Global Information Assurance Certification Paper

GSEC Practical Assignment Version 1.4c, Option1

Securing an Automated Highway System. A risk based approach

By Gerard Readett

Submitted on 14 march 2005

Information Security plays an important role in the relatively new domain of Intelligent Transportation Systems (ITS). A network of traffic lights and sensors is augmented by centralized traffic information and management systems to ease the flow of both normal and emergency services traffic. Weak security in such a system will only lead to the current chaos we all experience on the roads today. The example of an ITS I use in my novel, Roadworks, attempts to show the advantages as well as some flaws, especially in security.

Where Information Security really comes into its own and plays a vital role is in a future subset of ITS, the Automated Highway System (AHS). For long distances, dedicated roads will soon be built to allow rapid travel between major cities. Drivers of powerful cars relinquish control of their vehicle to join together in platoons of up to twenty five closely packed (as close as 10 centimetres) cars and tear down the motorway at speeds in excess of two hundred and fifty kilometres per hour. Incorrect information in such a configuration could be instantly lethal.

This paper will attempt to sketch broad guidelines for securing an AHS using current technology. We will start by describing the various networks and how they connect. Then for each part we will attempt to discover the vulnerabilities and countermeasures. As we will be taking the global view we will refrain from going into enormous detail in each specific domain.

AHS networks.

A user walking down the street trying to find where he parked his car will be using a Wireless Personal Area Network (WPAN) that links his pocket computer or organiser to a GPS inside his mobile phone. Once he has found his car and switches it on his pocket computer will link to the Wireless Vehicle Area Network (WVAN) that contains the car navigation systems. Once he has chosen his destination city devices in the car will indicate the road to take to join an Automated Highway System. The user will manually drive his car to the Highway.

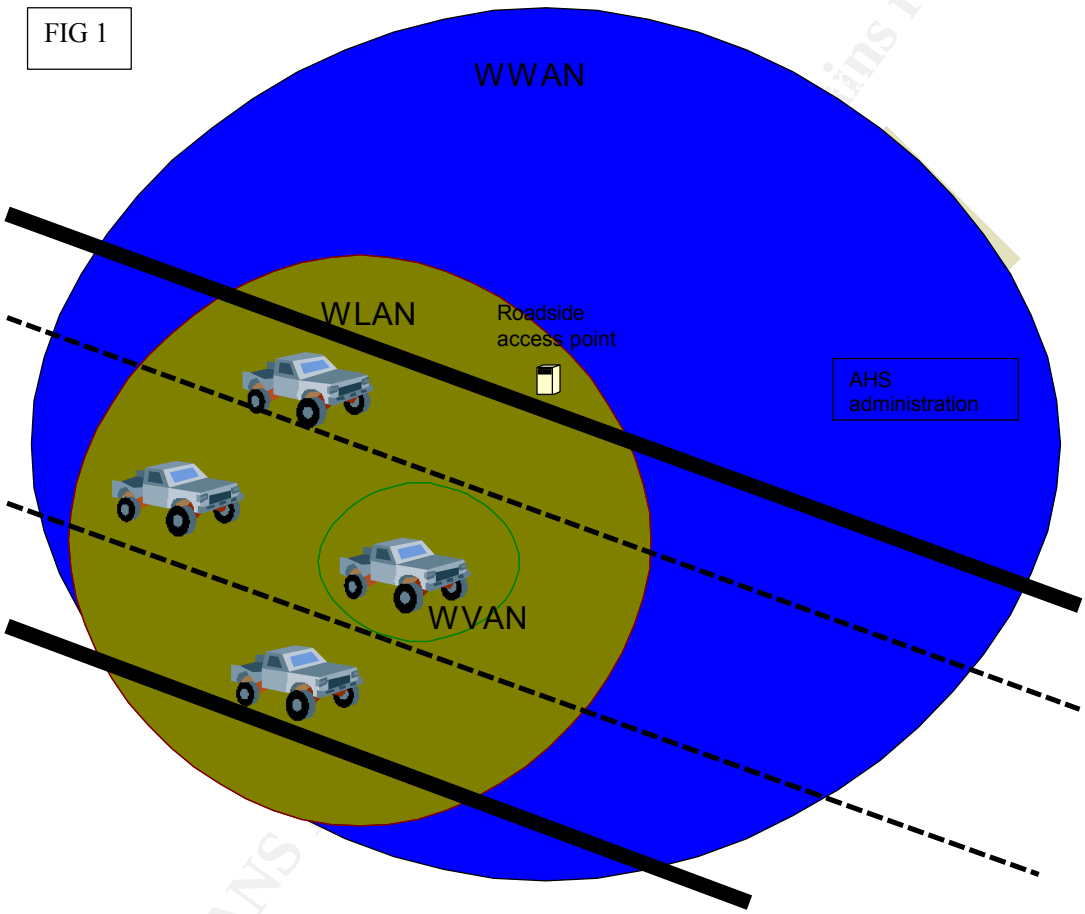
The entrance to the AHS will be informed by the user's WVAN of the destination city. The Automated Highway infrastructure will take control of the user's car and lead it onto the correct lane then join it to the next platoon of cars. At this point, the user will be in a Wireless Local Area Network (WLAN), which links the cars in the platoon between themselves and the roadside access points (APs). The access points will use Electronic Toll collection (ETC) to facilitate the payment of a toll without the user having to stop at a booth and handle cash. The roadside access points will also communicate with the platoon as a whole to ensure that it stays in lane. The cars in the WLAN will constantly communicate in a cooperative driving

system to keep the same speed, direction and avoid collisions between vehicles.

The AHS infrastructure will constantly check the users travel plan to be able to disconnect his car from the platoon in a timely manner to allow the driver to leave the highway at the correct exit. If the driver is not familiar with the destination city he may request a full travel map from the AHS as well as local current road and traffic conditions. The AHS infrastructure will communicate with the user's car via a Wireless Wide Area Network (WWAN).

While the AHS is controlling his car, the user can turn his attention to other matters. He can start surfing the internet to check his mails or communicate with his work, watch video-on-demand depending on the specific services provided by the AHS.

FIG 1



Basically an Automated Highway System is made up of three security zones represented as concentric rings in Fig 1, the Wireless Vehicle area network(WVAN), the wireless local area network(WLAN) and the wireless wide area network(WWAN).

The WVAN and Intra-Vehicle communication.

The primary risk is reliability. A system where high speed cars tear along at small distances from each other is inherently dangerous if each constituent piece of the system is not reliable. Any damage to or malfunction

of any of the working parts of a car driving in an AHS could lead to immediate disaster. A flat tire in the lead car of a platoon would cause the car behind to crash into it, the car behind that would crash into both and so on.

Another risk associated with this type of communication is breach of confidentiality, that is information can be intercepted when transmitted between devices. Personal details that the driver does not want to be made public as well as logins, and passwords and account details can be skimmed. Information specific to the car such as identification numbers can be used by car thieves or fraudsters.

The amount of electronic devices that control vital functions in a car is rising rapidly. The messages transmitted between two in-car devices can be intercepted and altered. If the driver can not trust the integrity of messages sent inside his car then he will not be able to determine his position or speed accurately. Worse still, altered data sent between devices may lead to disruption of the car's systems; possibly leading to a complete breakdown (i.e. the electronic controls go haywire and the car stops (at best) or behaves erratically (at worst).

This could also happen after a Denial of Service attack interrupting all communication between devices.

The devices in the user's car will probably be linked by a protocol similar to Bluetooth. Although the range of Bluetooth is limited (<10 metres) security in the WLAN will depend in part on the security measures applied in each WVAN. We need to focus on the following vulnerabilities that can arise during communications between on-board devices:

Since the cars in a platoon are so close together there could be interference between devices in one car and a device in a neighbouring car. A malicious user could use the AHS perfectly legally but while he's being safely driven to his destination attempt to intercept (or modify) information that he can get access to as he is in the 10 metre range of other drivers Bluetooth devices.

Two types of information can be intercepted or altered: private information transmitted by the user and navigation information. To avoid interception or alteration of either type of information some type of encryption is necessary. We are attempting to secure the AHS with current technology only. The replacement of the WEP security standard considered as too weak is the Wi-Fi Protected Access (WPA). The latest version WPA2 is based on the 802.11i protocol and specifically includes Advanced Encryption Standard (AES) encryption. AES is a symmetric block encryption algorithm (which is set to replace 3DES). It supports key sizes of 128 bits, 192 bits and 256 bits. AES is much faster than triple-DES in encrypting data and therefore can be used in a system where time is at a premium.

The driver must be also able to trust the devices inside his car in order to protect against malicious replacement or interference (voluntary or involuntary) with other cars. Syed M. Mahmud and Shobhit Shanker of Wayne State University propose a system which augments the Bluetooth security by adding a Network Device Monitor which is used as a gateway to link all the onboard devices. Each device has to register with the NDM and each time it wishes to communicate with another device it must first be authenticated by the NDM. Once communication has been established

between two on-board devices (and each has been authenticated) no other device can join the conversation. To allow communication between more than two devices Mahmud and Shanker came up with the concept of a session key, created by the NDM and distributed to each authenticated member of a session. This ensures that the devices can be trusted and that faulty devices can be removed or replaced by new devices which in turn will become trusted.

For a driver to be allowed to use an Automated Highway System, the AHS administration might add a requirement for users to have their WVAN configuration set up according to a pre-defined security standard. For example if they imposed the use of an NDM and AES encryption they would know that security was tight from the perspective of each car wishing to join the highway.

The fault tolerance of the working parts of the car, including the engine, the electronic controls and any on-board devices plays a crucial role here. Also it will probably be necessary to set up robust redundancy. For example if the NDM breaks down for some reason none of the devices will be able to talk to each other. This would obviously lead to immobilisation of the car.

Highly reliable sensors should be installed to constantly check tire pressure, engine power output, fuel level and other important indicators to be able to pro-actively warn the driver (and the AHS) of impending failures. This way the faulty car would be driven off the AHS in a timely manner.

WLAN and WWAN or (Inter-Vehicle and Vehicle to AHS infrastructure communication.

The risks associated with the communication in the WLAN (vehicle to vehicle or roadside) and communication in the WWAN (vehicle to AHS infrastructure) are closely linked. Since the AHS has already ensured security inside each WVAN (see above) it must now turn its attention to risks in the rest of the network.

A major concern is the confidentiality of information transmitted between the driver of a car and the AHS infrastructure. Firstly during transmission the personal details (sent to the AHS by the driver to request access) can be intercepted. Secondly, to determine who is an authorised user the AHS must keep a database containing details that identify the driver (e.g. his name and his billing address) and his car (e.g. licence plate). This is not simply a matter of privacy since a hacker could use this information to impersonate the user thereby avoiding road tolls and payment of services (e.g. internet access).

A hacker could either infiltrate an access point or hijack a driver's internet session. He could use the internet connection to access navigation devices in the car (e.g. to pinpoint and track specific individuals and maybe even glean routine travel habits), or other on-board devices like a personal computer, organiser (from where he could even retrieve personal information such as phone numbers, addresses, birthdays).

The integrity of the infrastructure may be breached if a roadside access point (that is used to communicate with cars in the AHS) is

vandalised or hacked. A broken access point will be unable to prevent lane drifting either by a single car or a platoon, so the risk is physical danger to drivers. A hacked access point may even be used to intentionally misdirect cars or platoons to crash into each other.

Another major issue is the availability of operations systems. In the event of a serious malfunction (like a power failure) platoons racing down the highway would not know when to stop, the AHS would have no way of producing either updated travel information or collision warnings and drivers wishing to join the AHS would be unable to do so.

Viruses in the software that runs on any systems (including the AHS database, the access points and communication devices) and Denial of Service attacks (like radio frequency jamming) may stop all communication and have the same consequences (e.g. unable to warn platoons of obstacles ahead).

The dangers associated with these risks are real and immediate. All it would take to cause a deadly crash is for one independent vehicle getting in the way of an Automated Highway System controlled car/platoon. This is probably one of the most serious risks as it could be a show stopper.

The WLAN will probably use communication based on the IEEE 802.11p protocol, which is the basis for Dedicated Short Range Communications, a project initiated by the US Department of Transport for vehicle based communications and is now called Wireless Access for the Vehicular Environment (WAVE). It contains features that allow for high mobility, better security and peer-to-peer authentication. (See also 802.11i).

First of all the AHS administration must be physically secure. The physical building where it is located should be restricted to authorised personnel only. It is not in the scope of this paper to examine this particular fundamental security aspect in any great detail but just to point it out. A security policy for any computer centre where confidential information is stored should be applied. There should also be a screening of personnel, training should be given both in the areas of operations and security. I would say that in the context of a high speed, computer controlled system like an AHS, operations and security staff training will play a vital role.

The most obvious next step is to ensure the physical integrity of the other nodes in the network, the Access Points (APs). Physical access to the Roadside Access points must be ensured. One way would be to install the APs high up on current highway lampposts. That would ensure that they could not be vandalised (at best) and tapped into (more serious).

Operations Systems failure is a major concern. In the event of a power failure on the AHS network all the platoons in movement would no longer receive information that they are moving out of lane or too fast with respect to other platoons. To avoid this, a solid disaster recovery procedure should be created detailing the use of no-break power supplies and fallback facilities. This is a crucial security concern in an AHS as the time for failover should be as close to nil as possible.

A normal AP, or any system in the AHS administrative domain could be infected by a virus or other malware. Here the use of anti-virus software and firewalls in all nodes and the central systems of the AHS administration

is essential. An anti-virus update policy should be put in place as well as a very regular audit of firewall logs and intrusion detection systems for irregular events.

A patch management policy together with a system hardening technique should be put in place.

Considering the safety issues with a high speed platoon that requires perfectly accurate information within extremely short time frames, any event should be thoroughly investigated and preferably immediately. Any successful intrusion would lead the AHS administration to only one solution, stopping the whole system.

Concerns about privacy arise in an ITS of any flavour. However in the realm of the AHS which is a closed system with a single administrative domain privacy requirements should be on the same level as current security measures in Commercial Airlines. It seems acceptable for the AHS administration to know the name and address of the car owners as long as that information remains inside highly secure databases.

The real threat to privacy is eavesdropping: personal information could be intercepted during communications between cars and the roadside. The use of 802.11p (which as far as I can glean will have similar security solutions as 802.11i) should use AES encryption. Continuous audit of the wireless network should be implemented.

However if a malicious person could act as a legitimate user (spoof or masquerading) and redirect or alter communication traffic between the roadside and the car/platoon then confidentiality is lost. A malicious node (a car or an AP) could redirect messages to the wrong car. In a high speed moving WLAN this could cause instant chaos. A car receives the message destined for another car and decides to move to (what it believes) is the correct position. Instant twenty five high speed car crash. To protect against this EAP and 802.1X network authentication protocol for mutual authentication should be applied.

A DoS attack (jamming) would stop communications between cars in a platoon and the roadside; it could also block the initial conversation between AHS and cars trying to join a platoon. This way the formation of a platoon could be denied and the AHS would never take over the control from the human driver.

Quick identification of Dos attacks by deployment of wireless intrusion detection systems is necessary. The administrators must be able react quickly to attacks and identify the attackers.

Dos attacks in an AHS may seem to pose little threat because if communication from/to one access point are being jammed, the speed with which a platoon of cars passes will mean that the next AP in the line will resume the conversation with the cars (and correct any configuration changes). However at speeds in excess of two hundred and fifty kilometres per hour and separated by only a few centimetres all it would take to have a car crash is for one car to momentarily change speed or shift lanes.

A rogue access point could be a roadside AP or a car which is badly secured providing a hacker with access to the network. A Wireless LAN security policy should include 24h detection of rogue access points coupled with a rapid reaction force.

Public Key Infrastructure

Many of the security issues in an AHS (in all three identified security zones) reside in the Identification and Authentication of all parties involved. Mutual authentication is needed between the AHS and the car, as well as between cars.

The best way of doing this is to set up a public key infrastructure. PKI uses data encryption for Confidentiality, digital signatures for non-repudiation (accountability) and verifies data integrity.

Public key cryptography or asymmetrical key cryptography uses what is known as a key pair, two mathematically linked cryptographic keys. One key is used to encrypt and only the second key can decrypt messages encrypted with the first key. (I.e. the first key will be unable to decrypt a message that it has encrypted). This means that the first key can be freely distributed with the certainty that only the person who holds the second key can decrypt messages.

A driver, let's call him driver A (intending to use the AHS) would have to create two keys. He would have to make a public key for other to encrypt messages to send to him. This key, as its name suggests, would be available to the general public. A Public Key Server would perform the function of stocking all the public keys of participants in the AHS, i.e. a public key for the AHS administration and the public key of all cars allowed to use the AHS.

At the same time driver A would have to create a private key which he will use to decrypt messages encrypted with his public key. This key he will keep safe and distribute to absolutely no one.

When driver B's car wishes to communicate securely with driver A's car it will user driver A's public key to encrypt a message. Driver A's car will use his private key to decrypt the message, safe in the knowledge that no one was able to read the message before him. Driver A's car can reply by encrypting his message using Driver B's public key. Driver B's car will decrypt using his private key.

However, Driver A and Driver B do not know each other and are reluctant to take each other at face value.

Driver B will create a digital signature by copying the message to send and some personal information and encrypting using his private key.

Driver A's car will decrypt the signature using Driver B's public key and verify the identity of Driver B (as well as integrity of the data).

The public keys though need to be validated by some trusted source. This is the role of the Certificate Authority. The idea behind the CA is that it is a source trusted by both drivers. The CA can issue a digital certificate which contains Driver B's public key and some personal information encrypted with the CAs private key (digital signature of the CA). The CAs public key is available on the Public Key Server.

Driver B's car sends a message and attaches his digital certificate before sending to Driver A's car. Driver A's car decrypts the digital certificate with the CAs public key to verify that it was issued by the CA and using Driver B's public key contained in the certificate can reply secure in the knowledge that Driver B is who he says he is and that he is approved by the CA.

It is likely that any particular AHS will be part of a country wide

hierarchy. The root PKI certificate authority would be the Ministry of Transport and one or more layers down would be the Registration Authorities. To unload some of the work from the Certificate authorities, Registration Authorities act as agents for vetting of user requesting a new certificate. The RA could be a regional ministry of transport office where drivers wishing to use an AHS would go to apply for a certificate. Once the RA has verified the driver's identity (most likely by checking the drivers licence) it sends its approval to the CA to issue a certificate.

A special service which exists within a Public Key Infrastructure is the Timestamp Service which confirms receipt of digital documents at specific times. This would probably be a requirement imposed by the Ministry of Transport.

By using a smart card a driver could couple several security measures. He could store his private key on the card which he carries around with him, thus preventing anyone who stole his car from using the certificate to use on an AHS. In addition he could use the smart card as the Network Device Monitor suggested by Mahmud and Shanker. This would prevent any car jacker from using any of the on-board devices and probably from even switching on the car.

Additional security measures

Wide range communications in a Wireless Wide Area Network (WWAN) with internet and the AHS administration would be via GSM which ensures session continuity. By the time Automated Highway systems become a reality the mobile phones using 802.11 standards (or their successors) should be common. A way of adding security to the wireless access protocol (WAP) is to add wireless transport layer security, or WTLS, end-to-end. This is very similar to SSL (secure sockets layer) which is widely used to secure communication across the internet.

On top of this WPA2 should be implemented along with the 802.1x (which authenticates and authorises devices to connect to specific ports) and transmits security information through EAP.

The default ssid of the phone or communication device should be changed and subsequently not broadcast.

A thorough risk assessment should be made to determine the impact of security breaches in this type of communication. In principle security of the GSM network will not need to be much stronger than common mobile phone security since security breaches here will not result in such disastrous consequences as message tampering in the WLAN.

Human factor

As with all security policies, the best security in the world will not protect anything against a user unintentionally bypassing security controls. By using social engineering a hacker could garner the password of careless AHS administration staff to access to the user database confidential information or access the operations systems that control the cars on the road.

Also slow reactions to problems in the network (accidental or

malicious) may result in system failures which would be disastrous for current users on the road. If a correct state is not re-established rapidly the cars and platoons on the road may begin to behave independently (which is sure to lead to accidents in a cooperative driving system).

The driver is probably the weakest human factor in the automated highway equation. In the event of an unexpected problem (e.g. the AHS does not allow him to join a platoon), drivers reactions may not always be predictable. He may swerve into the path of an approaching car rather than exit the AHS immediately. A driver may also be caught unawares (e.g. he is talking earnestly to his passenger) when the AHS hands control of his vehicle back to him.

Considering the security loopholes present in a wireless environment it will be necessary to include as a step in the overall Security Policy (which naturally should be approved by the Ministry of Transport since the safety of the general public is a primary objective) some of the following educational practises:

A complete Operations staff training program which describes the various vulnerabilities of the system and how they are addressed in the AHS, which should contain (at least):

A description of suspicious activity on a wireless network and what to do when it is discovered.

A full disaster recovery procedure detailing:

- the consequence of each type of possible disaster, who does what in the case of each type of disaster (e.g. if there is a power outage then Operations Manager may be in charge but if the disaster is in fact a security breach it is foreseeable that the Information Security professional will at least have a major role to play),
- the delay between failure and recovery

A complete patch management procedure with the shortest possible implementation time for installation of:

- Anti-virus software updates
- Software bug fixes
- Patches that close up newly discovered vulnerabilities

The information security staff will most likely have to be rather extensive given the 24h/7d type of support required will need to have:

An in depth map of the whole AHS infrastructure, how it works as well as how security is applied.

A complete security breach reaction plan detailing:

- All the type of attacks possible
- The urgency and danger created by each attack
- The countermeasures that should be used

A full vulnerability scanning plan, (which should be run very regularly) for pro-actively discovering:

- New (successful and unsuccessful) intrusion attempts
- Rogue access points
- Altered or unsatisfactory configurations in all AHS systems (firewall, APs...)

Also it will be essential to educate the users of the AHS (i.e. the drivers) on how to:

- Enter an AHS and join a platoon safely
- The importance of security measures (for their safety and privacy)
- The Ministry of Transport imposed standard to which their PAN and WVAN must conform to be allowed access to an AHS.
- What the possible failures/unexpected events are and what to do in such cases.

Conclusion

So, are we now able to say that with current technology and a lot of hard work we could secure an AHS if one was built tomorrow? The answer is yes, maybe. The technology would appear to permit the full lock down of such a system. However some of the controls are more than nice-to-have, they are must-haves.

Without on-board devices, navigation systems and electronic controls that are both highly reliable and fully redundant no car will be ready to join a high speed, closely packed platoon. Car manufacturers today are working on providing such high-tech gadgets for use in Intelligent Traffic Systems to manage inner-city traffic. Improvements leveraged by lessons learned during the adaptation of car technology for such implementations will be a good basis for applying this type of technology in an Automated Highway System.

Without an extremely detailed security policy and Information Security response teams which are superbly trained, highly efficient and brilliantly informed about new vulnerabilities in software, hardware and attack techniques, the AHS will not be able to completely allay fears for personal safety of users.

Planning the design and implementation of an Automated Highway system will in any case be a vast undertaking. Information Security will have to be addressed in each step of the project from initial design to day to day

operations. It is unlikely that this new type of road will spring up all over the place quickly. At first a few will be built between main cities and everyone will watch these with interest to see how the issues (security, operations, cost) are handled.

The work of the information security professional will not finish once an AHS has been built and a complete security policy, which spans the entire AHS infrastructure from entry point right up to the AHS administration building or buildings, has been developed.

The techniques, software, hardware, standard and protocols that such a highway will use are in constant flux. It will be the job of Information Security to keep up to date on new security issues, software and hardware upgrades, and techniques.

It is clear that being an Information Security professional in an Automated Highway administration will be a challenging and ever changing job.

References:

1. Roadworks. Gerard Readett 2002. http://users.skynet.be/fa032104/

2. Protecting Our Transportation Systems:
An Information Security Awareness Overview.
Miretek System for US Department of Transportation 1997 .
http://www.itsdocs.fhwa.dot.gov/JPODOCS/REPTS_TE/2$301!.PDF

3. Security of Wireless Networks in Intelligent Vehicle System. Syed M. MahmudandShobhit Shanker. 2003
http://proceedings.ndia.org/3570/session3/Mahmud.pdf

4. Network Access Control in OverDRiVE Mobile Networks. C. Barz, M. Frank, HY. Lach, C. Maihoefer, A. Petrescu, M. Pilz, L. Zömbik. June 2003
http://www.comnets.rwth-aachen.de/~o_drive/publications/NetworkAccess-UBN-final-submitted.pdf

5. Interactive Wireless Communications for Wider-range ITS Services.
Takashi Omata, Seiji Ukai, Makoto Katagishi, Shin'ichi Yoshida. 2000
http://www.hitachi.com/ICSFiles/afieldfile/2004/06/01/r2000_03_101.pdf

6. Automated Highway Systems. Bruce McMillin and Kristen L. Sanford.
http://web.umr.edu/~ff/IV/AHSpaper221.html

7. Intelligent Transportation Gets 802.11p. Samc at Daily wireless.
http://dailywireless.org/modules.php?name=News&file=article&sid=2815&src=rss09

8. Understanding Public Key (**PKI**) infrastructure. RSA Security, 1999.
http://www.computel.com.lb/Downloads/PKI.pdf

9. IEEE groups fight for control of key standards. Wireless Watch. January 2005. http://www.theregister.co.uk/2004/07/16/ieee_groups_slug_it_out/

10. 802.11i shores up wireless security. Ian Cohen and Bob O'hara. May 2003.
http://www.nwfusion.com/news/tech/2003/0526techupdate.html

More information:

WEP
http://www.webopedia.com/TERM/W/WEP.html short definition
http://www.wi-fiplanet.com/tutorials/article.php/1368661 more detailed explanation

WAP
http://www.webopedia.com/TERM/W/WAP.html short definition
http://www.w3schools.com/wap/wap_intro.asp more detailed

AES
http://www.webopedia.com/TERM/A/AES.html short definition
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci344759,00.html

WPA/WPA2
http://www.webopedia.com/TERM/W/WPA.html short definition
http://www.wi-fi.org/OpenSection/secure.asp?TID=2

802.11p
http://dailywireless.org/modules.php?name=News&file=article&sid=2815&src=rss09

802.11i and 802.1x
http://www.devx.com/wireless/Door/11413 802.11i standard
http://www.devx.com/wireless/Door/11266 802.1x standard

Article explaining link between 802.11i and 8021x
http://www.embedded.com/showArticle.jhtml?articleID=34400002

ITS information
http://www.itsa.org/
http://www.etsc.be/home.php