David Schirduan 9-5-11
TPMS Response Bowring

Flawed Systems

Both of these papers discussed flaws in "accepted" and implemented technologies. The Therac-25 machines have been in use for years before evidence of flaws surfaced, and there are still problems with modern radiation machines. The Tire Pressure Monitoring Systems are just about to be distributed all over the US and EU. Both of these technologies are not 100% secure or reliable, like any technology or software designed by human beings. The main difference being that the flaws in these two technologies have been recognized and solutions have been brought to the attention of the public through these two papers.

The radiation accidents were textbook examples of history repeating itself. The Therac-25 malfunctions were considered the worst series of radiation accidents in the history of medical accelerators. 6 people were killed from radiation overdoses caused by malfunctions in the software. More than 20 years later, over 400 people have been diagnosed with radiation overdose during a CT brain perfusion scan. Both of these problems are caused because software isn't reliable or safe. It is created by medical appliance companies, and is usually integrated software, seen as simple and fault-proof.

This problem should not be this widespread. One of the beautiful things about software is that it can be distributed to many testers and engineers in order to ensure safety and reliability. People often marvel at the stability and reliability of the Linux system. This is possible because linux software is modified and rebuilt by thousands of programmers before becoming and accepted piece of software. This refines it, with each alterations and bug fix making it a more solid and efficient piece of code.

If software in medical and safety related industries were tested more thoroughly, that would help to ensure how it would stand up to real-world distribution. I understand that it would be difficult to ensure the copyright or security of such code, but clearly the software in these machines are not being seen by enough competent programmers to ensure reliability.

Another problem could be that software engineering firms are not contracted to develop this software. If more attention is paid to hardware and engineering principles, the software could be seen as a way to keep costs down. After all, with such a simple machine, how complex could the software be? These sorts of oversights can result in major mistakes and miscalculations. If software is 99% reliant, then 1% of the radiation doses could be incorrect. When people's lives hang in the balance, more attention must be paid to the development and testing of the software that drives these machines.

The Tire Pressure Monitoring Systems also exhibit these problems, and will continue to do so unless a solution is found. The legislature was passed in order to ensure road safety, as well as efficient fuel consumption. Tires that are not at optimal pressure can present a legitimate threat. The Jeep Wrangler that I drive has a slow leak in the back left tire. I have to refill it every 2 weeks or so, and I can tell that the engine burns gas much faster to maintain normal speeds. In my case, it is a simple matter of the payoff (a working car) not being worth the cost (new tire) since now that I'm attending classes, I don't need a functional vehicle. However, in other cases, such a low-pressure warning system could prevent accidents, along with other negative results. Especially in an age where cars are seen as a black box, resulting in few people having a good understanding of how their car works, as well as how to maintain it.

Clearly the need for a TPMS exists, however this implementation has several flaws, all of which are exposed in the article. It is clear that the TPMS devices were developed and distributed with minimal attention paid to their security or safety. The researchers at CSE and Rutgers University have laid out an excellent case against using these devices, all prior to their distribution.

It was amazing to read how this team of researchers set out to hack these devices, and expose their

flaws. I have never read a paper wherein university researchers partake in “white hat” hacking in order to demonstrate their point. I like how they laid out how long it took them to develop their method to intercept and decode the signals sent from the TPMS; how it took a PhD-level expert a few days to develop, and students with no experience several week to reproduce. In an age where the internet allows for mass communication, and very few secrets, the threat of people devising a way to hack the TPMS and use them for nefarious purposes is assured. The ease of which would depend on the countermeasures that legislature would take. If a team of researchers could do it in a month or two, how long would it take the combined power of the internet?

It was also enjoyable to follow along with their train of thought as they reverse engineered the software and transmission protocols. Their explanations were well put, and it was easy to follow along, even without all of the details. I wondered how much this paper would aid someone who wished to take advantage of the system once it becomes integrated into most modern cars.

I can’t believe that this legislature was passed with such glaring flaws. Surely someone along the chain had pointed out that wireless devices in a car were susceptible to penetration. The push to get this technology out the door, and with as low cost as possible demonstrates sacrificing safety for profit. The supposed security measures developed flaw flat in the light of the efforts of the research team.

As I read the article, I was getting angry that no one had thought to seek the opinion of the experts in this field. If a country wanted to drill off the coast, it would have to get several teams of people to approve this decision. But installing unsafe wireless devices in every car on the road is overlooked and under-examined. I blame this largely on the lack of knowledge on computers and wireless network protocols. Most people view computers and related devices as black boxes. When companies and governments fail to take into account the complexity and flaws of technology, then it simply allows for those with experience to take advantage of such systems.