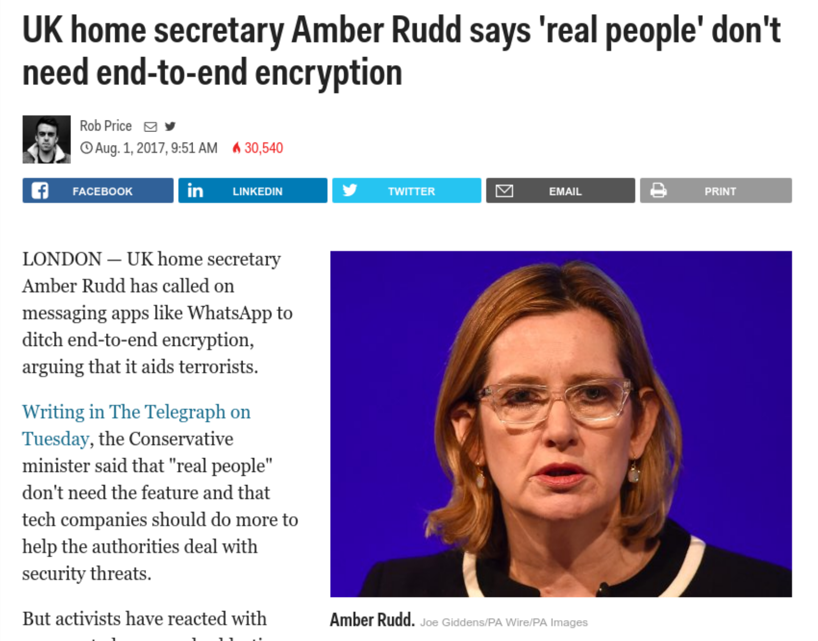
Leave crypto alone!

Myths, challenges and opportunities

Diego F. Aranha

Institute of Computing – University of Campinas

Motivation



UK home secretary Amber Rudd says 'real people' don't need end-to-end encryption

Rob Price

Aug. 1, 2017, 9:51 AM 30,540

LONDON — UK home secretary Amber Rudd has called on messaging apps like WhatsApp to ditch end-to-end encryption, arguing that it aids terrorists.

Writing in The Telegraph on Tuesday, the Conservative minister said that "real people" don't need the feature and that tech companies should do more to help the authorities deal with security threats.

But activists have reacted with

Amber Rudd. Joe Giddens/PA Wire/PA Images

Introduction

Context

Cryptography is the practice and study of techniques for secure communication in the presence of **adversaries**.

Security goals: confidentiality, origin authentication, data integrity, non-repudiation.

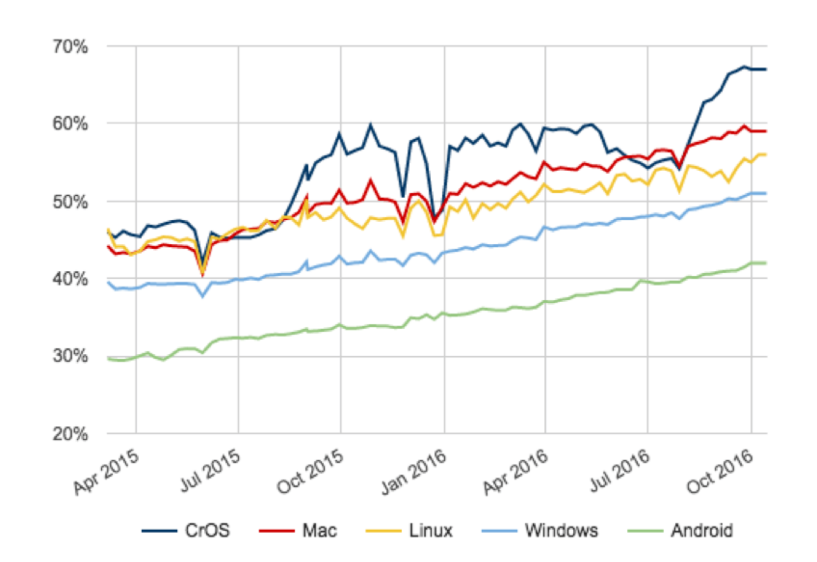
Cryptography is everywhere. Modern banking, e-commerce, multimedia, voting and messaging systems **all** use cryptography.

Cryptography is hard. It not only involves **mathematics** and **computer programming**, but many obstacles exist for secure deployment in practice.

Adversaries: **attack** or **bypass** cryptography to **break** security goals.

Context

HTTPS adoption is growing steadily across all operating systems.



Context

Classically, *privacy* is understood as "**the right to be left alone**" (Warren and Brandeis, 1890) or to **conceal** information.

But humans are social beings, and may give up privacy **selectively** in exchange of perceived **benefits**.

A **modern** definition of privacy follows the trend of **freedom to control** the disclosure of personal information. *Privacy is not only about secrecy anymore, but control.*

Myths

Myth 1: *Privacy is dead*

Privacy as a concept is **not** dead, perhaps it is **at most resting**:

- Users became used to the free-service Internet business model and **rationalized** privacy trade-offs.
- **Data has intrinsic value**, otherwise it would not be captured in troves and data-collecting companies would not be worth **billions**.
- Real risk of **industrial espionage**, targeted **identity theft** and violation of **intimacy**.
- **Massive surveillance** gives economic incentives for privacy-preserving research and services.
- The **nightmare** brought by the so-called Internet of Things will strengthen privacy further.

Myth 2: *Privacy versus Security*

There is no direct tension between privacy and security. Most privacy-intrusive mechanisms actually do not provide **real** security (false dilemma).

Privacy → Security:

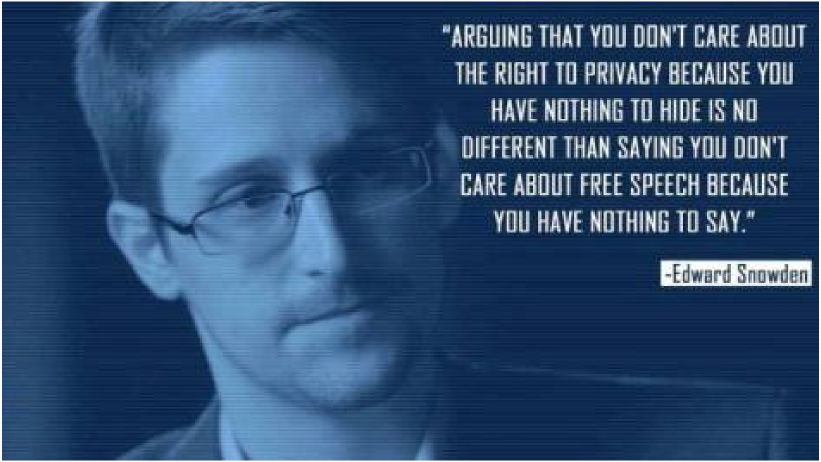
- **Blending into the crowd** (anonymity) avoids targeted attacks.
- **Financial privacy** prevents crime.
- **Medical privacy** against abuse and discrimination.
- **Political privacy** against coercion.
- **Internet privacy** against tracking.

Security → Privacy:

- **Secret data/metadata** are fundamental to privacy.
- Many privacy mechanisms are implemented through security tools, such as **cryptography** and **access control**.

Myth 3: *Privacy/crypto is for criminals*

Honest people have nothing to hide?



"ARGUING THAT YOU DON'T CARE ABOUT THE RIGHT TO PRIVACY BECAUSE YOU HAVE NOTHING TO HIDE IS NO DIFFERENT THAN SAYING YOU DON'T CARE ABOUT FREE SPEECH BECAUSE YOU HAVE NOTHING TO SAY."

-Edward Snowden

Myth 3: *Privacy/crypto is for criminals*

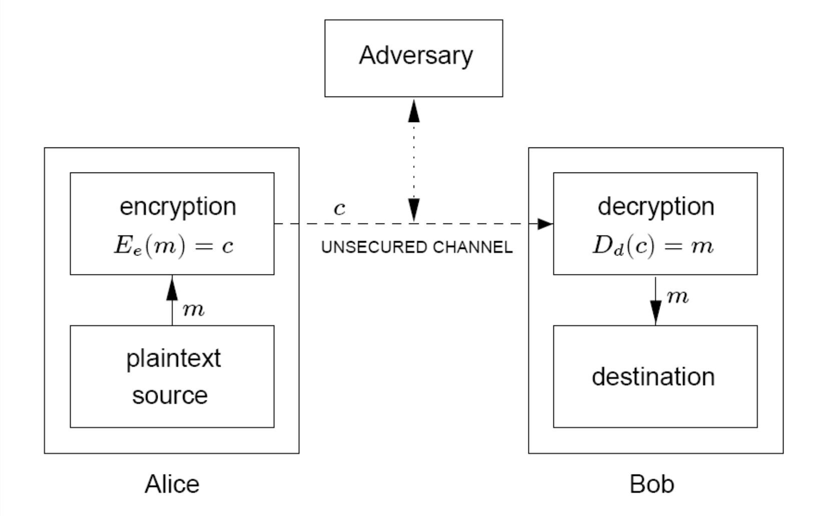
Lots of technologies widely available to criminals, let’s ban them.

Myth 3: *Privacy/crypto is for criminals*

Lots of technologies widely available to criminals, let’s ban them.

Myth 4: *End-to-end cryptography is new or special*

End-to-end cryptography is also known as simply **cryptography**.



Myth 4: *End-to-end cryptography is new or special*

Adversary: can be criminals, intrusive companies or even governments.

Humans already use **end-to-end** cryptography for centuries:

1. Ciphers were used in Ancient Rome and Greece.
2. Military communication systems protect against interception by **foreign enemies**.
3. SSL/TLS in banking/e-commerce systems is **designed** to protect the communication channel.
4. Disk/device encryption systems in mobile devices.
5. Electronic voting systems **must** provide ballot secrecy.

The tension only arises when **common** humans have easy access to cryptographic technology for communication at scale. *It comes from a fear of losing control over society.*

Myth 5: *Just like telephone wiretaps*

Encrypted communication have nothing in common with telephone calls.

Plain telephone lines are an **intrinsically insecure** communication channel. By using a secure encrypted phone, one can however have **encrypted telephone calls**.

Encrypted communication is to plain communication what encrypted calls are to telephone lines.

Myth 6: *Cryptography is enough*

Cryptography is a fundamental tool from a much larger set of tools to protect the entire attack surface of a system.

There are many other technological and procedural things to consider:

- Network security (firewalls and other appliances)
- Operational security (OPSEC)
- Software security (fixing vulnerabilities)
- Access control policies (who has access to what)
- Anonymization (protecting metadata)

Metadata is still a huge privacy problem, especially with recent law.

Challenges

And where they are

We live in a golden age of surveillance and data collection. Metadata is available everywhere.

The **real** challenge for law enforcement is how to filter **signal from noise**.

However, interfering with cryptographic systems is still a popular suggestion. We argue this is ineffective, also intrusive, will make systems insecure, and distort economic incentives.

Challenge 1: *Banning strong cryptography*

Cryptographic techniques are essentially mathematics turned into software. Banning access to strong cryptography amounts to:

1. Banning mathematics.
2. Blaming the tools, not the criminals.
3. Limiting the freedom to write code.
4. Limiting freedom of expression, because **code is speech**.
5. Limiting research and practice in information security.
6. Restricting strong cryptography just to criminals or government.

Challenge 1: *Banning strong cryptography*

Cryptographic techniques are essentially mathematics turned into software. Banning access to strong cryptography amounts to:

1. Banning mathematics.
2. Blaming the tools, not the criminals.
3. Limiting the freedom to write code.
4. Limiting freedom of expression, because **code is speech**.
5. Limiting research and practice in information security.
6. Restricting strong cryptography just to criminals or government.

Solution: Math is not chemistry and does not work like explosives.

Challenge 2: *Building backdoors in practice*

Inserting and protecting backdoors (design flaws) in cryptographic mechanisms will make systems less secure and more expensive to run. Other effects:

1. Complex systems and procedures have **more** vulnerabilities.
2. Keeping backdoors secret is **hard**, due to reverse engineering.
3. **Multiple** entities may request exclusive access.
4. Backdoors can be **leaked** and **repurposed**, as demonstrated in the real-world.

Challenge 2: *Building backdoors in practice*

Inserting and protecting backdoors (design flaws) in cryptographic mechanisms will make systems less secure and more expensive to run. Other effects:

1. Complex systems and procedures have **more** vulnerabilities.
2. Keeping backdoors secret is **hard**, due to reverse engineering.
3. **Multiple** entities may request exclusive access.
4. Backdoors can be **leaked** and **repurposed**, as demonstrated in the real-world.

Solution: There is no “middleground” or design trade-off.

Challenge 3: *Targeting only criminals*

Complex systems do not exist in a vacuum. Interfering with strong cryptography will:

1. Expose **activists** against oppressive governments.
2. Expose **sensitive sources** of investigative journalism.
3. Expose **whistleblowers**.
4. Conserve current conditions for **mass surveillance** efforts.

Challenge 3: *Targeting only criminals*

Complex systems do not exist in a vacuum. Interfering with strong cryptography will:

1. Expose **activists** against oppressive governments.
2. Expose **sensitive sources** of investigative journalism.
3. Expose **whistleblowers**.
4. Conserve current conditions for **mass surveillance** efforts.

Solution: Society becomes the target. Leave crypto alone!

Challenge 4: *Market incentives*

We should work to make systems more secure, not the contrary.
Limiting the strength of cryptography **distorts incentives** and:

1. Forces legitimate security companies into the **underground**.
2. Limits market for **forensic** capabilities.
3. Keeps law enforcement and investigation techniques **obsolete**.
4. Prevents cryptography from being used where **heavily** needed (law enforcement and investigations).

Solution: Good incentives selects good behavior.

Opportunities

Conclusion

Cryptography is hard. Let’s not make it even harder to secure in practice.

Interfering or not with cryptography is actually a choice between **privacy** and **mass surveillance**. *Beware of populist false dilemmas.*

Conclusion

Cryptography is hard. Let's not make it even harder to secure in practice.

Interfering or not with cryptography is actually a choice between **privacy** and **mass surveillance**. *Beware of populist false dilemmas.*

Opportunity 1: Use less intrusive alternatives for investigation such as metadata, cloud backup systems, endpoint analysis and forensic techniques.

Conclusion

Cryptography is hard. Let's not make it even harder to secure in practice.

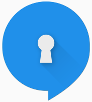
Interfering or not with cryptography is actually a choice between **privacy** and **mass surveillance**. *Beware of populist false dilemmas.*

Opportunity 1: Use less intrusive alternatives for investigation such as metadata, cloud backup systems, endpoint analysis and forensic techniques.

Opportunity 2: Adapt society, infrastructure and law enforcement to the usage of cryptography.

Opportunities

Use more crypto, it's great.

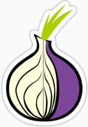


(a) Signal encrypted messaging

(b) Bitcoin cryptocurrency

(c) ZCash anonymous cryptocurrency

(d) TAILS Linux distro



(e) Tor anonymizing network

Suggested further reading

1. The Code Book (Simon Singh)
2. Keys Under Doormats (Anderson, Bellovin, Green, Blaze and many others)
3. Understanding cryptography (Paar)