What do Jeeps and Radiology Image Distribution have in common?

Well, when it comes to security, they have a lot in common. In July 2015 the magazine Wired published an article in which two known hackers, Charlie Miller and Chris Valasek, hacked into a Jeep Cherokee via the internet from their basement. Now this attack was not a complete surprise to the driver since he was the article writer (Andy Greenberg) and guinea pig for the test. As Andy was driving in St. Louis, the hackers started to blow cold air conditioning, mess with the wipers, apply the brakes, put hip-hop loudly on the radio and eventually just killed the ignition. This was all fun and games until an 18 wheeler was barreling up on Andy, when he panicked. The hackers released their control and Andy drove to safety. Fortunately, this was a test and car hacking has not become a form of entertainment for hackers or more diabolical with terrorists. So how does a problem with this much impact on people get resolved from a security perspective? What if this happened to you? Would want the most secure method of security available?

Most health care institutions agree that security is the number one concern in the movement or exchange of patient images. The most common method today is the tangible exchange of CDs or DVDs. Some of these are encrypted to help, but nonetheless can be broken, cumbersome, and still lack security. Other methods are to send the studies from a web interface to cloud storage to be downloaded by a credentialed user at another location with the same HTTPS web interface. HTTPS is considered secure, but when J.P. Morgan Chase was hacked, affecting 2 out 3 households in America, the technology was insufficient as it is in most banks. (Reported by CNN http://money.cnn.com/2015/06/23/technology/bank-websites-encryption/) And this is where your money is kept! Now let's assume that hackers could access your car and download controls to it from a weak HTTPS site- this would wreak havoc on the highways and be a target for terrorism. To deal with this potential disaster, car manufacturers turned to defense contractors to develop a secure unbreachable solution.

The solution is to employ a peer-to-peer hardware recognition program to create a secure P2P network that has trust management by having the sender and receiver recognize each other from independent end points. Basically, the receiver (car) allows the data to be sent to it because it knows the senders hardware signature that cannot be replicated by a hacker. If the trust recognition is not present, then no code will be received. Running these kinds of updates and transfer of data via the internet, even if utilizing HTTPS, is unsecure and ultimately dangerous. No one likes the thought of their care being taken over by a hacker going through a website.

From a security standpoint, P2P networks ostensibly offer inherent robustness and technology properties not easy to achieve in a traditional network design. For example, an attacker wishing to effect a denial of service in a traditional network can focus an attack on a relatively small number of centralized servers, whereas in a P2P network the attacker must compromise a relatively large number of servents in order to fully disconnect the network. A robust network design requires that peers in a P2P network be considered trusted, so to ensure integrity and confidentiality of shared data it is critical that P2P networks be secure. In recent years there has been a vast array of research towards enforcing the security guarantees necessary to achieve system-wide, end-to-end security policies in P2P networks.

One of the most challenging aspects of developing a secure P2P network is establishing a secure routing structure over which messages and data can reliably be exchanged in the presence of malicious hackers and other security threats. P2P networks provide the infrastructure to support various technology applications such as data management, collaboration, and best in class security technologies. These in turn support real-world applications including e-commerce, situation awareness, intelligence analysis, and transfer of medical images. Secure P2P networks can be used as a foundation for supporting trusted applications. P2P networks have been developed as a means of evenly balancing the computational expense associated with delivering network services and eliminating the need to store excess data in the cloud. In contrast to a traditional network, which divides its constituent hosts into servers and clients, P2P networks homogeneously treat all hosts as servents, assigning each both server and client functionality. This allows services to be delivered from a large number of servents rather than from a relatively small number of servers which creates a much broader network of secure end to end point destinations. For example, Nautilus Medical and their image exchange client MatrixRay, saves users money by storing image data on end-user machines rather than on a centralized cloud server. Users credential themselves and maintain their own hardware signatures, user names and passwords. Particular attention is devoted to the problem of developing secure routing protocols that constitute a suitable foundation for implementing their security system. Nautilus has employed munitions grade algorithms along with proprietary compression methods to achieve fast and secure transfer of medical images in an environment scrutinized for the handling of Protected Health Information, or personal health details.

You can purchase car insurance to protect your car in the event of a crash or damage- even if caused by a hacker. Only Nautilus Medical offers insurance for a breach of exchanged data underwritten for $1,000,000.00.