Impact of the Internet

- Impact
- Internet of Things
- Supplemental Reading for Internet of Things
- Gian: what he does in Android Security
- Privacy and Security
- Heather Adkins: keeping hackers out
- Learner Story: Melinda

Impact

There's no doubt that the Internet has made it much easier for us to connect with our friends and family. But it's also made it easier to connect with everyone else in the world. We're no longer confined to our local neighborhoods. Decades ago, if you wanted to sell something, you'd place your goods in your driveway and put up signs for a garage sale. The only way someone would see this is if they drove by your neighborhood and saw your sign. We got a little more savvy and started advertising in our local newspaper. We had to pay to list their ad, but at least we were able to reach more people in our neighborhood. Then the Internet boom happened, and we can use sites like Craigslist to post an advertisement for free and reach more people in our city. Then we were able to sell to people outside of our city, to cities and other states. Eventually, we could sell the people outside of our own country all thanks to the Internet. Globalization is the movement that let's governments, businesses, and organizations communicate and integrate together on an international scale. It's been made possible by the internet and information technology. Countries can communicate with each other faster. News happening on the other side of the world reaches us before we can blink and global and financial trade has increased dramatically. Globalization has transformed almost every aspect of human society as we know it. Media and social movements have become globalized too. In 2011, several countries in the Middle East started riots and protests against their government regimes, known as the Arab Spring protests. Because of outlets like social media, their movement gained worldwide attention and citizens of many different countries banded together to take collective action. Social media movements like this have been going on for years, gathering together people from all over the world and unifying them under a single cause. The Internet has also dramatically changed the way we consume entertainment. A few years ago, if you wanted to watch something on TV, you've got to actually sit in front of your TV right when it aired or else you'd miss it. Then we started recording our shows first on VHS and then on things like TiVo, so we can watch them later. But now we have access to more TV shows and movies than we can ever watch in our entire lifetime at our fingertips. What if you wanted to listen to a new song by your favorite band? You used to have to wait until they release their album in a store. You couldn't just buy one song, you had to buy the entire album on a CD, cassette tape, or even a vinyl record back in the day. If you want it to get the day's news, you had to wait until the next day when the newspaper would print it. Even then you weren't able to get a fraction of a fraction of a fraction of the news you can get on the Internet today. Retail stores aren't the only place you look when you want to buy something anymore. Now you can order food, clothes, books, and well, just about anything on the Internet. But you don't just buy stuff off the web. You can even get an education. Colleges and universities worldwide are taking education out of the classroom and putting it into your homes. Online courses are becoming a popular way for people to get a quality education at a more convenient location, time, and price. It's not just degrees. There's an almost infinite amount of educational tools available on the Internet. A few years ago, all this information on the Internet had to be reached through your laptop or desktop. Now, more than ever, people are going mobile and can access all of this information with their smartphones. It's truly an amazing time to be alive in this technological age. The takeaway here is that the only constant in the field of technology is change. As an IT support specialist, You'll have to stay on your toes to keep up with

this dynamic shifting landscape.

Internet of Things

You may have heard of the phrase Internet of Things or IoT. This concept is pretty new, but already has a major impact on the future of computing. The concept is fairly simple. Basically, more and more devices are being connected to the Internet in a smarter fashion. Did you know that there are now smart thermostats. Instead of manually programming them when you'll be out of the house, they'll just know when you leave and turn off the air conditioning for you. It's not just your thermostat. Many companies out there are making smarter household devices. There are fridges that can keep track of what foods you have in there, toasters that can be controlled by your smartphone, lights that can change depending on your mood and cars that drive you instead of you driving them. The world is moving towards connecting manual devices to the internet and making them smarter. These decisions have many societal implications though, especially when it comes to cybersecurity, or personal privacy. But there's also a huge potential for IoT to completely transform the world in ways we have yet to see. In the future, people may be shocked to learn that we had to do manual things like make your own coffee, or drive to the grocery store. While you may not experience working with an Internet of Things device, you should be aware that it will become a large part of the future of computing.

Supplemental Reading for Internet of Things

To learn more about the "Internet of Things," click here. (or just read my copy and paste below)

Smart toasters, connected rectal thermometers and fitness collars for dogs are just some of the everyday "dumb items" being connected to the web as part of the Internet of Things (IoT).

Connected machines and objects in factories offer the potential for a 'fourth industrial revolution', and experts predict more than half of new businesses will run on the IoT by 2020.

Here's everything you need to know about the increasingly connected world.

What is the Internet of Things?
In the broadest sense, the term IoT encompasses everything connected to the internet, but it is increasingly being used to define objects that "talk" to each other. "Simply, the Internet of Things is made up of devices – from simple sensors to smartphones and wearables – connected together," Matthew Evans, the IoT programme head at techUK, says.

By combining these connected devices with automated systems, it is possible to "gather information, analyse it and create an action" to help someone with a particular task, or learn from a process. In reality, this ranges from smart mirrors to beacons in shops and beyond.

"It's about networks, it's about devices, and it's about data," Caroline Gorski, the head of IoT at Digital Catapult explains. IoT allows devices on closed private internet connections to communicate with others and "the Internet of Things brings those networks together. It gives the opportunity for devices to communicate not only within close silos but across different networking types and creates a much more connected world."

Why do connected devices need to share data?
An argument has been raised that only because something can be connected to the internet doesn't mean it should be, but each device collects data for a specific purpose that may be useful to a buyer and impact the wider economy.

Within industrial applications, sensors on product lines can increase efficiency and cut down on waste. One study estimates 35 per cent of US manufacturers are using data from smart sensors within their set-ups already. US firm Concrete Sensors has created a device that can be inserted into concrete to provide data on the material's condition, for instance.

"IoT offers us opportunity to be more efficient in how we do things, saving us time, money and often emissions in the process," Evans says. It allows companies, governments and public authorities to re-think how they deliver services and produce goods.

"The quality and scope of the data across the Internet of Things generates an opportunity for much more contextualised and responsive interactions with devices to create a potential for change," continued Gorski. It "doesn't stop at a screen".

The latest Internet of Things news

Where does the IoT go next?

Even those who have purchased one of the myriad smart home products – from lightbulbs, switches, to motion sensors – will attest to the fact IoT is in its infancy. Products don't always easily connect to each other and there are significant security issues that need to be addressed.

A report from Samsung says the need to secure every connected device by 2020 is "critical". The firm's Open Economy document says "there is a very clear danger that technology is running ahead of the game". The firm said more than 7.3 billion devices will need to be made secure by their manufacturers before 2020.

“We are looking at a future in which companies will indulge in digital Darwinism, using IoT, AI and machine learning to rapidly evolve in a way we’ve never seen before," Brian Solis, from Altimeter Group, who helped on the research said.

IoT botnets, created using a network of out-of-date devices took large websites and services offline in 2016. A Chinese firm later recalled 4.3 million unsecured connected cameras. The ease of bringing down the internet using IoT devices was revealed when instead of malicious purposes, the botnet was revealed to have been created to game Minecraft.

But aren't there privacy implications?

Everything that's connected to the internet can be hacked, IoT products are no exception to this unwritten rule. Insecure IoT systems led to toy manufacturer VTech losing videos and pictures of children using its connected devices.

There's also the issue of surveillance. If every product becomes connected then there's the potential for unbridled observation of users. If a connected fridge tracks food usage and consumption, takeaways could be targeted at hungry people who have no food. If a smartwatch can detect when you're having sex, what is to stop people with that data using it against the watches' wearer.

“In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials,” James Clapper, the US direction or national intelligence said in 2016. Wikileaks later claimed the CIA has been developing security exploits for a connected Samsung TV.

We need reliable standards

At the centre of creating a vast, reliable IoT network lies one significant issue: compatible standards. Connected objects need to be able to speak to each other to transfer data and share what they are recording. If they all run on different standards, they struggle to communicate and share. The Institute of Electrical and Electronics Standards Association lists a huge number of standards being developed and worked on for different applications.

"Additional needs are emerging for standardisation," the Internet Society says. If standardisation happens it will let more devices and applications be connected.

To try and tackle this issue on an enterprise scale, Microsoft has introduced its own system for IoT devices. Called IoT Central, TechCrunch, reports the system gives businesses a managed central platform for setting up IoT devices. Microsoft claims the system will simply the creation of IoT networks.

Gorski described IoT, even among those with the most experience of the concept, as a "relatively immature market" but said 2016 may have been a turning point. The Hypercat standard is now supported by ARM, Intel, Amey, Bae Systems and Accenture and the firms are currently agreeing on a format for "exposing collections" of URLs, for example.

"In the short term, we know [IoT] will impact on anything where there is a high cost of not intervening," Evans said. "And it'll be for simpler day-to-day issues – like finding a car parking space in busy areas, linking up your home entertainment system and using your fridge webcam to check if you need more milk on the way home.

"Ultimately what makes it exciting is that we don't yet know the exact use cases and just that it has the potential to have a major impact on our lives."

This article was originally published in march 2023 It has since been updated with further IoT information.

Heads up: A big part of being successful in an IT role is the ability to be a self-led learner -- someone who finds key resources and reads up on the latest tech trends and solutions. The supplemental readings we've provided have been designed to show you just some of the support materials available to you online; they're not meant to be considered a comprehensive list. Feel free to add to the conversation by posting other useful resources for learners to this forum thread.

Gian: what he does in Android Security

My name is Gian Bokassa, and I'm a Program Manager with the Android Security Team. The Android Security Team is responsible for protecting over two billion Android devices are on the world. But specifically, what I do with the team is I work with anywhere from the end-users to our partners, all the way up to the engineering teams within Google on each Android dessert release, which is what we call versions of Android. Depending on what needs to be done for that release and that cycle, I'm the person. We have lots of discussions with external partners and phone manufacturers on helping them adopt new security features that run on Android for their next phone release. Internally, we're always trying to think one step ahead and try and think of what the next vulnerability or next area that we can improve the platform exists in. Security is important to everyone in the chain because as more and more of our data becomes digitized, it's even more important to keep it all protected. From a programming perspective, you can say build a secure system. But if there's one flaw somewhere in that software and that flaw could be one byte. The whole system could be open insecure and anyone can just take it down.

Privacy and Security

The added convenience made possible by the Internet also makes it harder and harder for us to maintain anonymity. When you purchase something online, you're buying habits can be logged, and you may be targeted with marketing, even when you want to do something simple, like book a dinner reservation, your name, phone number, email, and maybe even a credit card number are required. Now think about the information you post publicly; name, pictures, family, friends, and even your location may be available to anyone online. Be aware of what you're sharing by reviewing the privacy policy of the service before you use it. It's up to you to decide if the trade-offs of a service are worth sharing your personal information. In most cases, companies are trying to build great products that make our lives easier. They may offer their products for free because you provide them with free data. Just make sure your information won't fall into the wrong hands. Privacy doesn't just affect us on a personal scale. It's also become a concern for governments. In Europe, data regulation and privacy are strictly protected to help EU citizens gain more control over their personal information. COPPA, or the Children's Online Privacy Protection Act, also regulates the information we show to children under the age of 13. There are many more examples of government regulation of privacy. It's no longer something we can think of on an individual scale. Another concern that's grown with the rise of the Internet is the issue of copyright. Imagine you create a beautiful graphic and upload it on the web for your friends to see, then some random stranger takes your graphic, claims that as their own, and sells it for profit. Thankfully, several companies have been founded and designed specifically to help solve this issue of copyright and intellectual property theft. There are also efforts in place that you've learned about, like open source projects that benefit from being on the Internet. In these cases, open collaboration allows a project to thrive. On top of privacy and copyright considerations, computer security is another issue that you may face in both your personal and professional life. More and more companies are being targeted in cybersecurity attacks. For example, the WannaCry attack that started in Europe, infected hundreds of thousands of computers across the world. The financial loss of that attack has been estimated at over a billion dollars. Hospital computers were even infected. In a critical life threatening moment, every second matters. Not being able to perform basic medical duties, like pulling medical records took time away from doctors and nurses, and more importantly, the lives of their patients. Before the WannaCry attack, there were lots of other worldwide attacks. In 2011, the Sony PlayStation network was attacked and around 77 million user accounts had personal information exposed. Everything from entire governments to businesses that handle the data of millions of people have been compromised. Computer security is no longer the job of specialized security engineers. It's everyone's responsibility. As an IT support specialist, you'll need to have a fundamental understanding of computer security. I spend every day working in security. I love working in the field because I get to help protect people and their devices from all over the globe.

Heather Adkins: keeping hackers out

My name is Heather Adkins. I'm director of information security and privacy here at Google. And our job is to keep the hackers out. Every day at Google for me is a new day. It's like a new job every day. Hackers are very interesting and very diverse in the way that they do things. They're either hacking for fun and fame because they're intellectually curious and they want to understand how things work. Or they're hacking for money because they want to steal money from people or they're hacking because they want to steal information. And so for us we try to understand how the hackers work so that we can understand what kinds of things we have to do to prevent them from doing it. You have to understand how the internals work, you have to understand how the programmer built it, and this is really thrilling. You get to ride alongside the programmer and understand what they were thinking when they were designing the software and anticipate what mistakes they might have made. We prepare for being hacked by understanding how hacking works. And this is often the most exciting part of our work because we get to break the systems and I think a lot of us who get into the field think what would it be like to rob a bank, what would it be like to hack into a system? And here we get to play the other side of that. So we have hackers of our own who hack our systems and tell us how they did it. And we also study how the actual attackers in the world are hacking other people. I think that the field of security is so exciting for us, those of us who do it as a profession, because it's changing all the time. That presents us with new challenges every single day. And it also appeals to us, I think because it means that we're protecting users. Google has a service offered to billions of people on the planet, and we do it because we want to protect them.

Learner Story: Melinda

The world changes. Things change. I was cleaning up the other day, and I was throwing away old disks from our first computer, those little floppy disks. Nobody use that anymore. But I thought floppy disks were cool back then. So if I weren't a lifelong learner, I'd still be stuck like that floppy disk. I believe it's never too late to go in a new direction, and I think IT is my thing. I think that's going to be my thing.