A Discussion of Surveillance Backdoors: Effectiveness, Collateral Damage and Ethics

Matthew Smith, University of Bonn, Fraunhofer FKIE
Matthew Green, Johns Hopkins University

Febuary 5th, 2016

1 Introduction

After more than a decade of relative quite the crypto-wars are heating up again. Terrorist attacks such as in Paris [7] and San Bernardino [12] are being used by politicians as well as intelligence and law enforcement agencies to call for the weakening of security systems to aid surveillance and forensic analysis. A number of different strategies are being proposed. These include banning default encryption - such as the encryption found on iOS and Android; building backdoors into cryptographic protocols to allow government access in "exceptional" circumstances; software backdoors - such as "forced" data backup systems; and finally, stockpiling and using 0-day vulnerabilities instead of patching them. All of these strategies extend the power of intelligence and law enforcement agencies.

At the same time the rise of hacking/attack related security events is leading to a call for improved information security across the board. Thousands of critical software vulnerabilities (CVEs) are found every year, and estimates indicate that the cost of data breaches will exceed $2 trillion by 2019 [10]. These threats have not been confined to corporate networks; most worrying are the recent addition of attacks against cyber-physical systems and critical infrastructure. The first well known example is the Stuxnet virus discovered in 2010 which attacked and destroyed Iranian centrifuges in the Nantaz Uranium enrichment facilities.[3] A more recent example is the use of the BlackEnergy malware to breach the computer systems of the Ukrainian power system and then subsequently hack the SCADA control units causing a power-outage for around 80.000 Ukrainians in December 2015.[8] While these attacks are the most spectacular there are a whole range of serious incidents. Attacks against our banking system - such as those recently levied against the NASDAQ stock exchange[9] or babyphones[11] show that virtually no area is safe.

The debates around both these problem domains are heating up, however, they are often being discussed as separate issues. This is unfortunate, as on a technical level they are linked and should be discussed together. In this article we propose that the debate be framed in the context of collateral damage to help guide the decision making process.

2 Actors

There are a large number of actors and motivations involved in the security of our digital infrastructure. In the context of this discussion we will differentiate between the following actors. The actors are described from the perspective of the U.S. and Germany, i.e. states with high technological capacities but also high reliance on technology.

- State-own: This is our own national government, for which we are evaluating the options. While each government has many sub-actors, such as intelligence agencies, national and provincial law enforcement agencies, and the military, for the sake of simplicity we will subsume them as a single state level actor. Also to simplify the discussion, we will adopt a somewhat idealized assumption there are only two distinct motivations for the state: to keep it citizens and society safe (i.e. national security) and to keep its citizens and society free (i.e. privacy, freedom of speech, democracy, due process, etc.). We also assume that our state has an inherent wish to behave ethically, safeguarding both the security and rights of its citizens and avoiding unnecessary collateral damage when forced to act aggressively. This is naturally an over-simplification, however it will allow us to put the different technological possibilities into perspective.

- State-allies: These are states considered allies, i.e. states which have close ties in intelligence and surveillance matter, such as the "five-eyes" partnership of cooperating intelligence agencies. We assume that allied states operate under similar ethical structures as our own.

- State-friendly: These are states considered friendly, i.e. states which to a certain extent are likely to cooperate on some aspects of intelligence operations but on a case by case basis. We make fewer assumptions about ethical characteristics of these states, but assume that amongst these states there is a wish to avoid antagonism. Note that this does not imply that there is no governmental or industrial espionage going on, but merely that it is causes more of an outcry when it is uncovered, as with the revelation that the US was surveilling Angela Merkel the chancellor of Germany.

- State-adversary: These are states which are the targets of intelligence operations, and which represent threat actors against us.

- Terrorist-professional: For the sake of this article we consider terrorist to be non-state actors who have an interest in harming others for ideological reasons. In the context of this article we classify terrorists as professional if they have training and are motivated to keep their activities secret from the government and invest in counter-surveillance. Additionally we consider the fact that many organized terrorist groups have significant funds. For instance it is estimated that in 2014 the Islamic State received between $1 and $3 million U.S. dollars per day in oil revenue alone[17].

Terrorist are ethically unconstrained and will not only condone collateral damage but often actively seek it.

- Terrorist-amateur: In contrast to the professional terrorist we consider the amateur to have little or low training and lacks the skill to for instance install secure messaging apps or other security precautions. This is not to say that they are ineffective, merely that they do not benefit from organisational knowledge on how to protect their IT resources.

- Criminal-professional: We assume that professional criminals are motivated by profit and have a support infrastructure and sufficient funds to dedicate to counter-surveillance efforts. These criminals have a higher skill level and motivation to cover their tracks, and are thus willing and able to invest resources into using encryption and other security technology to remain undetected. We make no assumptions on the level of collateral damage criminals find acceptable. However, there is a tendency to want to avoid detection, which often makes limiting collateral damage a prudent move.

- Criminal-amateur: As above the amateur label is applied to the tech-skills of the criminal, i.e. these are criminals who do not have the knowledge or the skill to implement counter-surveillance methods. Again we make no assumptions about ethical constraints.

- Criminal-state-backed: This is the most interesting class of criminal. These actors are either covertly run by states or they have a tacit agreement with the state they operate in and thus operate without fear of prosecution. An example for this kind of group is the Russian aligned CyberBerkut hacking group,[14] and China's Axiom group.[**?**] What makes these groups particularly interesting is that they potentially have nation state capabilities and motivation, but provide deniability for their sponsoring governments. Consequently they are less ethically constrained than the states themselves. The combination of nation state attack capabilities and lack of consequences gives a significant attack advantage to states willing to employ these threat actors.

- Company-security-conscious: A tech-savvy company which is motivated and capable of installing and correctly using encryption and security software. We assume that companies are law abiding and have the same ethical characteristics of their parent state.

- Company: A normal company using only standard IT.

- Civilian-security-conscious: A tech-savvy civilian who is motivated and capable of installing and correctly using encryption and security software. We assume that civilians are law abiding and have the same ethical characteristics of their parent state.

- Civilian: A civilian using only standard IT.

3 Technology

The current debate over terrorist and criminal use of encryption technologies has led to a number of proposals, some of which have been formalized into proposed legislation. In this section we provide a summary of the various proposals that have been advanced.

3.1 Ban (default) encryption

Perhaps the simplest demand currently levied at the tech-industry is the request that companies such as Google and Apple turn encryption off by default or even remove encryption options entirely. We will now discuss the ramifications of this option for each of the actors.

- Terrorist-professional: This strategy will have little to no effect on professional terrorist, since installing after-market encryption is not difficult given the right support infrastructure. Indeed, both Al Queda and the Islamic State have published security guides for using open source encryption software.[19]
- Terrorist-amateur: A terrorist who is not aware of government surveillance or incapable of installing after-market encryption could be negatively impacted by these actions. It should be noted however that the Paris attacks were coordinated using unencrypted text-messages. Thus encryption was not the problem in this case and banning encryption would not have prevented the attacks.
- Criminal-amateur: Criminals who do not have the skill or motivation to install after-market encryption will be affected by this option.
- Criminal-professional: Professionals criminals, such as members of organized crime groups, will be largely unaffected.
- Criminal-state-backed: The same goes for state-backed criminals.
- Company-security-conscious: Naturally companies can install after market encryption. However, unlike above the additional costs must be seen as collateral damage. In large corporations deploying encryption solutions can easily run into the millions of dollars. This has driven the adoption of secure enterprise services such as BlackBerry's BES.
- Company: Unlike terrorist and criminals who have a very high intrinsic motivation not be caught by surveillance, most companies primary objective is not security. Thus, the additional costs of installing after-market encryption is too high for most companies and thus they become vulnerable to adversaries. This must also be seen as collateral damage.
- Civilian-security-conscious: Even though civilians can install after-market encryption, history has taught us that not many are interested in doing so.

This creates a big problem for encryption software, which relies heavily on network effects. To be useful, many people must install and use the software, creating a disincentive for early adopters. Indeed, email encryption software, which has been around since the 1990s, has seen little to no adoption even amongst the security conscious citizens, due to lack of adoption outside of security circles. While there will always be pockets of encryption such as amongst security researcher and in some cases dissidents, it is unlikely to ever become mainstream without it being a usable default. This must also seen as collateral damage, since these civilians are now more vulnerable to criminals and surveillance.[1] While from the point of view of the own state the latter might not be seen as damage but a positive capability, the lack of encryption also facilitates other states to spy on our citizens. It also opens the door for state overreach, which is a legitimate concern.[2]

- Civilian: Installing after-market encryption software is more than can be expected from most ordinary civilians. Thus a large swathe of innocent civilians will have no way to enforce their digital privacy. This particularly critical if a state is run by an oppressive regime.

- State-own: On the positive side the state has a much easier time reading messages. However, as described above this will mainly include the low level criminals and terrorist too inept to install after-market encryption software. Catching inept terrorist and low level criminals is naturally a good thing, however, it needs to be weighed against the amount of collateral damage this option creates.

- State-allies: This also holds for allies.

- State-friendly: This also holds for friendly states.

- State-adversary: Baning default encryption has the potential to benefit adversarial states. It makes spying on us easier. It also makes it easier for totalitarian states to spy on their population, which should also be seen as collateral damage for us, since strengthening totalitarian states can pose a danger to us.

Beyond the analysis above, the single greatest challenge in banning default encryption is determining which encryption is to be banned, and what legislative framework would enable this. This is made particularly challenging due to the availability of foreign service providers and installable "apps", which can easily substitute encryption capabilities even when they are removed as default options in products such as phones and computers. Moreover, banning encryption has speech implications that go well beyond the security issues that we address in this report.

[1] See [18] for a discussion of surveillance capability against low-adoption encryption protocols such as PGP.

[2] TODO

3.2 Cryptographic Backdoors

While banning default encryption is the simplest option technologically speaking, many legislators and technologists recognize that this could dramatically harm security. An alternative proposal is therefore to *preserve* end-to-end encryption capability, while adding a "backdoor" capability that governments may use in exceptional circumstances.

This option is one of the most technologically complex. Cryptographic backdoors can be implemented in several different ways. A first is by sharing the private keys with trusted third parties. This is akin to making a copy of your house key and providing it to the government. An example of a system that follows this model is the MIKEY-SAKKE system proposed by GCHQ[4, 6].

A different option is active "key escrow", in which the encryptor enciphers the communication under an additional law enforcement key or keys. This is akin to adding a second door with a government issued lock to your house. Aside from legal, sociological and ethical issues, these approaches have serious technical drawbacks. Foremost among these is the problem of securing and managing exceptional access keys, since key management at this scale is extremely complex and error prone. To be practical, many different organisations and a large number of staffers would need access to the key database, which poses a severe risk. Moreover, a compromise of this database would be catastrophic – not to mention next to impossible to detect and recover from. For a more in-depth look at the technical risks the reader is referred to [2]. Making this option even less feasible is the question of *who gets the backdoor keys*. In the United States, various proposals have placed this responsibility with U.S. companies such as Google and Apple, who would design backdoors and hold keys to use at the U.S. government's request. It is unlikely that other countries would be comfortable with such backdoors for devices sold in their country; or at the very least, they would expect to get copies of the keys as well. If any state opts out of the system, those threat actors with resources and motivation to use encryption can simply use devices purchased there. Naturally states can try and limit the important of such non-backdoored devices, however, considering the difficulty of stopping the illegal import of arms and drugs it seems unlikely that it is a viable option to stop the import of software. Since many products are multi-national, this issue gets even more complex.

The final type of crypto backdoors are those built on the algorithmic level, such as found in the NSA-designed Dual_EC_DRBG algorithm,[3] which was recently found to be present in devices manufactured by Juniper Networks. With this kind of backdoor the standardisation process of cryptographic protocols is manipulated to weaken the protocols in such a way that the manipulating actor can break the encryption, but hopefully no one else can. The security of this approach can rest on several factors.

- Obscurity: the hope that no one else figures out how the protocol was

[3] Dual_EC_DRBG is an algorithm proposed by the NSA and NIST in 2006. It was later withdrawn by NIST due to indications that the algorithm contained a surreptitious backdoor. See *e.g.,* [16]

weakened. Since cryptographic protocols receive a great deal of scrutiny this is often an unsafe option.

- Secret knowledge: The backdoor requires some secret knowledge to work, such as large prime numbers which were used to create public parameters. As with the key sharing approach this suffers from the fact that the secret knowledge is a master-key which would need to be both shared to be useful but kept absolutely safe so it is not stolen and abused. And also as above it is a problem when interacting with allies. As above recovering from compromise is extremely difficult, since it requires the public parameters of all devices to be changed.

- Computational Power: The backdoor decreases the amount of computational power needed to attack the system to a point where the actors resources are sufficient to break the system, but hopefully not to a point where other actors can also break it. At the time of the backdoor creation this might prevent criminals from abousing the backdoor, however other nation states can conceivably have similar resources and thus also use the backdoor. Advances in computing power add an additional layer of risk to this approach.

An additional consideration in adding algorithmic backdoors is the possibility that a sophisticated attacker may be able to *re-purpose* the backdoor mechanism to create a surveillance system aimed against the country and organizations promoting the original backdoor. Indeed, a recent vulnerability report from Juniper Networks provides strong evidence that such an attack may have occurred in 2012, when several Juniper devices were modified with "unauthorized code" that repurposed an existing Dual_EC_DRBG backdoor to create an encryption backdoor for some unknown attacker.[**?**]

All the above backdoors can added overtly or covertly. However, the two options based on cryptographic keys are harder to hide, since analysing the source code or binaries would uncover them.

If the backdoors are included openly such as with MIKEY-SAKKE they are likely to be as ineffective as the banning of encryption – merely adding operational costs to those actors intent on achieving secure communications. If the backdoors are hidden, they may become more effective since targeted actors would not know they need to use alternative systems. This is difficult to achieve, however, in a setting where protocols and source code are properly reviewed for security. When successful it is also an attack that damages the reputation of standardisation committees,[4] and leads to an unfortunate situation in which several potentially allied nations add vulnerabilities to the systems, all of which increase the chances of discovery and consequently collateral damage. The collateral damage however is slightly less likely since exploiting this kind of backdoor takes more effort, i.e. secret knowledge needs to be stolen and cryptanalysis capabilities are needed. However, the damage done to the reputation

[4]See *e.g.,* the steps NIST has taken to restore confidence in its encryption standards following the Snowden leaks, [15]

of the standardisation committee and the knock-on effect on business may be severe.

3.3 System Backdoors

The final way for law enforcement, intelligence agencies or criminal organisations to gain access to encrypted information is via system level backdoors. These backdoors allow some form of access onto the devices themselves. Again there are a number of ways these can be implemented.

- Log-in/Master-account: In systems which already contain user management an additional, potentially hidden, account is added to the system to allow the attacker to access the system with high privileges. If no user management/log-in functionality is present, it can be added as part of the backdoor. A good example of such a backdoor is the AMX case where accounts for "Black Widow" and "Batman" were added by unkown parties to the AMX AV systems. The AMX system are used amongst other by the White House and the US military.[1]

- Special-Purpose-Vulnerability: Similar to the master account the this backdoor code allows access to the system, however the code is camouflaged to look like a naturally occurring bug/vulnerability. This has two benefits, a) it is harder to find by others and b) it offers deniability. Such backdoors have been discovered in critical software, such as the Linux Kernel.[5]

- Naturally-Occurring-Vulnerability: Writing secure software is extremely hard, even without powerful actors intentionally inserting vulnerabilities, thus there are a host of naturally occurring vulnerabilities, which when found can be used as a backdoor. Indeed, this is currently one of the most fruitful techniques used by law enforcement and national security agencies, and is likely to continue to be productive for many years to come.

The first two types of backdoor are added intentionally and are under full control of the attacker. As before this can be done overtly or covertly. An advantage of adding the backdoor overtly is that the security of the backdoor can be examined. It would also be possible to use secure authentication techniques to the backdoor. However, when done overtly all problems from overt crypto-back door described in the previous section apply, making the system fairly ineffective. Actors with an interest evading surveillance will use alternative systems and the question who has access must be negotiated with allies. Neutral parties might steer clear of products with such overt backdoors. As before, the covert case is more effective, since without knowledge of the backdoor actors will not avoid them. However, an interesting observation can be made about such backdoors found in the wild. The authentication used to protect the backdoor is usually of very poor quality, e.g. there are hard-coded plain-text passwords contained in the backdoor. This doesn't make sense from a security perspective,

since these credentials can be reverse engineered giving further parties access to the backdoor. Possible reasons for this phenomenon are:

- Deniability: An actor creating a covert backdoors has an interest in not being exposed. This makes using secure authentication techniques more risky, since the capability to authenticate would be good evidence of authorship of the backdoor and thus culpability for it.
- Stealth: Secure authentication credentials can be harder to hide in the code, since they would show up as cryptographic artifacts.
- Incompetence: Similar to regular authentication systems some backdoor developers might just make bad judgement calls.

On a technical level the last possibility can be addressed, however the first two options seem the most likely, suggesting the problem of badly protected backdoors is inherent to the approach. This is unfortunate, since that means third-parties including criminals will continue to be able to detect and exploit these backdoors. This is a worst-case scenario, since such hard coded backdoors are much easier to exploit than the cryptographic backdoors, which at least require the attacker to obtain a privileged network position (*e.g.* to intercept traffic). These kind of backdoors also usually offer more access to the victims data than the cryptographic backdoors. Thus the potential for collateral damage is the greatest in this scenario.

4 Discussion

Finding the right balance between security, privacy and surveillance is a complex problem. The current practice of intelligence agencies adding covert backdoors into system deployed world wide is hugely risky and carries with it a significant potential for collateral damage, since criminals or adversarial states can misuse the backdoors. To the best of our ability to judge, the current calls by law enforcement agencies for overt backdoors will mainly impact people who do not think anybody would want to spy on them, i.e. they will not affect the terrorists or organised criminals who are the targets of the people bringing the anti-encryption arguments. However, overt backdoors will cause collateral damage and have negative impact on businesses and on the right to privacy.

What seems clear is that there are no perfect solutions. Governments need to be able to enforce their laws and protect their citizens from adversaries, however, this should not be done at any cost. Just as we place restrictions on ourselves in war, we need to place restrictions on ourselves in matters of surveillance. In war the debate is rooted in ethics and any benefits of a type of attack must be weighed against the potential for collateral damage.[13] We accept higher costs, even in the form of lives, to ensure that collateral damage is minimised. As we have argued above, in our case policymakers must also take

into account the probability that sophisticated actors will find alternative communication channels that largely neutralize any government action; potentially leaving policymakers with all of the costs and limited benefit.

Unfortunately, currently the surveillance debate is polarised with absolutes being pushed by both sides. It is highly unlikely that either extreme – total surveillance or total privacy – is good for our society. Finding the right balance should be framed as an ethical debate centred around the potential for collateral damage. Clearly identifying and quantifying which threat-actors could be caught with which forms of surveillance and weighing the benefits to society against the actual and/or potential collateral damage should help both sides to see the problem more clearly.

References

[1] Deliberately hidden backdoor account in several AMX (HARMAN Professional) devices. http://blog.sec-consult.com/2016/01/deliberately-hidden-backdoor-account-in.html. Accessed: 2016-02-13.

[2] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. A. Specter, and D. J. Weitzner. Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of ...*, 1(1):69–79, Sept. 2015.

[3] N. Anderson. Confirmed: Us and israel created stuxnet, lost control of it. http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/. Accessed: 2016-02-13.

[4] C. Bell. Analysing mikey-sakke: A cryptographic protocol for secure multimedia services. http://pubs.doc.ic.ac.uk/mobius-mikey-sakke-analysis/mobius-mikey-sakke-analysis.pdf. Accessed: 2016-02-13.

[5] E. Felten. The linux backdoor attempt of 2003. https://freedom-to-tinker.com/blog/felten/the-linux-backdoor-attempt-of-2003/. Accessed: 2016-02-13.

[6] D. Fisher. Uk government voice encryption standard built for key escrow, surveillance. https://www.onthewire.io/uk-voice-encryption-standard-built-for-key-escrow-surveillance/. Accessed: 2016-02-13.

[7] D. Froomki. Signs point to unencrypted communications between terror suspects. https://theintercept.com/2015/11/18/signs-point-to-unencrypted-communications-between-terror-suspects/. Accessed: 2016-02-13.

[8] D. Goodin. First known hacker-caused power outage signals troubling escalation. http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/. Accessed: 2016-02-13.

[9] D. Goodin. How elite hackers (almost) stole the nasdaq. http://arstechnica.com/security/2014/07/how-elite-hackers-almost-stole-the-nasdaq/. Accessed: 2016-02-13.

[10] Juniper Networks. Cybercrime will cost businesses over $2 trillion by 2019. Available at http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion, May 2019.

[11] D. Lee. Hacker 'shouts abuse' via foscam baby monitoring camera. http://www.bbc.co.uk/news/technology-23693460. Accessed: 2016-02-13.

[12] S. LEE. Did the san bernardino shooters use advanced encryption or not? http://europe.newsweek.com/san-bernardino-shooters-encryption-fbi-407938?rm=eu. Accessed: 2016-02-13.

[13] J. F. Murphy. Some Legal (And A Few Ethical) Dimensions Of The Collateral Damage Resulting From NATO's Kosovo Campaign. pages 1–27, July 2012.

[14] P. Pawlak and G. Petkova. State-sponsored hackers: hybrid armies? http://www.iss.europa.eu/uploads/media/Alert_5_cyber___hacktors_.pdf. Accessed: 2016-02-13.

[15] N. PERLROTH. Government announces steps to restore confidence on encryption standards. http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/. Accessed: 2016-02-13.

[16] N. PERLROTH, J. LARSON, and S. SHANE. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html. Accessed: 2016-02-13.

[17] A. Swanson. How the islamic state makes its money. https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money/. Accessed: 2016-02-13.

[18] I. Thomson. Cops hate encryption but the nsa loves it when you use pgp. http://www.theregister.co.uk/2016/01/27/nsa_loves_it_when_you_use_pgp/. Accessed: 2016-02-13.

[19] K. Zetter. Security manual reveals the opsec advice isis gives recruits. http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/. Accessed: 2016-02-13.