Global Information Assurance Certification Paper

Wireless LANs are on the Move

SANS Security Essentials
GSEC Practical Assignment
Version 1.2e
Current as of December, 2000 (amended May 22, 2001)

Glenda Spencer
November 15, 2001

This paper was inspired by Jeff Crume's book "Inside Internet Security, What Hackers Don't Want You To Know".

Table of Contents

I. Foreword

With consumers demanding more and more from automobile manufacturers, the idea of putting "smart" cars on the road opens the door to new security risks and vulnerabilities. The advent of smart car telematic systems offers the consumer a revolutionary service that allows the driver access to information ranging from weather reports to navigational instructions, even emergency and roadside assistance, with just a touch of a button. This system provides the consumer with convenience, reliability, and entertainment, in addition to safety and security.

Smart car telematic systems consist of a computer with a wireless connection and a global positioning system (GPS). The system is then connected to either an operator or data services such as an Internet Service Provider (ISP) via a Wireless Local Area Network (WLAN).[10]

If the technology is successful with consumers, and the many products offering increased security are successful, the emergence of smart car telematic systems will furnish hackers with a target-rich environment if the emerging WLANs are not completely secure. Consumers seeking higher levels of personal security may not realize the seriousness of the threat of security-related issues, such as privacy breaches and unauthorized access in wireless environments. Consumers are even less likely to consider less well-known security issues with wireless LANs including spoofing, denial of service (DoS) attacks, and unsecured transmissions. These last three issues will be the focus of this paper.

II. Main Text

A. Imagine the World of Tomorrow.

You are driving down the road when your smart car system detects a problem with one of its' computerized components. The car automatically reports the problem to the service provider. An automated system at the service provider quickly reviews the information and diagnoses the problem. A solution consisting of updated code is sent back to the car for implementation. The smart car system reviews the solution and determines that the fix is a simple adjustment that it can implement without notifying the driver. The occupants of the car never realize that a modification has taken place.[1]

The technology of combining computers and telecommunication systems is known as telematics. Smart car telematic systems provide the consumer with an enhanced feeling of safety, security, and convenience. These services are provided through the use of wireless web interfaces and/or voice communications and include:

- Automated vehicle performance monitoring and adjustments;
- Driving condition alerts, traffic reports, and route guidance;
- Roadside assistance with automatic and manual emergency-call features.

It is important to note that these systems will also allow the driver access to the Internet for web browsing and email access.

The world of tomorrow is not that far away. Right now, car companies such as GM, Cadillac, Mercedes-Benz, Nissan/Infinity, Jaguar, Lord/Lincoln, and Subaru are working with service providers and major manufacturers like Motorola to provide these types of services.[2] Companies, such as LoJack, are transitioning to provide smart car telematic services such "as notifying police automatically if the car is involved in a wreck."[3] 2002 Acura 3.5 RL owners can expect "emergency services, automatic notification of airbag deployment, stolen vehicle tracking, remote door unlocking, roadside and accident assistance, and an optional Med-Net feature."[4]

B. What are Smart Car Telematic Systems?

Telematics is derived from the French word télématiques, which was created to define the convergence of telecommunications (télécommunique) and computers (informatique).[19] Smart car telematic systems are defined as the technology of integrating computers and wireless telecommunications in a vehicle. These systems provide navigation, multimedia, email access, web browsing, and emergency-only systems. All of these systems communicate using existing cellular networks.

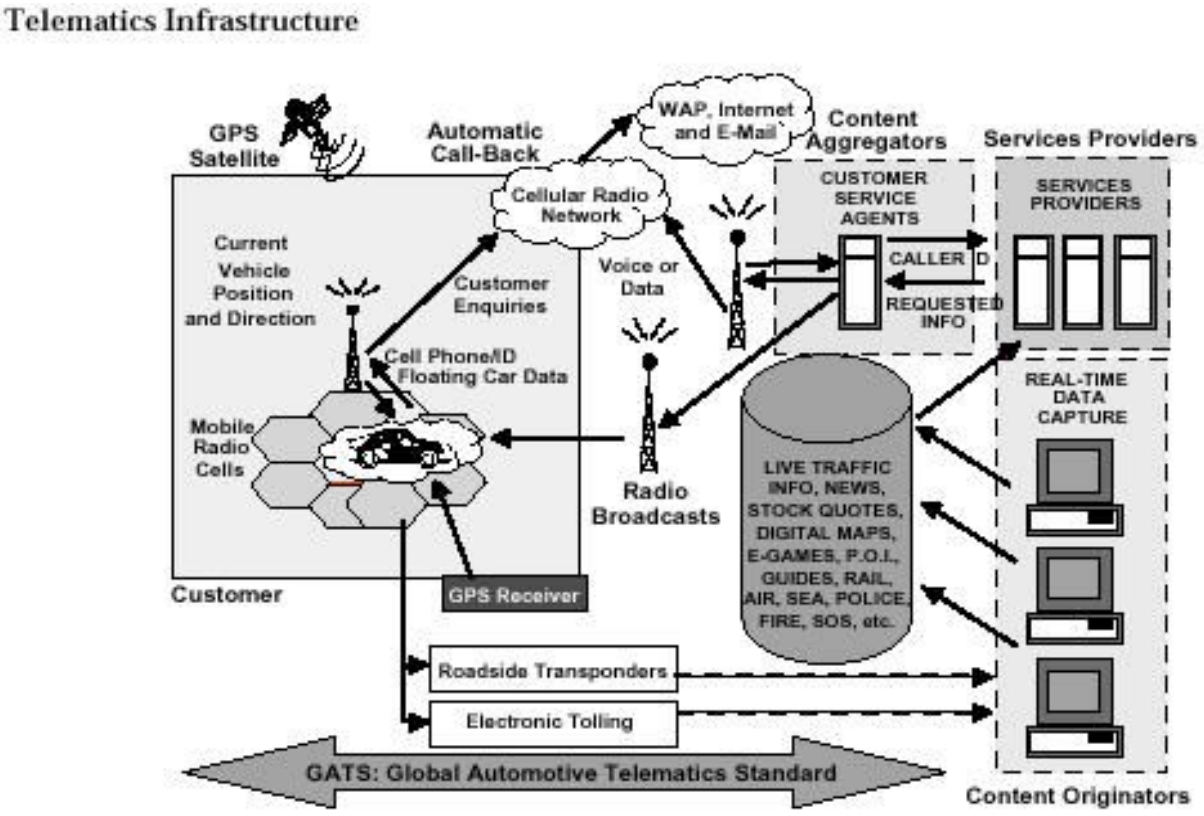
The smart car telematic systems are made up of various interconnected systems including: voice synthesis, global positioning devices, multimedia, traffic information, emergency services, email, and Internet access. Additional information about the various systems are provided below based on a report by Intex Management Services Ltd:[12]

- Internal bus systems. The various systems communicate with each other using internally connected buses. Two popular internal buses are CAN and MOST.

- Voice synthesis. This system allows the driver to interface with all the other systems. Currently, voice recognition is limited thus requiring providers to supply a personal touch – live operators offering assistance.
- Global Positioning Systems. This system includes such devices as Global Positioning Systems (GPS) to help navigate the vehicle, provide directional assistance, and emergency location services.
- Advisory system. This system provides the driver with helpful information about the surroundings such as the location of the nearest restaurant or gas station. The advisory system provides a list of suitable locations for the driver based on his/her needs. Once a location has been determined, the system would then provide dynamic route guidance to the final destination. go2.com offers this service on any wireless device.
- Multimedia-based interface systems. DVDs can hold several volumes of detailed digital maps on one disk and can provide navigational assistance in both audio and video. This system can interface with the advisory system.
- Traffic information system. This system provides the driver with information about traffic conditions and is used in conjunction with the navigation and advisory systems. The function is to provide dynamic route guidance based on traffic accidents, road construction, and general traffic congestion.
- Navigation system. This system interfaces with the GPS and traffic information system to determine the best possible route to any given final destination.
- Monitoring systems. This system includes the ability to control basic car functions. For example, the monitoring system is able to lock and unlock the vehicle's doors, inform the driver if the tires are low, and make simple service repairs to the engine.
- Emergency services system. This system provides the driver with roadside assistance, accident assistance, and medical assistance.
- Cell phone access. This system provides access to the internal phone system allowing the driver to make phone calls. The system interfaces with caller ID to inform the driver of incoming calls and requests how to handle them. This entire system is hands-free.
- Wireless web interfaces. This system uses all the features of the wireless web, using Wireless Application Protocol (WAP), which allows the driver access to read and write emails, search the web, and do other web functions hands-free.
- Electronic tolling. This system interfaces with the tolling systems. When a smart car with electronic tolling enabled passes through a tollbooth, the system automatically pays the fee, allowing faster passage.
- Entertainment system. This system includes access to DVD movies, online streaming movies, and eBooks that are read to the occupants.

According to a report by Intex Management Services Ltd, most smart car telematic systems use a 32-bit RISC microprocessor, flash memory, DRAM, with some systems also requiring a hard drive. The system makes use of the digital wireless devices with the communication protocols being WAP and Bluetooth. The operating systems being used are Windows CE and JavaOS with LINUX as a close contender.[12]

The figure below was taken from a report distributed by Gartner Dataquest. It shows the relationship of these systems to the vehicles and service providers.[13]



P.O.I. = point of interest
Source: Gartner Dataquest (December 2000)

C. The Flaws of Wireless Encryption.

Security for the 802.11b standard is achieved via Wired Equivalent Privacy (WEP) algorithm. In February of 2001, it was discovered that WEP contained a number of security flaws. According to a report posted on ISAAC's web site by Nikita Borisov, Ian Goldberg, and David Wagner, these security vulnerabilities revealed a susceptibility to the following types of attacks:[5]

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

Below is a summary and example of how a hacker could use this information to compromise a smart car telematic system. All the technical details concerning the security flaws were taken from the report posted on the ISAAC's web site.[5]

1. Passive Attack to Decrypt Traffic.
The first vulnerability exploits a weakness discovered in the RC4 key scheduling. The flaw enables a hacker to decrypt a message encoded with the 802.11 WEP encryption keys. The weakness is exploited as follows:

- IP traffic contains redundant data. The attacker can intercept all wireless traffic until two initialization vectors (IV) collisions occur in order to obtain the redundant data.
- By using XORing on two IV collision packets, the attacker can obtain the XOR of the two plaintext messages.
- The resulting XOR can then be used to determine the contents of the two messages.
- The resulting XOR can then be used to decode the message by inferring the contents of the package.

2. Active Attack to Inject Traffic.
Once the attacker knows how to decrypt the messages, the attacker can then encrypt packets and send them back to the access point. These messages would then be accepted as valid packets.

3. Active Attack from Both Ends.
Decrypting packets by guessing the packet header information is the third vulnerability. By determining the header information, the hacker can then switch the destination IP address. The packet would then be sent to the alternate machine where the message would be decrypted on the attacker's machine and then the plaintext message would be revealed.

4. Table-based Attack.
Due to the small space of possible initialization vectors, the attacker can easily build a decryption table in a day. Once a few messages have been decrypted, the attacker can compute the RC4 key stream generated by the IV used. This can then be used to decrypt all other packets being sent over the WLAN.

With the availability of specialized tools such as AirSnort and WEPCrack, decrypting the 802.11 WEP encryption keys has become automated using the method described above. Both AirSnort and WEPCrack are WLAN tools that can recover the encryption keys in a reasonable amount of time, allowing a feasible compromise of WEP protected systems.

D. What are the Security Issues with Smart Car Telematic Systems?
Unfortunately, the rush to provide functionality often creates new opportunities for hackers. If a hacker can break into these systems, then the hacker could unleash all types of havoc upon unwary customers. Below are just a few examples:

- Hackers could break into vulnerable systems and send unauthorized commands to lock and unlock the car's doors; misalign the GPS; adjust the car's tuning; and perhaps cause a malfunction, even stall the car in traffic. The more prominent the occupant of the vehicle, the better.
- The hacker could break into the service provider's network, thus controlling all the vehicles being managed by the service provider.
- A hacker could flood the service provider network with bogus traffic creating a Denial of Service attack against your car. The customers would be prevented from 'calling in' legitimate problems or unable to get directions.
- Finally, the Internet and email interfaces of the smart car are potentially vulnerable to viruses, worms, and Trojan horses.

According to an article published by Internet Security Systems, "attacks against 802.11b and other wireless technologies will undoubtedly increase in number and sophistication over time".[8] These risks can be placed in the following categories:

- IP Spoofing
- Denial of service attacks
- Unsecured transmissions

1. IP Spoofing

"The U.S. Transportation Secretary, Rodney Slater, urged the automotive industry to install smart accident avoidance systems on up to 10 percent of new cars and small trucks and 25 percent of new commercial vehicles by 2010. The Transportation Secretary also wants to see collision warning systems installed at selected intersections in 25 metro areas by 2010."[6] Just imagine the damage a hacker could inflict if these accident avoidance systems are vulnerable to spoofing attacks.

IP "Spoofing is the creation of TCP/IP packets using somebody else's IP address."[9] There are variations of IP spoofing attacks. These include man-in-the-middle, routing redirection, source routing, blind spoofing, and SYN flooding. Smart car telematic systems are vulnerable to each of these. Consider the following example:

A hacker finds a target host and launches a man-in-the-middle attack. The hacker discovers that there is a trust relationship between the vehicle and the service provider. The hacker launches a DoS attack on the vehicle so that it cannot respond to the service provider, thus disabling communications. Once the vehicle is impersonated (spoofed), a connection attempt is made to the service provider. If successful, the hacker then executes a simple command to create a backdoor for later use.

Consider another example using the same scenario. The hacker finds a target host and launches a man-in-the-middle attack. The hacker determines the IP address and encryption codes used to pass packets between the vehicle and service provider. Consider another example of a vehicle in need of some engine adjustments. When the service provider sends the updates back to the vehicle, the hacker is able to capture the

packets and redirects them by changing the header information to a different IP address. The net affect is that changes are made to the wrong vehicle.

2. Denial of Service Attacks

"And in 2001, when the expected 3 million-plus subscribers press their little blue and white buttons, is OnStar going to be ready to handle that kind of traffic? Or will your call be forwarded to an automatic voice-activated system, holding you in electronic hell while you sit idly on the highway, pining for a connection? Only time will tell. A lot of companies can talk about providing professional personal service, but few do it, or at least do it well for an extended period of time."[2] Realistically, hackers could create the same conditions.

An example of a Denial of Service (DoS) attack is when a device floods other devices with bogus packets. Duplicate IP or MAC addresses can also cause a disruption on the network. The attacker can fool the smart car telematic system by using the service provider's IP address and by being closer to the sending vehicle than the service provider. Since the attacker is in close proximity to the vehicle, the system will attempt to log into the masquerading IP address thus giving away pertinent information to the hacker.[8]

DoS attacks on smart car telematic systems could be done with a twist. Remember the first hacker who placed the backdoor in the service provider's system earlier? Today the hacker decides to create a DoS attack on the service provider. First the hacker uses the backdoor created previously. Then the hacker sends a command to unlock/lock/unlock, repeatedly, all the vehicle doors registered in the system. Of course, it is late at night, so the majority of the vehicles in the service provider's range have their doors locked and their alarms set for the night. Once the command has been received, the doors are unlocked without the alarm reset initiated. This action will trigger the alarm system in the car. Like good smart cars, they immediately call the service provider to inform them of the break-in. The service provider then issues a 9-1-1 call to the local police department to inform them of the ensuing theft (hopefully this is not automated). Not only is the service provider being overloaded with three million reports of break-ins (hopefully they figured out the problem before now), but also the local police have been dispatched to multiple false alarms. From the customer point of view (i.e., the owners of the vehicles), they need to figure out how to stop the car from locking and unlocking while trying to turn off their alarm systems because the neighbors are complaining. A similar incident occurred in Japan when "their phones automatically dialed Japan's emergency response number."[21]

Another type of DoS attack is known as jamming. Jamming is where the frequency is flooded with invalid traffic creating a DoS. By flooding the communications frequency, the signal becomes corrupted and ceases to function and then valid traffic cannot reach the intended parties. Special equipment is not needed to create a DoS attack on the 2.4 GHz frequency. Every day items such as; cordless phones, baby monitors, and microwaves; operate on the 2.4 GHz frequency which could be used to disrupt wireless

networks.[8] In addition, products such as C-Guard Mobile Phone Sensor from Netline Technologies have the ability to block this frequency.

A different type of DoS attack could result from an attacker breaking into the service provider and reporting a vehicle as stolen. Imagine the response customers would have after being pulled over for driving a stolen vehicle. The smart car system may be programmed to shut itself down if it believes it is being stolen. The stranded motorist would not only be inconvenienced by the delay, but would need to explain this to the highway patrol.

3. Unsecured Transmissions

As mentioned in an article published by Internet Security Systems, there are several points of failure that can occur when setting up secure transmissions for WLANs. The main issue deals with encryption of the transmissions.

Wired Equivalent Privacy

The flaw discovered in the Wired Equivalent Privacy (WEP) algorithm will not be addressed before 2002. Yet, there are already tools available to exploit this vulnerability. Both AirSnort and WEPCrack are available specialized tools that have the ability to feasibly decrypt the 802.11 WEP encryption keys.

Wireless Application Protocol

Currently, the telematic infrastructure is using the Wireless Application Protocol (WAP). This puts the telematic infrastructure at risk due to the security risk inherent to its design. A flaw within the *totally secure, fully authenticated, encrypted transmission* of WAP 1.1, is that there "is a moment at the WAP gateway, a fraction of a second, when the information is not encrypted and in theory, the owners of the WAP gateway could print off your information."[14] A worst-case scenario could be a hacker developing and unleashing malicious code on a WAP gateway to collect this information for them.

As of August 1, 2001, the WAP Forum released the WAP 2.0 specification for public review. WAP 2.0 does not have the same security weakness of temporarily decryption on the carrier's gateway. Hopefully the automotive industry will consider replacing WAP.

Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol (PPTP) is the networking protocol that Windows CE uses for transfer of data by creating a virtual private network (VPN) across a TCP/IP-based network using MS-CHAPv2 encryption.[17] Windows CE's PPTP is a subset of the features provided in Windows 2000's implementation, making it vulnerable to the same attacks as Windows 2000. The main security weakness with PPTP using MS-CHAPv2 encryption is the dependency on the user's password complexity.

E. Is there a Solution?

Several weaknesses need to be addressed to help protect smart car telematic systems from hackers. Four of these weaknesses are addressed below:

- Secure transmissions between the vehicles and the service providers.
- Prevent unauthorized access to smart car telematic systems.
- Determine how to update the smart car telematic software securely.
- Service providers need to be responsible for keeping all systems updated.
- Service providers need to constantly scrutinize their security stance.

1. Secure transmissions between the vehicles and the service providers.
Unless the entire transmission route between service provider and vehicle is secure and encrypted, the infrastructure is at risk of being successfully hacked. Windows CE does support Point-to-Point Tunneling Protocol (PPTP), but PPTP is full of vulnerabilities making it a poor choice.

If automakers and security solution providers were willing to work together to provide a robust security solution for small footprint operating systems such as Windows CE, a complete solution could be developed. Software solutions such as PGP Corporate Desktop Security 7.0 provide a personal firewall, personal Intrusion Detection System (IDS), Virtual Private Network (VPN), and file encryption; unfortunately, PGP Corporate Desktop Security 7.0 does not currently run on Widows CE.

2. Prevent unauthorized access to smart car telematic systems.
Providing a defense in depth system for each smart car telematic system would help prevent unauthorized access. A defense in depth system incorporates multiple layers of security methods, which operate in conjunction to protect the data, or in this case the telematic systems. A personal firewall, an IDS, and a VPN with file system encryption would provide the additional layers of security required.

- Personal firewall software would provide a strong first line of defense against attackers. Firewalls examine both the inbound and outbound traffic and enforce preset security rules between the telematic systems and the service provider.
- Personal IDS provide a powerful defense against attackers by detecting and blocking known attacks. Utilizing both a centralized and local alerting system, hostile attacks can be blocked and tracked.
- VPNs provide encrypted point-to-point communication. Strong authentication of the VPN is a must, a possible application of biometrics.
- File encryption, such as PGPWireless, allows the secure exchange of data between devices.[16]

There are a variety of solutions for each of these layers on operating systems other than Microsoft's Windows CE. Unfortunately, the small footprint of the smart car telematic systems places additional restrictions on the software deployed.

Personal firewalls.
Windows CE does have a networking add-on pack that includes Internet Connection Sharing that acts as a "personal firewall to reject connections on a specific network adaptor."[17]

Personal IDS.
At the time of this writing, there are no suitable personal intrusion detection systems for Windows CE.

VPN.
Windows CE uses PPTP to securely transfer of data remotely.[17] As previously mentioned, PPTP is full of vulnerabilities.

File encryption.
PGPWireless is a security solution for Microsoft Windows CE. The fact that the majority of smart car telematic systems are using Microsoft Windows CE, makes it a viable option. Moreover, with the use of PGPWireless, the data can be securely transferred from the vehicle to the provider.

There are two issues with the PGPWireless solution:

- First is the fact that encrypted communications are illegal in some parts of the world. Click the link bellow to see which countries restrict the use of encryption. http://cwis.kub.nl/~frw/people/koops/cls-sum.htm
- The second issue is key management. Key management can either be centralized using a certification authority or be distributed by using the web of trust.
  Centralized certification authority. If a hacker manages to steal the certificate, all systems will believe that the hacker has the rights to make changes to the system.
  Distributed – web of trust. Creating and maintaining keys for each vehicle would be immense, but to have the same private key on all systems would give the hacker a vulnerability to exploit. The hacker would just need to purchase a system and discover how to exploit any encryption key vulnerabilities. If the system allowed the customer the ability to create new keys, the user would need to understand how to create and use keys properly for the system to remain secure and to function securely.

Most personal firewalls, IDS, and VPNs do not fit on the small footprint of the smart car telematic systems

3. Determine how to update the smart car telematic software securely.
It is expected that three million subscribers will have some form of smart car telematics in their vehicles by the end of the 2001. Installing new systems is usually done as quickly as feasible which could result in security misconfigurations.[8]

It is a fact that the majority of computer attacks are based on well-known, unpatched vulnerabilities. Now comes the challenge. How does one go about providing security updates for three million subscribers? Considering the flaws discovered in the WAP encryption, how would manufacturers push out the design changes to all the smart car telematic systems as they become available?

The question of the day is: How does one keep the software on three million systems up-to-date? The solution is software distribution tools. Synchrologic's iMobile Suite has the ability to provide updates to smart phones and other wireless Windows CE devices over WLANs.[18] This technology can be adapted for updating smart car telematic systems.

Once WAP 2.0 has become intergraded with the current systems, the service providers can use WAP Push to distribute software upgrade. Since WAP 2.0 will not be released until the end of 2001, it may take a while to be widely distributed.

4. Service providers need to be responsible for keeping all systems updated.
It will be up to the service providers to take an active role to ensure all known vulnerabilities are patched immediately. A lack if action by the service providers will only open the doors wider for attackers. As discussed above, updating the vehicle's smart car telematic systems will be the challenge.

5. Service providers need to constantly scrutinize their security stance.
Service providers need to be as anxious to bolster their security, as they are to introduce the latest DVD based entertainment feature. They need to constantly monitor their networks for evidence of intrusions and attempts to intrude. They need to be active participants in the legal issues that will arise relating to telematics.

F. Summary

The smart car telematic systems of tomorrow are already here. The technological integration of telecommunications and computer systems has the potential for enormous benefits. Smart car telematic systems offer safety, security, and convenience for drivers.

However, the same concerns that currently plague wireless security are also applicable for smart car telematic systems. These concerns include IP spoofing, DoS attacks, and unsecured transmissions.

The newly discovered flaws in WEP, WAP 1.1, and PPTP are slowly being addressed. However, a major concern for smart car telematic systems is how to react to the next new series of vulnerabilities. Eliminating IP spoofing and DoS attacks while providing secure transmissions are a must to ensure the success of smart car telematic systems.

Until secure transmissions can be guaranteed, drivers will not have the safety, security, or convenience offered by the smart car telematic systems. Solutions such as providing defense in depth for the telematic systems; securing WAP; incorporating security tools similar to PGPWireless; and software distribution tools such as iMobile Suite, will help to provide protection against attacks. Above all, the service providers must take the initiative and provide a safe and secure environment for their customers.

III. Additional Reading

A. For Further Information

ZDNet: Why WEP can't secure your WLAN, Cracking 128-bit WEP
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2810563-2,00.html

The IEEE Wireless Standards
http://standards.ieee.org/wireless

Wireless Vulnerable to Hack Attacks
http://www.techtv.com/print/story/0,23102,3309868,00.html

Deriving 3 DES Keys from the NT Password Hash
http://mopo.informatik.uni-freiburg.de/pptp_mschapv2/node5.html

B. Similar Papers

Mehta, Princy C. "Wired Equivalent Privacy Vulnerability." April 4, 2001. URL: http://www.sans.org/infosecFAQ/wireless/equiv.htm

Griffin, Sean. "Security and the 802.11b Wireless LAN." September 16, 2001. URL: http://www.sans.org/infosecFAQ/wireless/80211b.htm

Flynn, Jeff. "Mobile Internet Connected Devices: Our Next Big Achilles Heel." 19 November 2000. URL: http://www.sans.org/infosecFAQ/wireless/achilles_heel.htm

IV. Glossary:

802.11b	Defines the standards for wireless local area networks using the 2.4 GHz frequency.
Access Point	A piece of hardware that passes data between a wireless network and a wired network.
Blind Spoofing	Redirects responses from a host, allowing commands to be sent, but can't get immediate feedback.[9]
Controller Area Network (CAN)	A communication serial network standard used to transmit data between the various kinds of embedded electronic modules in automobiles
Decrypt	Translate an encrypted message back into a readable format.
Denial of Service (DoS)	An overt attempt by attackers to inhibit legitimate users from using a particular service.
Digital Versatile Disks (DVD)	A type of media that holds a minimum of 4.7 gigabytes of information.
Encrypt	Translate information into an incomprehensible format.
Firewall	Either a hardware or software solution, which prevents unauthorized access to or from a private network.
Flash Memory	A solid state storage device. Solid state means that there are no moving parts – everything is electronic instead of mechanical.[11]
GHz	One thousand million Hz. A measure of radio frequency.
Global Automotive Telematic Standard (GATS)	The industry standard set by the mobile phone and automotive industries for transport telematic systems.
Global Positioning System (GPS)	A space-based radio positioning system used to as a locator.
Hz	Cycles per second. A measure of radio frequency.
IEEE	Institute of Electrical and Electronics Engineers
IP Address	An identifier for a device on a TCP/IP network.
IP Spoofing	The creation of TCP/IP packets using somebody else's IP address.[9]
ISP	Internet Service Provider
ISAAC	Internet Security, Applications, Authentication and Cryptography
Internet Service Provider	A company that provides customers access to the Internet [10]
Intrusion Detection System (IDS)	Either a hardware or software solution that inspects all inbound and outbound network traffic, identifying suspicious patterns that may indicate an attack.
IV collision packets	Initialization Vector (IV). The algorithm component used to keep expanded keys from repeating.[7]
Jamming	A type of DoS attack where the 2.4 GHz frequency is flooded with invalid traffic.[8]
JavaOS	A compact version of the Java operating system.

LINUX	An open-source implementation of UNIX.
Local Area Network (LAN)	An architecture that connects computer devices over a relatively small area.
Man-in-the-middle	Packets are sniffed on links between the two end points. Hackers can then pretend to be one end of the connections.[9]
Media Oriented Systems Transport (MOST)	A network technology based on synchronous data communication.
Microsoft Windows CE	A small footprint operating system designed for mobile devices, based on Microsoft Windows.
Point-to-Point Tunneling Protocol (PPTP)	A network protocol that transfers data securely from client to server by creating a VPN over a TCP/IP network.
Pretty Good Privacy (PGP)	A public key encryption program used to encrypting messages.
RC4 Key	A stream cipher designed in RSA laboratories by Ron Rivest in 1987, which is used widely in commercial applications.
Routing redirect	Redirects routing information from the original host to the hacker's host.[9]
Smart Car Telematic Systems	The incorporation of telematic systems in a vehicle.
Source Routing	Redirects individual packets by hackers host.[9]
SYN Flooding	SYN flooding fills up the receive queue from random source addresses; smurf/fraggle spoofs victims address, causing everyone to respond to the victim.[9]
TCP/IP	A suite of communications protocols used to connect devices on the Internet.
Telematics	A technology of combining computers and telecommunications.
Virtual Private Network (VPN)	An encrypted connection from one point to another over any network.
Wired Equivalent Privacy (WEP)	A security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, designed to provide a WLAN with the same level of security and privacy as a wired LAN.[15]
Wireless Application Protocol (WAP)	A set of standards used to provide Internet applications to mobile devices.
Wireless Local Area Network (WLAN)	A local area network that uses the 802.11b standard instead of wires to communicate.
XOR	"Known as the exclusive OR operator, a Boolean operator that returns a value of TRUE only if just one of its operands is TRUE. In contrast, an inclusive OR operator returns a value of TRUE if either or both of its operands are TRUE."[20]

V. References

1. Crume, Jeff. Inside Internet Security, What Hackers Don't Want You To Know. Great Britain: Addison-Wesley, 2000. Pages: 227-228.

2. Schexnayder, Gonzo. "OnStar Technology." edmunds.com News. Last updated: 2001-01-25. URL: http://www.edmunds.com/news/innovations/articles/43031/article.html (15 November 2001).

3. Lewis, Mark. "Forbes.com: LoJack Could Be a Steal." Yahoo Finance. Monday September 10, 4:13 pm Eastern Time. URL: http://biz.yahoo.com/fo/010910/0910lojack_1.html (15 November 2001).

4. SOURCE: Acura. "Acura 3.5 RL Adds Virtual Advisor and Personal Calling Features To OnStar(R) System." Press Release. Yahoo Finance. Monday August 27, 8:00 am Eastern Time. URL: http://biz.yahoo.com/prnews/010827/lam001.html (15 November 2001).

5. Borisov, Nikita, Ian Goldberg, and David Wagner. "Security of the WEP algorithm, Executive Summary." ISAAC: Internet Security, Applications, Authentication and Cryptography. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (15 November 2001).

6. Arlen, Gary. "Smart cars hitting the roads? Well, something to dream of." 2000 Post Newsweek Tech Media Group. August 14, 2000. URL: http://www.washtech.com/washtechway/1_15/forefront/3025-1.html (15 November 2001).

7. Franklin, Curtis. "A Cracked Spec." Internet Week, Reviews. March 12, 2001. URL: http://www.internetweek.com/reviews01/rev031201-2.htm (15 November 2001).

8. "Wireless LAN Security, 802.11b and Corporate Networks." Internet Security Systems. Pages 4 – 8. URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf (15 November 2001).

9. "Spoofing, Pretending to be someone else." Network Ice. URL: http://advice.networkice.com/Advice/Underground/Hacking/Methods/Technical/Spoofing (15 November 2001).

10. Dunne, Danielle. "What is Telematics?" Technology Made Simple. Learning Curve. May 24, 2001. URL: http://www.idg.net/go.cgi?id=483822 (15 November 2001).

11. Tyson, Jeff. "How Flash Memory Works." How Stuff Works. URL: http://www.howstuffworks.com/flash-memory.htm (15 November 2001).
12. Intex Management Services Ltd. "The Worldwide Market for Car Navigation, Multimedia & Emergency-only Systems." White Paper. April 2000.

13. Williams, Mike. "Telematics: Directions for the Connected Car." Gartner Dataquest. Research Brief. December 2000.

14. "How about WAP and security?" Frequently Asked WAP Questions. mobone.com (+), Mobile made easy. URL: http://www.mobone.com/faq/?id=security (15 November 2001).

15. "Wired Equivalent Privacy." Networking.com. Sep 06, 2001. URL: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci549087,00.html (15 November 2001).

16. Source: PR Newswire. "PGP Security Extends PGPwireless Platform Support to Include Microsoft Windows CE." CNET NEWS.COM. 9/11/01 5:02 AM. URL: http://news.cnet.com/investor/news/newsitem/0-9900-1028-7127621-0.html (15 November 2001).

17. "Microsoft Windows CE 3.0 Add-On Pack Feature Sheet." Microsoft Windows Embedded. Posted: Tuesday, September 26, 2000. URL: http://www.microsoft.com/windows/embedded/ce/guide/features/30aopoverview.asp (15 November 2001).

18. "iMobile Suite: Total Mobile and Wireless Infrastructure. Synchrologic. URL: http://www.synchrologic.com/about/about_imobile.html (15 November 2001).

19. Blagrove, Maggy. Telematics Update Magazine. Publisher's Notes. URL: http://www.eyeforauto.com/telematicsupdate/telematics6.pdf (15 November 2001).

20. XOR OPERATOR. XOR operatorThe Lycos Tech Glossary Definition. URL: http://lycos.webopedia.com/TERM/X/XOR_operator.html (15 November 2001).

21. Gohring, Nancy. "Motion Sickness." Interactive Week, Special Reports. October 29, 2001. URL: http://www.interactiveweek.com/article/0,3658,s%253D619%2526a%253D17267%2526app%253D1%2526ap%253D2,00.asp (15 November 2001).

Last Updated: October 24th, 2017

Upcoming Training

San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event