Keys Under Doormats: mandating insecurity by requiring government access to all data and communications

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matthew Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Peter G. Neumann, Susan Landau, *Ronald L. Rivest*, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

Enigma Conference
San Francisco
January 27, 2016

1990s – Crypto Wars 1.0

- U.S. government expresses concerns about the potential impact on law enforcment of widespread use of encryption.
- Govt. proposes mandated use of “*Clipper Chip*” (1993)...

- Clipper Chip proposal eventually abandoned...
- “The risks of key recovery, key escrow, and trusted third-party encryption," 1997 report by many of the same authors as new report.

2015 – Crypto Wars 2.0

- James Comey (Director, FBI) expresses concern that recent changes (by Google and Apple, in particular) will result in law enforcement being unable to access data on phones, even when LE has a warrant. LE access will “go dark”, because of encryption with keys not known to Google or Apple.
- David Cameron (UK Prime Minister) expresses similar concerns.
- They call for law enforcement to have “exceptional access” to content (somehow – there are no technical specs or proposals on how to do so).

Keys Under Doormats (2015)

- Our report, “Keys Under Doormats” reviews and expands upon our earlier report.
- Summary: *the world has become much more complicated since the 90s, and the idea of providing “exceptional access” for law enforcement is even more dubious now than it was then.*
- We give some key points...

The problem specs are missing!

- What does LE really want? Have they thought this through?
- Like saying “The bad guys are using fast cars to get away! Fix this problem so they can’t go faster than the police!” *Huh? This is not a problem specification.*
- *Jurisdictional* aspects may be a show-stopper. Does every country get exceptional access? Can China access iPhones of traveling U.S. officials?

The cure is worse than the disease!

- *Exceptional access makes the internet less secure* both directly (new intended vulnerabilities) and indirectly (it will be complex, meaning new unintended vulnerabilities).
- We have a cybersecurity crisis, and exceptional access makes an essential tool (cryptography) more expensive and difficult to use.
- Exceptional access requires violation of best practices in cryptography (forward security and authenticated encryption).
- Likely consequence is serious long-term damage to our national security.

Many Unanswered Questions

- Sufficient justification?
- Coverage (technical, jurisdictional)?
- Millions of apps and services now available worldwide!?
- Human rights! (Privacy, anonymity)
- Public design review? Standards?
- Cost estimates? Impact on US companies?
- Oversight, compliance, regulation?
- Unintended consequences (reduced use of crypto?)

Such questions need answers before a credible proposal is even possible...

What can you do?

- Try to imagine how a requirement for exceptional access could affect your company's products and services.
- Get your company or organization involved in the fight against perhaps well-motivated but poorly throught-through proposals to restrict the use of cryptography.

For more information...

To find our report, google for “Keys Under Doormats” or look at URL:

`http://people.csail.mit.edu/rivest/pubs.html#AABBx15x`