Keys Under Doormats

Mandating Insecurity by Requiring Government Access to All Data and Communications

Steven M. Bellovin
https://www.cs.columbia.edu/~smb

Nomenclature Note

- I’ll be referring to a country that doesn’t respect human rights or the rule of law
- We’re an international group—so I’ll refer to it as Andromeda, as in the galaxy
- You may mentally substitute any real country you wish

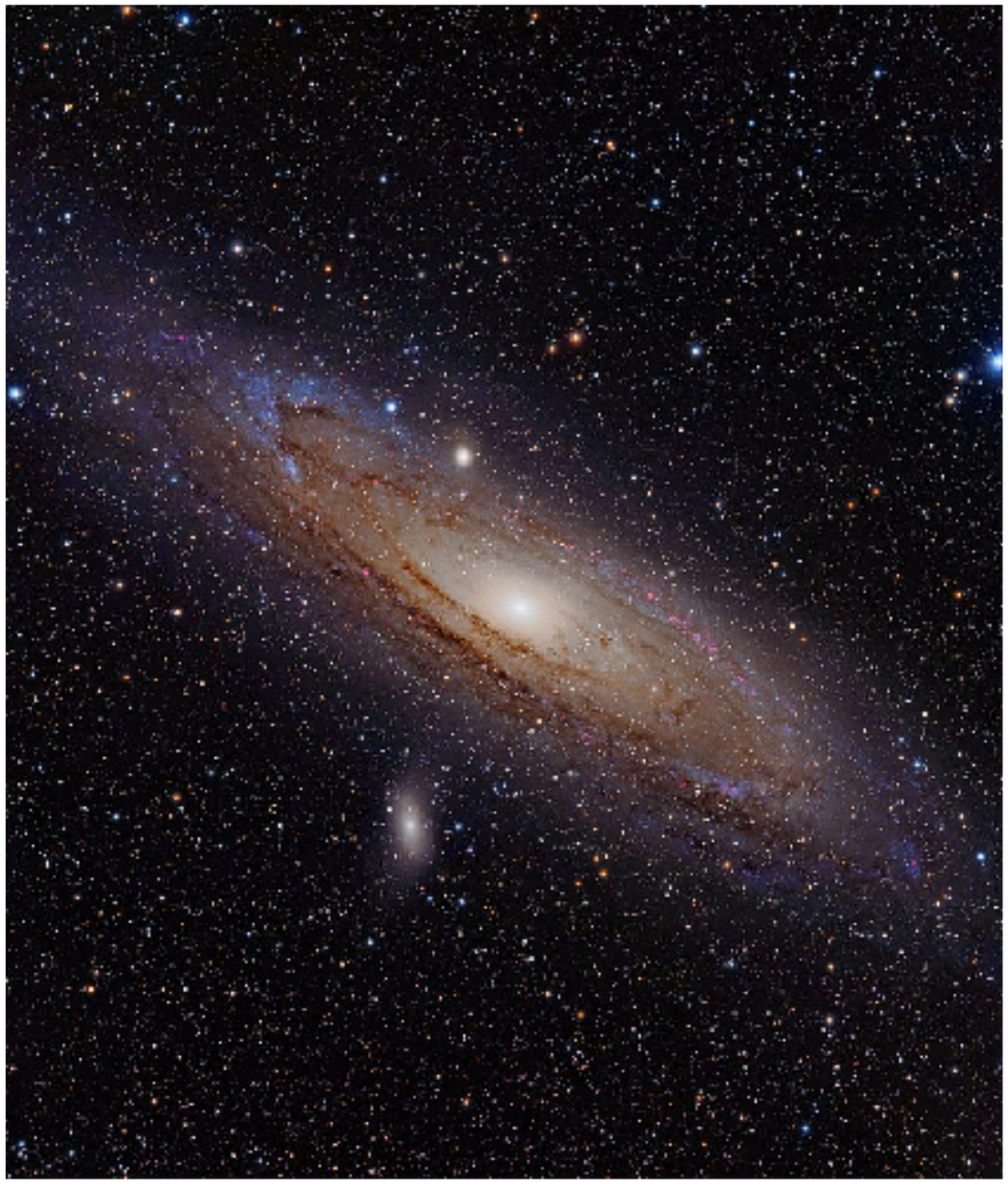

Photo by NASA

Cryptography is Strong

- Modern cryptography, if done properly, is effectively unbreakable
- We have a very good idea about the essential strength of algorithms like RSA and AES
- Even DES—almost 45 years old!—has resisted every reasonable attack we can launch today except for brute force, and that weakness was known at the time (and was deliberate)

Cryptography is a Problem

- For several decades, the NSA and the FBI have worried about the spread of strong cryptography

- The FBI claim it's “going dark” and is being hindered by the spread of encryption, especially on-by-default encryption

- They've called for *exceptional access* (AKA a “golden key” or a “back door”) to let them read encrypted content

Keys Under Doormats?

- Most cryptographers think that exceptional access is a really bad idea
- Why?
- Because we haven't “nerded harder”?
- *No—it's because we think it's inherently unsafe*
- *Maybe* we can get the protocol right—but it will be a low-assurance solution; we won't *know* that it's correct

Cryptography is Hard

- When doing encryption, you need a protocol—a stylized set of messages and data formats
- Getting these wrong can result in security problems
- The very first academic paper on the subject (Needham and Schroeder, 1978) ended with a warning

  > Finally, protocols such as those developed here are prone to extremely subtle errors that are unlikely to be detected in normal operation. The need for techniques to verify the correctness of such protocols is great, and we encourage those interested in such problems to consider this area.

- They were right—a simple flaw in their scheme went unnoticed for 18 years

Historical Example: Enigma

- Picking non-random letters for the session key was a fatal flaw
- Encrypting the session key twice was a fatal flaw
- Sending the same, simple message every day was a fatal flaw
- Sending a message consisting of nothing but the letter “L” was a fatal flaw

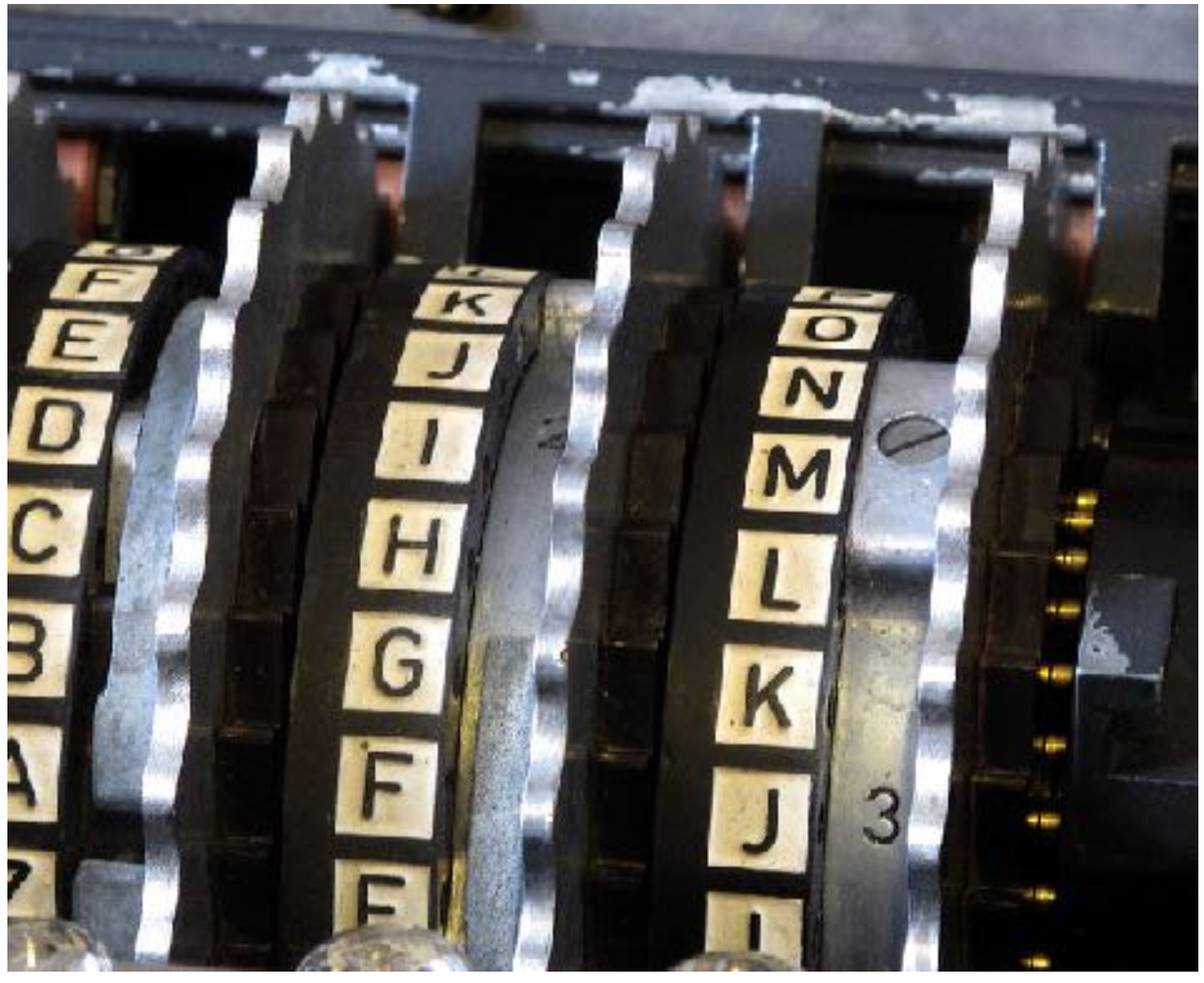

Photo: public domain

Examples

- Incorrectly padding a short message to match the encryption algorithm's requirements has resulted in security flaws
- Not authenticating every encrypted message has resulted in flaws. (That was the essential flaw recently found in Apple's iMessage protocol.)
- Omitting sequence numbers from encrypted messages has resulted in flaws
- The existence of older, "exportable" algorithms in the key and algorithm negotiation protocol has resulted in flaws
- Trying to provide an "additional decryption key" for the government has resulted in flaws

It's a Systems Problem

- Simply “fixing” the protocol doesn't solve the problem

- There are many, many other issues, including authorization for access and technically protecting the access mechanisms

- “You don’t go through strong security, you go around it.”

Authentication and Authorization

- Who is authorized to request decryption?
- Law enforcement? Which agencies? From which countries? Andromeda? Their customs agents?
- How does the designated unlocking agent (probably the vendor) authenticate the requester? How is this done internationally?

How Are Golden Keys Protected?

- Protecting code-signing keys—used tens of times per year—may be feasible

- Golden keys would be used tens of times per day or more—can you protect them from the Andromedans?

- What about protection of the keys that requesters to authenticate their requests?

- If requests are very frequent, are they carefully vetted?

Exceptional Access for Communications

- If some agency somewhere wants to read a communication, how did they acquire it? Legally? From where?

- This is especially serious for international access requests, including, of course from Andromeda

Exceptional Access for Devices

- An easier problem than for communications, because you can use possession of the device as an authentication factor

- But: was the device taken “legitimately”? According to what countries’ standards?

- What about travelers crossing borders into Andromeda, which doesn’t respect the rule of law?

- Remember that phones are very commonly used as authenticators to other services

International Issues

- If one major country has the ability to bypass encryption, every other country will want the ability, too
- Are golden keys locked to some country? How?
  - What about border-crossings or international communications?
  - What about imported phones?
- Does the vendor's country have veto power over another country's unlock requests? How well will that play with other countries?
  - Even knowledge of unlock requests can be sensitive

Conclusions

- The exceptional access problem is not one problem but many
- Some of the issues are political, not technical; this can make them harder to solve
- But the technical difficulties are daunting enough!
- Strong encryption is essential for security; the debate here is not privacy versus security, it's security versus security

Recommendations for Law Enforcement

- Hack into endpoints
- Devote more resources to forensic examination of encrypted devices
- Find other approaches to solving certain crimes
- Accept that the tradeoff for inability to solve a few crimes is more than balanced by the crimes that strong encryption prevents

Questions?