TAINTED LOVE: HOW WI-FI BETRAYS US

F-Secure

CONTENT

INTRODUCTION

A comprehensive investigation into wi-fi technology, supported by Europol, raising serious doubts about the security of the communication system

The independent investigation was undertaken by the Cyber Security Research Institute and the German penetration testing company SySS on behalf of the ethical computer security company F-Secure. It found hundreds of people routinely logging onto a 'trojanized' free wi-fi hotspot specially created for the experiment.

The research into the wi-fi technology, which is used by over 73% of the UK's households and 25% of households worldwide found a reckless attitude to security with over 250 people logging onto our Trojan hotspot in a 30 minute period.

Even more worryingly, at an earlier **experiment** at a coffee shop in the Canada Square financial district, the **'free wi-fi hotspot'** carried a terms and conditions page which contained a deliberately ridiculous term – dubbed 'the Herod clause' by the researchers – which stated that, in return for free wi-fi, the individual using the service was prepared to **'render up their eldest child for the duration of eternity.' Despite this, six people decided that it was a fair exchange and signed up.**

The research also exposed a significant weakness in the wi-fi system which allows the usernames and passwords for those using email accounts on the widely used POP3 protocol to be clearly seen when they send emails though wi-fi hotspots. This weakness would allow any criminal operating a wi-fi hotspot to harvest account information that would allow them to masquerade as that person via their email account.

The experiment which has been endorsed by the UK Information Commissioner's Office, has underlined the total disregard for computer security by people when they are mobile – a finding borne out by a recent survey from the broadcasting watchdog Ofcom, which found that over 77% of people were not concerned about the security of public wi-fi.

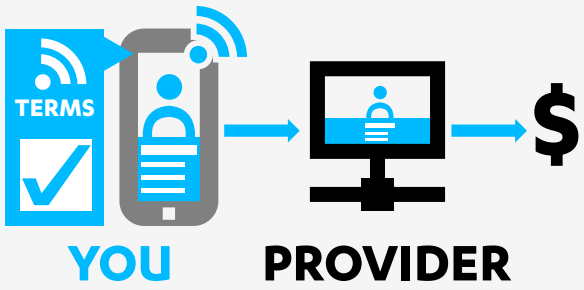
EUROPOL'S WI-FI WORRIES

1 **Providers can set wi-fi up so they see most of the traffic. If it's set up in public places – according to Europol – the providers of those systems can see the people who log on and see their traffic that they do. It's usually not encrypted or secure and the providers can see what kind of pages you are visiting.**

2 **It's very easy for someone to mount a man in the middle attack because, for most of us, we don't want to spend money on anything, so when we are in a public place the first thing we do is look for free wi-fi and the criminals know this, so they also provide this service.**

"The problem with this is that this is much more insecure than 99% of our population know. With public wi-fi, you could just as easily put it up on a big white screen wherever you are," said Troels Oerting, Europol's Assistant Director and the Head of the organisation's European Cybercrime Centre (EC3). He added that Europol has already seen criminals exploiting the public weakness for free wi-fi.

"We have got reports from member states that criminals have provided free wi-fi in areas where they want to steal people's information. So we have already seen this in operation."



Wi-fi providers could see your traffic.	**They can collect data about you and sell it...**	**...and you probably agreed to this through the T&Cs.**

Oerting also pointed out that the wi-fi hotspots provided by many legitimate organisations still represented security concerns.

"We have found that the security on many wi-fi hotspots is rather low. So because they are not set up in the proper way, the criminals don't even need to set up their own service. They can simply look into the service that is providing the wi-fi to get what they want."

While according to F-Secure's Security Advisor Sean Sullivan, the opportunities wi-fi hotspots present can go even further.

"It's possible to disrupt legitimate sources, mimic the name, catch the target first by having a stronger signal and then pass the traffic onwards to the legitimate source so they actually do connect but through you as a conduit. You don't replace their wi-fi connection – you just act as a middleman and you can see everything that's passing through to their endpoint."

This effectively means that you can blast out an existing hotspot by transmitting a stronger signal, catching the traffic and then passing it on to where it is meant to go. Other concerns raised by security experts involve copying the wi-fi access point's name and blanking out the legitimate point with a stronger signal and then allowing the computers using that access point to reconnect without the need to sign in.

Other techniques now being used by criminals involve simply creating access points that have a similar name to an organisation but which masquerade as a free or guest account – all potential dangers that, according to Sullivan, most people do not consider when looking for access to the internet.

"People when they travel nowadays, wouldn't trust a net café with a hardwired computer because they don't trust that computer. But somehow, because they trust their own personal device, they don't think anything of the connection that their device is making. And just as you wouldn't trust some computer in a lobby somewhere, you shouldn't trust some wi-fi that's just sitting there to connect to your personal device," said Sullivan.

Misplaced trust that the investigation put to the test using a mobile hotspot device built by SySS for less than £160 from a Raspberry Pi, an extended battery pack and a wi-fi and UTMS aerial, the team provided a 'free wi-fi' service in locations around London as part of an experiment to discover what precautions people use when mobile.

In the experiment carried out for F-Secure, a significant number of passers-by took advantage of the free hotspot in two locations, London's Canary Wharf and the Broad Sanctuary outside the Queen Elizabeth Centre opposite Westminster Cathedral and the Houses of Parliament. They logged on to upload information to the internet, unaware that their devices were also broadcasting enough information about them for a cyber-criminal to be able to identify them and their accounts. Information legitimately yielded by the mobile devices being used by these users broadcast on average the last 19 access points where they had connected. It's a particularly disturbing development as recent research has shown that individuals can be accurately identified by using just the last four access points where they have logged on.

"I would be very surprised if people realised just what information is being broadcast by their handsets. Most people are walking around London with their wi-fi switched on. Their mobile phones are broadcasting devices and, by leaving the wi-fi switched on, that device is broadcasting out to the surrounding area information not only on your device but where your device has previously been connected," said Mark Deem, an expert on technology law for the lawyers Edwards Wildman, who has personal concerns about the sending out of access point data and raised the issue to the report's authors.

“I once heard it described like this: You’re in a black room, very dark. You’re trying to work out who else is in that room and you can’t see anybody there. What you’re doing is effectively saying ‘I am Mark. I know Bill, I know Charles, I know Dave and I know Jane. Bill, Charles, Dave, Jane – are you there? It is hoping that somebody in that dark room will suddenly say ‘I am Dave. I am here. I will connect with you Mark.’ That’s what’s going on. If the information is being put out there, it’s not just one person’s name. It is for example the fact that you have connected to Starbucks, you might have gone to a hotel, you might have connected to a company website and you might have connected to a lawyer’s website. Somebody can aggregate all that information which is freely being broadcast by your device and build up a very accurate profile – not only of your working practices, but also potentially of who you are and that is quite troubling.”

The F-Secure investigation comes against a backdrop of increasing public reliance on wi-fi that is also seeing mobile phone companies offering a blend of cellular and wi-fi which in many cases uses lists of open wi-fi hotspots.

This additional danger deepens public exposure, as most mobile internet consumers are totally unaware that their service is being seamlessly switched between the different networks. As the F-Secure investigation proves, setting up a free wi-fi hotspot to maliciously siphon personal data from people as they are mobile is a very real danger.

“At best, your device is only leaking information about you – at worst, your passwords are being spilled into a publicly accessible space, and it’s not just spilling details to those that control the network – anybody on the network can see your information,” said Sullivan.

WI-FI THE HISTORY

Wi-fi – along with technologies such as the mobile phone, text messaging and the internet itself – is one of the success stories of the technological age and, like those, its success was unexpected.

According to Sir Bryan Carsberg, in 1984 the first director of Oftel (the UK telecoms regulator now known as Ofcom), when the first mobile phones appeared, Oftel was sure that it would only be a minority market, at most accounting for only around 100,000 customers in the UK.

It was a similar story with wi-fi according to Vic Hayes, acknowledged by many as the father of wi-fi, who had been asked by the US company NCR to come up with a technology for cash registers that would give NCR a competitive advantage.

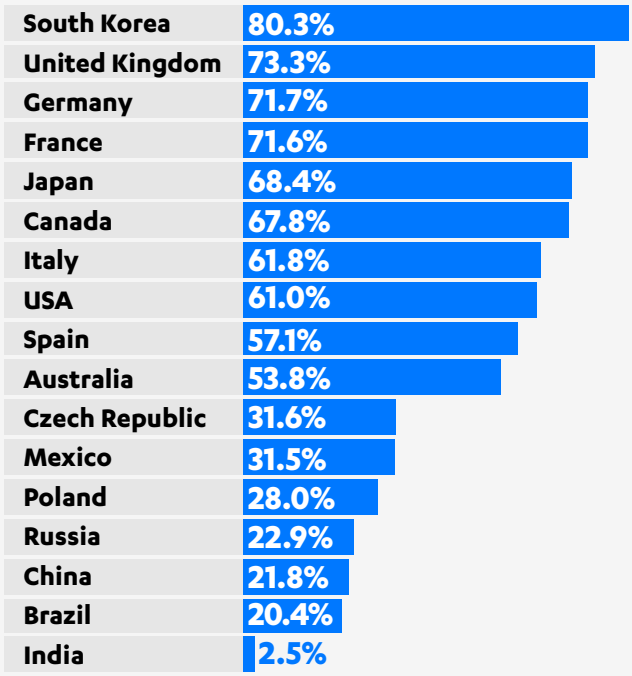
At the time, Hayes was working for NCR's Dutch arm, a 60 strong engineering group when they were tasked with making cash registers wireless.

"So our man at headquarters said: 'If we can make a wireless connection then we will have an advantage'," said Hayes.

His innovative development gained momentum in July 1999 when Apple incorporated the technology into its laptops as the 'AirPort connector', an invention that kick-started the adoption of wi-fi and saw the adoption of domestic access points rise by around 15 million a year.

But wi-fi, like the internet itself, suffers from one inherent weakness: it was never designed with security in mind. As with the internet, the first criterion is to provide a connection. Despite that, the appetite for wi-fi that has shown no signs of diminishing.

WI-FI HOUSEHOLDS – PENETRATION OF TOTAL HOUSEHOLDS: 17 SELECTED COUNTRIES IN 2011



Source – Strategy Analytics

"In 1985, when the US FCC made the regulations that made the wi-fi spectrum available at our NCR headquarters, we had a guy who said: 'Wait we a minute. We have point of sale terminals and we sell to large department stores and they want to change their floor plan from time to time, but because the cash register needs to be connected to the computer they have to drill holes and they don't like the holes in their marble floors."

In 2013, according to the wi-fi industry body, Wi-fi Alliance, two billion wi-fi devices were sold and the technology is now in 25% of homes worldwide.

According to the research company Strategy Analytics, by 2016, some 800 million households worldwide will have adopted wi-fi representing a global penetration of around 42%.

It is still fraught with peril, as consumers and most organisations are happy to rely on the new password technologies deployed on the routers, though many neglect to install passwords on the routers themselves.

This is a weakness that Europol's Oerting admits also worries him: **"Most people's wi-fi at home is rather easy to hack."**

Europe and the UK in particular have been at the forefront of adopting this technology since its development, with inhabitants not only using the technology at home, but increasingly demanding it while on the move.

According to the UK telecoms company BT, it has around 5 million wi-fi hotspots in the UK which it says are: **"Hotspots where you want them – coffee shops, high streets, shopping centres, pubs & bars, train stations, airports, city centres and homes."**

BT is not alone. The Microsoft-owned Skype has also announced plans to install wi-fi hotspots in every shop in the UK, a trend being mirrored by other technology companies with the BskyB-owned Cloud wi-fi operator increasing its hotspot coverage and the UK Post Office is expected to announce plans to roll out a free wi-fi hotspot network from its network of post offices in autumn 2014.

The trend is driven not just by an insatiable demand for wi-fi access from consumers but also as part of a business case. With many employees now choosing to use their own devices at work, wi-fi represents an easy way to connect those devices and a way of placating staff workplace expectations, offering a service to customers and visitors and a means to supply access to the social networks that are currently being seen as advantageous to businesses.

According to the industry publication *Wireless*, wi-fi access is now seen as essential in the retail, hospitality and even healthcare sectors.

Due to this inexorable move to total coverage, Wireless points out that it is also inevitable that those deploying the technology will seek to differentiate themselves from competitors by offering enhanced performance and connectivity – factors the publication points out come at a price – a development which *Wireless* states is already seeing two new trends emerge: analytics and 'bandwidth wholesaling'.

WI-FI EXPECTATIONS – BUSINESS, THE CONSUMER, THE INTERNET COMPANIES

From a security point of view, the consumers have now been hoist on their own petard and are victims of their own wi-fi demands because they want data on the move but are not prepared to pay for it.

As Europol's Cybercrime Centre head Oerting points out, our appetite for data is making us vulnerable: **"because most of us don't want to spend anything, so the first thing that we do when we are in a public place is look for the free wi-fi and then start surfing, and of course the criminals know this."**

The answer to what is fast becoming the 21st century visitor's first question 'Do you have wi-fi?' is now a symbol prominently displayed in cafes, shops and hotels up and down the High Street with no questions asked by those logging-on about the security of the system.

It is a question that is driven by an insatiable demand for data. In 2013, according to the communications company Cisco, from a global population of 7,161 million people, 2,521 million were using 12,386 million devices in the main to access the internet.

By 2018, Cisco forecasts that the number of people will have only risen to 7,562million but the number of people using technology will have risen to 3,912million from 20,633 million devices with the main driver being video. And according to the experts interviewed for this report, the main method for accessing that data, particularly on the move, will be wi-fi.

As Moray Rumney, a wireless expert and lead technologist for Agilent, the test and measurement company recently spun out of HP, points out, **"Most people's experience of wireless actually comes from wi-fi and not from cellular technologies. The reason for that is that most people's experience of the internet is actually coming from wires and wireless local area network (LAN) is just an extension of those wires."**

EC STUDY: EUROPE LOVES WI-FI

The combined use of wi-fi and other small cell infrastructures (which complement traditional macro cell mobile base stations) can relieve congestion on the 3G/4G networks by providing "backhaul" functionality outside those networks, while minimising costs to both network operators and users.

Wider use of these technologies could allow operators to save tens of billions of euros as they go about upgrading networks to meet customer demand. Consumers would save money by using wi-fi instead of paying for mobile data when they are actually near a wi-fi hotspot. Small cells can also extend network coverage into hard to reach places, including inside large buildings.

The study recommends

- to make spectrum from 5150 MHz to 5925 MHz available globally for Wi Fi;
- to continue making the 2.6 GHz and the 3.5 GHz bands fully available for mobile use and to consult on future licensing options for 3.5 GHz and other potential new licensed mobile frequency bands; and to reduce the administrative burden on the deployment of off-load services and networks in public locations.

Such demands, as *Wireless* point out, present a challenge to businesses to attract and retain customers and an additional cost to do so. For mobile phone companies and internet service providers, wi-fi presents an opportunity to cut the costs of installing cellular infrastructure, and gives them an incentive to pay for the use of wi-fi access points.

The locational and behavioural information that the wi-fi routers can generate offers another potential opportunity to those businesses wishing to offer an enhanced experience to their customers and an incentive – as Oerting has pointed out – to collect large amounts of data on those customers.

It is an experience in connectivity that Neelie Kroes, the European Union vice president, and an avowed critic of surveillance, is ironically seeking to encourage by developing a further extension to shared public hotspots, while perhaps being unaware of the security, privacy and surveillance issues.

2016

78%

of wireless data traffic is expected to be delivered using wi-fi

Source – European Commission study, 2013

According to a European Commission study published in August 2013, Europeans are **"flocking to use wi-fi internet and the trend is set to continue. 71% of all wireless data traffic delivered in 2012 to smartphones and tablets in the EU was delivered using wi-fi, possibly rising to 78% by 2016."**
The results show how the cheaper cost to consumers of using wi-fi hotspots is changing behaviour, and the study recommends extra spectrum be made available across the EU to support this rising demand.

"Wi-fi is a huge success. It's a win for everybody involved," said vice-president Kroes, adding, " I will make sure the European Commission helps to spread use of wi-fi through extra spectrum and lighter regulation."

According to the study titled **"Europe Loves wi-fi":** **"While 3G/4G networks are essential for truly mobile activity, it is currently expensive to buy the spectrum rights needed to run these networks. Consumers pay significant prices to use 3G/4G – for example when roaming – and the networks are already congested in many parts of Europe because of a lack of allocated spectrum.**

"Systems where you share your wi-fi network with others are a great example of how we can crowd-source a better internet for everyone. Everyone in Europe should be able to benefit from internet when they are away from home and work," Kroes said.

This is a slightly puzzling statement from the EC vice-president and current European Commissioner for Digital Agenda because the mobile phone companies have been taking advantage of public wi-fi hotspots since the demand for mobile data started.

RELIANCE ON WI-FI INCREASES MOBILE VULNERABILITIES

The situation has become even more worrying due to a mobile industry practice of blending together wi-fi and mobile networks to meet their customers' expectations of a data-rich service.

This practice, according to all the experts interviewed for this report, inevitably means that customer data must spill from the system.

The research by the CSRI has found that the 2G, 3G and 4G data experience would not be possible without wi-fi and indeed, that it has become an essential part of the service offered by mobile phone companies. One example is the wi-fi now available on the London Underground.

This point was underlined by a number of leading wi-fi authorities in interviews given to the CSRI's sister organisation Future Intelligence for its PassWord radio programme at Cambridge Wireless, one of the world's leading conferences on wireless issues.

"The mobile networks plan a network in the spectrum they have been allocated, that aims to provide a certain quality of service," said Agilent's Rumney "but they did not bargain for the demand that they are now encountering and that can have an impact on their service if they do not turn to wi-fi."

It's a point echoed by Professor Simon Saunders, a director of technology for the independent wireless consultancy Real Wireless, which advises the UK Government on wireless issues.

"There is now an incredible volume of traffic and the networks were not designed for that. The density of demand is absolutely staggering and it's still rising very fast," said Professor Saunders, who is also a member of the Ofcom Spectrum Advisory Board.

THE INDUSTRY VIEW: THE MOBILE INFRASTRUCTURE COMPANY ERICSSON MAKES THE CASE FOR WI-FI IN THE NETWORK

Delivering additional radio network capacity and coverage through the deployment of small cells as part of a heterogeneous network is central to most mobile operators' mobile broadband strategies, and wi-fi is a key element.

With wi-fi fully integrated into mobile access and core networks – offering seamless, secure roaming, SON-based access selection, real-time traffic steering and carrier-grade scalability and manageability – users will enjoy seamless access to high-performance mobile broadband, whether they are connected over 3GPP or wi-fi, and operators will be able to choose connectivity to optimise the user experience.

In addition, having wi-fi access included in operators' policy and charging systems opens up new business opportunities by supporting a variety of business models simultaneously, for individual subscribers, enterprise customers and partners.

Source – Ericsson wp-wi-fi-in-heterogeneous networks.pdf

To cater for this demand, and to ensure that the customers' quality expectations are met, networks use a blend of cellular and wi-fi to provide service infill that can be quickly and flexibly deployed.

"As operators were rolling out 4G, they were looking for a heterogeneous network to try and complement their service. They were trying to think about how to roll-out 4G, but at the same time have a corresponding network of wi-fi that would give them a more robust system," says Dave Fraser, CEO of the wi-fi hotspot company Devicescape.

"There is a real difficulty in delivering rich communications over wireless and it argues for an operator using all possible improvement technologies to give them spectral efficiencies and a better delivery of service."

This has led to a mobile industry practice of seamlessly off-loading data demands from the cellular network and onto a wi-fi network, according to Samuel Buttarelli, vice-president of CommScope, a company specialising in providing small-cell and wi-fi infill.

"The problem is that 4G is a lot of investment for the operators and the type of data demand that we are seeing is so big that the wireless operators cannot really support all of this traffic on the 4G networks that they have deployed.

"So wi-fi is part of the strategy at least from a mobile operator's point of view, to take and offload the network in specific areas – buildings being a good example."

Buttarelli's essential point is that there are places that people tend to temporarily congregate – sporting stadiums or tourist attractions for example – where there will be a high concentration of demand which will have an adverse effect on network coverage.

If such demand is a long way from the nearest cell then the impact, particularly with 4G, is huge as serving a mobile connection with a poor signal pulls more capacity from the system than one with a good signal because of the extra power needed to send data over larger distances.

> **"Wi-fi has always lead cellular in terms of performance. A lot of people look upon wi-fi as the superior technology, particularly the young."**
> **Moray Rumney**

The obvious solution is to take advantage of any wi-fi in the surrounding area to maintain the quality of customer experience for all of those using the network and for those people who are generating short-term demand.

As Buttarelli points out, this might even be in an office, a warehouse or a train – places that can be particularly resistant to radio waves due to the modern practice of using reflective glass and steel.

As a result of this, and to meet the demands for connectivity to their devices from employees, clients and customers, companies have found that they need to install wi-fi access points, or a purpose-made unit known as a femtocell, which operates in a similar fashion to a wi-fi router by driving data traffic into the wired broadband network. The femtocell also operates as a router for mobile voice traffic.

"For the mobile operator, this wi-fi achieves two things. It provides connectivity into a building but equally importantly it offloads the outside network from this traffic."

The mobile operators have worked to make this practice as seamless as possible. In some cases (such as the London Underground), customers have to go through a one-off sign-up for the service. In other cases, wi-fi networks such as 'BT wi-fi' (the UK-wide network of 5 million wi-fi networks), the service is bundled together as part of an internet account package for home customers.

Virtually all customers favour this system as it does not interfere with whatever they are doing and is, in a sense, in their interests according to Professor Saunders.

"The general idea is that people don't know what they are connecting through, so long as it works well. On the whole, that's a good thing because why should we be worried so long as it does work well?"

Mark Deem makes the point very well, though this time as a consumer rather than a lawyer: – **"Automatic connection goes some way to explaining the issue. With my own mobile operator, I get access to some public wi-fi hotspots and I find it incredibly frustrating when my phone drives me to those hotspots because sometimes it can just slow the whole process down."**

This frustration is very familiar to the mobile industry. As Professor Saunders has earlier pointed out, it works hard to try to ensure that it is one that consumers encounter less and less.

Devicescape is one of the companies that help the mobile service providers do this, according to Fraser.

"Devicescape is a company that is all about helping mobile operators deliver a product to subscribers to give them best possible experience in real-time. What that means is that we have software that lives on a smartphone and a cloud service that manages the connection, and what we are able to do is to measure in real-time the quality of the connection and select the best possible network for a subscriber to be on."

The last 2-4 networks your phone joined are enough to accurately identify you (though, on average, your phone will broadcast the last 19 networks it joined)

Source – Dave Fraser, CEO of the wi-fi hotspot company Devicescape

AN EXPERT VIEW

"Wi-fi offload is now a huge deal. I don't know when it was first discovered that the demands for data on the cellular network were not able to be met but when it was, offload onto wi-fi obviously became very important.

"The integration of that offload has got better and better. In the early days, it was really bad because you had to remotely switch your phone from cellular to wi-fi and often stop your cellular connection altogether.

"Now the technology to do this offloading has become much more sophisticated, and you can move from a cellular data session to a wireless LAN almost seamlessly which is the ultimate in integration.

"How this will work is still to be worked out, for example with Google Maps and the potential for people to be able to predict what you will be doing at a particular time. So the potential for value added services is huge, but with it is the potential for that information to be misused.

"And I think we are in this twilight period of people discovering the potential of what can be done with the harvesting of personal data and for it to be used in positive ways, but people are also starting to become aware about how that data can be used and what that means for their privacy.

"In the context of ethical companies, there's not really much of a problem with where that might go, but then you have the potential for the less ethical elements to come in and potentially exploit that ability to gather data from people."

Moray Rumney – Wireless expert for Agilent and delegate to the Third Generation Cellular Partnership Programme.

"The CSRI experiment showed, on average, the last 19 access points where the user had connected, and that strikes me as a defect in the way these products are set up to use wi-fi access points." said Fraser.

In most cases, Devicescape has found the best connection will be a wi-fi mobile one.
"So what we bring to this heterogeneous network world is the ability to intelligently select the right network in the first place," says Fraser, "but secondly, we also bring what we call a 'curated virtual network', which is a network we've created based on all of the world's free and openly available wi-fi hotspots."

This network has huge potential and is still growing – according to Netscape, there are 350 million wi-fi hotspots in the world already and the number is still increasing, as we have seen from the statements from BT, the Post Office, Skype and a number of other hotspot providers. In addition, there is the trend pointed out earlier from businesses looking to recoup the costs of wi-fi and Neelie Kroes and the EU encouraging the development of ad-hoc personal networks.

"The rate of increase is huge," says Fraser. **"Retail and business owners are all seeing it is good for their business to have wi-fi in their shops or in their offices. So, more and more, we are beginning to see wi-fi proliferate in all corners of the world.**
"For example, when we started to look at all of the world's wi-fi with our technology, we saw about 120 million hotspots around the world.
"Our technology crowd-sources hotspots. From that initial 120 million, we curated that down to 11 million hotspots that we think of as high quality carrier grade that an operator would consider to be acceptable. We are now up to 350 million and from that we have a curated network of 20 million. By 2017, we expect our network to have grown to 100 million."

Devicescape and a number of other companies automate the process so that the travelling mobile phone customer is not inconvenienced by having to log on to a wi-fi service.

"We know that people are going into stores and coffee-shops and using wi-fi because we can see it, so if we know that a lot of people are going into a particular store then we'll just automate that process."

The speed of increase in wi-fi hotspot deployment is now in itself representing a significant security risk. The global tally of mobile hotspots now stands at over 350 million, close to a 300% increase in two years. This development potentially massively increases the risk of rogue wi-fi hotspots creeping into the networks of free wi-fi, because checks are not made on the credentials of the people offering the service, or whether they have had their access point corrupted, or the data that they are collecting on it.

The reliance on the wi-fi network for what the telecoms industry calls 'wi-fi off-load' has not gone unnoticed. Indeed, the mobile operator EE claims not to be using wi-fi to bolster its 4G network and is seeking to make marketing capital out of this fact by stressing that this makes its customers more secure.

It's a marketing pitch that both Professor Saunders and F-Secure's Sean Sullivan support, stressing that the cellular network is currently the only wireless technology that offers customers effective data security.

"People can be confident in the security of their operator's cellular network – mobile data connections offer excellent security. But the same cannot be said of wi-fi. It's not even close. Using your device on a wi-fi network in a public space is public – as in completely open to the public," said Sullivan.

Moray Rumney of Agilent Technologies is a delegate to the global body overseeing developments in wireless technology – the Third Generation Cellular Partnership Programme. He said the organisation is now very concerned about the potential for abuse via the proliferation of wi-fi hotspots.

"There is work ongoing to deal with bad hotspots in a more organised fashion within 3GPP, which is the body that develops the bulk of the cellular standards in the world. They have plans to handle the offload between trusted and non-trusted wireless local area network providers (an industry shorthand for LAN which is often a synonym for wi-fi).

"So there is an ability to do some form of screening, but it's early days in terms of understanding and protecting people from what may happen."

As we can see from the above, the current situation is dangerous to say the least. There is little to prevent unscrupulous individuals inserting a malicious hotspot into a network, whether they are criminals or simply a company seeking to generate an income to pay for a wireless network and provide additional revenue for the company itself.

As Europol's Troels Oerting points out, he has personal experience of seeing the scale of the data collected by companies and admitted that he has concerns about the privacy implications.

And as Rumney points out, there is concern among the governing bodies for the wireless sector about the possibilities for abuse, concerns that the headlong rush into the Internet of Things can only intensify.

It is a situation that is made worse by our appetite for data. We are not only massive consumers of data, but we will become even more so as our love affair with mobile access to the internet increases.

Mark Deem said this appetite is fuelled by the technology and entertainment industries which now see mobile computing as their principle source of revenue.

"What is really driving people onto hotspots is the very data-rich environment in which we are now operating and the limitations of mobile data on handsets.

"At the moment we are downloading a lot of apps and logging on to a lot of websites that are very data-rich in their content. In order to get a satisfactory customer experience of that website or that application, you really want to have some fast and sustainable internet access.

2013'S DATA WORLD

- **Global mobile data traffic grew 81 percent in 2013.** Global mobile data traffic reached 1.5 exabytes per month at the end of 2013, up from 820 petabytes per month at the end of 2012.
- **Last year's mobile data traffic was nearly 18 times the size of the entire global Internet in 2000.** One exabyte of traffic traversed the global Internet in 2000, and in 2013 mobile networks carried nearly 18 exabytes of traffic.
- **Mobile video traffic was 53 percent of traffic by the end of 2013.**
- **Global mobile devices and connections in 2013 grew to 7 billion, up from 6.5 billion in 2012.** Smartphones accounted for 77 percent of that growth, with 406 million net additions in 2013.
- Globally, smart devices represented 21 percent of the total mobile devices and connections in 2013, they accounted for 88 percent of the mobile data traffic. **In 2013, on an average, a smart device generated 29 times more traffic than a non-smart device.**
- **In 2013, a fourth-generation (4G) connection generated 14.5 times more traffic on average than a non 4G connection.** Although 4G connections represent only 2.9 percent of mobile connections today, they already account for 30 percent of mobile data traffic.
- **Smartphones represented only 27 percent of total global handsets in use in 2013, but represented 95 percent of total global handset traffic.** data traffic).
- **Globally, there were nearly 22 million wearable devices (a sub-segment of M2M category) in 2013 generating 1.7 petabytes of monthly traffic.**
- **Globally, 45 percent of total mobile data traffic was offloaded onto the fixed network through wi-fi or femtocell in 2013.** In 2013, 1.2 exabytes of mobile data traffic were offloaded onto the fixed network each month. Without offload, mobile data traffic would have grown 98 percent rather than 81 percent in 2013.

Source: – Cisco (http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html)

"I think that is driving people away from using the traditional cellular connection and that is not sufficiently fast these days for a satisfactory consumer experience."

According to the statistics, video is seen as the main reason for the preference for wi-fi, particularly among the young.

As we have stated, wi-fi is viewed as the conduit of choice for that traffic and it is a situation that is also about to undergo an even more meteoric increase, according to the telecommunications company Cisco. Given the present lack of awareness of the risks from wi-fi from the general public, this represents a significant risk.

"People when they travel these days wouldn't trust a net café over a wired connection for good reason, because they don't trust the computer that's attached to it. But somehow, because they have their own personal device and they trust their personal device, they don't think anything of the connection that their personal device is making," said F-Secure's Sullivan.

"Just as you wouldn't trust some computer sitting in a lobby somewhere to check your email, you shouldn't trust some wi-fi connection that is there to connect your device through. I think that there is a psychology there, which is I trust my iPad, so I will connect to the wi-fi and I am safe."

THE SPECIFIC RISKS FROM WI-FI

Public wi-fi is insecure and security must be a priority, especially when moving into the fast developing area of Hotspot 2.0. Often our phones automatically connect to these access points, while very little work has been done to verify the identity of the organizations behind the hotspots.

For over a decade, fears have existed over the security of wi-fi. The technology was deployed without completely understanding it. So wi-fi access points were routinely set up without access codes enabled on them. As a result, all of the traffic passing across them could be easily monitored – a weakness demonstrated by Peter Warren, this report's author, who carried out the first survey of open wi-fi access points across London in 2001 as part of an investigation published in the *Financial Times* and *Computing* magazine. That investigation found that most wi-fi in the capital had been installed without turning on the security, leaving the networks of the companies using it open to use by casual passers-by and their data open to capture by criminals.

The current security concerns about free wi-fi access points, public access points and the developing commercially available access points known as Hotspot 2.0 is that, quite simply, very little work has taken place to verify the identity of the organisations behind the access points. They are easy to mimic and an overly trusting public is quick to use them, while having very little means of verifying who is providing them.

This situation almost exactly mirrors the state of wi-fi in 2001, except that now the casual passer-by is used to finding free and open wi-fi and so has become the potential victim of criminals and those wishing to capture their information.

As Troels Oerting and Mark Deem say, the naivety of people keen to continue their digital entertainment is aided and abetted by a telecoms world that is as keen as them to ensure their positive consumer experience, because it is seen as the potential money-making area. But, as a result, the connectivity is actually making those same consumers vulnerable to technological exploitation. Rumney says they can be exploited potentially by unscrupulous companies and, as Oerting says, by criminals who are already taking advantage of this naivety.

The awareness of the potential insecurity of wi-fi is widespread across the mobile industry. At the recent Cambridge Wireless Conference in August of this year, it was mentioned frequently by many speakers including Professor Saunders and Moray Rumney, and CommScope's Samuel Buttarelli, in an interview for this report underlined this weakness: **"Very often you may think that wi-fi is an insecure environment, and you would be absolutely right, because security and access to the network is an area in which we see a lot of activity from people trying to standardise on this.**

"Wi-fi is insecure and security has to be an area – especially when moving to this area of Hotspot 2.0 – where your phone is automatically connecting to these access points. We do see a need for a lot of security applications."

As *Wireless* has underlined, one of the principle ways that the business model for wi-fi operates will be to interpret data about individuals, a detail that presents a fundamental weakness.

Our devices are broadcasting valuable information about us, the telecoms industry wants us to do that so that it can exploit the fact, but it is going to be very difficult to prevent other people from picking up that information because our phones are broadcasting devices.

But as F-Secure's Sullivan states, this is something of a challenge: "Just one uniquely named wi-fi network could easily be enough to identify you, many people name their home networks after themselves. But to have 19 known networks broadcasting from your device is a real disaster – it almost certainly provides enough of a footprint for anybody to be identified. And once your device is identified as being yours, all the data it leaks puts your identity at risk. Identity theft, bank fraud, data theft – prevention all depends on protecting your anonymity."

As ever, the cyber criminals have shown themselves to be adept at exploiting any technological weaknesses.

Something that they can do very easily with wi-fi, as the devices we use to connect to wi-fi access points are broadcasting data that can be picked up. The access points themselves can be mimicked by a person being conned into believing that a free wi-fi service is being offered by an organisation, such as a hotel or a conference centre. An existing wi-fi service can be 'forced out' by using a wi-fi access point with a stronger signal and no password on it that allows everyone using that service to re-connect without realising that they are now on a rogue system. The latter technique can allow a company's wi-fi network to be hijacked.

Immediately after our investigation in 2001, cyber security experts told the authors that they had seen criminals exploiting the weaknesses in wi-fi routers and seeking open routers and breaking the access codes on ones that had been set up to prevent access using a method known as war-dialling.

Europol has already detected criminals using 'poisoned access points' which have been set up to collect data. So what can a 'poisoned access point' give you?

THE EVOLVING NEW DATA-RICH WORLD

- The number of mobile-connected devices will exceed the world's population by 2014.
- Due to increased usage on smartphones, smartphones will reach 66 percent of mobile data traffic by 2018.
- Tablets will exceed 15 percent of global mobile data traffic by 2016.
- There will be more traffic offloaded from cellular networks (on to wi-fi) than remain on cellular networks by 2018.

- **Global mobile data traffic will increase nearly 11-fold between 2013 and 2018.** Mobile data traffic will grow at a compound annual growth rate (CAGR) of 61 percent from 2013 to 2018, reaching 15.9 exabytes per month by 2018.
- **By 2018, there will be nearly 1.4 mobile devices per capita.** There will be over 10 billion mobile-connected devices by 2018, including machine-to-machine (M2M) modules – exceeding the world's population at that time (7.6 billion).
- **By 2018, over half of all devices connected to the mobile network will be "smart" devices.** The vast majority of mobile data traffic (96 percent) will originate from these smart devices by 2018.
- **Mobile video will increase 14-fold between 2013 and 2018**, accounting for 69 percent of total mobile data traffic by the end of the forecast period.
- The amount of mobile data traffic generated by tablets by 2018 (2.9 exabytes per month) will be 1.9 times higher than the total amount of global mobile data traffic in 2013 (1.5 exabytes per month).
- By 2018, aggregate smartphone traffic will be 11 times greater than it is today.
- **By 2018, over half of all traffic from mobile-connected devices (almost 17 exabytes) will be offloaded to the fixed network by wi-fi devices and femtocells each month.** Without wi-fi and femtocell offload, total mobile data traffic would grow at a CAGR of 65 percent 2013-'18 (12-fold growth), instead of the projected CAGR of 61 percent (11-fold growth).

Source: – Cisco (http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html)

THE F-SECURE WI-FI EXPERIMENT

For the purposes of the experiment carried out on behalf of F-Secure, the exercise was conducted under strict legal guidelines established by Mark Deem of lawyers Edwards Wildman.

Experts from the German penetration testing company SySS built a portable wi-fi access point using a Raspberry Pi mini-computer system, a UTMS aerial, a wi-fi aerial, a battery pack with a life of around two days, a USB port and a number of elastic bands.

The system is not much bigger than the Raspberry Pi device. It took around two days to build and program at a total cost calculated by Finn Steglich of SySS of around £160.

While the end product was not something that would have made it through security at an airport without exciting a considerable amount of suspicion when assembled, when broken into its component parts it easily made the journey from Germany to London.

When assembled, the result was a highly portable wi-fi hotspot that could have been easily concealed in a woman's handbag and could be deployed in seconds. It could be easily interrogated by an operator with a laptop to access the data it had captured.

A portable wi-fi access point consisting of a Raspberry Pi mini-computer system, a UTMS aerial, a wi-fi aerial, a battery pack with a life of around two days, a USB port and a number of elastic bands

According to our technical expert, Finn Steglich, the device could be built by anyone.

"Most of the information needed to build one of these things is either common knowledge or anyone who has any idea of networks can do this. Or you can easily get the information you need from the internet," said Steglich, adding: "I looked up some of the things that I needed myself. If you had some time – maybe a week or so to do this – you could probably learn everything that you needed to. Basically anyone can do this."

Two separate experiments were carried out in London. The first was at the Café Brera in Canada Square, in the Docklands financial district and the second outside the Queen Elizabeth Centre by the Houses of Parliament at Westminster.

In the first experiment, our mobile access point was placed on a table in the Café Brera while we filmed the exercise. For this experiment, a detailed 'terms and conditions page' was constructed that included the clause that 'in return for free wi-fi access the recipient agrees to assign their first born child to us for the duration of eternity.'

During the short time that this was running in Canada Square, some six people in the capital's financial heartland signed up to our terms and conditions and enjoyed free wi-fi 'in return for their eldest child'.

We have yet to enforce our rights under the terms and conditions but, as this is an experiment, we will be returning the children to their parents. Our legal advisor Mark Deem points out that – while terms and

conditions are legally binding – it is contrary to public policy to sell children in return for free services, so the clause would not be enforceable in a court of law.

After around an hour and a half, we took the terms and conditions page down and allowed people free wi-fi access without the need to sign in for the rest of the experiment at the Café Brera.

The next stop was Broad Sanctuary in the heart of London – a stone's throw from the Houses of Parliament, the headquarters of the Labour and Conservative parties and the National Crime Agency. It yielded huge amounts of data.

We placed the improvised mobile wi-fi access point on the parapet of the seating area outside the Methodist Central Hall and the Queen Elizabeth Conference Centre and carried on filming prominently pointing to the access point and the laptop while doing so, as people from the three events on at the Central Hall conference centre left for the day and turned on their mobiles.

The upsurge in traffic from the attendees at the Royal Town Planning Institute's Planning Convention, a Government department meeting at Central Hall, and a conference for the Energy Institute blended in with connections from casual tourists in the area.

As a result, the amount of information collected by the wi-fi access point also increased and we registered around 250 contacts in 30 minutes. Each of these connections left behind details of – on average – the last 19 access points where they had connected.

This is a deeply troubling statistic: according to industry research, to positively identify an individual it is only necessary to recover details of the last four access points visited.

During the same half hour period, 33 devices began actively using the access point to carry out web searches and send data and email.

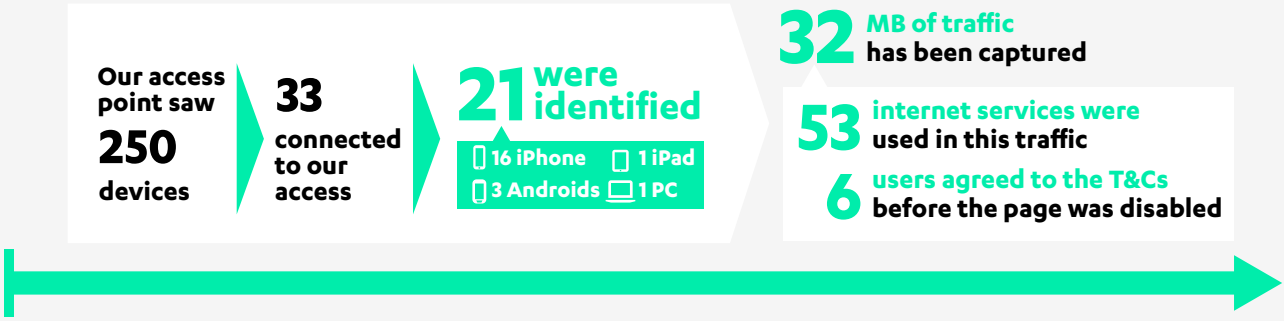
The sending of email caused the researchers some unexpected issues. We had not realised that user and password data from the highly popular Pop3 email protocol is visible as it passes through wi-fi access points and we had to take steps to anonymise this.

One such email had been sent from the managing director of a large London office lettings agency – we then took steps to prevent this happening again.

The existence of the Pop3 vulnerability was first revealed by CSRI in 2001, when its first survey of wi-fi access points discovered that complete emails, along with passwords and usernames, could be easily picked up by intercepting the traffic between computers and access points. This proves that, in well over a decade, the technology industry has done little to address the issue.

It is a weakness that has profound implications. Pop3 is widely used and access to a username and password can effectively mean that all of an individual's data can be stolen as many people use the same details for multiple accounts, such as online banking, and an email address is often used as a username.

WHAT HAPPENED IN 30 MINUTES?



The facts and figures from thirty minutes of our open access point

While being able to open an email account can also provide a criminal with details of the bank used by the account's rightful owner and any other online services used all of which can usually be reset by email.

"There is an awful amount of information being put out there which is very sensitive information. We all know from lots of different surveys that people don't tend to change their passwords often enough," said Deem.

"Passwords are weak in the way that they are put together and they tend to be used again and again by individuals across a whole host of applications from their home access points, through to websites and online accounts."

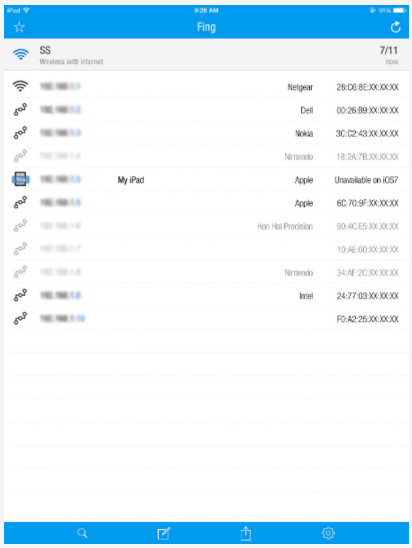
Indeed, as F-Secure's Sullivan points out, contact and engagement with an access point allows the casual passer-by to have personal data stolen. The criminals are also still able to pull data from the network about other people on it with relative impunity by using tools that are freely available on the web.

One such software application which has been well known to hackers from the very beginning of the web is 'fingering'.

Sullivan demonstrated this as part of the experiment by using an application called 'Fing' to discover all the devices using one of F-Secure's wi-fi networks.

Essentially, the exercise showed that information is freely available to both the people running a network and to the people accessing the network, if they have the tools to do so.

"Fing can be used on Android and iOS to see just how many other devices are on the same network as yourself. It's very useful for a network administrator, but also useful as a demonstration of just how many other nodes you need to trust. And of course, in an open wi-fi environment, you should trust no one. It isn't much better in a password protected public space either. Any device in the hotel would be able to see the others once signed on," said Sullivan.



Fing – can be used on Android and iOS to see just how many other devices are on the same network as yourself

CONCLUSION

The population is massively dependent on wi-fi technology, but is unaware of the capabilities this technology holds for surveillance and intrusion into their lives.

The experiment carried out by the CSRI should not be underestimated. While it may appear trivial and easy to do, its importance is underlined by the widespread ignorance it reveals among the population at large on the issue of wi-fi security.

Our results illustrate the very real problem of the modern world which is that – while massively dependent on the technology – the population is unaware of its capabilities for surveillance and intrusion into their lives.

The problem is that people implicitly trust their technology and are not aware of the implications of that trust.

Further to that: the current problems with technology insecurity all revolve around an unholy pact that has been allowed to develop between the technology and entertainment industries and the public which is designed to foster the idea that the internet is a zone that operates independently of normal rules.

The public is keen to use internet technologies, yet unwilling to pay for the cost of them. So the technology community has become innovative in developing ways to give customers the seamless access to technology that they desire – apparently for free. The costs and the ways in which the consumer actually pays for the service are hidden. Indeed, the technology itself is designed to conceal its workings, so that it is not apparent whether a device is connected to a relatively secure cellular network – the one that appears on the phone bill – or an unsecured wi-fi hotspot.

There is an insatiable pursuit of bandwidth, driven mainly by the desire to have video, data-rich apps and superfast website performance on the move. This appetite for bandwidth (just like the appetite for free things and software on the internet) has blinded consumers to the risks that they are taking. In pursuit of free bandwidth, people are prepared to do anything as our experiment showed with its draconian terms and conditions.

RECOMMENDATIONS

The industry should be more transparent

There is collusion between different branches of the industry. The telecoms industry, desperate to provide consumer confidence and an enhanced consumer experience has short-cut security. The industry needs to be transparent about what it is offering, clearly alerting people to the fact whenever they are on wi-fi that their security is at risk. They should also clearly state what data is being taken from the customer's device in return for that service over and above the terms and conditions.

Network providers should offer device sanctity

Device sanctity means that the personal data – location, contacts, pictures, web searches and preferences – held on a smartphone, tablet or wearable device belongs to the device owner. Network operators and Internet service providers do not have the right to access, harvest or exploit this data without the explicit prior permission of the device owner.

Regulators should act

Strict controls should be imposed and implemented on the way that wi-fi access points can be used to harvest consumers' personal information.

Wi-fi access points should be certified as safe in the same way that https:/ websites display a padlock and colour the URL green to show that they are safe to use.

Regulators, such as the Office of the Information Commissioner (ICO), should do more to alert consumers to potential risks. The ICO has issued a warning about rogue apps, following publication of the Global Privacy Enforcement Network's survey which shows that 85% of apps failed to clearly explain how they were collecting, using and disclosing users' data. But this does not go far enough and there is a need for guidelines that are clear and easy to understand in addition to the legal terms and conditions.

Consumers should protect themselves

Our report includes recommendations from Europol and the ICO about how to protect your security – use a Virtual Private Network (VPN), turn off the wi-fi on handheld devices when on the move and only use trusted wi-fi access points secured with a password.

During the course of this experiment, no user was compromised at any point nor user data exposed in a way that it could have been subject to misuse. We have not logged any user information and, during the experiment, a lawyer supervised all our activities to avoid breaching any laws.

QUESTIONS OR FEEDBACK? PLEASE CONTACT US:

pr@f-secure.com