Chapter 2 : The Internet of Things

1. ***Listening activity :***

From : https://www.youtube.com/watch?v=eiplo_gWns8

Watch the video and answer the questions in French :

- What is the Internet according to the video ?

- What is the Internet of Things ?

- What does control all the connected things ?

- Can you give examples using the Internet of Things ?

- What is ANSYS ?

Fill in :

This is ____ development. Without it, the Internet of Things would not be possible. The complexity of smart devices could not be tested. Technology like Mens, _________________ _____________, Wireless Power Transfer, ________________________________, 5G Communication Speeds and _________________________________ all demand a totally new approach to product engineering.

2. ***Reading activity :***

From : http://www.theguardian.com/media-network/2014/nov/06/internet-of-things-data-security

Defining the internet of things – time to focus on the data

As the internet of things passes into mainstream consciousness, more specific definitions are needed in order to secure it. The data it creates could be a good place to start.

From air traffic control to fridges; the internet of things is incredibly broad and would benefit from clearer definition.

You could be forgiven for believing that the internet of things (IoT) is a well-defined term and that everyone is on the same page. But you would be mistaken to say the least, given the huge variety of intelligent connected devices that this term refers to. In fact, the thing about the IoT is that it could mean almost anything. In some ways it is better to think of it as the internet of everything.

Topping nearly every 2015 predictions list in town, including Gartner's renowned Strategic Technology Trends forecast, the world is beginning to acknowledge that the internet of things, is in fact, a multitude of very different things, ranging from the mundane to the life-and-death. The IoT is smart fridges, it's the Apple Watch, it's air traffic control technology and environment monitoring systems. It's space satellite systems, and pacemakers embedded in the human body. But, looking beyond the clutter, from a risk and security perspective, it's perhaps most important to focus on the data that is captured, processed, and communicated (often in real time) between these devices.

As the conversation matures and the industry develops, we will need to move away from the temptation to bundle all these very different things under one generic umbrella term. Much like cloud or big data, it's incredibly overused, and to some degree, almost too vague to be useful.

We saw cloud go through a similar evolution not so long ago. Five years ago, we were talking about cloud as though it were one model. Now, largely propelled by the Cloud Security Alliance, we have the taxonomy to discuss and refer to different architectures, chiefly; platform as a service, infrastructure as a service, software as a service and even security as a service.

These distinctions are important, as each requires the business using the service to negotiate a different balance between trust and control with the cloud provider. Where is the data? Who controls it? Who has access to it? And crucially, what measures are in place to protect it?

There is rarely a one-size-fits-all solution when it comes to security, and this certainly applies to the cloud. For businesses to take advantage of the cloud effectively, they must assess the sensitivity of the various data types within the business, so as to define the appropriate security measures to apply. Keeping secrets is much more expensive than guarding non-sensitive data – it would be madness to invest in protecting all data to the same degree.

Like any big technology trend, the internet of things comes with considerable baggage, as well as some unanswered questions regarding security. It is a significant challenge to establish trust and control across this enormous range of 'things', particularly when they are widely distributed, and often deployed on a scale of millions, to highly untrusted locations, or are handling particularly sensitive data. The information flowing through a network of smart fridges is very different from the information generated by an air traffic control system or array of tsunami detectors.

It is with this logic, and the need to have a sensible conversation about security, that we must begin to separate the IoT. Failing to do so will lead to trying to secure all data on all devices – which amounts to trying to boil the ocean. Unlocking the positive potential of the internet of things will rely on taking a data-centric approach to security – the very data that brings this network to life and makes it intelligent.

The technology required to underpin this security is not new. Cryptography, used in encrypting data and proving digital identity for devices, is the centre of security for ensuring safe identification, confidentiality and integrity – the same technologies that secure nearly every website on the planet, and the payment systems we use every day. The next few years – or even decades – will be a very interesting time as the security industry works to secure the internet of things. Or rather the data of the things, wherever they might be scattered across the internet.

Richard Moulds is vice president of strategy at Thales e-Security

Find the words from the text that match with the following definitions :

Definitions from : www.collinsdictionary.com

Words	Definitions
	the main current
	(of a piece of software) made an integral part of other software“ ”
	a disordered heap or mass of objects
	an interconnected group or system
	the science or study of analysing and deciphering codes, ciphers, etc; cryptanalysis

Answer the following questions in French :

- What is needed to secure the Internet of Things ?

- In what can we find the IoT ?

- Cloud isn't one model… explain

- Why is it important to distinguish it ?

- Are all data protected the same way ? explain why ?

- What can be considered of being the centre of security for ensuring safe surfing ?

3. ***Listening activity :***

From : https://www.youtube.com/watch?v=Q3ur8wzzhBU (Intel)

Listen to the video and answer the questions :

- What is the IoT ?`

- What happens if different devices connect with each other ?

- Can you name advantages of the IoT in our daily lives ?

Fill in

- Billions of devices will be ____ and soon hundreds of billions of devices.

- Here is an example of the big picture : imagine an _______________________________ such as a smart traffic camera. The camera can monitor the road for congestion, accidents and weather conditions and communicate that status to a gateway that ____, creating an intelligent citywide traffic system.

Chapter 2 : The Internet of Things

4. ***Reading activity :***

From :https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?utm_term=.e6a0f3433834

How a fish tank helped hack a casino

By Alex Schiffer July 21

Hackers stole data from a casino by hacking into an Internet-connected fish tank, according to a new report. (iStock)

Hackers are constantly looking for new ways to access people's data. Most recently, the way was as simple as a fish tank.

The hackers attempted to acquire data from a North American casino by using an Internet-connected fish tank, according to a report released Thursday by cybersecurity firm Darktrace.

The fish tank had sensors connected to a PC that regulated the temperature, food and cleanliness of the tank.

"Somebody got into the fish tank and used it to move around into other areas (of the network) and sent out data," said Justin Fier, Darktrace's director of cyber intelligence.

The casino's name and the type of data stolen were not disclosed in the report for security reasons, Darktrace said. The report said 10 GB of data were sent out to a device in Finland.

"This one is the most entertaining and clever thinking by hackers I've seen," said Hemu Nigam, a former federal prosecutor for computer crimes and current chief executive of SSP Blue, a cybersecurity company.

As more products with the ability to connect to the Internet become available, opportunities for hackers to access data through outside-the-box ways have risen. The report, which was first reported by CNN, comes a few days after the FBI warned parents about the privacy risks of toys connected to the Internet, which could help a hacker learn a child's name, location and other personal information.

Fier said that with the recent FBI toy warning and the many ways by which hackers are trying to break into systems, he wouldn't be surprised if the government eventually got involved in regulating Internet of Things, IoT, products. But he said, even if it did, that would raise other questions.

"Everything has to go through FTC approval, I'd be curious to see if that happens on the cyber front," he said. "That you have to do the bare minimum to protect these products. But that's just for the U.S. How do you do this globally?"

As for what people can do to protect themselves against these kinds of attacks, customers should educate themselves about IoT products and take advantage of any security protection the product offers, Nigam said. He added that people should use the latest operating systems and software and constantly update them.

The fish tank incident was one of nine unique threats mentioned in Darktrace's annual report of innovative hacks. Some of the other threats mentioned included hackers using company servers to acquire bitcoin, a digital form of currency, and former employees using their old login credentials to steal company data.

Answer the questions with the text above :

- What happened ?

- What is the particularity of the fish tank ?

- How di dit happen ? What did the Hackers do ?

- Why do opportunities for hackers rise ?

- Can you give another example of hacking on IoT ?

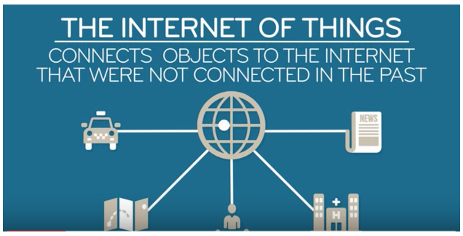
- Why is it difficult to secure « IoT products » ?

- Which advice is given to help people protecting themselves ?

5. ***Listening activity :***

From : https://www.youtube.com/watch?v=8qF4ts4r6PQ

Prepare this video for the first test (see calendar for the date)


THE INTERNET OF THINGS
CONNECTS OBJECTS TO THE INTERNET THAT WERE NOT CONNECTED IN THE PAST
NEWS

6. ***Reading Activity***

From : http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.

As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car's digital display: Charlie Miller and Chris Valasek, wearing their trademark track suits. A nice touch, I thought.

The Jeep's strange behavior wasn't entirely unexpected. I'd come to St. Louis to be Miller and Valasek's digital crash-test dummy, a willing subject on whom they could test the car-hacking research they'd been doing over the past year. The result of their work was a hacking technique—what the security industry calls a zero-day exploit—that can target Jeep Cherokees and give the attacker wireless control, via the Internet, to any of thousands of vehicles. Their code is an automaker's nightmare: software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.

To better simulate the experience of driving a vehicle while it's being hijacked by an invisible, virtual force, Miller and Valasek refused to tell me ahead of time what kinds of attacks they planned to launch from Miller's laptop in his house 10 miles west. Instead, they merely assured me that they wouldn't do anything life-threatening. Then they told me to drive the Jeep onto the highway.

"Remember, Andy," Miller had said through my iPhone's speaker just before I pulled onto the Interstate 64 on-ramp, "no matter what happens, don't panic."1

Charlie Miller (left) and Chris Valasek hacking into a Jeep Cherokee from Miller's basement as I drove the SUV on a highway ten miles away. WHITNEY CURTIS FOR WIRED

As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission.

Immediately my accelerator stopped working. As I frantically pressed the pedal and watched the RPMs climb, the Jeep lost half its speed, then slowed to a crawl. This occurred just as I reached a long overpass, with no shoulder to offer an escape. The experiment had ceased to be fun.

At that point, the interstate began to slope upward, so the Jeep lost more momentum and barely crept forward. Cars lined up behind my bumper before passing me, honking. I could see an 18-wheeler approaching in my rearview mirror. I hoped its driver saw me, too, and could tell I was paralyzed on the highway.

"You're doomed!" Valasek shouted, but I couldn't make out his heckling over the blast of the radio, now pumping Kanye West. The semi loomed in the mirror, bearing down on my immobilized Jeep.

I followed Miller's advice: I didn't panic. I did, however, drop any semblance of bravery, grab my iPhone with a clammy fist, and beg the hackers to make it stop.

Wireless Carjackers

This wasn't the first time Miller and Valasek had put me behind the wheel of a compromised car. In the summer of 2013, I drove a Ford Escape and a Toyota Prius around a South Bend, Indiana, parking lot while they sat in the backseat with their laptops, cackling as they disabled my brakes, honked the horn, jerked the seat belt, and commandeered the steering wheel. "When you lose faith that a car will do what you tell it to do," Miller observed at the time, "it really changes your whole view of how the thing works." Back then, however, their hacks had a comforting limitation: The attacker's PC had been wired into the vehicles' onboard diagnostic port, a feature that normally gives repair technicians access to information about the car's electronically controlled systems.

A mere two years later, that carjacking has gone wireless. Miller and Valasek plan to publish a portion of their exploit on the Internet, timed to a talk they're giving at the Black Hat security conference in Las Vegas next month. It's the latest in a series of revelations from the two hackers that have spooked the automotive industry and even helped to inspire legislation; WIRED has learned that senators Ed Markey and Richard Blumenthal plan to introduce an automotive security bill today to set new digital security standards for cars and trucks, first sparked when Markey took note of Miller and Valasek's work in 2013.

As an auto-hacking antidote, the bill couldn't be timelier. The attack tools Miller and Valasek developed can remotely trigger more than the dashboard and transmission tricks they used against me on the highway. They demonstrated as much on the same day as my traumatic experience on I-64; After narrowly averting death by semi-trailer, I managed to roll the lame Jeep down an exit ramp, re-engaged the transmission by turning the ignition off and on, and found an empty lot where I could safely continue the experiment.

Miller and Valasek's full arsenal includes functions that at lower speeds fully kill the engine, abruptly engage the brakes, or disable them altogether. The most disturbing maneuver came when they cut the Jeep's brakes, leaving me frantically pumping the pedal as the 2-ton SUV slid uncontrollably into a ditch. The researchers say they're working on perfecting their steering control—for now they can only hijack the wheel when the Jeep is in reverse. Their hack enables surveillance too: They can track a targeted Jeep's GPS coordinates, measure its speed, and even drop pins on a map to trace its route.

Miller attempts to rescue the Jeep after its brakes were remotely disabled, sending it into a ditch. ANDY GREENBERG/WIRED

All of this is possible only because Chrysler, like practically all carmakers, is doing its best to turn the modern automobile into a smartphone. Uconnect, an Internet-connected computer feature in hundreds of thousands of Fiat Chrysler cars, SUVs, and trucks, controls the vehicle's entertainment and navigation, enables phone calls, and even offers a Wi-Fi hot spot. And thanks to one vulnerable element, which Miller and Valasek won't identify until their Black Hat talk, Uconnect's cellular connection also lets anyone who knows the car's IP address gain access from anywhere in the country. "From an attacker's perspective, it's a super nice vulnerability," Miller says.

From that entry point, Miller and Valasek's attack pivots to an adjacent chip in the car's head unit—the hardware for its entertainment system—silently rewriting the chip's firmware to plant their code. That rewritten firmware is capable of sending commands through the car's internal computer network, known as a CAN bus, to its physical components like the engine and wheels. Miller and Valasek say the attack on the entertainment system seems to work on any Chrysler vehicle with Uconnect from late 2013, all of 2014, and early 2015. They've only tested their full set of physical hacks, including ones targeting transmission and braking systems, on a Jeep Cherokee, though they believe that most of their attacks could be tweaked to work on any Chrysler vehicle with the vulnerable Uconnect head unit. They have yet to try remotely hacking into other makes and models of cars.

After the researchers reveal the details of their work in Vegas, only two things will prevent their tool from enabling a wave of attacks on Jeeps around the world. First, they plan to leave out the part of the attack that rewrites the chip's firmware; hackers following in their footsteps will have to reverse-engineer that element, a process that took Miller and Valasek months. But the code they publish will enable many of the dashboard hijinks they demonstrated on me as well as GPS tracking. Second, Miller and Valasek have been sharing their research with Chrysler for nearly nine months, enabling the company to quietly release a patch ahead of the Black Hat conference. On July 16, owners of vehicles with the Uconnect feature were notified of the patch in a post on Chrysler's website that didn't offer any details or acknowledge Miller and Valasek's research. "[Fiat Chrysler Automobiles] has a program in place to continuously test vehicles systems to identify vulnerabilities and develop solutions," reads a statement a Chrysler spokesperson sent to WIRED. "FCA is committed to providing customers with the latest software updates to secure vehicles against any potential vulnerability."

If consumers don't realize this is an issue, they should, and they should start complaining to carmakers. This might be the kind of software bug most likely to kill someone.

Unfortunately, Chrysler's patch must be manually implemented via a USB stick or by a dealership mechanic. That means many—if not most—of the vulnerable Jeeps will likely stay vulnerable. Chrysler stated in a response to questions from WIRED that it "appreciates" Miller and Valasek's work. But the company also seemed leery of their decision to publish part of their exploit. "Under no circumstances does FCA condone or believe it's appropriate to disclose 'how-to information' that would potentially encourage, or help enable hackers to gain unauthorized and unlawful access to vehicle systems," the company's statement reads. "We appreciate the contributions of cybersecurity advocates to augment the industry's understanding of potential vulnerabilities. However, we caution advocates that in the pursuit of improved public safety they not, in fact, compromise public safety."

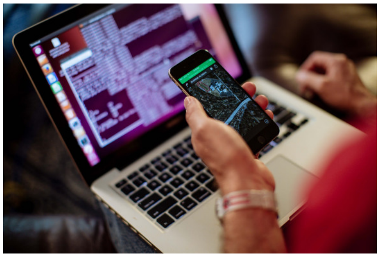
The two researchers say that even if their code makes it easier for malicious hackers to attack unpatched Jeeps, the release is nonetheless warranted because it allows their work to be proven through peer review. It also sends a message: Automakers need to be held accountable for their vehicles' digital security. "If consumers don't realize this is an issue, they should, and they should start complaining to carmakers," Miller says. "This might be the kind of software bug most likely to kill someone."

In fact, Miller and Valasek aren't the first to hack a car over the Internet. In 2011 a team of researchers from the University of Washington and the University of California at San Diego showed that they could wirelessly disable the locks and brakes on a sedan. But those academics took a more discreet approach, keeping the identity of the hacked car secret and sharing the details of the exploit only with carmakers.

Miller and Valasek represent the second act in a good-cop/bad-cop routine. Carmakers who failed to heed polite warnings in 2011 now face the possibility of a public dump of their vehicles' security flaws. The result could be product recalls or even civil suits, says UCSD computer science professor Stefan Savage, who worked on the 2011 study. "Imagine going up against a class-action lawyer after Anonymous decides it would be fun to brick all the Jeep Cherokees in California," Savage says.2

For the auto industry and its watchdogs, in other words, Miller and Valasek's release may be the last warning before they see a full-blown zero-day attack. "The regulators and the industry can no longer count on the idea that exploit code won't be in the wild," Savage says. "They've been thinking it wasn't an imminent danger you needed to deal with. That implicit assumption is now dead."

471,000 Hackable Automobiles



Miller and Valasek's exploit uses a burner phone's cellular connection to attack the Jeep's internet-connected entertainment system. WHITNEY CURTIS FOR WIRED

Sitting on a leather couch in Miller's living room as a summer storm thunders outside, the two researchers scan the Internet for victims.

Uconnect computers are linked to the Internet by Sprint's cellular network, and only other Sprint devices can talk to them. So Miller has a cheap Kyocera Android phone connected to his battered MacBook. He's using the burner phone as a Wi-Fi hot spot, scouring for targets using its thin 3G bandwidth.

A set of GPS coordinates, along with a vehicle identification number, make, model, and IP address, appears on the laptop screen. It's a Dodge Ram. Miller plugs its GPS coordinates into Google Maps to reveal that it's cruising down a highway in Texarkana, Texas. He keeps scanning, and the next vehicle to appear on his screen is a Jeep Cherokee driving around a highway cloverleaf between San Diego and Anaheim, California. Then he locates a Dodge Durango, moving along a rural road somewhere in the Upper Peninsula of Michigan. When I ask him to keep scanning, he hesitates.

Seeing the actual, mapped locations of these unwitting strangers' vehicles—and knowing that each one is vulnerable to their remote attack—unsettles him.

When Miller and Valasek first found the Uconnect flaw, they thought it might only enable attacks over a direct Wi-Fi link, confining its range to a few dozen yards. When they discovered the Uconnect's cellular vulnerability earlier this summer, they still thought it might work only on vehicles on the same cell tower as their scanning phone, restricting the range of the attack to a few dozen miles. But they quickly found even that wasn't the limit. "When I saw we could do it anywhere, over the Internet, I freaked out," Valasek says. "I was frightened. It was like, holy fuck, that's a vehicle on a highway in the middle of the country. Car hacking got real, right then."

That moment was the culmination of almost three years of work. In the fall of 2012, Miller, a security researcher for Twitter and a former NSA hacker, and Valasek, the director of vehicle security research at the consultancy IOActive, were inspired by the UCSD and University of Washington study to apply for a car-hacking research grant from Darpa. With the resulting $80,000, they bought a Toyota Prius and a Ford Escape. They spent the next year tearing the vehicles apart digitally and physically, mapping out their electronic control units, or ECUs—the computers that run practically every component of a modern car—and learning to speak the CAN network protocol that controls them.

When they demonstrated a wired-in attack on those vehicles at the DefCon hacker conference in 2013, though, Toyota, Ford, and others in the automotive industry downplayed the significance of their work, pointing out that the hack had required physical access to the vehicles. Toyota, in particular, argued that its systems were "robust and secure" against wireless attacks. "We didn't have the impact with the manufacturers that we wanted," Miller says. To get their attention, they'd need to find a way to hack a vehicle remotely.

Charlie Miller. WHITNEY CURTIS FOR WIRED

So the next year, they signed up for mechanic's accounts on the websites of every major automaker and downloaded dozens of vehicles' technical manuals and wiring diagrams. Using those specs, they rated 24 cars, SUVs, and trucks on three factors they thought might determine their vulnerability to hackers: How many and what types of radios connected the vehicle's systems to the Internet; whether the Internet-connected computers were properly isolated from critical driving systems, and whether those critical systems had "cyberphysical" components—whether digital commands could trigger physical actions like turning the wheel or activating brakes.

Based on that study, they rated Jeep Cherokee the most hackable model. Cadillac's Escalade and Infiniti's Q50 didn't fare much better; Miller and Valasek ranked them second- and third-most vulnerable. When WIRED told Infiniti that at least one of Miller and Valasek's warnings had been borne out, the company responded in a statement that its engineers "look forward to the findings of this [new] study" and will "continue to integrate security features into our vehicles to protect against cyberattacks." Cadillac emphasized in a written statement that the company has released a new Escalade since Miller and Valasek's last study, but that cybersecurity is "an emerging area in which we are devoting more resources and tools," including the recent hire of a chief product cybersecurity officer.

After Miller and Valasek decided to focus on the Jeep Cherokee in 2014, it took them another year of hunting for hackable bugs and reverse-engineering to prove their educated guess. It wasn't until June that Valasek issued a command from his laptop in Pittsburgh and turned on the windshield wipers of the Jeep in Miller's St. Louis driveway.

Since then, Miller has scanned Sprint's network multiple times for vulnerable vehicles and recorded their vehicle identification numbers. Plugging that data into an algorithm sometimes used for tagging and tracking wild animals to estimate their population size, he estimated that there are as many as 471,000 vehicles with vulnerable Uconnect systems on the road.

Pinpointing a vehicle belonging to a specific person isn't easy. Miller and Valasek's scans reveal random VINs, IP addresses, and GPS coordinates. Finding a particular victim's vehicle out of thousands is unlikely through the slow and random probing of one Sprint-enabled phone. But enough phones scanning together, Miller says, could allow an individual to be found and targeted. Worse, he suggests, a skilled hacker could take over a group of Uconnect head units and use them to perform more scans—as with any collection of hijacked computers—worming from one dashboard to the next over Sprint's network. The result would be a wirelessly controlled automotive botnet encompassing hundreds of thousands of vehicles.

"For all the critics in 2013 who said our work didn't count because we were plugged into the dashboard," Valasek says, "well, now what?"

Chris Valasek. WHITNEY CURTIS FOR WIRED

Congress Takes on Car Hacking

Now the auto industry needs to do the unglamorous, ongoing work of actually protecting cars from hackers. And Washington may be about to force the issue.

Later today, senators Markey and Blumenthal intend to reveal new legislation designed to tighten cars' protections against hackers. The bill (which a Markey spokesperson insists wasn't timed to this story) will call on the National Highway Traffic Safety Administration and the Federal Trade Commission to set new security standards and create a privacy and security rating system for consumers. "Controlled demonstrations show how frightening it would be to have a hacker take over controls of a car," Markey wrote in a statement to WIRED. "Drivers shouldn't have to choose between being connected and being protected…We need clear rules of the road that protect cars from hackers and American families from data trackers."

Markey has keenly followed Miller and Valasek's research for years. Citing their 2013 Darpa-funded research and hacking demo, he sent a letter to 20 automakers, asking them to answer a series of questions about their security practices. The answers, released in February, show what Markey describes as "a clear lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle." Of the 16 automakers who responded, all confirmed that virtually every vehicle they sell has some sort of wireless connection, including Bluetooth, Wi-Fi, cellular service, and radios. (Markey didn't reveal the automakers' individual responses.) Only seven of the companies said they hired independent security firms to test their vehicles' digital security. Only two said their vehicles had monitoring systems that checked their CAN networks for malicious digital commands.

UCSD's Savage says the lesson of Miller and Valasek's research isn't that Jeeps or any other vehicle are particularly vulnerable, but that practically any modern vehicle could be vulnerable. "I don't think there are qualitative differences in security between vehicles today," he says. "The Europeans are a little bit ahead. The Japanese are a little bit behind. But broadly writ, this is something everyone's still getting their hands around."

Miller (left) and Valasek demonstrated the rest of their attacks on the Jeep while I drove it around an empty parking lot. WHITNEY CURTIS FOR WIRED

Aside from wireless hacks used by thieves to open car doors, only one malicious car-hacking attack has been documented: In 2010 a disgruntled employee in Austin, Texas, used a remote shutdown system meant for enforcing timely car payments to brick more than 100 vehicles. But the opportunities for real-world car hacking have only grown, as automakers add wireless connections to vehicles' internal networks. Uconnect is just one of a dozen telematics systems, including GM Onstar, Lexus Enform, Toyota Safety Connect, Hyundai Bluelink, and Infiniti Connection.

In fact, automakers are thinking about their digital security more than ever before, says Josh Corman, the cofounder of I Am the Cavalry, a security industry organization devoted to protecting future Internet-of-things targets like automobiles and medical devices. Thanks to Markey's letter, and another set of questions sent to automakers by the House Energy and Commerce Committee in May, Corman says, Detroit has known for months that car security regulations are coming.

But Corman cautions that the same automakers have been more focused on competing with each other to install new Internet-connected cellular services for entertainment, navigation, and safety. (Payments for those services also provide a nice monthly revenue stream.) The result is that the companies have an incentive to add Internet-enabled features—but not to secure them from digital attacks. "They're getting worse faster than they're getting better," he says. "If it takes a year to introduce a new hackable feature, then it takes them four to five years to protect it."

Corman's group has been visiting auto industry events to push five recommendations: safer design to reduce attack points, third-party testing, internal monitoring systems, segmented architecture to limit the damage from any successful penetration, and the same Internet-enabled security software updates that PCs now receive. The last of those in particular is already catching on; Ford announced a switch to over-the-air updates in March, and BMW used wireless updates to patch a hackable security flaw in door locks in January.

Corman says carmakers need to befriend hackers who expose flaws, rather than fear or antagonize them—just as companies like Microsoft have evolved from threatening hackers with lawsuits to inviting them to security conferences and paying them "bug bounties" for disclosing security vulnerabilities. For tech companies, Corman says, "that enlightenment took 15 to 20 years." The auto industry can't afford to take that long. "Given that my car can hurt me and my family," he says, "I want to see that enlightenment happen in three to five years, especially since the consequences for failure are flesh and blood."

As I drove the Jeep back toward Miller's house from downtown St. Louis, however, the notion of car hacking hardly seemed like a threat that will wait three to five years to emerge. In fact, it seemed more like a matter of seconds; I felt the vehicle's vulnerability, the nagging possibility that Miller and Valasek could cut the puppet's strings again at any time.

The hackers holding the scissors agree. "We shut down your engine—a big rig was honking up on you because of something we did on our couch," Miller says, as if I needed the reminder. "This is what everyone who thinks about car security has worried about for years. This is a reality."

Update 3:30 7/24/2015: Chrysler has issued a recall for 1.4 million vehicles as a result of Miller and Valasek's research. The company has also blocked their wireless attack on Sprint's network to protect vehicles with the vulnerable software.

1Correction 10:45 7/21/2015: An earlier version of the story stated that the hacking demonstration took place on Interstate 40, when in fact it was Route 40, which coincides in St. Louis with Interstate 64.

2Correction 1:00pm 7/27/2015: An earlier version of this story referenced a Range Rover recall due to a hackable software bug that could unlock the vehicles' doors. While the software bug did lead to doors unlocking, it wasn't publicly determined to exploitable by hackers.

Answer the questions with the text above :

- What happened at the beginning of the experience ?

- Was this a suprise for the driver ?

- What does this mean for car builders ?

- What did the Hijackers do to better simulate the experience ?

- Is this the first experience of that kind ?

True or False : explain.

☞ *The developed tools can only trigger the dashboard functions.*

☞ *The hack enabled to control but not to keep cars under surveillance.*

- According to Miller, what is a interesting vulnerability for attackers ?

- Explain how Miller and Valasek could attack the car :

- What did Miller and Valasek with dozens of vehicles' technical manuals and wiring diagrams ?

Match the following ideas :

a. Uconnect computers	1. Miller and Valasek's release.
b. The auto industry watchdogs	2. confirmed that every vehicle had some sort of wireless connection.
c. Reveal new legislation	3. befriend hackers.
d. 16 automakers	4. tighten cars' protections against hackers.
e. carmakers	5. Sprint's cellular network.

7. *Transcripts of the videos*

Video 1 :

Transcript :

This is a thing, a robot, a wristwatch, a wind turbine. This is the Internet : digital information delivered to a personal device near you. Now the Internet connects two things other than a computer like your sunglasses, your kitchen, a highway system, a human heart. This is the Internet of Things : a vast network of embedded intelligence. By 2020 over 200 billion of things will be connected to and controlled by cloud computing giving us really cool stuff like intelligent cities, individualized health care, implanted electronics, quantum computing, autonomous vehicles, these and countless other smart things yet to be invented.
This is the ANSYS logo, it too is a thing, a symbol of innovation, a risk-free low cost virtual space, enabling engineers to quickly consider thousands of design options. Millions of tests scenarios using this thing, letting you test build and launch the most sophisticated products with absolute confidence.
This is simulation driven product development. Without it, the Internet of Things would not be possible. The complexity of smart devices could not be tested. Technology like Mems, Self-aware Sensors, Wireless Power Transfer, 3D Integrated Circuits, 5G Communication Speeds and Embedded Software all demand a totally new approach to product engineering.
The Internet of Things requires simulation tools that can mirror and manage this immense complexity. It requires a comprehensive multi visits platform to test whole systems, to test and validate complete virtual prototypes, it requires the most advanced simulation software on earth. If you're designed for the Internet of Things, ANSYS is just the thing you're looking for.

Video 2

Transcript :

By now you may have heard the term Internet of Things. It sounds interesting. But what does the Internet of Things actually mean ? IoT is an evolution of mobile, home and embedded applications that are being connected to the internet integrating greater compute capabilities and using data analytics to extract meaningful information.
Billions of devices will be connected to the internet and soon hundreds of billions of devices. As related devices connect with each other, they can become an intelligent system of systems and when these intelligent devices and systems of systems share data over the cloud and analyze it. They can transform our businesses, our lives, and our world in countless ways whether it's improving medical outcomes, creating better products faster with lower development costs, making shopping more enjoyable, or optimizing energy generation and consumption.
Here is an example of the big picture : imagine an intelligent device such as a smart traffic camera. The camera can monitor the road for congestion, accidents and weather conditions and communicate that status to a gateway that combines it with data from other cameras, creating an intelligent citywide traffic system. Now imagine that intelligent traffic system connected to other citywide transportation system which get data from their own intelligent devices creating an ever-larger intelligent system of sytems. The really big possibilities come from analyzing end and data across that system of systems.
For example, let's say the cities intelligent traffic system detect massive congestion due to an accident. That insight can be sent to the citywide transportation system which get analyze the accident impact on other city systems. Recognizing the accident is near the airport and two city schools, it could notify those systems so they can adjust flights and school schedules. You can also analyze and derive optimal routes around the accident and send those instructions to the city's digital sign-in system to guide drivers around the accident that's just one example of the potential benefits they can happen with intelligent devices share insight with other systems forming ever-expanding systems of systems.

But how do we get there ? Regardless of the solution, Intel processors are designed to help you get to market faster and easier. You can scale solutions across a variety of performance, power and price points with a single set of application code that runs on every Intel processor so what will you develop to help drive an accelerated Internet of Things.
We'd love to help, so please contact your local Intel representative of visit us on the web at www.intel.com/iot to find out more.