12 MIN READ

Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns

View all articles

BY NERMIN HAJDARBEGOVIC - TECHNICAL EDITOR @ TOPTAL

#InternetOfThings #IoT #IoTSecurity

850 SHARES

The Internet of Things (IoT) has been an industry buzzword for years, but sluggish development and limited commercialization have led some industry watchers to start calling it the “Internet of NoThings”.

Double puns aside, IoT development is in trouble. Aside from spawning geeky jokes unfit for most social occasions, the hype did not help; and, in fact, I believe it actually caused a lot more harm than good. There are a few problems with IoT, but all the positive coverage and baseless hype are one we could do without. The upside of generating more attention is clear: more investment, more VC funding, more consumer interest.

THE INTERNET
OF
INSECURE
THINGS

However, these come with an added level of scrutiny, which has made a number of shortcomings painfully obvious. After a couple of years of bullish forecasts and big promises, IoT security seems to be the biggest concern. The first few weeks of 2015 were not kind to this emerging industry, and most of the negative press revolved around security.

Was it justified? Was it just “fear, uncertainty and doubt” (FUD), brought about by years of hype? It was a bit of both; although some issues may have been overblown, the problems are very real, indeed.

From “Year Of IoT” To Annus Horribilis For IoT

Many commentators described 2015 as “the year of IoT,” but so far, it has been a year of bad press. Granted, there are still ten months to go, but negative reports keep piling on. Security firm Kaspersky recently ran a damning critique of IoT security challenges, with an unflattering headline, “*Internet of Crappy Things*”.

Kaspersky is no stranger to IoT criticism and controversy; the firm has been sounding alarm bells for a while, backing them up with examples of hacked smart homes, carwashes and even police surveillance systems. Whether a hacker wants to wash their ride free of charge, or stalk someone using their fitness tracker – IoT security flaws could make it possible.

Wind River published a white paper on IoT security in January 2015, and the report starts off with a sobering introduction. Titled *Searching For The Silver Bullet*, it summarizes the problem in just three paragraphs, which I will condense into a few points:

- Security must be the foundational enabler for IoT.
- There is currently no consensus on how to implement security in IoT on the device.

- A prevalent, and unrealistic, expectation is that it is somehow possible to compress 25 years of security evolution into novel IoT devices.
- There is no silver bullet that can effectively mitigate the threats.

However, there is some good news; the knowledge and experience are already here, but they have to be adapted to fit the unique constraints of IoT devices.

Unfortunately, this is where we as system security developers stumble upon another problem, a hardware problem.

U.S. Federal Trade Commission chairwoman, Edith Ramirez, addressed the Consumer Electronics Show in Las Vegas earlier this year, warning that embedding sensors into everyday devices, and letting them record what we do, could pose a massive security risk.

Ramirez outlined three key challenges for the future of IoT:

- Ubiquitous data collection.
- Potential for unexpected uses of consumer data.
- Heightened security risks.

She urged companies to enhance privacy and built secure IoT devices by adopting a security-focused approach, reducing the amount of data collected by IoT devices, and increasing transparency and providing consumers with a choice to opt-out of data collection.

Ramirez went on to say that developers of IoT devices have not spent time thinking about how to secure their

"The small size and limited processing power of many connected devices could inhibit encryption and other robust security measures," said Ramirez. "Moreover, some connected devices are low-cost and essentially disposable. If a vulnerability is discovered on that type of device, it may be difficult to update the software or apply a patch – or even to get news of a fix to consumers."

While Ramirez is spot on in most respects, I should note that the Internet went through a similar phase two decades ago. There were a lot of security concerns, and the nineties saw the emergence of the internet-borne malware, DDoS attacks, sophisticated phishing and more. Even though Hollywood depicted a dystopian future in some films, we have ended up with kittens on social networks and a high-profile security breach here and there.

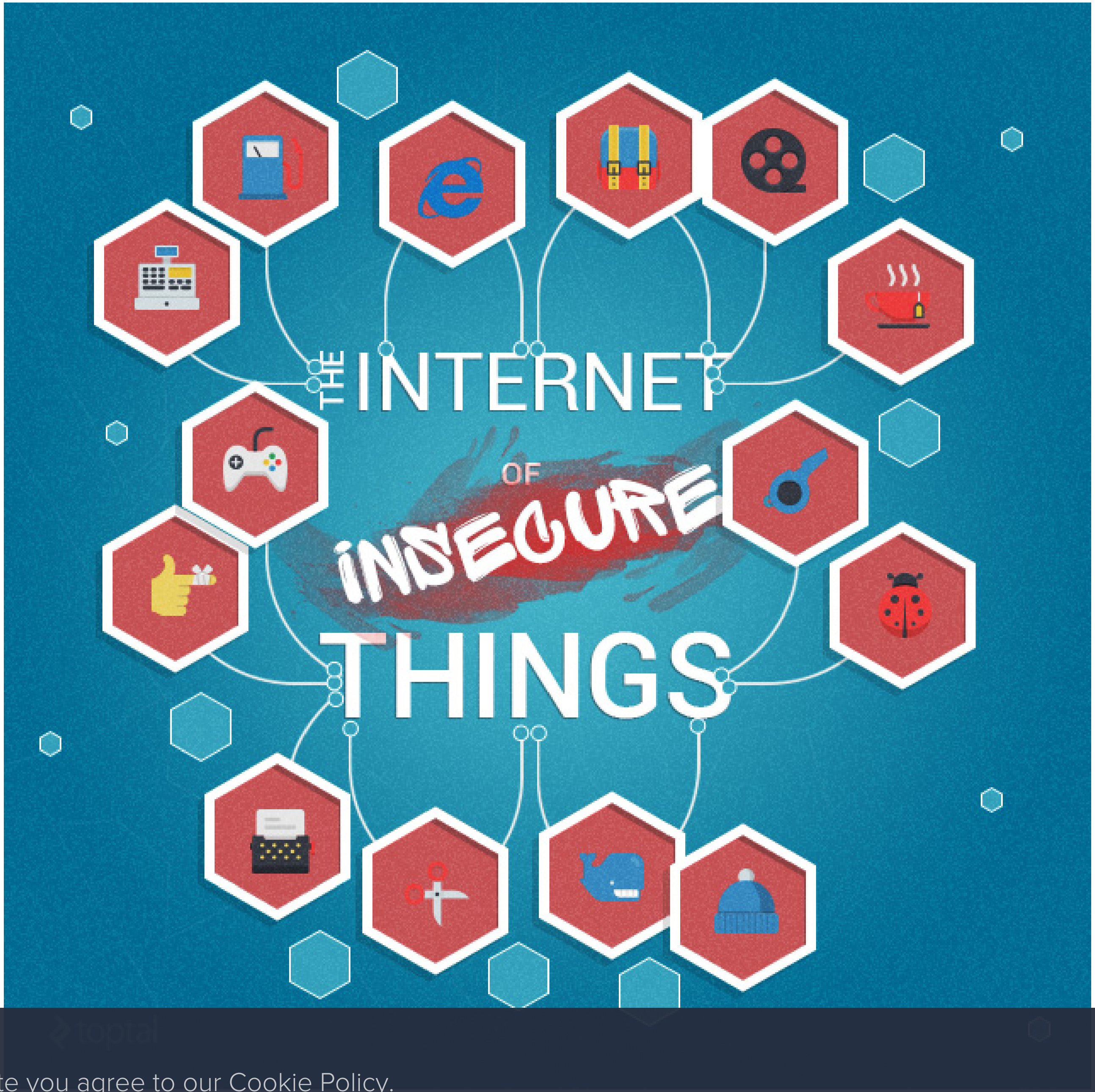
The Internet is still not secure, so we can't expect IoT to be secure, either. However, security is constantly evolving to meet new challenges, we've seen it before, and we'll see it again, with IoT and subsequent connected technologies.

IoT Hardware Is And Will Remain A Problem

Some of you will be thinking that the hardware issues mentioned by the FTC boss will be addressed; yes, some of them probably will.

As the IoT market grows, we will see more investment, and as hardware matures, we will get improved security. Chipmakers like Intel and ARM will be keen to offer better security with each new generation, since security could be a market differentiator, allowing them to grab more design wins and gain a bigger share.

Technology always advances, so why not? New manufacturing processes generally result in faster and more efficient processors, and sooner or later, the gap will close, thus providing developers with enough processing power to implement better security features. However, I am not so sure this is a realistic scenario.


THE INTERNET
OF
INSECURE
THINGS
toptal

First of all IoT chips won't be big money-makers since they are tiny and usually based on outdated architectures. For example, the first-generation Intel Edison platform is based on Quark processors, which essentially use the same CPU instruction set and much of the design of the ancient Pentium P54C. However, the next-generation Edison microcomputer is based on a much faster processor, based on Atom Silvermont cores, which is in many Windows and Android tablets, today. (Intel shipped ~46m Bay Trail SoCs in 2014.)

On the face of it, we could end up with relatively modern 64-bit x86 CPU cores in IoT devices, but they won't come cheap, they will still be substantially more complex than the smallest ARM cores, and therefore will need more battery power.

Cheap and disposable wearables, which appear to be the FTC's biggest concern, won't be powered by such chips, at least, not anytime soon. Consumers may end up with more powerful processors, such as Intel Atoms or ARMv8 chips, in some smart products, like smart refrigerators or washing machines with touchscreens, but they are impractical for disposable devices with no displays and with limited battery capacity.

Selling complete platforms, or reference designs for various IoT devices, could help chipmakers generate more revenue, while at the same time introduce more standardisation and security. The last thing the industry needs is more unstandardized devices and more fragmentation. This may sound like a logical and sound approach, since developers would end up with fewer platforms and more resources would be allocated for security, however, security breaches would also affect a bigger number of devices.

Money Is Pouring In, Analysts Remain Bullish, What Could Possibly Go Wrong?

One of the most common ways of tackling any problem in the tech industry is to simply throw money at it. So, let's see where we stand right now in terms of funding rather than technology.

According to research firms IDC and Gartner, IoT will grow to such an extent that it will transform the data centre industry by the end of the decade. Gartner expects the IoT market will have 26 billion installed units by 2020, creating huge opportunities for all parties, from data centres and hardware makers, to developers and designers. IDC also expects the IoT industry to end up with "billions of devices and trillions of dollars" by the end of the decade.

Gartner's latest IoT market forecast published in May 2014 also includes a list of potential challenges, some of which I've already covered:

- **Security:** Increased automation and digitization creates new security concerns.
- **Enterprise:** Security issues could pose safety risks.
- **Consumer Privacy:** Potential of privacy breaches.
- **Data:** Lots of data will be generated, both for big data and personal data.
- **Storage Management:** Industry needs to figure out what to do with the data in a cost-effective manner.
- **Server Technologies:** More investment in servers will be necessary.

- **Data Centre Network:** WAN links are optimised for human interface applications, IoT is expected to dramatically change patterns by transmitting data automatically.

All these points (and more) must be addressed sooner or later, often at a substantial cost. We are no longer talking about tiny IoT chips and cheap toys based on such chips, this is infrastructure. This is a lot of silicon in server CPUs, expensive DDR4 ECC RAM and even bigger SSDs, all housed in expensive servers, in even bigger data centres.

That's just the tip of the iceberg; industry must tackle bandwidth concerns, data management and privacy policies, and security. So how much money does that leave for security, which is on top of Gartner's list of IoT challenges?

A lot of money is already pouring into the industry, VCs are getting on board and the pace of investment appears to be picking up. There were also a number of acquisitions, often involving big players like Google, Qualcomm, Samsung, Gemalto, Intel and others. There is a list of IoT-related investments on Postscapes. The trouble with many of these investments, especially those coming from VCs, is that they tend to focus on "shiny" things, devices that can be marketed soon, with a potentially spectacular ROI. These investments don't do much for security or infrastructure, which would basically have to trail IoT demand.

Big players will have to do the heavy lifting, not VC-backed startups and toymakers. Agile and innovative startups will certainly play a big role by boosting adoption and creating demand, but they can't do everything.

So let's think of it this way, even a small company can build a car, or tens of thousands of cars, but it can't build highways, roads, petrol stations and refineries. That same small company can build a safe vehicle using off-the-shelf technology to meet basic road safety standards, but it couldn't build a Segway-like vehicle that would meet the same safety standards, nor could anyone else. Automotive safety standards could never apply to such vechicles, we don't see people commuting to work on Segways, so we cannot expect the traditional tech security standard to apply to underpowered IoT devices, either.

Having commuters checking their email or playing Candy Crush while riding their Segways through rush hour traffic does not sound very safe, does it? So why should we expect IoT devices to be as safe as other connected devices, with vastly more powerful hardware and mature operating systems? It may be a strange analogy, but the bottom line is that IoT devices cannot be expected to conform to the same security standards as fully fledged computers.

But Wait, There Weren't That Many IoT Security Debacles...

True, we don't see a lot of headlines about spectacular IoT security breaches, but let me put it this way: how many security related headlines did you see about Android Wear? One? Two? None? It is estimated there are fewer than a million Android Wear devices in the wild, so they're simply not a prime target for hackers, or a subject for security researchers.

How many IoT devices do you own and use right now? How many does your business use? That's where the "Internet of NoThings" joke comes from, most people don't have any. The numbers keep going up, but the average consumer is not buying many, so where is that growth coming from? IoT devices are out there and the numbers are booming, driven by enterprise rather than the consumer market.

Verizon and ABI Research estimate that there were 1.2 billion different devices connected to the internet last year, but by 2020, they expect as many as 5.4 billion B2B IoT connections.

Smart wristbands, toasters and dog collars aren't a huge concern from a security perspective, but Verizon's latest IoT report focuses on something a bit more interesting: enterprise.

The number of Verizon's machine-to-machine (M2M) connections in the manufacturing sector increased by 204 percent from 2013 to 2014, followed by finance and insurance, media and entertainment, healthcare, retail and transportation. The Verizon report includes a breakdown of IoT trends in various industries, so it offers insight into the business side of things.

The overall tone of the report is upbeat, but it also lists a number of security concerns. Verizon describes security breaches in the energy industry as “unthinkable,” describes IoT security as “paramount” in manufacturing, and let’s not even bring up potential risks in healthcare and transportation.

How And When Will We Get A Secure Internet of Things?

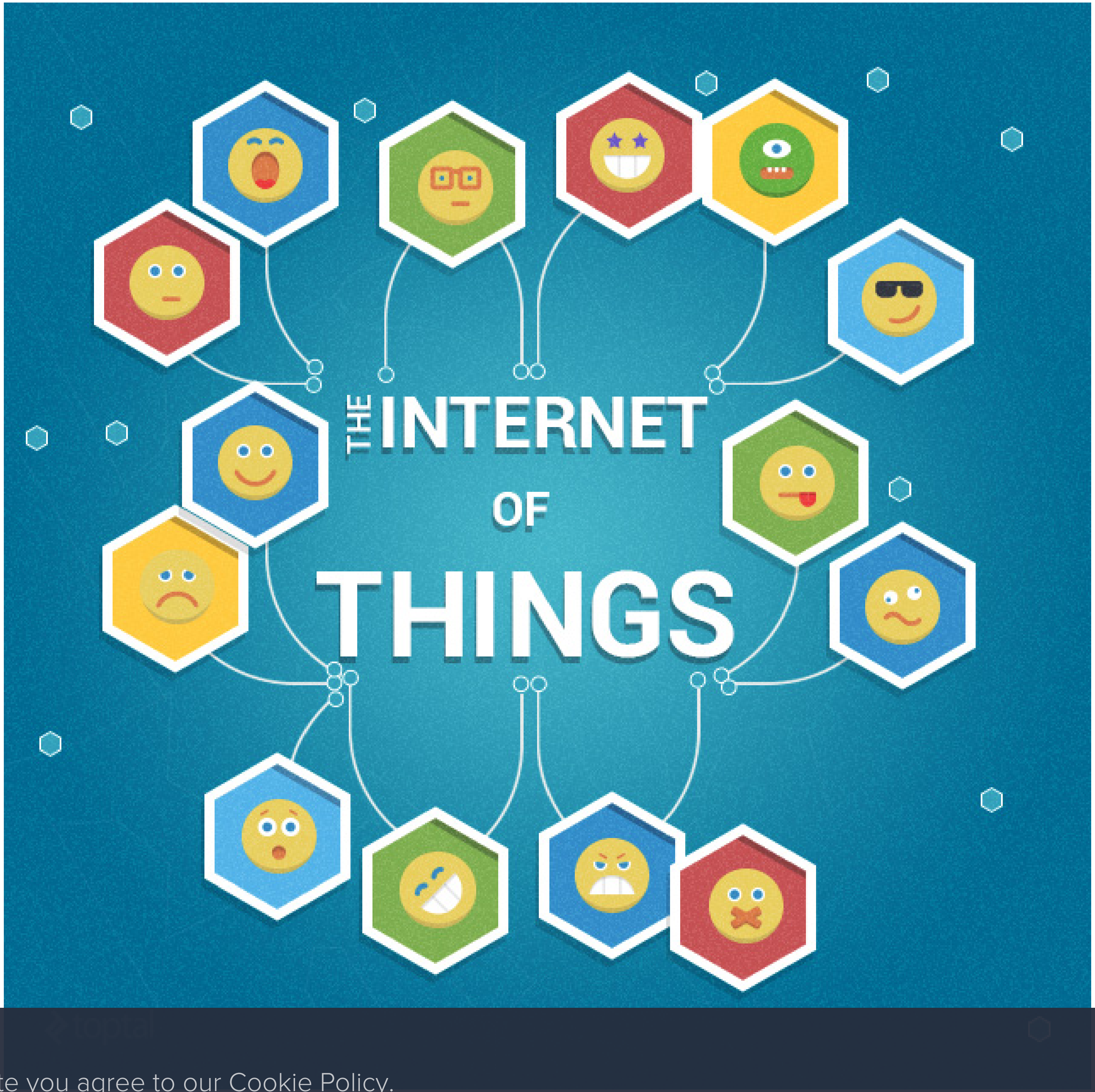
I will not try to offer a definitive answer on how IoT security challenges can be resolved, or when. The industry is still searching for answers and there is a long way to go. Recent studies indicate that the majority of currently available IoT devices have security vulnerabilities. HP found that as many 70 percent of IoT devices are vulnerable to attack.

While growth offers a lot of opportunities, IoT is still not mature, or secure. Adding millions of new devices, hardware endpoints, billions of lines of code, along with more infrastructure to cope with the load, creates a vast set of challenges, unmatched by anything we have experienced over the past two decades.

That is why I am not an optimist.

I don’t believe the industry can apply a lot of security lessons to IoT, at least not quickly enough, not over the next couple of years. In my mind, the Internet analogy is a fallacy, simply because the internet of the nineties did not have to deal with such vastly different types of hardware. Using encryption and wasting clock cycles on security is not a problem on big x86 CPUs or ARM SoCs, but it won’t work the same way with tiny IoT devices with a fraction of the processing power and a much different power consumption envelope.

More elaborate processors, with a biger die, need bigger packaging and have to dissipate more heat. They also need more power, which means bigger, heavier, more expensive batteries. To shave off weight and reduce bulk, manufacturers would have to resort to using exotic materials and production techniques. All of the above would entail more R&D spending, longer time-to-market and a bigger bill of materials. With substantially higher prices and a premium build, such devices could hardly be considered disposable.


THE INTERNET
OF
THINGS
toptal

So what has to be done to make IoT secure? A lot. And everyone has a role to play, from tech giants to individual developers.

Let’s take a look at a few basic points, such as what can be done, and what is being done, to improve IoT security now:

- Emphasise security from day one
- Lifecycle, future-proofing, updates
- Access control and device authentication
- Know your enemy
- Prepare for security breaches

A clear emphasis on security from day one is always a good thing, especially when dealing with immature technologies and underdeveloped markets. If you are planning to develop your own IoT infrastructure, or deploy an existing solution, do your research and stay as informed as possible. This may involve trade-offs, as you could be presented with a choice of boosting security at the cost of compromising the user experience, but it’s worth it as long as you strike the right balance. This cannot be done on the fly, you have to plan ahead, and plan well.

In the rush to bring new products and services to market, many companies are likely to overlook long-term support. It happens all the time, even in the big leagues, so we always end up with millions of unpatched and insecure computers and mobile devices. They are simply too old for most companies to bother with, and it is bound to be even worse with disposable IoT devices. Major phone vendors don’t update their software on 2-3 year old phones, so imagine what will happen with $20 IoT devices that might be on your network for years. Planned obsolescence may be a part of it, but the truth is that updating old devices does not make much financial sense for the manufacturer since they have better things to do with their resources. Secure IoT devices would either have to be secure by design and impervious from the start, or receive vital updates throughout their lifecycle, and I'm sure you will agree neither option sounds realistic, at least, not yet.

Implementing secure access control and device authentication sounds like an obvious thing to bring up, but we are not dealing with your average connected device here. Creating access controls, and authentication methods, that can be implemented on cheap and compact IoT devices without compromising the user experience, or adding unnecessary hardware, is harder than it seems. As I mentioned earlier, lack of processing power is another problem, as most advanced encryption techniques simply wouldn't work very well, if at all. In a previous post, I looked at one alternative, outsourcing encryption via the blockchain technology; I am not referring to the Bitcoin blockchain, but similar crypto technologies that are already being studied by several industry leaders.

Si vis pacem, para bellum – if you want peace, prepare for war. It is vital to study threats and potential attackers before tackling IoT security. The threat level is not the same for all devices and there are countless considerations to take into account; would someone rather hack your daughter's teddy bear, or something a bit more serious? It's necessary to reduce data risk, keep as much personal data as possible from IoT devices, properly secure necessary data transfers, and so on. However, to do all this, you first need to study the threat.

If all else fails, at least be prepared for potential security breaches. Sooner or later they will happen, to you or someone else (well, preferably a competitor). Always have an exit strategy, a way of securing as much data as possible and rendering compromised data useless without wrecking your IoT infrastructure. It is also necessary to educate customers, employees and everyone else involved in the process about the risks of such breaches. Instruct them in what to do in case of a breach, and what to do to avoid one.

Of course, a good disclaimer and TOS will also help if you end up dealing with the worst-case scenario.

Don't miss out. Get the latest updates first.

Enter your email address...

No spam. Just great articles & insights.

Get Exclusive Updates

18 Comments Toptal 1 Login

♡ Recommend 5 Tweet Share Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Evan Wieland · 4 years ago

Great article Nermin! Love your simple yet essential list...

-Emphasise security from day one

-Lifecycle, future-proofing, updates

-Access control and device authentication

-Know your enemy

-Prepare for security breaches

3 ^ | v • Reply • Share ›

JoeCapitalist • 4 years ago

The main problem with the "Internet of Things" is the whole data architecture of the system. I don't want my thermostat talking directly to my refrigerator or my smoke alarms sending text messages directly to my phone. I don't want my lights to come on because my security alarm knows how to send direct commands to the light controller. I don't want all my sensor data uploaded to some Internet web site (encrypted or not) so that some company can gather statistics on what time I go to bed.

I want a data management layer that sits between all my smart devices and lets me control everything. I want that data layer to be able to exist on storage devices that I control, not some third party. The data layer would allow all the smart devices to create "smart data objects" that can store sensor information and to take specific actions if certain data objects exist. The only things that smart devices need to know is how to create these data objects and how to take specific actions when other kinds of data objects exist. Security and privacy are handled by this data management layer, not the devices themselves.

With such a system in place, the only thing my smart smoke detector needs to be able to do is create a "smoke detected" data object or a "current battery level" data object. It doesn't need to know how to take any kind of action beyond that. Now all I need is an application that I control that is monitoring the data storage layer for any "smoke detected" objects. This application will check my custom policy (that I created) and determine if it should create a "call fire department" data object. My smart phone (that knows how to call the fire department) watches for such objects and will call if it finds one. The smoke detector and the smart phone don't need to know anything about each other. If later I decide that I want to change my policy so that my garage door also opens and my smart car backs itself out of the garage when a "smoke detected" object appears, then neither the phone nor the

see more

2 ^ | v • Reply • Share ›

PilotDave ➜ JoeCapitalist • 2 years ago

What you are describing was created by x10 some 20 years ago... their devices then where not IP based, but they are now...

Reply • Share ›

Robert Emma • 2 years ago

internet of things is a security nightmare. though it gives convenience and now becoming necessity but it has also make ease of internet hackers and privacy invaders to track everything read more about this issue on https://goo.gl/o9e7qG

Reply • Share ›

nkonnect infoway • 2 years ago

Very Nice Blog in Internet of thing. I like It this blog. this blog useful in my business. my business is Internet things relented Like gps treaking system etc more product and work More information so visit https://www.nkonnect.net/

Reply • Share ›

Paul Cook • 2 years ago

Wow, what a wonderful read. I am really glad you shared this. I have come across this article which may interest you.
https://goo.gl/0Twyby

Reply • Share ›

Parry Mil • 2 years ago

Its always confusing to understand the new tech with IoT it is even more so. I read a same report http://bit.ly/2dcUt89 explaining the challenges of secure IoT.

Reply • Share ›

CIO White Papers • 2 years ago

"Internet of Things" security is hilariously broken and getting worse!!
What's the future of IoT and why we need to fix IoT security ?? Find out here:
http://internet-of-things.c...

Reply • Share ›

cinnamonmagazine • 3 years ago

I think that this is true "Whether it’s IoT or not, the way that adversaries look at all systems is what’s known as a stepping-stone attack. You attack the weakest device , and an IoT device usually has weak or no authentication with other devices on that same network." http://www.designmycity.com...

Reply • Share ›

Zhang Zuzuki • 3 years ago

Get Free Solar Power-plant and Security Installation at Home and Offices

As a reputable company with the best Solar power and security solutions in the World, we are offering off-sales services/solution for installation of both residential and commercial facilities free of charge anywhere in the world Starting February 1st till May 30th, 2016. For more information and subscription kindly email us at: wei_zhang@suntech-powercompany.com

Reply • Share ›

nitin • 3 years ago

Hi
I am also working on development of an IoT product. We are using IPSEC protocol for secure communication across the devices and servers. We feel it is safer. But I am not really sure why people is not using IPSEC or are there issues with that, which I have not addressed ?

Reply • Share ›

Suraj S Kattige • 3 years ago

Great article!
Love the way the problems were listed and explained. A must read for all the tech aficionados!

Reply • Share ›

avinash Jain • 3 years ago

its good but we can apply firewall....security on which type of iot is that device...we have all the technologies to ensure the better tomorrow...access control...ips...secure booting...updates and patches.. these works together correctly manner...i think there wont be issue for that

Reply • Share ›

Patrick D. • 4 years ago

Check this : http://www.forgerock.com

Reply • Share ›

Chuck Batson • 4 years ago

Good stuff. Personally I agree with the need to emphasize security from the beginning. However my experience has been that the decision makers within an organization just don't see it the same way, and only seem to be motivated after a crisis has already occurred. Any advice on how to persuade others to not be short-sighted when it comes to security? I have not yet found any arguments that work.

Reply • Share ›

Nermin Hajdarbegovic Mod → Chuck Batson • 4 years ago

"only seem to be motivated after a crisis has already occurred"

That's a good point. Maybe it will take a highly publicized security debacle for the rest of the industry to start taking IoT security seriously?

That could be a problem with small companies and very cheap IoT products - they will only care about their margins, not user security.

Reply • Share ›

Emma Ban → Nermin Hajdarbegovic • 4 years ago

Great remark! But I would also point out here the recent security patch
issued by BMW for their in-car "connected" system:
http://oemhub.bitdefender.c...
If they overlooked basic security measures when they built the smart
car system, what can we expect from manufacturers with smaller budgets
and less of a reputation to care about?

Reply • Share ›

Nermin Hajdarbegovic Mod → Emma Ban • 2 years ago

Well, it took two years, but we finally got that huge debacle I was talking about:

http://www.pcworld.com/arti...

Let's see if this is enough to get decision-makers thinking. IoT is becoming a huge liability.

^ | ⌄ • Reply • Share ›

✉ Subscribe Add Disqus to your site 🔒 Disqus' Privacy Policy DISQUS

SUBSCRIBE

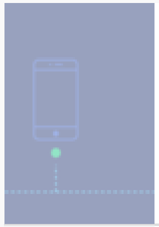
FREE EMAIL UPDATES

Get the latest content first.

Get Exclusive Updates

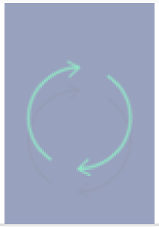
No spam. Just great articles & insights.

TRENDING ARTICLES



Guide to Monorepos for Front-end Code

about 1 hour ago



Working with Google Sheets and Apps Script

2 days ago

Using Spring Boot for OAuth2 and JWT REST Protection

6 days ago

Smart Node.js Form Validation

8 days ago

Working with the React Context API

9 days ago

Advanced Concurrency in Swift with HoneyBee

13 days ago

How to Make a Discord Bot: an Overview and Tutorial

20 days ago

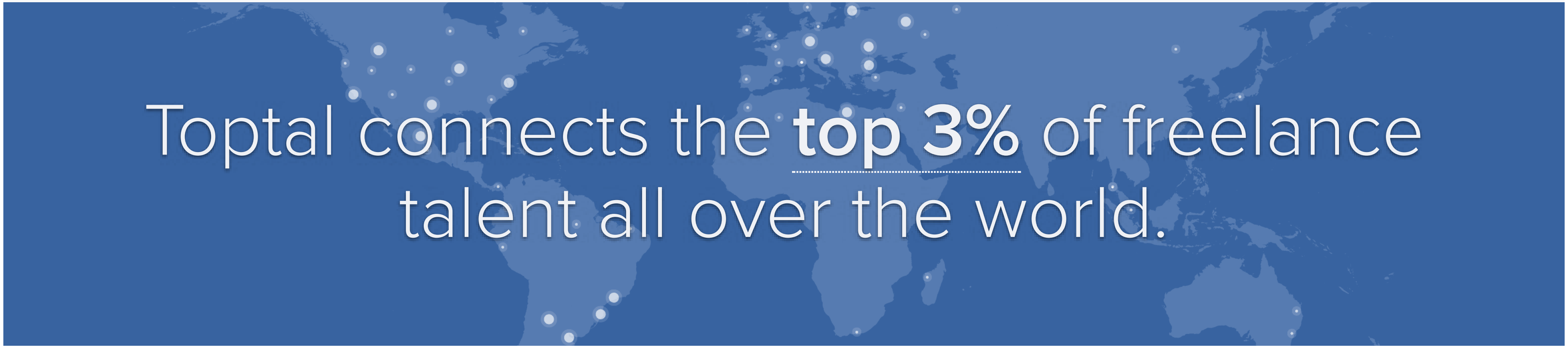
Architecting Optimization Algorithms with HorusLP

24 days ago

By continuing to use this site you agree to our Cookie Policy.

Got it

- IT
- Enterprise
- Mobile
- Internet of Things



Toptal connects the **top 3%** of freelance talent all over the world.

Toptal Developers

Android Developers

AngularJS Developers

Back-End Developers

C++ Developers

Data Scientists

DevOps Engineers

Freelance Developers

Front-End Developers

Full Stack Developers

HTML5 Developers

iOS Developers

Java Developers

t Developers

Machine Learning Engineers

Magento Developers

Mobile App Developers

.NET Developers

Node.js Developers

PHP Developers

Python Developers

By continuing to use this site you agree to our Cookie Policy.

Got it

React.js Developers
Ruby Developers
Ruby on Rails Developers
Salesforce Developers

Scala Developers
Software Developers
Unity or Unity3D Developers
Virtual Reality Developers

Web Developers
WordPress Developers

SEE MORE FREELANCE DEVELOPERS

Learn how enterprises benefit from Toptal experts.

Join the Toptal community.

HIRE A DEVELOPER OR APPLY AS A DEVELOPER

HIGHEST IN-DEMAND TALENT

iOS Developers
Front-End Developers
UX Designers
UI Designers
Financial Modeling Consultants
Interim CFOs
Digital Project Managers

ABOUT

Top 3%
Clients
Freelance Developers
Freelance Designers
Freelance Finance Experts
Freelance Project Managers
Freelance Product Managers

About Us

CONTACT

Contact Us

Press Center

Careers

FAQ

SOCIAL