M2M: A general-purpose Technology

Leadership paper by Tim Phillips

A general-purpose Technology

Economists call ideas like M2M a general-purpose technology: a single way of organising innovation that makes many different types of company more productive, and so delivers growth, profit and customer benefit out of all proportion to the investment in the technology, like the steam engine or the personal computer. Like this, when M2M's working well, it makes all sort of other innovations more efficient.

But for M2M to succeed, we need to collectively solve two problems. Without effective ways to deal with roaming and security, the M2M ecosystem cannot flourish. Therefore M2M service providers need appropriate security, as many of these devices will be performaning economicially important or safety-critical functions. If there are to be billions of devices in secure communication on our existing networks, that's a step change in identity management.
Also, the devices which communicate may roam outside their home territory, either because they are sold globally, or because they can move around (for example, because they are in a car).


Challenge n#1
M2M Security, a risky future ahead?

How many connected devices?

By 2020, estimates vary from 20 billion to 50 billion. We have plenty of evidence that, unless we design security efficiently as well, the explosion in the number of devices will also mean an increase in the vulnerability of enterprises to attack.

Reports points out that, in recent testing, seven out of 10 of the most commonly used IoT devices contained vulnerabilities, and 56% of companies said they would be unable to detect a sophisticated attack on them. Today, the vast majority of these attacks are automated: you don't have to be important or visible to become a target. An example is the recent rise in ransomware: attacks that are called off after the victim pays the attacker. Osterman research shows that 47% of orgnaisations have been attacked in the last 12 months, often by attackers using ransomware-as-a-service.

Security is not a cost

There isn't a Chief Security Officer anywhere with an unlimited budget to manage this problem (or, if there is, that CSO is understandably keeping quiet about it). So there is a trade off between security and cost, but also between security and the ability to do business.

The first trade off is obvious: spending on security is investment that will not be made in another part of the business. Therefore it's not a question of how much that the desired level of security would cost, but how best to apply the available budget.

Security against cost is not the only trade-off. Locking down security too tight will impact the ability to do business (for example, by making it too hard to connect, or reducing flexibility to respond to changes in the ecosystem).

That's why a thought-through security posture, matched to budget and risk appetite, is a business benefit, not a cost. Because when businesses are confident that their critical systems are secure, they are confident to connect to their M2M partners to realize efficiencies today, and to innovate in response to market opportunities tomorrow.

Proactive M2M security

But, if spending has to be targeted, where to? The principle is that security must be engineered into the application design, specifically into the networks used to exchange data, from the outset. In most cases, the cost of reactive security measures is higher than the cost of a data breach. The direct losses per capita can still be measured in the tens of cents, but the indirect losses from sub-optimal security design, such as adding defenses to existing insecure networks in response to an attack, or being unable to grasp a new opportunity because of security worries, were more than 10 times greater. Therefore, creating an M2M service must employ network security experts from day one, and the more network connections there will be, the more important their contribution.

That will create, for example, systems that ensure that suspicious activity, once detected, is flagged and acted on immediately. It means protection against DDoS attacks and encryption of data. But, most important, it will require a deep partnership between everyone involved in the M2M ecosystem at the planning stage. Whatever the security posture an M2M service adopts, it can never be an afterthought.

Challenge n#2

M2M roaming

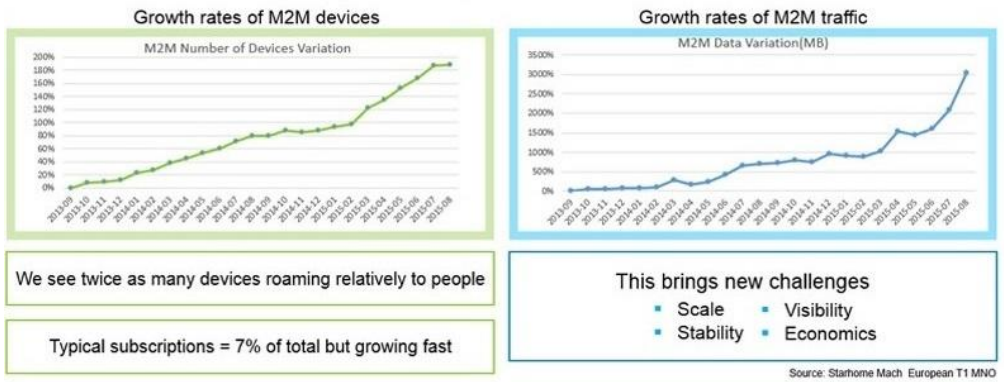
Can operators track this traffic?

Statistics show that the supply of global M2M applications isn't stuck. We know this because M2M roaming, in which the device communicates from outside its "home" market, jumped in importance in 2015: Machina Research measured the amount of global M2M roaming, and found that the number of roaming registrations that can be attributed to M2M devices increased by 100% in compared to the previous year, and is now 7% of all roaming connections: "It is entirely possible that there will be as many machines as people roaming by 2020", it added.

What drives this growth?

Some M2M architectures are obviously globalised by default. For example, a "connected car" service which needs to operate across borders, or logistics services for globalized companies.

Operators have considered M2M roaming to be a huge potential source of revenue, so this growth in devices using their networks should be excellent news. But it's only half good: in a recent survey by Starhome Mach and Machina Research, 86% of mobile network operators were earning revenue providing outbound M2M services, but 70% admitted they were unable to detect when M2M devices roamed into their networks.



When the numbers of connections and the volume of data are small, it's probably not a priority to fix this. But there are at least two good operational reasons for operators to make managing M2M roaming a priority. First, the providers of M2M services, quite reasonably, demand it. Second, the nature and frequency of M2M connections varies widely, and impose different types of load on the network. So the less operators know about the macro trends in network use, the less they can do to build the networks, and the back-end support, to make global M2M the general purpose technology that it should become.

But, for mobile network operators, simply upgrading their own offering isn't enough; this will require multilateral cooperation so that M2M service providers can manage their global deployments efficiently. In the words of one of them: "We don't want to pay 50 carriers every month". Global telecoms has, in the past, often managed to strike a balance between fierce competition and market-making cooperation. The Global M2M Association and the Bridge Alliance - both examples of M2M service cooperation agreements between Tier 1 operators - will be fundamental to the success of M2M, because without managed M2M roaming, the huge potential benefits of M2M as a globalised general-purpose technology would be smaller, if they happened at all.

Bresnahan, T.F., Trajtenberg, M., 1995. General purpose technologies "engines of growth"? Journal of Econometrics 65, 83–108.

Machina Research, 11 January 2016. The inexorable rise of M2M roaming http://bit.ly/1XtlLaC

About Tim Phillips

Tim Phillips has more than 20 years of experience, writing for more than 200 magazines and newspapers, including the Wall Street Journal, The Guardian, Management Today and Fast Company. He is the author of 12 books on management and business. His most recent book, Game of Thrones on Management, has been nominated for the Chartered Management Institute's management book of the year 2015.

THANK YOU FOR READING

M2M: A GENERAL-PURPOSE TECHNOLOGY