Keys under doormats

Abstract

- 20 years ago lea wanted companies to ensure access to all encrypted data
- was abandoned, even though "going dark" was feared
- innovation flourished, lea found new ways to gather even more data
- now again they are calling for that, and the same people from back then are coming together to explore this topic
- possible damage is even greater than back then
- "forward secrecy" would need to be reversed
- complexity makes consequences impossible to predict
- how such systems would be globally governed is difficult to say; need to respect human rights and the rule of law

Executive Summary

- US and UK argue that encryption will hinder lea's access to info
- they want *exceptional access* to be implemented
- it's unworkable in practice, big legal and ethical problems and would undo progress made towards a secure internet
- lea have failed to account for the risks of such systems – they often lurk in the technical details
- they take no issue with the goal to enforce law and prosecute criminals
- anyone who wants AE should propose concrete technical requirements which can then the analyzed and discussed
- 1997 had the Clipper Chip, which was better defined: store keys with a trusted third party that would turn over the keys to authorities given the correct paperwork
- key-escrow at scale was not possible at the time because of cost, risk, governance issues
- telecommunication systems have had narrower requirements imposed on them, and that had problems which would have been worse had they been present on a large scale
- LEA's fear of going dark was not true, they have even more data at their fingertips than at any other time before
- now we'd have much more severe security risks, imperil innovation and issues for human rights and international relations
- three general problems:
    1. u-turn from best-practices: *forward secrecy* where keys are permanently destroyed after use so that theft of an old key is not a threat and *authenticated encryption* which ensures that messages have not been tampered with and are still confidential
    2. system complexity would be increased: complexity is the enemy of security, more interaction means more chance for insecurity; with hundreds of thousands of devs and applications all implementing these systems it would be a mess and hard to test in any case
    3. *exeptional access* would create concentrated targets for bad actors; LEA, the platform provider or other third parties would have to store millions of keys – any attacker would enjoy the same privileges as LEA if they get a hold of the keys; required quick access would make more secure storage of keys impractical; **OPM example of losing data if one link in the chain is not secure**
- this holds for access to plaintext as well as just keys – such a backdoor would be vulnerable to attack and a big target; **Google being surveilled by China example**
- jurisdiction is a huge problem as well: even with one LEA it would be risky – but for example the **CLOUD ACT** allows UK agencies to demand the same data that the US can demand; other countries would probably follow suit
- how would EA work across borders, with non-democratic states?
- how could anyone approve all the new products that come to the market?
- who would fund and supervise this system?
- **without concrete technical requirements and answers to the questions in this report, policymakers should reject calls for AE out of hand**

Background

- Comey and Cameron warned of going dark – same as in 1990s – so same group again for the smackdown
- back then they suggested the Clipper Chip, which held a gov master key that enables the access of encrypted data
- another proposal was key-escrow – depositing keys with trusted third parties
- it was abandoned because of industry pressure during the dotcom boom and the EU, among others

Current Debate summary

- LEA have not provided any specifics about their plan
- **Comey statement**: they don't want backdoors, they want clear and transparent front door approaches; encryption might leave the gov in a dead end; **Camero**: do we want messaging that we cannot read in the most extreme cases? No, we must not.
- can this be done without creating unacceptable risk?

Findings from 1997 analysis

- any key-escrow system has requirements that place great cost on the end user and that it would have been really difficult to implement
- for quick access you need highly sensitive but always available keys – great risk for exposure, high software complexity and economic costs
- keyholders are a risk as they might have bad actors or get attacked by such and then have catastrophic results
- additional complexity only makes this worse: back then all the known systems had substantial flaws
- then the whole system would involve millions of actors would have to work together in some way to ensure that everything is secure and available
- all this would also add to the total cost of the whole operation
- **key-escrow 1997: less secure, more expensive and complex than normal systems**

Changes since 1997

- encryption is vital for operating something like the internet with any kind of security – it's not different today, fundamental importance is still the same
- now the amount of things dependant on such encryption is far greater
- export controls in the US in 1990 were loosened because they were counterproductive
- **Crypto Wars** began in the 1970s about export of computers with strong encryption and publishing of cryptography papers, then it moved on to browsers and software
- the war has remained the same
- the biggest challenge is not the mathematics behind encryption, but the engineering in the implementation, **examples of failed systems of scale**
- **more examples of breaches that endanger people's data**
- more attacks on govs are a concern; **more breaches** of key generation tokens as well as personnel records undermine the future security of any such systems, even more with key-escrow
- Commercial Off The Shelf strategy for important equipment has the issue that it can only work if the COTS is safe in the first place
- **some examples of breaches related to lawful access by bad actors**
- this puts all actors at risk
- as we are in need to make infrastructure more secure, any attempt to make is less secure should be treated with skepticism

Scenarios

- there is not enough info to really examine anything

- here are two common scenarios regarding exceptional access

EA to global secure messaging systems

- global messaging system currently using e2e encryption
- e.g. Signal, OTR, WhatsApp, TextSecure
- can these comply with exceptional access?
- direct key access is one option:
  - generally data is encrypted using a symmetric key, then encrypt this key with an asymmetric public key; this is then sent securely and the recipient decrypts the symmetric key using their private key, then decrypt the message
  - common is to say the symmetric key is encrypted with a public escrowing key, to enable lawful access
  - three main problems:
    1. this practice is becoming obsolete as if the private key is ever breached, all data ever sent is open – forward secrecy is the new hit – new keys for each transaction, making it much more secure and requiring more active attackers – as forward secrecy is incompatible with key-escrow that is a huge problem, as the data should be accessible for some time, if not forever; another trend is messaging where the messages disappear after some time, making key-escrow either useless or stopping this trend
    2. encryption today relies on *authentication* and *confidentiality* – if the key for authentication is provided to a third party, this is no longer guaranteed – forging of traffic becomes a threat; if separate keys are used, this would greatly increase the computational effort and make design more difficult
    3. Who would control the escrowed keys? Would the FBI hold the master keys? how would foreign countries react if the US government could access their data? Would'nt they use local systems instead? Would data transfer between two countries be escrowed by both govs? Could there be a neutral authority to handle that? But the how do you handle access?
- such systems would require global agreement on how such systems work, not very likely

EA to plaintext on a smartphone

- e.g. collect some unique device ID and sends that request to the vendor who could then supply the key or unlock the device remotely
- this is already happening to some extend – scaling to global levels is another story though
- here, generally a key-encrypting key is used to take the user password to encrypt the actual key that encrypts the contents of the device
- there might also be some internal code from the device used, as well as mechanism like limited guess rates that slow down attacks
- for key-escrow this key would need to be encrypted with another type of key
- if the vendor has the key, how can they verify the request from thousands of LEAs? they need to have remote access, but some devices don't even boot without a key, so that is bad – fixing glitches and stuff in deployed hardware is almost impossible
- when LEA have the keys the problems are similar, keys have to stored for long times and those keys have a lot of power over the device

Summary of scenarios

- EA will pose significant security risks:
  - improvements in security will be negated
  - increased risk if keys are distributed or stored for long times
  - if law enforcement has easier access, so do criminals
  - multiple agencies in multiple countries having access is even worse, as control and security are even less certain
  - the more complex something is the more exploitable flaws it has

- **SSL TSL analysis and explanantion**: it is used for all secure internet transactions and you kind of have to trust it
- e.g. a missing bounds check that left 17% of all websites vulnerable for two years
- some of this is actually due to the Crypto Wars, where stuff was restricted – many different implementations were created which all have to work together and are thus less secure
- **examples of EA backfiring and hurting govs**
- innovation at the moment depends on embedding intelligence: there is an app for almost anything and a lot of stuff comes with an app now
- if all of those apps had to be accepted by local govs, many countries would just use their local stuff

EA requirements and their security impact

- Access to communications content
  - most countries allow police to access relevant comms data
  - but if two people in two different countries communicate, how will that be regulated?
  - first of all, their security would be at risk just through the presence of KE
  - controlling for location is hard, as one might just buy from another place or spoof one's location
- access to communications data
  - e.g. call detail records, location history and the like
  - because e.g. email is encrypted in traffic, one must subpoena the provider, which is difficult across borders
  - also, just not using a service that cooperates would be a good solution
- access to data at rest
  - almost all police can access data
  - warrants and stuff have and impose certain limits
  - KE is already used for corporate data at rest
  - suspects could use software that does not escrow, or that just fails
  - *just does not work on a global scale*
  - getting vendors to access the data with their help is not that hopeful, as that would hurt trust etc

Conclusion

- all these systems will open doors that can also be used by bad actors
- high cost, damage innovation, hard to predict influence on economic growth