Security Lancaster | Lancaster University

The Future of Mobile Devices
Security and Mobility

Dr Daniel Prince and Mr Oliver Fitton

Foreword

Contents

Consumption of computing services has been revolutionised over the last two decades with the advent of extensive cheap communications networks and the development of increasing capable mobile computing devices.

The digital divide has been breached due to the falling prices of consumer hardware and connectivity such that in developing countries it is more common to find mobile phones as the primary device for consuming information beyond the television or wired computers.

The mobile phone has become 'smart', tablet computers have moved from science fiction to science fact and wearable technology has gone mainstream. Growing alongside new categories of consumer electronics is a fundamental shift in the way people do business, share information and ideas and how they interact with one another.

The rate of change in society caused by this revolution in mobile computing is increasing and presents a fertile ground of complexity where unforeseen security opportunities and problems can arise. This report facilitates the discussion of mobile device futures by presenting a framework utilising immutable traits of mobile computing and exploring the trends of this technology. Based on this the report presents a thought exercise and two practical experiments to explore the potential security implications.

Introduction

The concept of a self-contained, connected and easily portable device has been with us since the dawn of science fiction. It was not until Alan Kay's PhD Thesis The Reactive Engine (credited as being the first workable conceptualisation of portable computing[1]) that there was a concerted effort to create the first tablet computer. This effort led to the development of the Dynabook and the GRiDPad[2].

Today it is easy to forget that the mobile computer and the mobile telephone were until recently very separate technologies. The mobile telephone began life as military radio communication systems eventually produced for the civilian market as an early car phone in the 1940s.[3] By the time the first iPad was launched in 2010 four billion mobile phone subscriptions were active worldwide.[4] Today smartphones are the nexus for the convergence for these technologies. Smartphones house the processing power of a computer in a handheld, pocket sized device. They offer continuous connectivity to various networks both mobile (e.g. GSM, 3G, LTE) and local (e.g. Wi-Fi, Bluetooth, NFC) as well as being an 'always on' personal organiser and connection to social media.

The advent of the smartphone has gone hand in hand with the development of Apps or applications. Today the Google Play Store and the Apple App Store each house more than 1 million Apps.[5, 6] These Apps can take the form of games, e-commerce tools, productivity tools even user interfaces for Industrial Control Systems (ICS). The App revolution has turned a device which was once a simple portable telephone into an advanced system which allows the user to perform all the tasks possible on a desktop PC on the move.

As well as Apps, peripherals and controllable devices have propagated in support of the burgeoning mobile market. Games consoles, car entertainment systems, medical and even drone technologies can be controlled through mobile devices. The mobile device has become the hub of our personal Internet of Things (IOT), it has become the gateway through which we interact with electronics in our home, at work and at play.

[1] Atkinson, P. "A Bitter Pill To Swallow: The Rise And Fall Of The Tablet Computer" in Design Issues, (2008), Vol. 24, No. 4. pp. 3-25: p 10

[2] Ibid

[3] AT&T. *Technology Timeline: 1946 - First Mobile Telephone Call*, available at: http://www.corp.att.com/attlabs/reputation/timeline/46mobile.html, [Accessed 03/04/2014]

[4] Heeks, R. "Beyond Subscriptions: Actual Ownership, Use and Non-Use of Mobiles in Developing Countries" in ICTs for Development, (22nd March 2009), available at: http://ict4dblog.wordpress.com/2009/03/22/beyond-subscriptions-actual-ownership-use-and-non-use-of-mobiles-in-developing-countries/, [Accessed 03/04/2014]

[5] Rowinski, D. "Google Play Hits One Million Android Apps", Readwrite.com, (24th July 2013), available at: http://readwrite.com/2013/07/24/google-play-hits-one-million-android-apps#awesm=~oA5TF7vDEfBT7g, [Accessed 03/04/2014]

[6] Ingraham, N. "Apple Announces 1 Million Apps In The App Store, More Than 1 Billion Songs Played On iTunes Radio", The Verge, (22nd October 2013), available at: http://www.theverge.com/2013/10/22/4866302/apple-announces-1-million-apps-in-the-app-store, [Accessed 03/04/2014]

Mobile devices: smartphones, tablets, phablets, wearable devices like smart watches have changed how we communicate, access data, capture data, use data and interact with the world around us. The data processing power and data storage capability of a standard smartphone that can be carried in a pocket, across borders or into secure locations is currently comparable to desktop computing capabilities. What was once the reserve of science fiction is now a reality that challenges our current understanding of protection, security and privacy.

In order to start understanding these challenges Security Lancaster held a two day interdisciplinary workshop exploring the future of mobile technology and the possible security issues that could arise. The workshop brought together technical and conceptual experts in fields ranging from Computer Science to International Relations with the aim of exploring the future of mobile devices and their impacts on the security landscape. Contributors formed either a conceptual discussion group or one of two technical teams. The conceptual discussion group considered the future of mobile technology while the technical teams developed new attack scenarios either using mobile technology as a target or as an integral facilitator of the attack.

This report presents the findings of the workshop by outlining the challenges that mobile devices could pose in the future and develop a framework by which the future of mobile devices can be explored. In ***Thinking About The Mobile Future*** the challenges and opportunities created by mobile technology are discussed. Here a framework to map possible future technology landscapes is presented based on three immutable traits of mobile computing – connectivity, storage and processing –and how key trends are shaping that landscape. In ***Mobile Future Shock*** three scenarios of the future based on the previous discussion are presented as thought experiments (in the case of ***London Spring 2025***) or technical proofs of concept (in the cases of ***Pandemic Mobile Malware*** and ***Control Systems***). Finally a conclusion summarizes the findings of this report and recommends areas of further research.

Thinking About the Mobile Future

While the 20th and 21st centuries have seen a level of technological development unprecedented throughout human history, the ability to see into the future still eludes us. Naturally any discussion of future trends in mobile devices can only be based on observations of what is past, what is present and subjective predictions of future demand. What is clear is that demand is increasing.

The western world has an unquenchable thirst for new mobile technology. However this trend is not a peculiarity of the west. Around the world, mobile devices are becoming the primary tool through which the population access information. Demand is increasing in China with Huawei (China's largest mobile device manufacture) seeing a 34% rise in profits mostly due to a booming domestic market for mobile devices.[7] Africa too is seen as a territory of growth for mobile devices. "Somalia has one of the most efficient and affordable cell phone infrastructure in Africa, if not the world."[8] In Kenya the explosion in mobile device adoption (from less than 3% in the 1990's to 93% in 2011) has contributed to economic prosperity.[9]

With this huge increase in demand comes a change in the demography of the internet. Ronald Deibert argues that the biggest factor in the uncertainty of the future of cyberspace is the migration of the next billion people to the Internet.[10] Those billion people will bring with them new perspectives giving rise to new challenges and opportunities as most of them will access the internet through mobile devices. Mobile devices are here to stay and they are going to facilitate a radical change in the internet. However there are a multitude of uncertainties which should be explored in order to get a clear understanding of the way mobile devices will shape our future.

A common assumption is that future mobile technology will continue to perform all of the tasks that current mobile technology does only faster and more efficiently. This results in a further assumption that the use of a mobile computing device will become ubiquitous and socially normative. Considering the plethora of Apps and sensors currently available on mobile platforms (either built into the device or as a peripheral) it becomes difficult to explore what further functionality could be required from these devices. The assumption therefore is that these devices will simply do what they

[7] Huawei Press Release. "Rotating And Acting CEO Eric Xu: Create A Better Connected World", *Huawei Press Centre*, (31st March 2014), available at: http://pr.huawei.com/en/news/hw-331129-annualreport.htm#.UzmEJvldWSp, [Accessed 03/04/2014]

[8] Deibert, R. *Black Code*, (Toronto: Signal), 2013: p. 82

[9] Demonbynes, G & Thegeya A. "Kenya's Mobile Revolution And The Promise Of Mobile Savings", The World Bank – Policy Research Working Paper 5988, (March 2012): p.16

[10] Diebert Op Cit: p. 15

do today only better. This is a common trait found in those technologies that follow Moore's law[11]. These assumptions are also arguably a pure 'technologists' view point, technology changes to accommodate improvements and advances in technology. However, mobile computing has some specific peculiarities that need to be considered in order to start to understand how mobile technology is radically changing our potential future.

In order to help understand and frame future environments, a framework is introduced that enables a user to explore unknown future environments in a robust and repeatable manner. The foundation of the framework is a model of three immutable traits of mobile commuting that were identified during the workshop and via subsequent research. These traits provide the backdrop against which key trends play out. These key trends play a dual role; they identify the most likely course of development based on what has been observed in the development of the field; they identify the most significant loci for singularly disruption events likely to change the terrain of the future environment. The key trends are the dominate forces carving the terrain defined by connectivity, storage and processing, it therefore stands to reason that any significant perturbation in that trend would significantly disrupt the development of the future terrain.

The Immutable Traits of Mobile Computing

Future mobile computing technology and the way mobile computing technology is employed by users will have a symbiotic impact on the evolution of mobile computing. There are three key traits which will develop over time: Data consumption, Data storage and Data processing. Exactly how these traits of the technology evolve will dictate the future landscape of mobile computing. Each of these three immutable traits of mobile computing will be explored here and a model will be developed to facilitate discussion of possible futures.

Data Consumption and Connectivity

Consumption of data is the first immutable trait of mobile computing. Data consumption will be based upon user need just as it is today however user need will most likely increase as Apps develop, lead to new possibilities and as individuals become increasingly active in the digital world. Constant connectivity will therefore be an essential part of the future of mobile computing. Exactly what this constant connectivity will look like is much more difficult to predict. Two possible paths are suggested here which are believed to be at the extreme ends of a spectrum of connectivity.

Firstly it is possible that a single mobile network will replace all other networks this hyper-mobile broadband would allow you to be connected wherever you are through a single provider. This model is justified by the plan put forward by Internet.org which hopes to connect those parts of the world currently unconnected, by creating a patchwork of transmitters using low cost antenna and even high orbit drones.[12] Internet.org and its backers (including Facebook and several mobile technology manufacturers) would then supply the area with a single resilient, high quality connection. In this scenario the plethora of RF chips required to keep a present day mobile device connected would be reduced to just one. Project Loon[13] from Google's Moonshot department is another example of future models of connectivity. Project Loon involves the floatation of high atmosphere balloons

[11] [TODO] Moore's Law Reference.
[12] Internet.org initiative is detailed on their website: www.internet.org
[13] http://www.google.com/loon/

which create a vast network across large expanses of the earth currently left disconnected due to their remoteness. The Loon network beams broadband from a transmitter on the ground to receivers in remote locations via a network of balloons in the air. It's like the world's largest Wi-Fi hotspot. Currently Loon receivers are necessarily large, they have to be mounted like satellite dishes or high gain aerials but it is possible to imagine receivers inside mobile devices serviced by a Loon type infrastructure which ensures a constant high quality connection wherever you go. In these circumstances a single network makes perfect sense.

The alternative route is that networks will instead be even more multiple than they currently are and devices will become adept at scavenging whatever networks are available in order to supply the user with constant access to data. This model takes into account the current proliferation of networks from home, work and public Wi-Fi hotspots to mobile networks like 3G, LTE and GSM. In order to become more adept at handling the changing connections as the device moves, new intelligent methods will have to be developed in order to route through the most useful connection. Mesh networks have been used in various situations where a constant, high quality, secure communication system is not available or indeed not preferable. For example The Free Network Foundation which emerged from the Occupy Wall Street Movement aims to produce a decentralized peer-to-peer network across the US in response to the for-profit networks which dominate connectivity provision.[14]. In more recent times demonstrators in Hong Kong have used ad hoc mesh networks to avoid detection and coordinate their efforts. A more commercial venture in this space is GoTenna[15] which connects to existing mobile phones but provides an alternative communications channel to send and receive messages independent of any central framework

Each of these paths uses a very different method and technology would require a concerted effort in one direction or another in order to achieve these ideals, however the user experience is the same in each of these routes. For the person accessing the email or documents on the cloud they are always connected.

Data Storage

Cloud storage is becoming common place in both personal and business computing. However the futures of cloud service providers are at risk due to privacy concerns and the ease at which personal Network Attached Storage (NAS) systems can be created.

Cloud storage allows the user to store data in a remote location for a fee on a sliding scale depending on the amount of storage required. These remote locations come in the form of server farms which are environmentally controlled and secured by the cloud service provider. Examples of current cloud storage systems include Onedrive (Microsoft), Google Drive and Dropbox. These services allow users to access their data from anywhere they can get a data connection using web interfaces or Apps.

Recent revelations about data privacy such as those made public by Edward Snowden have led to concerns about exactly how cloud storage services operate and whether personal data can ever be truly secure when it is trusted to a third party. These concerns have led some to create their own cloud storage systems using NAS systems either made at home from componentry or bought off the shelf from companies like Western Digital. This allows the user to access their data anywhere in the

[14] http://mashable.com/2011/11/14/how-occupy-wall-street-is-building-its-own-internet-video/
[15] http://www.gotenna.com/

world but does not include the environmental controls and physical security which cloud services provide because the storage is attached to a home network.

The alternative to cloud storage (in either of the forms mentioned above) is to store all data on the device itself. The concept of holding all of your data in a single place is contrary to current trends, but it is possible that an event which drastically undermines public confidence in cloud storage would generate demand for centralized data. Such attacks on cloud storage have already begun, several celebrity users of Apple's iCloud service fell victim to online data theft which resulted in personal photographs being published on social media. Although this incident has not lead to a mass exodus from cloud storage it was limited to a few high profile targets – some mass exfiltration event may have more serious consequences.

Data Processing

Data processing is currently performed by the mobile device, mobile phone manufacturers compete tirelessly to pack the fastest processors into an ever thinner form factor. However there is an alternative to this system. If processing could be performed remotely over a reliable connection the need for energy thirsty processing would no longer exist in a mobile device.

In this scenario mobile devices become "dumb" no longer requiring incredible processing power. At this stage the devices become windows onto the machine on which the processing is done. This scenario is similar to the use of Remote Desktop connections which are used by travelling workers and IT technicians the world over. There are huge advantages in this system, firstly the device becomes much more energy efficient as it becomes the point of interaction between the user and a remote machine. It no longer needs to be able to process complex data requests, this will have a positive effect on the energy efficiency of the device. In this scenario the remote machine may be managed by a cloud processing service in a similar way to cloud storage services. Therefore security and performance would be maintained as part of the terms of services, your devices therefore perform as well as possible according to your contract or the services capabilities rather than based on if you have acquired the latest version of the device from the manufacturer.

Modelling

Based on the examination of these traits, as outline above, it is possible to model each trait as a continuum of possibilities which become a dimension on the possible mobile landscape. The trends, described in the next section, and key disruptive events will help shape that landscape. Connectivity may either come in a uniform mode where the device connects consistently to a single network everywhere or the device will become a scavenger seamlessly connecting to the best network possible based on location, either way constant high quality connectedness will be required. Storage would move on a continuum from entirely cloud based and distributed to entirely based on a device. Similarly processing may occur locally in the device at ever increasing speeds and efficiencies or remotely turning mobile devices into "dumb" machines or windows onto a processing machine. This can be visualised as given in Figure 1

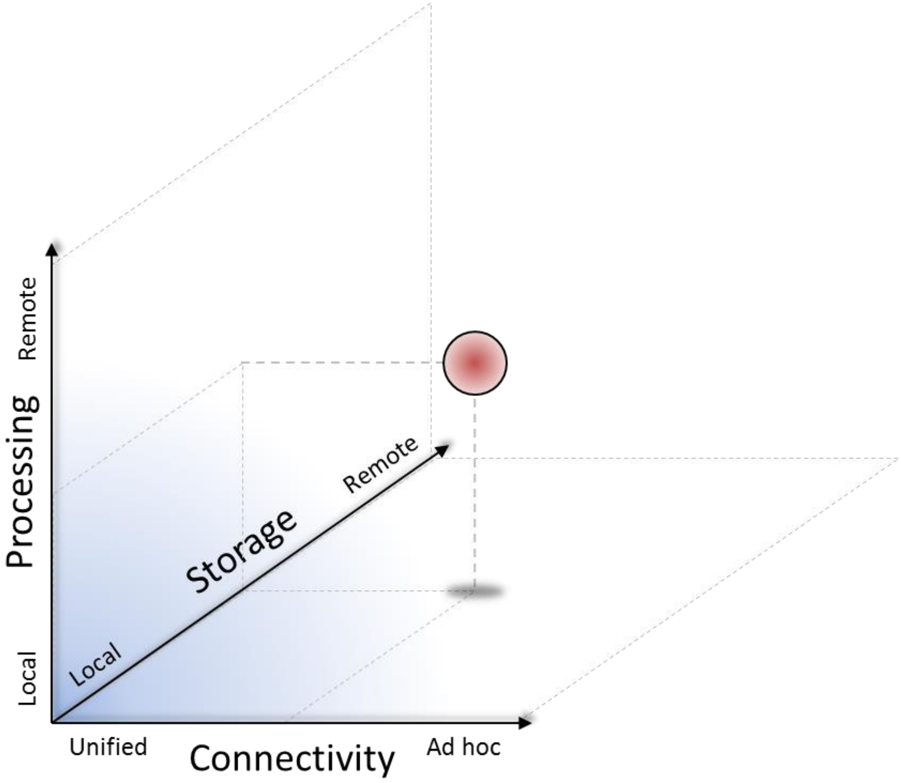


Figure 1: Model of key traits of Mobile Technology

This model was used during the workshop to identify a previously missed combination regarding storage and processing. By decoupling the two during consideration, it is possible to imagine an environment where all the data is held locally on the device, while all the processing is completed remotely. This model has a number of interesting possible drivers, for example, processing is the most energy intensive component so it makes sense to offload this to where energy can be more concentrated. However, storing data locally, including any results generated from the processing, resolves numerous privacy issues.

In Figure 1 a position is modelled that identifies a middle ground in each of the key traits, denoted by the red circle. It can be argued that this is the current state of mobile technology as; the current systems enable significant storage of information locally, but connect to cloud based storage; users take advantage of common providers and roaming coupled with local networks (Bluetooth and WiFi) for localised connectivity; devices have significant processing capability coupled with the potential to run processes and applications in cloud based environments over the web. What will effect this position are a series of key trends that relate to the field. These are identified in the next section.

The Mobile World 10 Years From Now: Key Trends

Given the terrain as described by the core traits of connectivity, processing and storage, it is possible to explore how that might change given key emergent trends. A multi-disciplinary approach was taken to the development of these trends and as indicated it can be argued that these trends provide the dominant mechanisms that will change the terrain of mobile devices. Given their dominance they also highlight the most likely areas that will cause the most significant disruption, for example, consider Energy. It is common place that a modern smart phone rarely gets through a single working day without the need for charging. This has led to a secondary industry in the provision of external power packs and aftermarket batteries. A significant disruption in this trend, a new advancement in power storage or environment power harvesting, would have a major impact on mobile devices ability to process more or have longer range communications systems. Could such a change create a model where mobile devices move away from cloud processing to do all processing locally, or perhaps a move to a unified communications system?

The Next Billion Connected Users

How technology is employed by users forms part of the dichotomy which dictates how mobile technology will evolve in the future. How users employ their technology depends on their location, motivations, objectives and resources. The internet was first developed from a US defence and academic project, the World Wide Web was developed from a European research initiative, it therefore stands to reasons that the first adopters of the internet were those fortunate enough to live in the west.

Today for every person with access to the internet there are two who are unable to connect. Those people are mostly located in areas of Africa, Asia and South America, but they will not stay disconnected for long. The internet possesses too many opportunities for developing communities; including supplying educational resources, medical advice and even weather reports to farmers. The adoption of the internet throughout the developing world will see a demographic shift in the internet. Who the next billion users of the internet are, how they want to use the internet and the content they add to it will change the character of the internet dramatically.

The majority of internet users in developing regions are connecting through mobile devices rather than desktops. There are various advantages to this: portability, cost and flexibility being chief amongst them. This trend is likely to continue which will result in mobile devices evolving to meet these demands. Project Ara[16] seeks to develop a new concept of mobile devices to appeal to suck markets. User can add and remove hardware 'blocks' from the device depending upon their need. This keeps costs to a minimum, a user can purchase a single chassis and the upgrade their device over time based on their needs. If a camera is required the Ara user could simply purchase a camera 'block' and slide it into the device chassis rather than buy an entirely new handset. Innovative projects like Ara have the potential meet the requirements of new internet users and to forge a new path for technology in the region. Once those people who can benefit most from Project Ara type handsets get their hands on them it is difficult to predict what the next user driven technology innovation will be.

[16] http://www.theverge.com/2014/4/15/5615880/building-blocks-how-project-ara-is-reinventing-the-smartphone

Consumerism

Considering the volume of people still not connected it is no surprise that technology giants are in heavy competition to secure their next crop of customers. The hunt for profit and consumerism will continue to dictate the development of mobile devices as it does today. New models of monetization will continue to be developed in an effort to gain the upper hand in the scramble for the next billion users. Technology companies do not just sell functionality they sell a lifestyle with their products, this trend will continue but stands to be undermined by the freedom which 3D printing will bring to the market place.

Google's project Loon and the Facebook supported Internet.org are clear examples of technology giants targeting the internet's future demography. By controlling connectivity they will be able to sell their wares to new markets and develop new products to satisfy the needs of new customers. In an effort to achieve dominance in new markets Google and Facebook are attempting to bring the cost of connecting to their products to zero. This "zero-rating" is achieved through negotiations with telecoms providers (made easier if you *are* the telecoms provider, as Google and Internet.org hope to be). By reducing the costs of their services technology companies open themselves up to developing markets, increasing advertising revenue and the sale of their other services.

Another form of consumerism which is set to define the future of mobile devices is the commoditization of personal information. Sites like Facebook create revenue from user's personal information, such information guides advertising investment and allows highly directed marketing. In recent years there has been a backlash against such practices and a call for more stringent privacy guidelines to be used by technology companies. However this threat to privacy could be seen as an opportunity for the user if they were offered recompense for their personal information. This recompense could be in the form of products, services or discounts. In return the technology company would receive personal data without the privacy headaches and a more detailed profile to sell to advertisers.[17]

While function will no doubt be the paramount concern for mobile devices in developing markets fashion drives mobile device sales in developed markets. This trend is likely to continue as long as manufactures continue to sell a lifestyle alongside their products. The obvious example of this is Apple's aggressive marketing, famously the "I'm a Mac, I'm a PC" advert series which left the consumer in no doubt that buying an Apple product was a lifestyle choice not a functional one. Indeed some mobile users become factional in their devotion to their devices, operating system and the lifestyles attached to them. Apples latest product category the Apple Watch is an explicit convergence of fashion and technology. However for the first time there is a potential challenge to the dominance of these marketing techniques. 3D printing in the home will mean that users will have the ability to develop their own hardware undermining the monopoly of technology giants over the devices available to them. Already it is possible to print new cases for mobile devices, soon mobile devices themselves or at least their shells may be manufactured at home.

The Personal in Personal Devices

A smartphone is often considered to be a personal device. However, there is something much more personal about such a device, over and above say a Personal Computer. A personal computer is a computing device that is consistently used by a single individual that can be customised to that

[17] http://www.bbc.co.uk/news/technology-11571513

individual in terms of desktop background, fonts, the way information is stored and organised, the types of hardware that does the processing and storage. In contrast a mobile phone is an intimate device. It goes everywhere with the owner often being carried close to the body. The data it contains includes methods of communication with important peers and highly personal imagery since photography functionality has been consumed by the ubiquity of the mobile device. In fact mobile devices have become the touchstone for our digital personae across multiple social media. The smartphone has also become the eyes and ears of our digital personae, feeding relevant physical data, images and audio to each of our digital avatars.

This functionality creates a much more personal 'relationship' with the device, which has been extrapolated to the nth degree in the recent Spike Jonze film *Her*, which sees an individual fall in love with the AI in his mobile device. The relationship between user and device fuels a more dynamic driver to shape the functionality, performance and capability of the device. In fact it can be argued that for mobile computing, the societal input provides as much evolutionary stimulus as advances in technical capability. Therefore, advances in mobile technology will not only come about through advancements in technology, but also in the way the individuals and societies create demands on the personal interaction with such technology.

Today we access data using Human Machine Interfaces (HMI) such as a keyboard or a mouse. There are trends in more direct connections such as the Kinect (Microsoft) which users advanced imaging to track body movements directly or Leap Motion an alternative to a mouse capable of translating human hand motions into three dimensional computer instructions. Google Glass provides a floating heads up display that can be navigated through using voice commands or a touch pad on the side of the wearable device. Work continues into direct neurological control over machines however it is hard to see such techniques becoming common place in the next 10 years.

Today mobile devices are nearly entirely controlled using a multi-touch screen with the option to add a peripheral keyboard and in some cases an integrated QWERTY keyboard. At this point fashion and manufacturing techniques intersect. There is little chance that the fashion side of the consumer electronics industry will slow over the next 10 years as manufacturers sell a lifestyle associated with their products rather than simply their technical capabilities. When this is combined with new manufacturing methods such as 3D printing it is possible to envisage a future in which mobile devices are infinitely customizable based on personal taste and fashion. The Google project Ara[18] and Phoneblocks[19] are starting to extend this flexibility concept in the form of a smart device that will enable users to buy new modules to upgrade capabilities in a similar fashion to that which is found in current desktop systems. This concept affords the opportunity for mobile computing platforms to become infinitely customisable to the personal taste of the individual, include the possibility of using additive manufacturing (as seen in project Ara[20]) to fully customise the look and feel of the mobile platform.

Mobile devices are not only our primary window onto the vast data that the internet provides us with nor are they simply devices for the sake of fashion. Mobile devices are advanced sensing equipment with high quality cameras for photography and video recording, they include microphones, accelerometers, thermometers and even 3D imaging capabilities. While it is hard to

[18] http://www.projectara.com/#project-ara
[19] https://phonebloks.com/en
[20] http://youtu.be/_Q1JzJadgHY

imagine adding any more sensors to a mobile device (again they are likely simply to get better at what they do) it is possible to consider how these personal devices might impact our health.

Already there are peripheral devices such as the Nike Fuel Band or Scanadu medical tricorder which sense, record and analyse biological information about the user. These consumer electronics and fitness products are just the tip of the iceberg, insulin pumps and pacemakers are now controllable wirelessly.

In the future medical technology will be controlled and monitored through mobile devices. Using these devices will allow medical professionals to be able to quickly and efficiently diagnose and treat individuals based on telemetry from mobile devices. The mobile phone or tablet will become a key fixture of the medial landscape, saving health services large amounts of time and money by reducing the amount of time it takes to diagnose an illness. Indeed these mobile devices may become so effective and cost saving that it becomes a requirement of health insurance providers or national health services that individuals poses a mobile device. Mobile devices could become prescription.

The adoption of mobile devices by the health industry will also have an impact on the demography of mobile device users. Prescribing mobile devices is likely to be a much greater incentive to a resistant older generation than traditional marketing tactics.

For more about the emerging mobile health market see the authors' previous article "Why Apple is pitching for the health market" (https://theconversation.com/why-apple-is-pitching-for-the-health-market-27781)

Energy

Part of the mobility concern for mobile devices includes self-containment. Each device therefore needs to perform all of its functions in a single compact form factor; from human input to how it displays data, connects to communication networks or records audio and video. All of these functions define modern mobile devices and require energy. Battery life and size will therefore become an increasingly important factor in the production of mobile devices. Apps and hardware will allow users to perform ever more demanding tasks which will require ever increasing quantities of energy. For example the mining of crypto currency like Bitcoin, a high energy consumption activity.[21]

Batteries will not be the only consideration in the name of energy efficiency, more efficient componentry will have a huge impact on the amount of energy required. One example of where componentry might be reimagined in the name of energy efficiency is Radio Frequency (RF) chips which are used in all mobile devices to transfer data through various radio networks such as 3G or Wi-Fi. The number of networks a device can connect to is dependent on the RF chips present in the device. A reaction to a push towards more efficient devices could see RF chip functionality being combined into single chips or the removal of certain network connections entirely.

Boarders

The use of mobile computing devices is fundamentally redefining the way that individuals and governments are thinking about borders and sovereignty. The Westphalian state system provides a traditional view of sovereignty and of country borders that are easily definable in terms of physical

[21] Tabarrock, A. "The Real Cost Of Virtual Money", *Marginal Revolution,* (3rd December 2013), available at: http://marginalrevolution.com/marginalrevolution/2013/12/the-real-costs-of-virtual-money.html, [Accessed: 03/04/2014]

geography. This concept of borders specifically identifies how an individual transitions from one set of legislation to another, it is nearly impossible to be subject to the laws of the home nation state and the foreign state. In this way state legislation does not intersect. However, human mobility, coupled with digital technology punches “wormholes” through these borders, thus presenting an individual that is present in at least two, if on three nations simultaneously, thus causing a nation state intersection.

Much effort has gone into legislating the control of information in terms of privacy and access, with the result that even in the European Union there are a complex number of laws that can be applied to a specific situation in regard to data access. For example, an American company would be subject to the Patriot Act which would allow the US government to access data held on the company’s servers wherever they may be sited in the world. However, within the EU nations, there are tighter restrictions regarding such access. Therefore, an EU citizen utilising an American company’s service would have a variety of legislation applied to them when they access data generated or held by that service. This results that this individual would create a new intersection between nation states, specifically their respective law, which is not tied to the physical topography and also has a very specific time based component; the intersection only occurs during the time of access.

The use of the term intersection here is intentional. The Westphalian model does not allow for the notion that nation states can overlap, they can only exist bordering one another. Within this construct of an individual accessing the services/data of a company subject to the laws of another nation state, then for all intents and purposes that individual exists under the jurisdiction of both nations simultaneously creating a “pocket” intersection of the two nations. This concept can be extended further if the individual is not within their own home nation. Here, the citizen would have an overlap of the laws from the home nation, the visiting nation, and the service provider’s nation for the duration of access.

In this approach the physical individual is treated as the nexus of the overlap. However, the individual can be considered as a virtual self, existing as a set of automated processes in the environment of the service provider and therefore subject to the providers computational rules. These processes automate the task of information aggregation and dissemination to a defined social group. An example of this is Facebook. Facebook provides a set of services to communicate either instantly or via posted notifications. In addition, to this Facebook provides the capability to aggregate information from other social media sites, such as photos form Flickr or Instagram, geotagging from Foursquare. This integration is often automated, so a post to Foursquare will automatically appear on Facebook making life simpler for the user. Therefore, as with the physical notion of an intersection for that individual and set of nations, the virtual self has that same effect in the background.

An important concept here is that the configuration of the intersection is time-bound as it only exists when the individual accesses the data/service provided by a company in a different nation state. This concept of adding time as a dimension is vital to understanding the intersection. The complexity by which services in different nations are combined to provide utility for an individual in another is facilitated by constant additions of new services configured using a number of different services. Unlike traditional approaches to combining or establishing comparable legislation, the way the service accessed function may change on a daily, weekly or monthly basis. The concept of the cloud is an example of this flexibility in infrastructure. Services and/or data provided by a cloud infrastructure can be seen as transient, for example consider a cloud based email service. During one 24hour period a British user may access the processing part of the service which is running on hardware based in Ireland, while the data is held in storage maintained in a data centre in Germany. Yet the flexibility of the cloud infrastructure enables the processing capability in Ireland to fail and the service to seamlessly migrate to processing hardware in say France. The impact of access a service from the UK, with processing in France and data held in Germany is not felt until the user (or a digital representation, actually uses the service. The complexity of the underlying model can be increased by considering these added dimensions, more services interacting in more nation states, and therefore increasing the complexity of the intersection. But that complex intersection only exists within specific time bounds which may be very short lived and is infinitely customisable based on the user, the services to which they subscribe and even the type data they produce.

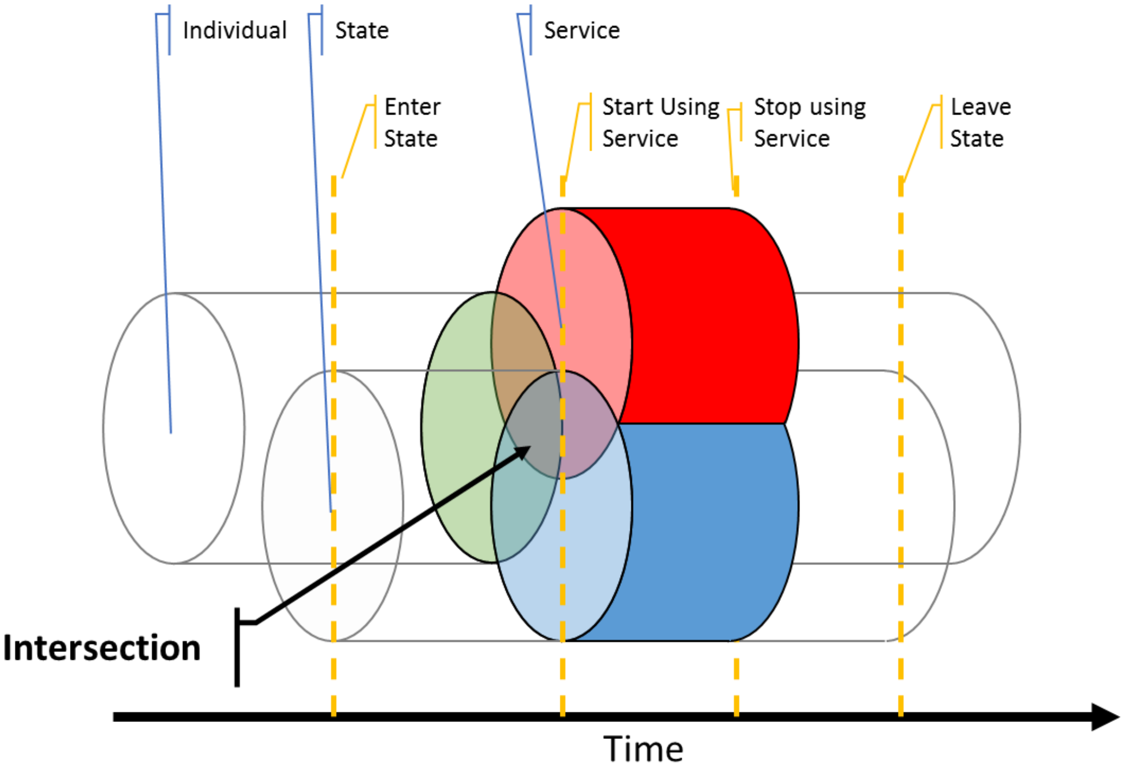


Figure 2: Model of how mobile computing breaks down the traditional notion of borders

Mobile Future Shock

In order to contextualize mobile futures 10 years from now and to consider security threats which might emerge from those trends three scenarios will be discussed. Each of these scenarios is based in either historic events being reframed in the context of future mobile technology or on mobile technology which is available now which could become more common place in the future.

The first scenario discussed is the **London Spring 2025** a riot scenario which mimics the London riots of 2011. This scenario was constructed entirely based on conceptual discussions between experts about how future mobile devices could be used by both protestors and responders if civil unrest were to break out again in central London in 2025.

Alongside the conceptual debate technical exercises were carried out to push the boundaries of mobile device security. The following section details two experiments mounted by Security Lancaster Researchers. The aim of these exercises was to demonstrate what is feasible today in order to inform debate of what may be feasible in the future. Two teams were each given two days to demonstrate their vector of attack.

The second scenario **Pandemic Mobile Malware** is taken from a technical exercise using currently available mobile devices and software in order to demonstrate the threat of mobile malware. The technical team developed a method to infect mobile phones using an ad hoc Wi-Fi network which bypasses corporate security systems. This scenario points to the technical threats which cybercrime poses to mobile devices.

The third scenario **Control Systems** demonstrates the ability of mobile devices to attack control systems. This is a technical demonstration which used malware launched from a current smartphone to shut down an Industrial Control System. This technical exercise will be removed from the industrial environment and the implication of this kind of attack applied to medical equipment for example an insulin pump.

London Spring 2025

14 years after the riots which tainted the summer of 2011 the population of the British capital is once again discontent. In 2025 the population is connected at all times via mobile devices which have become more energy efficient and faster with more detailed sensing equipment. These mobile devices offer new opportunities for the protestors but they also allow responders new methods by which to take action, before during and after the events.

Mobile devices will offer protesters advantages as a communication and organisation platform and as a sensory platform. The objective for the protester will be to effect some form of political change (no time was spent on considering the exact cause of the riots but the general assumption was an economic imperative, either unemployment or financial hardship) by destroying property and demonstrating discontent publicly. This would no doubt involve clashes with security forces and high profile stunts or attacks. In order to effect political change the riot movement will need to be organised (Where are demonstrations going to take place? What is to be targeted for destruction?) and publicised.

Communication Platform

Because everyone is constantly connected in 2025 communication between protestors will be extremely easy. In 2011 rioters used social media and instant messaging Apps to organise where to meet in numbers.[22] In 2025 it is reasonable to assume that this coordination would again be desirable. By 2025 current social media and instant messaging App such as Facebook and Twitter or Whatsapp and BlackBerry Messenger may become redundant either being replaced by services which better fulfil the needs of the market or because users distrust social media and messaging services with their personal information in the light of privacy revelations as discussed in the previous section.

Privacy concerns may lead to more sophisticated and less easily tractable forms of communications such as Peer-to-Peer instant messaging service where communication is entirely decentralized such as GoTenna. In 2014 there are Apps which allow communication between mobile devices which are theoretically immune to man-in-the-middle attacks thanks to the use of in person key exchange such as SafeSlinger.

Darknets

An important consideration her is the ease with which completely decentralised ad hoc networks may be formed in order to support communication. Currently mobile platforms rely on central communications infrastructure to provide data access. This provides a crucial control mechanism, both in terms of completely restricting access, denying access to the central infrastructure, and monitoring communications, everything has to go through the central infrastructure providing easy access points to tap communications, even peer to peer.

Current mobile communications platforms provide a wide variety of communication mechanism, from the 3G/4G infrastructure based communication services to WiFi, Bluetooth and a plethora of homebrew communication add-ons. Many of these communication systems already support an ad hoc mode that enables groups of individuals to form a communication group for the transfer of data independently of any core infrastructure. What is not widely deployed is the technology to form what is called a multi-hop network where messages can hop from one user to another beyond the immediate group. However, this technology does exist and has been under active research for over two decades. The ability to send messages privately relying on the support of others, rather than through a central infrastructure makes it much harder to control access to, or monitor, communications between individuals. In the context of a riot this ability would be advantageous; being able to co-ordinate without a reliance on an infrastructure that is controllable by the government of the day. This type of network infrastructure was discussed in the modelling section as a completely scavenged ad hoc network.

[22] Mackenzie, I. “Is Technology To Blame For The London Riots?”, BBC News (8th August 2011), available at: http://www.bbc.co.uk/news/technology-14442203, [Accessed: 03/04/2014]

What is lacking is the impetus to make such technology mainstream so it is available to be used in the context of the environment of the London riots 2025. However, clearly a privacy push resulting from one or more events could be the trigger. The production of the "redphone" which provides encrypted call services is the first spearhead of such a push, however, this has still yet to be widely adopted. Another more likely driver is that of cost. The ad-hoc multi-hop network would significantly reduce down the cost of access to information as the peer formed network does not rely on a paid for service to access the communications infrastructure. With the cost of smartphones significantly falling resulting in mass adoption, coupled with a free communications service as an economic driver this type of network infrastructure becomes viable. The overall result is the provision of a network in which the communications are hard to trace and prevent.

Sensor Platform

As discussed in the previous section mobile devices are not expected to contain a vast quantity of new sensors beyond those that are already available and have been staples of mobile devices for some years now. However the integration and quality of these sensors will no doubt be much better than today. 3D imaging, higher quality imaging in low lighting and higher quality video imaging sent real time over a network could all have noticeable impacts on a riot movement. However it is likely that the key impact that a more advanced sensor platform would have for riots in London in 2025 would be as a means of distributing real time information for publicity purposes.

Precedent of this was set during the protests commonly referred to as the Arab Springs of 2011. While it would be a mistake to suggest that the revolutions and political restructurings in the Arab world were due to mobile devices and social media (only 5.5% of the Libyan population had access to the internet before the 2011 revolution[23]), mobile technology did play a key part in televising the revolution and drawing the international community into the movement. Still and video images of protests and the often heavy handed response of security forces were captured by citizen journalists on their mobile devices and then uploaded to video sharing sites like Youtube or sent directly to regional television networks like Al Jazeera where they were relayed to the world. Protesters now had the platforms on which to tell their stories and to attract support both locally and from international actors including states, international organisations and diaspora communities.

It is easy to imagine that an enormous amount of real time data could be generated by rioters using mobile devices in 2025. This data might be direct video, photography or audio shared at will through social media or it might be data created without the user's knowledge or direct action such as location data. This data will create a wealth of information available for the social and conventional media which will publicise the events.

Response

While mobile devices offer great opportunities for rioters in this scenario they also offer the various responders new or advanced opportunities. While responders to riot situations could really include paramedics, business owners, politicians, charities and more this scenario only considers the response of the various security forces which would be charged with maintaining order in the event of riots.

[23] Scott-Railton J, "Revolutionary Risks: Cyber Technology and Threats in the 2011 Libyan Revolution" in CIWAG Case Study On Irregular Warfare And Armed Groups, (CIWAG: Newport, 2013): p. 19

Monitoring

The privacy revelations which have been discussed throughout this report will not deter security forces from monitoring communication networks. Indeed the revolutions of 2011 and the disturbances in London and other UK cities acts not to deter security services but promotes them to attain greater levels of monitoring and to be able to process monitored data more effectively. This monitoring may be embedded either in code or in the forms that Edward Snowden has so far discussed with disclosures from corporations. The constant connectivity of mobile devices and their expanded roles in our lives due to their projected capabilities will make the amount of data collected in this monitoring and the quality of that data an extremely valuable resource for security forces who will try to disrupt destructive protests before they can gain traction.

In 2014 it is possible to monitor riot activities without going so far as to invade the privacy of a population. Indeed it is possible to use public information such as social networks in order to build up a picture of events as they unfold, it is sensible to assume that techniques for processing this data will become more advanced in the next 10 years and also that the amount of real time personal data available online will increase. Social Media monitoring will therefore form a large part of the security forces response to London Riots in 2025.

Unplugging

The Arab Springs taught us a great deal about how responses play out in civil conflicts where the internet is used as a tool of decent. Authoritarian regimes have been known to go so far as to completely cut access to the internet to the entire population in response to unrest. This has happened occasionally in Syria and also, with interesting effects in Libya.

Libyan internet was controlled by the state and remained active well into the Civil War. Rebels used the Libyan internet infrastructure in order to communicate between themselves and to send instructions to external partners. For example NATO was sent Google Maps which located Gaddafi's assets by rebel spotters on the ground. This was a primitive but effective form of information sharing. In order to stop this activity the Gaddafi shut down Libyan internet with the intention of stopping the rebel's main source of communication.

However in an attempt to gag the Libyan rebels the regime blinded itself. The rebels simply started using other networks, particularly VSAT systems which used satellites to access the internet rather than the land based infrastructure. Because rebel traffic was no longer going through the Libyan system Gaddafi's forces could no longer eavesdrop on the communications, Gaddafi had driven his enemies to more secure forms of communication and information was still getting out to NATO.[24]

When this scenario is considered along with the sheer dependence of the UK on the digital economy it is impossible to envision a scenario in which the government would shut down networks in an effort to stagger the protesting movement.

Proxy Army

There is another more sinister lesson which could be learnt from the Libyan experience of 2011. With no way of spying directly on rebel communications the Libyan regime set up the Libyan Electronic Army in order to monitor and disrupt the rebellion online. Civilians in Tripoli were paid to use social media to send disinformation and even malware to key rebel figures. It would be political

[24] Ibid p. 38

suicide for a democratic western government to start attacking its own citizens in cyber space, but "On the Internet, nobody knows you're a dog."[25]

It is entirely plausible that security forces could pose as one or more hacktivist groups who are pro-government (like the Syrian Electronic Army) or are in some way oppositional to the rioters and use any means they like in order to disrupt the movement under the camouflage of the internet's ability to make every user anonymous. In this instance the lack of attribution which hinders legal challenges by governments would work in their favour as they spread malware, phishing attacks and subversive information while disguised as a non-government affiliated hacktivist organisation. These lessons have been learnt from the Assad regime's relationship to the Syrian Electronic Army (SEA). The relationship between the two is murky which allows Assad to plausibly deny knowledge of the SEA's activities while benefiting from their endeavours.

This is an extremely troubling possibility but it is the payoff for individual anonymity online. Governments can enjoy it too.

Prediction

There has been a great deal work done in an attempt to predict riots, even down to studies into the ambient temperature which most likely lead to riots.[26] These studies are traditionally done after the fact once data sets have been collected and cross referenced but in 10 years it is likely that these kinds of studies could take place using data collected from mobile devices as the riots take place or even before.

In the introduction it was suggested that health devices will monitor our state of wellbeing and control medical equipment. It stands to reason that the government would step in to secure medical information about the British population rather than allow it be in the public domain. In this scenario mobile devices send live information about a person's wellbeing (heart rate, blood oxygen levels, stress etc) to a government controlled datacentre secured for privacy purposes. This information could be cross referenced with publically available social media and GPS data in order predict when riots are likely to happen as stress levels rise amongst amassed groups. Naturally accurate predictions would require a great deal of study into the biological signature which rioting behaviour provokes or which provokes rioting behaviour before this could be workable but it is not beyond the realms of fantasy.

Legal Proceedings

The much more likely scenario is that the response from the British Government and its security forces would be the same as it was in 2011, the security forces would exercise restraint where possible and very little would be done in order to invade the privacy of rioters and disrupt communication networks. Instead the security forces would concentrate on building evidence against rioters in the hopes of convicting them in a court of law at a later date. Mobile devices offer

[25] The New York Times, "Cartoon Captures Spirit Of The Internet", The New York Times Archives, (14th December 2000), available at: http://www.nytimes.com/2000/12/14/technology/14DOGG.html?pagewanted=1&ei=5070&en=f0518aafeccf36fd&ex=1183089600, [Accessed 03/04/2014]

[26] Merril Carlsmith, J & Anderson, C A. "Ambient Temperature And The Occurrence Of Collective Violence: A New Analysis" in *Journal of Personality and Social Psychology*, (1979), Vol. 37, No. 3, pp. 337-344: p.337

responders a wealth of evidence with which do prosecute a rioter and in the future it is possible to suggest that the indelible digital fingerprint of a rioter will be more detailed than it is today.

Mobile devices push personal information into the public sphere. This could be done by conscious choice (checking in to a location on a social media site), by mistake (if the user has not turned off location data on certain Apps and they are not off by default) or by information being leaked into the public domain (for example Wikileaks or various hacktivist data exfiltration examples). In this situation the user themselves leaves a trace for responders to collect as evidence in a public domain either intentionally or unintentionally.

Because mobile devices will be constantly connected in 2025 and because they will have advanced as a sensory platform the responders will also have a much great wealth of information to trawl through in order to locate a person not simple a device to an event. High quality, even 3D video taken by rioters and uploaded to public environments will make facial recognition of rioters a simple task. It therefore becomes very easy for the responders to allow the riot to continue as safely as possible while collecting a wealth of data to be used in prosecutions when the situation is over.

Pandemic Mobile Malware

Contributors: Pauline Anthonysamy, Philip Garner, Rajiv Ramdhany

Mobile phones are a ubiquitous data storage processing and transmission platform, intrinsically trusted by their owners and by others via inference of trust in their owners. Further, these devices are discrete, so while it is assumed that the majority of people are carrying them it is not obvious whether they are on or what capabilities (types of wireless connectivity etc) are enabled. These features present new opportunities to develop malware that can be distributed by exploiting these unique properties in comparison to more fixed computing capability such as the Desktop PC. This experiment sought to explore the possibilities in the space for the advanced distribution of malware to bypass existing approaches to preventing access to systems and data within a target organisation.

A significant number of data breach incidents (examples include: US retailer Target data theft, Dexter malware campaigns, Neiman Marcus data breach) point to organised criminal gangs as cybercrime perpetrators who actively seek to steal data from organisations for monetary gain. Advanced Persistent Threats (APTs) and nation state actors are sophisticated perpetrators targeting the theft of intellectual property for financial/competitive gain or attacking critical infrastructure for strategic and economic motives. The Stuxnet, Flame and Duqu attacks saw sophisticated malware penetrate systems with previously unparalleled sabotage or espionage consequences thus exemplifying the virulence of these new threats and the level of sophistication open to a range of threat actors.

In the face of this increasing technological threat typical approaches seek to increase the strength of their technological defences through improvements in defensive technologies such as firewalls, network anti-virus and intrusion detection systems. More sophisticated, data-exfiltration-aware organisations deploy data loss protection solutions within their network infrastructure and take measures to detect and prevent sensitive data from leaving their control. Very sensitive data may be placed in specialist networks that are isolated or ‘air-gapped’ meaning they are not connected to any other networks.

However, all these approaches have one thing in common, a set of human operators. Therefore the human infection vector enables an opportunity for novel solutions to bypass these previously identified defences and others. And what better way to do that than to control the personal mobile computing platforms those humans carry with them. Mobile phones and ad hoc network connectivity are therefore a significant potential attack vector for infiltration target systems and networks with the aim of obtain control of them and exfiltration of sensitive data.

A command and control structure is often used by attackers when attempting to control a large number of computing devices that have been compromised. The aggregation of the compromised devices into a large group is often referred to as a BotNet and enables the owner of the command and control infrastructure and compromised devices, known as a BotHerder, to issue commands to the 'bots' to carry out different types of attack. Traditional command and control-based attacks can be disrupted reconfiguring parts of the core infrastructure of the Internet to primarily stop the bots from talking to the command and control systems. This can be achieved for example by stopping the Bots from finding the controller computers by reconfiguring the Domain Name Service, the mechanism that maps human readable names for computers, to machine addresses on the Internet, to ignore requests to known controller computers. But what if the command and control infrastructure and the bots did not need a core network to communicate. A plausible scenario is therefore using mobile phones to host the command and control server in an exfiltration attack. Even in the case of air-gapped systems, malware installed on the hosts can connect to a command and control server hosted on an attacker's phone; the phone acts as a mobile hotspot.

The sequence of actions in this exfiltration scenario is as follows:

1. The targeted host is infected with custom malware via spear-phishing or social engineering means.
2. The malware remains hidden on the host but occasionally will wake up and scan the WiFi spectrum for wireless networks.
3. The attacker turns 'on' a C2 Server Android app on his phone and walks across/ around a building where the compromised hosts are found.
4. The C2 Server app turns the mobile phone into a WiFi hotspot
5. When the phone is within wireless range, the malware instances detect the presence of the mobile hotspot (through a specific SSID) and register with the C2 server.
6. The registration handshake protocol allows the malware to push hosts details to the C2 Server and receive configuration commands (sleep periods, enumeration , etc) or tool updates.
7. After the brief handshake, the malware uploads collected and aggregated data files to the command and control server
8. The command and control server can, if the attacker wishes, upload the received data to other servers (email, cloud-storage, social media)

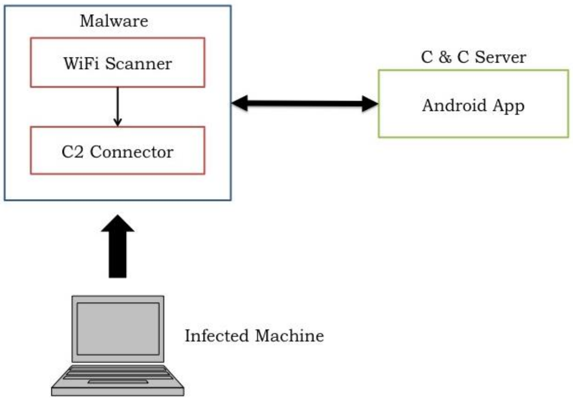


Figure 3 Bring C2 in stealthy proximity to compromised hosts

The feasibility of the concept outlined above was demonstrated through the implementation of a C2 server application for the Android platform and a piece of Java malware for PC based targets. As can be seen in Figure xx.

A particular variant of this exfiltration scenario is having the C2 Server itself running as malware on the mobile phones. This would require an additional infection vector in order to compromise the mobile phone, such as through visiting a compromised website or Wi-Fi hotspot. Multiple mobile phones could be infected in order to run separate C2 Server instances to form a pervasive and resilient stealthy C2 infrastructure that can coordinate the operation of data collection malware. The infection vector may be via either those identified previously, or by one infected phone utilizing wireless connectivity, wi-fi or Bluetooth, to exploit vulnerabilities to infect vulnerable devices. Through the use of ad-hoc routing protocols, they can even provide multi-hop connectivity to malware on hosts, bypassing the corporate network entirely for data exfiltration.

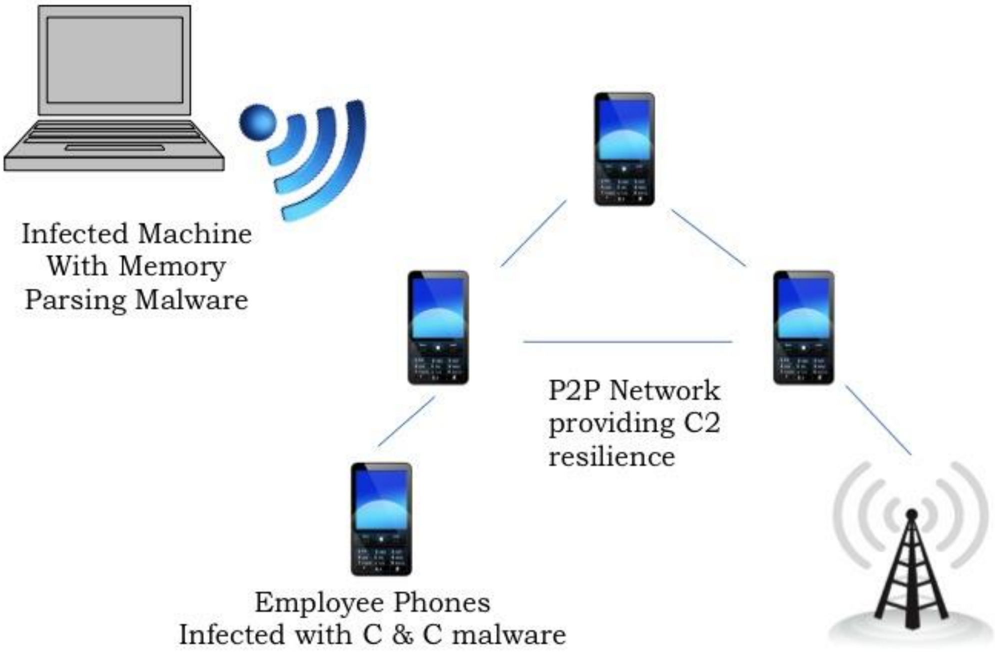


Figure 4: BYOD? When C2 comes to the workplace

Conclusion

The presented scenario, coupled with the developed demonstration shows the feasibility of this type of attack. Mobile phones are computationally powerful, highly connected devices. With the right software they are able to form completely independent ad hoc networks that can be used to transmit data independently of any core network connectivity, such as the mobile phone data network. If this capability was used in conjunction with a C2 platform and software able to exploit vulnerabilities in wirelessly connected devices it would be possible to establish a Bot infrastructure that would be difficult to track and very virulent in its ability to replicate and grow.

Control Systems

Contributors: Benjamin Green, Ben Paske and William Knowles

In the future mobile devices will be a key way in which we interact with control systems in industrial setups such as power plants, utility stations and transportation networks and in our daily lives including our personal health. Control systems are starting to become pervasive as home automation becomes increasingly popular. This scenario and proof-of-concept demonstrates how an Advanced Persistent Threat (APT) could damage a nation state's critical infrastructure through exploiting the personal mobile devices of individuals that support these systems. These mobile devices would not need to be used within the critical infrastructure itself; through being carried upon the engineer's person they can be used as points of access into the network infrastructures that support the industrial control systems. The ability to target a control systems using a mobile phone demonstrates the feasibility of using mobile phone to target other control systems used in other domains such as in the heath sector for example insulin pumps or pace makers.

The three main design requirements for the proof-of-concept mobile malware:

1) It should be able to identify and fingerprint devices used within critical infrastructures.
2) It should able to execute exploits that impact the operations of critical infrastructures.
3) The malware should provide remote shell access to the attacker.

Fingerprinting of devices was achieved using a publically available tool called PLCScan. This was modified to run on the Android platform using the Scripting Layer for Android (SL4A). In addition, a native, simple Java app version was implemented that provided a simple fingerprint capability of attempting to connect to devices using the S7 protocol port of 102. This application also hide the activities of the scan inside what appeared to be a harmless application and ran the malicious code in the background.

The exploit used in this demonstration was developed by NSS Labs and has the ability to send CPU Stop commands to S7-300 programmable logic controllers (PLCs). This exploit is normally run inside the Metasploit penetration testing framework which is not available for the android platform. Again SL4A was used to provide execute the exploit code by exporting it from Metasploit as a python script that can run on SL4A.

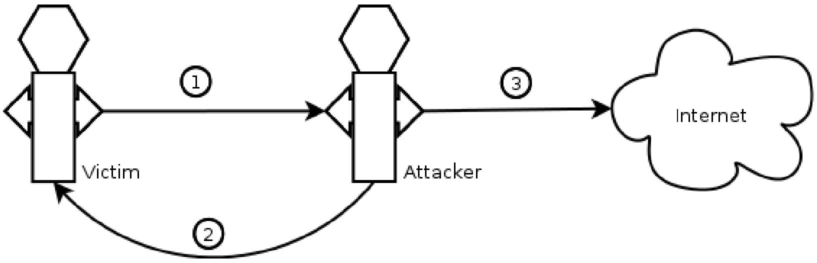
To provide access to the compromised device Metasploit was again used for generating an Android-based reverse shell payload either providing access to a basic command shell or using their inbuilt meterpreter engine. Either could be used for the proof-of-concept malware, and their functional performance was confirmed over a simple test scenario on the critical infrastructure WLAN network. In the actual malware scenario described later, this shell would operate over a phone's 3G connection. Maintaining a persistent reverse connection to a victim's device would likely impose a large computational load on the device itself which would increase chances of discovery. To overcome this issue we propose (but have not implemented) the use of Android's Geofencing functionality. Using this functionality, it is possible for an App to lay dormant until the device falls with a set distance from a designated location (e.g. as determined by GPS location). In the malware scenario the reverse shell connection would only be initiated when the victim is in the proximity of the critical infrastructure sites that the APT wishes to attack.

Attack Scenario

An attacker performs passive reconnaissance of the critical infrastructure that they wish to attack. The main aim would be to identify the employees within the target organisation (e.g. through LinkedIn profiles).

If implementing GeoFencing an attacker would also need to identify the GPS locations of sites within the critical infrastructure that they wish to attack this could be done using Google Maps. Once identified they would need to be integrated within the malware using Android's Geofence functionality.

Once the malware is constructed the attacker would need to get the malware onto the victim's device. A multitude of potential exploit vectors are possible here. For example, the attacker could set up a rogue access point and conduct a man-in-the-middle attack within a public setting (e.g an Internet Café or Hotel). On request of a webpage from the victim's device, the attacker could intercept this communication and launch an exploit that allows remote code execution to download and install the malware onto their device. An example exploit that could be used is that of the “Android Browser and WebView addJavascriptInterface” which was released in February 2014.An example of this type of MITM attack can be seen in Figure 5



1. Victim connects to Attacker thinking Attacker provides network access

2. Attacker transfers Malware to Victim

3. Attacker provides network access

Figure 5: Example Man In the Middle Attack

In this scenario it is assumed the Attacker has targeted a support engineer that travels to remote field sites within the critical infrastructure. At this point, the malware is on the victim's personal device. This device is not used for any purpose by the engineer beyond personal use. However, when this engineer arrives at a field site that has been identified by the APT as a target site, the malware becomes active. The attacker should then receive the reverse TCP connection to the engineer's personal mobile device over the 3G network.

The attacker can then use this remote shell as pivot point to attack the critical infrastructure. Wireless access points are increasingly being used within critical infrastructures; the security of these systems have been repeatedly called into question. This includes reports of wireless access points with poor (e.g., WEP or weak keys) to no authentication. An APT could use their remote shell to then connect (via command line) to the critical infrastructure wireless access point, fingerprint devices on the network, and then launch attacks that impact their operations (e.g., using the aforementioned script to stop a PLC).

This mobile malware presents a threat to the critical infrastructure purely through an engineer carrying their personal device with them when visiting the field site. The threat is the result of the infamously weak security controls within critical infrastructures. By attacking a critical infrastructure in such fashion, an APT is provided with a means of masking the true origin of the attack through a novel exploitation vector, while also minimising personal risk exposure resulting from any environmental damage which may occur.

Conclusion

The work demonstrates three interesting attack variants against industrial control systems. The first is the potential for an automated disruption attack against the system. This can be triggered a malicious attack who gains physical and wireless access to the network infrastructure that runs the industrial control systems. This attack is made feasible by the fact that a mobile phone would not normally be considered an attack platform. Alternatively an unsuspecting individual who works on the infrastructure could be compromised and utilising geofencing malicious software designed to disrupt the operation of the ICS's launch when that individual comes into their proximity. The final mode is high jacking an unsuspecting individual's phone and using it as a bridge into a restricted network for an attacker external to the physical perimeter controlling access to the ICS. It is clear that the mobile phone, with its increasing power and complexity can act as a versatile attack platform that can be used to undermine targeted Industrial Control Systems.

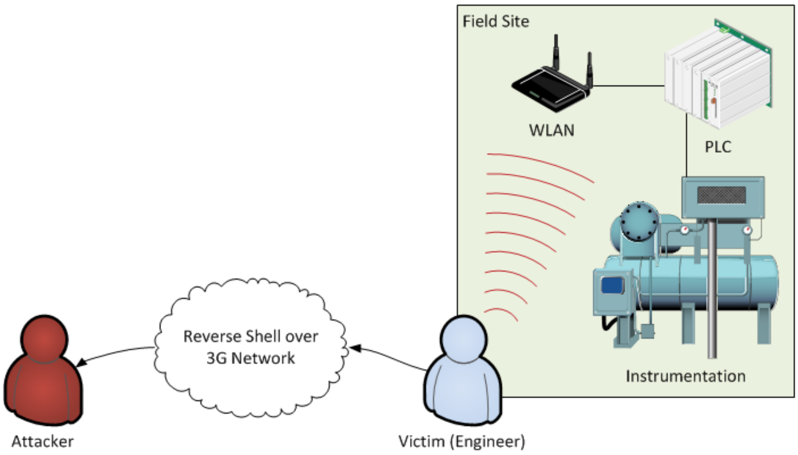


Figure 6: Remote Attack of a target Industrial Control System

Conclusion

The workshop and our research has highlighted key areas that will shape the future of mobile computing and provided a framework in which future environments can be explored. There will always be complexity in attempting to predict the future; however the approach identified provides a repeatable approach to considering such environments. Ultimately the use of such a framework is to utilise it in order to understand the potential security considerations that may arise in possible future environments so that we can plan now for future issues.

It is clear that the use of mobile computing is radically changing the nature of society, both in the developed and developing countries. In fact it can be seen that the developing countries are bypassing stages of technological evolution and jumping straight to technological levels found in the developed world. The predominant use of wireless mobile platforms for telephone in African nations rather than progressing through traditional landlines is an example of this. This bypassing of evolutionary steps generates significant cultural differences in the way that these services are consumed and utilised by a society. It is therefore likely that these different cultural trends are just as likely to cause security issues due to assumptions and misconceptions of use between societies. For example, this report highlights the personal nature of the mobile device and the likelihood that this trend will continue, however, it has been noted that in some less affluent developing countries – particularly in rural areas- mobile phones are bought by households[27].What this work has tried to do is to separate out the evolution of the technology into the three immutable traits and then provide an approach to explore how these type of trends affect them. Through the generation of future mobile device scenarios it becomes possible to explore future security situations as achieved in the ***London Riots 2025*** scenario. The exploration of this scenario identified both a likely backdrop and imagined a significant event. The riot event was then used to consider how this might then effect the trends shaping that type of environment.

In order to ground the potential future security scenarios technical development teams developed two unique approaches to utilising mobile devices to attack different types of infrastructure. Both approaches rely on the personal nature of the device – the fact that the victim carries a device with them wherever they go – along with the fact that current devices have significant processing capability to run exploits. The trend for best and faster capabilities has the potential to make these even more capable attack platforms. What is potentially interesting is the impact of energy consumption. At the moment smartphone devices are designed on the edge of power consumption – the power consumption of chip sets on the phone are tightly controlled to maximise utilisation of

[27] http://www.aspeninstitute.org/policy-work/communications-society/programs-topic/communications-policy/india/cs-joint-roundtable-co

the battery. Given that in both cases the mobile devices would be running unexpected and potentially power consuming malicious functions, the fact that your battery goes flat faster could be an indicator that your device is not behaving as expected. Beyond this, what both scenarios highlight is the level of sophistication and complexity in the attacks that can be facilitated by modern mobile platforms. This has potentially dramatic repercussions in the design other systems such as corporate networks or industrial control systems.

During the workshop the level at which mobile computing could be used to generate disruptive events became clear. Given the current trends of increased mobilisation of the computing platforms, wired connectivity seems to be entering the minority, the majority of Internet users are wireless. The protection of this mobile majority becomes and increasing concern as reports of mobile malware on the rise[28] and reports of governments utilising mobile device hacking to monitor citizens[29]. It is clear that mobile devices have generated a fertile ground for both the development of disruptive technology and societal disruption.

[28] http://www.forbes.com/sites/katevinton/2014/06/24/mobile-malware-is-on-the-rise-mcafee-report-reveals/

[29] http://www.wired.com/2014/06/remote-control-system-phone-surveillance/

Writing Team

About the Authors

Dr Daniel Prince: Associate Director for Business Partnerships and Enterprise at Security Lancaster

Daniel Prince is an associate director for Security Lancaster, managing business partnerships and enterprise. Prior to this he was the course director for the multi-disciplinary MSc in Cyber Security teaching penetration testing, digital forensics and information security risk management. Daniel holds a PhD in Computer Science and has worked on projects with numerous large technology companies such as Cisco and Microsoft.

Oliver Fitton: PhD Student in Politics Philosophy and Religion

Oliver Fitton is researching for a PhD in International Relations in the department of Politics, Philosophy and Religion at Lancaster University. His research focus is cyber attacks using social engineering techniques in conflict, how and why individuals turn to digital technology for political and other ends.

About the Contributors

Jay Abbot: Managing Director of Advanced Security Consulting

Jay Abbot is the Managing Director of Advanced Security Consulting Limited, and a celebrated key-note speaker who is regularly quoted in the media on the subject of Cyber Security. Jay's background is in the "design it, build it & break it" space, where he has spent most of his career engineering technical solutions to business problems. Jay has held senior positions with organisations including PricewaterhouseCoopers LLP, Electronic Arts and Barclays Bank to name but a few.

Dr Ruzanna Chitchyan: Lecturer in Software Engineering

Dr Ruzanna Chitchyan is a lecturer in Software Engineering at the Department of Computer Science, University of Leicester. Her research interests include development of novel requirements engineering techniques for future (sustainable) systems, as well as study of the potential misuse and abuse of emerging technologies.

Dr Karolina Follis: Security Lancaster Research Fellow

Faculty Fellow in Security Lancaster. In addition to her research role, she lectures in the Department of Politics Philosophy and Religion, currently on the Politics of the European Union. Current research follows up on the previous work on European Union borders. Dr. Follis studies the ongoing digitalization of borders in the European Union and beyond, a process which unfolds under the banner of 'smart borders.'

Dr Pauline Anthonysamy

Pauline Anthonysamy’s PhD research focuses on developing computational approaches for privacy policy synchronisation and traceability with a system’s runtime functionality. Specifically tracing privacy policies to privacy controls on social networking sites (SNS). She has developed a specialisation in identifying and demonstrating traceability relationships and information asymmetries between natural language texts and the runtime implementation of a system. Her research has pioneered a means to automate traceability between user expectations of their own privacy to the machine code that implements the system.

Philip Garner: PhD student in Computer Science

Philip Garner received his Computer Science degree from Lancaster University in 2011. His PhD Research based at Lancaster University’s School of Computing and Communications focuses on investigating and developing novel ways of extracting information from relational databases. Philip is also a successful Android application and educational software developer.

Rajiv Ramdhany: PhD student in Computer Science

Rajiv Ramdhany is a PhD student at Lancaster University and a technology envangelist who delights in developing and making use of technology to build smart Internet-based solutions for different application areas. He has extensive experience in building systems that require middleware/Internet (Web Services, Messaging) for high-performance communication.

Benjamin Green: PhD Student in Computer Science

After spending two years working in the satellite communications industry, and five years supporting industrial control systems (ICS) for one of the UKs largest water and waste water operators, Benjamin Green returned to education on a part-time basis. Over two years Benjamin successfully completed Lancaster University MSc in Cyber-Security. Upon completion Benjamin was pointed in the direct of his current PhD, researching Social and Technical Objects for Resilience and Cyber-Security (STORC) within the field of ICS.

Ben Paske: PhD Student in Computer Science

Ben Paske is a PhD student at Lancaster University researching security within industrial control systems. He previously completed an MSc in Computer Science at Oxford University and a BSc in Mathematical Physics at Edinburgh University.

William Knowles: PhD Student in Computer Science

William Knowles received his Master's degree in Cyber Security at Lancaster University. He is currently involved in an EPSRC Industrial Case PhD that is supported by the Airbus Group. The research area for this engagement is security metrics for SCADA systems

Bibliography

AT&T, *Technology Timeline: 1946 - First Mobile Telephone Call*, available at: http://www.corp.att.com/attlabs/reputation/timeline/46mobile.html, [Accessed 03/04/2014]

Atkinson, P. "A Bitter Pill To Swallow: The Rise And Fall Of The Tablet Computer" in Design Issues, (2008), Vol. 24, No. 4. pp. 3-25

Deibert, R. *Black Code*, (Toronto: Signal), 2013: p. 82

Demonbynes, G & Thegeya A. "Kenya's Mobile Revolution And The Promise Of Mobile Savings", The World Bank – Policy Research Working Paper 5988, (March 2012): p.16

Heeks, R. "Beyond Subscriptions: Actual Ownership, Use and Non-Use of Mobiles in Developing Countries" in ICTs for Development, available at: http://ict4dblog.wordpress.com/2009/03/22/beyond-subscriptions-actual-ownership-use-and-non-use-of-mobiles-in-developing-countries/, [Accessed 03/04/2014]

Huawei Press Release, "Rotating And Acting CEO Eric Xu: Create A Better Connected World", *Huawei Press Centre*, (31st March 2014), available at: http://pr.huawei.com/en/news/hw-331129-annualreport.htm#.UzmEJvldWSp, [Accessed 03/04/2014]

Ingraham, N. "Apple Announces 1 Million Apps In The App Store, More Than 1 Billion Songs Played On iTunes Radio", The Verge, (22nd October 2013), available at: http://www.theverge.com/2013/10/22/4866302/apple-announces-1-million-apps-in-the-app-store, [Accessed 03/04/2014]

Mackenzie, I. "Is Technology To Blame For The London Riots?", BBC News (8th August 2011), available at: http://www.bbc.co.uk/news/technology-14442203, [Accessed: 03/04/2014]

Merril Carlsmith, J & Anderson, C A. "Ambient Temperature And The Occurrence Of Collective Violence: A New Analysis" in *Journal of Personality and Social Psychology*, (1979), Vol. 37, No. 3, pp. 337-344

Rowinski, D. "Google Play Hits One Million Android Apps", Readwrite.com, (24th July 2013), available at: http://readwrite.com/2013/07/24/google-play-hits-one-million-android-apps#awesm=~oA5TF7vDEfBT7g, [Accessed 03/04/2014]

Tabarrock, A. "The Real Cost Of Virtual Money", *Marginal Revolution,* (3rd December 2013), available at: http://marginalrevolution.com/marginalrevolution/2013/12/the-real-costs-of-virtual-money.html, [Accessed: 03/04/2014]

The New York Times, "Cartoon Captures Spirit Of The Internet", The New York Times Archives, (14th December 2000), available at: http://www.nytimes.com/2000/12/14/technology/14DOGG.html?pagewanted=1&ei=5070&en=f0518aafeccf36fd&ex=1183089600, [Accessed 03/04/2014]

Security Futures' mission is to is create a space where we could develop innovative techniques to think about the future, techniques that draw together the insight and expertise of researchers working across different disciplines. In this collaborative space, researchers and other partner organisations have the freedom to explore questions about security and technology. But also to formulate the questions that we might need to start asking about the emerging trends in technology, society and security. A space where we can bring together people working on the cutting edges of technology, social, legal and political disciplines to ask questions about the world we live in. A space where we might begin to imagine new horizons and start to see the problems that

Security Lancaster is a university wide research centre on security and protection sciences. It delivers research and education that innovates and creatively challenges the way that individuals, organisations and societies secure and protect themselves. This is achieved via engagement and collaboration with organisations from a range of sectors along with governments. The centres approach delivers the very best use-inspired and pure research alongside cutting edge education that delivers real impact and social change.

This work was funded by Security Lancaster via the auspices of Lancaster University's Faculty of Science and Technology.

Science and Technology Business Partnerships and Enterprise

As well as working with a range of external partners, ICT and Security form part of a wider theme based team across Science and Technology at Lancaster who offer expertise in:

- Advanced Manufacturing
- Energy
- Environment
- Health & Human Development
- Quantum Technologies
- Mathematics and Statistics

Working in Partnership

Across the themes we form collaborative partnerships around these 5 key areas:

- Collaborative Research and Consultancy
- Training and Education
- Co-location and Secondment
- Student Placements
- Product Development and IPR

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, Lancaster University, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

Copyright Lancaster University ©2014

For more information on the research work that Security Lancaster undertakes and information on how you can collaborate with us please visit our website

http://www.security-centre.lancaster.ac.uk