systems maybe forgot to problem of their information security. This is present elementary requirement in computer networks. It's important give attention to this part of development, because this omission could bring great problems in the future. One of the methods how to secure above mentioned communication in intelligent transportation systems is in using virtual private network technology. The more it will be users of intelligent transportation systems in the future, the better they will need secure system and will believe in their error free running.

- [1]CONNECT. 2006. *General Project Description*. [online]. CONNECT: Project, 2006-08-24, [cit. 2006-08-24]. Available on Internet: <<http://www.connect-project.org/index.php?id=9>>
- [2]DVOŘÁK, Z., DOLNÁK, I. 2006. Inteligentné dopravné systémy a riešenie krízových situácií v doprave. In: *LOGI 2006 : Externí poskytování logistických služeb : 7. konference s mezinárodní účastí*. Lázně Bohdaneč : Institut Jana Pernera, o.p.s., 2006, s. 14-19. ISBN 80-86530-30-2
- [3]PŘIBYL, T. 2006. „Vé-pé-enky“. In: *Security : Magazín o bezpečnosti v kybernetickém světě*, 2006, roč. 3, č. 8, s. 34-35. ISSN 1214-794X
- [4]WIKIPEDIA. 2006a. *Information security*. [online]. Wikipedia : The Free Encyclopedia, 2006-08-24, [cit. 2006-08-24]. Available on Internet: <http://en.wikipedia.org/wiki/Information_security>
- [5]WIKIPEDIA. 2006b. *Intelligent transportation system*. [online]. Wikipedia : The Free Encyclopedia, 2006-08-16, [cit. 2006-08-24]. Available on Internet: <http://en.wikipedia.org/wiki/Intelligent_Transportation_System>