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

CRYPTO rump session
August 18, 2015

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

- Our new report, “Keys Under Doormats” reviews and expands upon our earlier report.
- Quick summary: the world is much more complicated since the the 90’s, and the idea of providing “exceptional access” for law enforcement is very much more dubious than it was in the 1990’s.

Some Key Points

- Introducing “exceptional access” means introducing new vulnerabilities.
- Violates forward secrecy and authenticated encryption.
- Would seem to entail authorized access by LE of any country? Jurisdiction!?
- Millions of apps and services now available worldwide!?
- Complexity !!! –> Insecurity
- No clear specs for what is desired.

Many Unanswered Questions

- Sufficient justification?
- Coverage (technical, jurisdictional)?
- 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 on the table...

For more information...

Our report can be found by googling for “Keys Under Doormats” or at

`http://people.csail.mit.edu/rivest/pubs.html#AABBx15`