TRUSTED COMPUTING GROUP WHITE PAPER

June 2012

Secure Embedded Platforms with Trusted Computing: Automotive and Other Systems in the Internet of Things Must Be Protected

In this paper...

- Embedded Systems Market
- Business Drivers
- Solutions

Trusted Computing Group

3855 SW 153rd Drive
Beaverton, OR 97006

Tel (503) 619 – 0562
Fax (503) 644 – 6708

admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

As published originally on http://johndayautomotivelectronics.com/ May 2012

The embedded systems market is going through a profound transformation right now. Historically, embedded systems builders assumed that their systems were ultimately built to stand alone. Typical embedded systems, such as those in today's automobiles, might contain more than a hundred individual processors, with multiple in-vehicle networks and millions of lines of code. Even so, the vehicle is a *closed* system. There are a few ways for the outside world to access the vehicle's embedded processors, but they almost all require physical presence with the vehicle.

At the same time, as the cost of computing technologies decreases, embedded systems are quickly becoming more resource rich. Designers are taking advantage of this richness to increase the software content of embedded processors, including the addition of telecommunications hardware and TCP/IP networking. There are strong business drivers to make this change happen, just to name three:

- Customer care: Enhanced ability to diagnose and respond to problems in the field means happier customers. This might also appear as an ability to update platform firmware or software, adding new features or fixing bugs. (http://blogs.insideline.com/straightline/2011/06/remote-diagnostics-top-car-tech-among-consumers.html)
- New or expanded revenue opportunity: in the case of cars, the opportunity for an auto manufacturer to offer in-vehicle entertainment and information packages that are Internet-based and for-fee. (http://www.popularmechanics.com/cars/news/industry/toyota-entune-to-bring-drivers-closer-to-the-cloud).
- Reduced cost of managing deployed systems: If the older generations of deployed systems do not have a networking capability, then to manage or collect data from these systems, a person must go visit the system. Remember power company meter readers? (http://en.wikipedia.org/wiki/Smart_meter)

Designers are taking advantage of this richness to increase the software content of embedded processors, including the addition of telecommunications hardware and TCP/IP networking.

This very same network connectivity also makes it possible for attackers to gain access to

platforms that have never before been available to them. In today's Internet, the primary motive for cyber attack is money, although there are often other motivations. Considering the three business drivers in favor of networking embedded systems. It's inevitable that money and mischief will follow, as they have in the PC and mobile device worlds now under continual cyber attack. For example:

- Customer care: One source of money here is *denial of service.* If the system offers any sort of control options through its networked interface, then maybe someone else will use that for mischief. A Berlin student demonstrated he could use his iPhone to control a minivan in 2009. The article points out that several auto manufacturers now support smart phone apps that can be used to control a car. It's not hard to imagine trouble if someone interferes with a vehicle as it is being operated. (http://www.helium.com/items/2299797-could-hackers-take-control-of-your-new-car).
- In-vehicle entertainment. In the previous point, lone actors (such as the Berlin student) have been known to take advantage of a network interface to a platform for purposes that were not intended by the manufacturer. In a different case, a company, News Corp., funds a cyber attack team for the purpose of sabotaging a rival's info-tainment offering. In this case, it is reported that News Corp. funded an effort that cracked the security mechanism used by its competitors (secrets stored on smartcards). The reason given for this is that News Corp. used this information to forge counterfeit smartcards for sale on a black market with the intention of depriving revenue to their competition. http://www.msnbc.msn.com/id/46874745/ns/business-world_business/t/report-news-corp-pirated-rivals-cable-boxes/
-

Embedded systems are relatively new to the Internet, but given the history of PC cyber attacks, many in the industry are looking at how to prevent such attacks.

Centralized management of distributed platforms is a marvelous way to save money –unless the network is unavailable, or unless the platforms being managed have been hacked and are either no longer responsive or under someone else's control. Why would someone disrupt a business like this? Extortion could be a reason, http://chris-epley.suite101.com/cyber-crimes-part-one-cyber-extortion-a252801 and http://articles.businessinsider.com/2012-02-08/news/31036628_1_smart-grids-utilities-power-meters.

Embedded systems are relatively new to the Internet, but given the history of PC cyber

attacks, many in the industry are looking at how to prevent such attacks.

In the automotive sector we see forward thinking action on this problem. In the European Union we see http://evita-project.org/. This open consortium took as its task:

> "…the objective of the EVITA project is to design, verify, and prototype an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle." http://evita-project.org/objectives.html

On the industry standards front, Toyota recently joined the Trusted Computing Group (TCG - http://www.trustedcomputinggroup.org/). TCG is an open consortium of companies interested in improving the security posture of platforms and networks. They write the specifications that define the Trusted Platform Module (TPM), define how self-encrypting drives can be managed (the OPAL specification) and define ways that network security can be improved and better managed (Trusted Network Connect – TNC). All of these technologies to date have been oriented to protecting PCs, servers and traditional networks, but can apply to non-PC systems.

For example, the TPM can be used to protect vehicles. In any application, whether a PC or embedded system, the TPM (as a discrete or integrated component) can verify whether program code has been changed, as might happen when an attacker installs malware. Google Chromebooks use the TPM for that purpose (http://chrome.blogspot.com/2011/07/chromebook-security-browsing-more.html). So could on-vehicle networks.

TPM can be used to protect vehicles. In any application, whether a PC or embedded system, the TPM (as a discrete or integrated component) can verify whether program code has been changed, as might happen when an attacker installs malware.

TPMs can also protect cryptographic keys used for identity and encryption. That makes it possible for a system to verify its own identity (using a key that is unique to itself and bound inside its TPM. It also makes it possible for that system to recognize another system (because it recognizes that platform's unique key).

Trusted Computing principles also make it possible for those two systems to exchange information securely by using shared keys (protected by both TPMs) to encrypt data traffic. In this TPM-based security model, a car won't talk to a possible attacker because it doesn't know the attacker (the crypto keys are not recognized). Eavesdropping on conversations

between the car and the manufacturer are prevented, because the keys used to encrypt the traffic are not available.

Cars can store a lot of data now too. Some of that data is personal data about the owner. Some is financial information, like the account number he uses to pay for his entertainment system. Other software runs various vehicle systems and should be protected against attack. Self- encrypting drives based on TCG specifications offer a solution to that problem – these drives encrypt all data all the time on the fly, with no impact on performance. The drives can only be unlocked by authorized users and are virtually tamper-proof.

TCG's TNC network security architecture could also be applied to the problem of securing car-to-car and car to manufacturer networking. An important element of TNC is validation of the identity and health of a system before the platform is system to connect to a network. This can apply to on-car networks. For example, during service, an easily accessible module in the car is replaced with one that is not correct or has malware. When the rightful owner starts the car, the nefarious module is rejected, because it does not have the right identity credentials and its program code wouldn't measure to the right value.

In another example, perhaps hackers target a specific automaker. The attacker purchases a car from that manufacturer so as to compromise its network of processors, and then that compromised on-car network is directed to attack the Toyota corporate network that supports cars in the field. If the automaker was using TNC to check the identity and health of every car when that car tries to connect, once again, it would fail because its valid identity could not be confirmed. Even if it does, the software measurements (called "integrity measurements") would not match what Toyota's records would show they should be.

Conclusion

There is a rush to network connect billions of platforms that were not designed to protect themselves in a networked world. Among these platforms are the hundreds of millions of on-car networks. When this happened to PCs, the PC world was swept with a flood of cyber crime that is still in full force today. Lots of people are pointing to the PC and saying, "How will we protect all these newly networked platforms?" Lots of answers are being suggested. Some of those answers can be found at the Trusted Computing Group. The TCG has been around for 10 years, has developed widely used and vetted specifications, and hundreds of millions of PCs are equipped with TPMs today. TCG's TPM, OPAL and TNC all offer practical methods for securing embedded platforms and networks in a cost-effective way.