Interview: Mustafa Al-Bassam

Limn talks with security expert **Mustafa Al-Bassam** (a.k.a "**tflow**") about the responsibility for information security, the incentive problems it creates and the available solutions.

Gabriella Coleman: Based on what you've seen and reported do you think we (not just lay people, but experts on the subject) are thinking clearly about vulnerability? Is our focus in the right place (e.g. threat awareness, technical fixes, bug bounties, vulnerabilities disclosure), or do you think people are missing something, or misinterpreting the problem?

Mustafa Al-Bassam: Based on the kind of vulnerabilities that we [LulzSec] were exploiting at Fortune 500 companies, I don't think that there is a lack of technology or knowledge in place to stop vulnerabilities from being introduced, but the problem is that there is a lack of motivation to deploy such knowledge. We exploited extremely basic vulnerabilities such as SQL injection, in companies like Sony, that are quite easy to prevent.

I believe the key problem is that most companies (especially those that are not technology companies – like Sony) don't have much of an incentive to invest money in making sure their systems are vulnerability-free, because security isn't a key value proposition in their business model, it's merely an overhead cost to be minimized. Sony fired their entire security team shortly before they got hacked over 30 times in 2011. For such companies, security only becomes a concern for them when it becomes a PR disaster. So that's what LulzSec did: make security a PR disaster.

We've seen this before: when Yahoo! was breached in 2014, the CEO made the decision not to inform customers of the breach. Because it would have been a PR disaster for them, that may have seen them lose customers to their competitors, causing them to lose money.

That begs the question: how can we expect companies to do the right thing and inform customers of breaches, if doing the right thing will cause them to lose money? And so, why should companies bother to invest in keeping their systems free of vulnerabilities, if they can simply brush compromises under a carpet? After all, it is the customer that loses from having their information compromised, rather than the company, as long as the customer keeps paying.

So I think if we can incentivize companies to be more transparent about their security and breaches, customers can make better-informed decisions about which products and services to use, making it more likely for companies to invest in their security. One way this might happen in the future is through the rise of cybersecurity insurance; more and more companies are signing up to cybersecurity insurance. A standard cybersecurity insurance claim policy should require the company to disclose to its customers when a breach occurs. That way, it makes more economic sense for a company to disclose breaches and also invest in security to get lower insurance premiums or avoid PR disasters.

GC: I wanted to ask about the rise of cybersecurity insurance and whether major firms all already have purchased policies, what the policies currently look like, and whether they actually prevent good security since the companies rely on insurance to recoup their losses?

Christopher Kelty: Yes, I don't actually understand what cybersecurity insurance insures against— does

it insure brand equity? Does it insure against government fines? Lawsuits against a corporation for breach of duty? all of these things? Just curious.

GC: Exactly, I don't think many of us have a sense of what this insurance looks like and if you can give us a picture, even a limited picture of what you know and how the insurance works, that would be a great addition to our issue.

MAB: The current cybersecurity insurance market premium is $2.5 billion but it's still early stages because insurance companies have very little data on breaches to be able to calculate what premiums should be (Joint Risk Management Section 2017: 9). As a result, premiums are quite high and too expensive for small and medium sized businesses, and this will continue to be the case until cybersecurity insurance companies get more data about breaches to properly calculate the risks.

Cybersecurity insurance has been used in several high-profile breaches, most notably Sony Pictures which received a $151 million insurance payout for its large internal network breach alleged to be by North Korea (Joint Risk Management Section: 4).

These policies cover a wide range of losses including costs for ransomware payments, forensic investigations, lost income, civil penalties, lost digital assets, reputational damage, theft of money and customer notification.

I think in the long-term it's unlikely that companies will adopt a stance where they stop investing in security and just rely on the insurance to recoup losses, because insurance companies will have a concrete economic interest to make sure that payouts happen as rarely as possible, and that means raising the premiums of companies that constantly get breached until they can't ignore their security problems. Historically, this economic interest is shifted to the customer because it's usually the customer that loses when their data gets breached and the company doesn't report it.

If anything, I believe that cybersecurity insurance will make companies more likely to do the right thing when they are breached and inform customers, because the costs of customer notification and reputational damage would be covered by the insurance. At the moment if a company does the right thing and informs their customers of a breach, the company suffers reputational damage, so there is little incentive to do the right thing. This will prevent incidents from occurring such as when Yahoo! failed to disclose a data breach affecting 500m customers for over two years (Williams-Alvarez 2017).

CK: I wonder if there is more of a spectrum here— from bug bounties to vulnerabilities equities processes (VEP) to cybersecurity insurance— all of them being a way to formalize the knowledge of when and where vulnerabilities exist, or when they are exploited. What are the pros and cons of these different approaches (I can imagine that a VEP is really overly bureaucratic and unenforceable, whereas insurance might produce its own incentives to exploit or over/under-report for financial gain). Any thoughts on this?

MAB: Bug bounties and cybersecurity insurance policies are controlled purely by the market and are an objective way to measure the economic value or impact of vulnerabilities, whereas VEP is a more subjective process that is subject to political objectives.

In theory VEP should be a safeguard to be used situations where it is in the public interest to disclose vulnerabilities that may otherwise be more profitable to exploit, but this is not the case in practice. Take the recent WannaCry ransomware attack for example, which used an exploit developed by the National Security Agency, and affected hundreds of companies around the world and the UK's National Health Service (NHS). You have to ask if the economic and social impact of that exploit falling in the wrong hands was really worth all the intelligence activities that the NSA used it for. How many people died because the NHS couldn't treat patients when their systems were offline?

GC: Do you have a sense of what the US government (and others around the world) are doing to attract top hacker talent—for good and bad reasons? Should governments be doing more? Should it be an issue that we (in the public) know more about?

MAB: In the UK, the intelligence services like the Government Communications Head Quarters (GCHQ) run aggressive recruitments campaigns to recruit technologists. Even going so far as to graffiti 'hipster' adverts on the streets of a techy part of London (BBC NewsBeat 2015). They have to do this because they know that their pay is very low compared to London tech companies. In fact, Privacy International – a charity which fights GCHQ – will pay you more to campaign against GCHQ than GCHQ will pay you to work for them as a technologist.

So in order to try to recruit top tech talent, they have to try and lure people in by the promise that the work will be interesting and "patriotic", rather than it paying well. That is obviously becoming a harder line to toe though, because the intelligence agencies are less popular with technologists in the UK than ever, given the government's campaign against encryption. Their talent pool is extremely limited.

What I would actually like to see however, is key decision makers in government becoming more tech savvy themselves. Technology and politics are so intertwined these days that I think it's reasonable that at least a few Members of Parliament should have coding skills. Perhaps someone should run a coding workshop or class for interested Members of Parliament?

CK: I have trouble understanding how improved technical knowledge of MPs would lead to better political decisions if (given your answer to the first question) all the incentives are messed up. This is a very old problem of engineers vs. managers in any organization. The engineers can see all the problems and want to fix them; the managers think the problems are different or unimportant. Just to play devil's advocate, is it possible that hackers, engineers, or infosec researchers also need a better understanding of how firms and governments work? Is there a two-way street here?

MAB: I mean this in a more general sense: politicians make poor political decisions when they deal with technical information security problems they don't understand, for example with the recent encryption debate. In the UK, the Investigatory Powers Bill was recently passed, which allows the government to force communications platforms based in the UK to backdoor their products if they use end-to-end encryption.

Luckily most of these platforms aren't based in the UK, so it will have little impact. But this has a harmful effect on the UK technology sector, as no UK technology company can now guarantee that their customer's communications are fully secure, which means UK tech firms are less competitive.

A classic example of poor political decisions in dealing with such problems is the EU cookie law, which requires all websites to ask users before they place cookies on their computers (The Register 2017). In theory it sounds great but in practice most users always agree and click yes because the request dialogs are disruptive to their user experience. Even so, a saner way to implement such a policy would be to require the few mainstream browsers to only set website cookies after user approval, rather than ask millions of websites to change their code.

There are already plenty of hackers and engineers who are involved in politics, but there are very few politicians who are involved in technology. Even when engineers consult with the government on policies, their advice is often ignored, as we have seen with the Investigatory Powers Bill.

MUSTAFA AL-BASSAM *("tflow") is a doctoral researcher at the Department of Computer Science at University College London. He was also one of 6 core members of the hacking collective LulzSec.*

BIBLIOGRAPHY

BBC News Beat. (2015). "Spy agency GCHQ facing fines for 'hipster' job adverts on London streets." November 27th. http://www.bbc.co.uk/newsbeat/article/34941261/spy-agency-gchq-facing-fines-for-hipster-job-adverts-on-london-streets

Joint Risk Management Section of the Society of Actuaries. (2017). "Cybersecurity: Impact on Insurance Business and Operations." Report by Canadian Institute of Actuaries, Casualty Actuary Society, the Society of Actuaries. https://www.soa.org/sections/joint-risk-mgmt/cyber-security-impact.pdf

The Register. (2017). "Planned 'cookie law' update will exacerbate problems of old law – expert." March 1st. https://www.theregister.co.uk/2017/03/01/planned_cookie_law_update_expert/

Williams-Alvarez, Jennifer. (2017). "Yahoo general counsel resigns amid data breach controversy." *Legal Week*, March 2nd. http://www.legalweek.com/sites/legalweek/2017/03/02/yahoo-general-counsel-resigns-amid-data-breach-controversy/