On “exceptional access”

Ronald L. Rivest

Institute Professor
MIT, Cambridge, MA

CSAIL PI Lunch
May 31, 2018

In the beginning...

- Cryptography was all about military intelligence.

In the beginning...

- Cryptography was all about military intelligence.
- World War II, Enigma, Bletchley Park, Colossus

In the beginning...

- Cryptography was all about military intelligence.
- World War II, Enigma, Bletchley Park, Colossus
- FISA (Foreign Intelligence Surveillance Act, 1977)

Then it was about e-commerce and theory

- DES (Data Encryption Standard) approved 1976

Then it was about e-commerce and theory

- DES (Data Encryption Standard) approved 1976
- Public-key encryption and RSA: Diffie, Hellman, Merkle, Rivest, Shamir, Adleman (1976-77)

Then it was about e-commerce and theory

- DES (Data Encryption Standard) approved 1976
- Public-key encryption and RSA: Diffie, Hellman, Merkle, Rivest, Shamir, Adleman (1976-77)
- Goldwasser and Micali (1982)

Then it was about e-commerce and theory

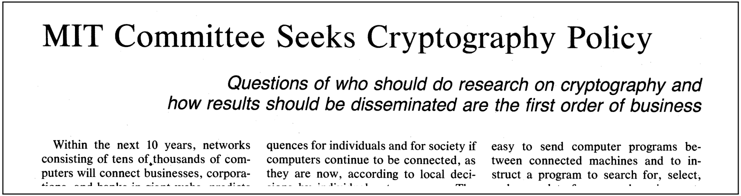
- DES (Data Encryption Standard) approved 1976
- Public-key encryption and RSA: Diffie, Hellman, Merkle, Rivest, Shamir, Adleman (1976-77)
- Goldwasser and Micali (1982)
- Ray Ozzie (Iris/IBM; Lotus Notes) was one of first RSA licensees (1986).

Then it was about e-commerce and theory

- DES (Data Encryption Standard) approved 1976
- Public-key encryption and RSA: Diffie, Hellman, Merkle, Rivest, Shamir, Adleman (1976-77)
- Goldwasser and Micali (1982)
- Ray Ozzie (Iris/IBM; Lotus Notes) was one of first RSA licensees (1986).
- Tim Berners-Lee, The World-Wide Web (1990)

Crypto Wars 1.0

- U.S. government initially tried to control and limit public-sector research and use of cryptography
- Attempt to chill research via ITAR (1977)
- MIT "Changing Nature of Information" Committee (1981; Dertouzos, Low, Rosenblith, Deutch,Rivest,...)



MIT Committee Seeks Cryptography Policy

Questions of who should do research on cryptography and how results should be disseminated are the first order of business

Within the next 10 years, networks consisting of tens of thousands of computers will connect businesses, corpora-

quences for individuals and for society if computers continue to be connected, as they are now, according to local deci-

easy to send computer programs between connected machines and to instruct a program to search for, select,

Science, 13 Mar 1981

Crypto Wars 1.0

- U.S. government tried to mandate accessibility of all encryption keys via “key escrow” and/or “Clipper Chip” (1993)

Crypto Wars 1.0

- U.S. government tried to mandate accessibility of all encryption keys via “key escrow” and/or “Clipper Chip” (1993)

Crypto Wars 1.0

- U.S. government tried to mandate accessibility of all encryption keys via “key escrow” and/or “Clipper Chip” (1993)

- Ray Ozzie promoted scheme in 1995 giving 24 bits of 64-bit encryption keys in export products to NSA. (Encrypted with NSA PK.) Swedish Parliament has conniptions.

Crypto Wars 1.0

- U.S. government tried to mandate accessibility of all encryption keys via “key escrow” and/or “Clipper Chip” (1993)

- Ray Ozzie promoted scheme in 1995 giving 24 bits of 64-bit encryption keys in export products to NSA. (Encrypted with NSA PK.) Swedish Parliament has conniptions.
- With defeat of “Clipper Chip”, it seemed “crypto wars” were over; strong crypto was recognized as necessary for commerce and for national security...

“Keys Under Doormats” Report (2015)

- FBI continues to push for “exceptional access”
  Claims law enforcement is “going dark”
  Others say we are now in “golden age of surveillance”

“Keys Under Doormats” Report (2015)

- FBI continues to push for “exceptional access”
  Claims law enforcement is “going dark”
  Others say we are now in “golden age of surveillance”
- “Keys Under Doormat” report (2015) has 15 authors, including MIT authors Abelson, Rivest, Schiller, Specter, Weitzner.

“Keys Under Doormats” Report (2015)

- FBI continues to push for “exceptional access”
  Claims law enforcement is “going dark”
  Others say we are now in “golden age of surveillance”
- “Keys Under Doormat” report (2015) has 15 authors, including MIT authors Abelson, Rivest, Schiller, Specter, Weitzner.
- Report documents vagueness of LE request, and technical difficulties of achieving LE access without introducting catastrophic modes of failure.

Crypto Wars 2.0

- December 2015 San Bernadino case

Crypto Wars 2.0

- December 2015 San Bernadino case
- Apple resists FBI suit to modify OS to achieve access

Crypto Wars 2.0

- December 2015 San Bernadino case
- Apple resists FBI suit to modify OS to achieve access
- FBI drops case when it gets access (via Cellebrite?) in March 2016

Ozzie's CLEAR proposal

- FBI seeks technologists to provide “front door” solution

Ozzie’s CLEAR proposal

- FBI seeks technologists to provide “front door” solution
- Meanwhile, Cellebrite and Grayshift provide super-cheap access to locked iPhones.

Ozzie’s CLEAR proposal

- FBI seeks technologists to provide “front door” solution
- Meanwhile, Cellebrite and Grayshift provide super-cheap access to locked iPhones.
- Ray Ozzie floats “CLEAR” proposal.

Ozzie’s CLEAR proposal

- FBI seeks technologists to provide “front door” solution
- Meanwhile, Cellebrite and Grayshift provide super-cheap access to locked iPhones.
- Ray Ozzie floats “CLEAR” proposal.
    - Only for phones; only for “data at rest” in phone

Ozzie's CLEAR proposal

- FBI seeks technologists to provide "front door" solution
- Meanwhile, Cellebrite and Grayshift provide super-cheap access to locked iPhones.
- Ray Ozzie floats "CLEAR" proposal.
  - Only for phones; only for "data at rest" in phone
  - Requires LE to possess phone

Ozzie’s CLEAR proposal

- FBI seeks technologists to provide “front door” solution
- Meanwhile, Cellebrite and Grayshift provide super-cheap access to locked iPhones.
- Ray Ozzie floats “CLEAR” proposal.
  - Only for phones; only for “data at rest” in phone
  - Requires LE to possess phone
  - Vendor (Apple) has Apple PK embedded in phone. Idea is that managing SK is like managing “code-signing key”

Ozzie's CLEAR proposal

- FBI seeks technologists to provide "front door" solution
- Meanwhile, Cellebrite and Grayshift provide super-cheap access to locked iPhones.
- Ray Ozzie floats "CLEAR" proposal.
  - Only for phones; only for "data at rest" in phone
  - Requires LE to possess phone
  - Vendor (Apple) has Apple PK embedded in phone. Idea is that managing SK is like managing "code-signing key"
  - LE can get phone to spit out phone encryption key, encrypted with Apple PK.

Ozzie's CLEAR proposal

- FBI seeks technologists to provide "front door" solution
- Meanwhile, Cellebrite and Grayshift provide super-cheap access to locked iPhones.
- Ray Ozzie floats "CLEAR" proposal.
  - Only for phones; only for "data at rest" in phone
  - Requires LE to possess phone
  - Vendor (Apple) has Apple PK embedded in phone.
    Idea is that managing SK is like managing "code-signing key"
  - LE can get phone to spit out phone encryption key, encrypted with Apple PK.
  - LE enters phone encryption key obtained from Apple, and gets data, but phone is bricked.

Problems with Ozzie's proposal

- NASEM report on encryption debate (Goldwasser, Landau, Boneh and others)

  http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25010

  A framework; no recommendations. E.g.:
  "Will the proposed approach be effective?"
  "How would it affect privacy, civil liberties, and human rights of targeted individuals and groups?"

Problems with Ozzie's proposal

- NASEM report on encryption debate (Goldwasser, Landau, Boneh and others)

  http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25010

  A framework; no recommendations. E.g.:
  "Will the proposed approach be effective?"
  "How would it affect privacy, civil liberties, and human rights of targeted individuals and groups?"
- "Man in the middle attack" by Eran Tromer:

  https://www.cs.columbia.edu/~smb/blog/2018-05/2018-05-02.html

Problems with Ozzie's proposal

- NASEM report on encryption debate (Goldwasser, Landau, Boneh and others)

  `http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25010`

  A framework; no recommendations. E.g.:
  "Will the proposed approach be effective?"
  "How would it affect privacy, civil liberties, and human rights of targeted individuals and groups?"
- "Man in the middle attack" by Eran Tromer:

  `https://www.cs.columbia.edu/~smb/blog/2018-05/2018-05-02.html`
- Matt Green blog post:

  `https://blog.cryptographyengineering.com/2018/04/26/`

  `a-few-thoughts-on-ray-ozzies-clear-proposal/`

Problems with Ozzie's proposal

- NASEM report on encryption debate (Goldwasser, Landau, Boneh and others)

  `http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25010`

  A framework; no recommendations. E.g.:
  "Will the proposed approach be effective?"
  "How would it affect privacy, civil liberties, and human rights of targeted individuals and groups?"
- "Man in the middle attack" by Eran Tromer:

  `https://www.cs.columbia.edu/~smb/blog/2018-05/2018-05-02.html`
- Matt Green blog post:

  `https://blog.cryptographyengineering.com/2018/04/26/`

  `a-few-thoughts-on-ray-ozzies-clear-proposal/`
- Ars Technica article:

  `https://arstechnica.com/information-technology/2018/05/`

  `op-ed-ray-ozzies-crypto-proposal-a-dose-of-technical-reality/`

Some details

- Key vault would effectively need to be online, as it would be used continually.

Some details

- Key vault would effectively need to be online, as it would be used continually.
- Key vault is a **very** juicy target: enables unlocking of billions of phones.

Some details

- Key vault would effectively need to be online, as it would be used continually.
- Key vault is a **very** juicy target: enables unlocking of billions of phones.
- Metaphor that it is “like managing a code-signing key” doesn’t hold water: look up “Stuxnet”

Some details

- Key vault would effectively need to be online, as it would be used continually.
- Key vault is a **very** juicy target: enables unlocking of billions of phones.
- Metaphor that it is “like managing a code-signing key” doesn’t hold water: look up “Stuxnet”
- “Hardware security modules” (HSMs) have also shown vulnerabilities.

Some details

- Key vault would effectively need to be online, as it would be used continually.
- Key vault is a **very** juicy target: enables unlocking of billions of phones.
- Metaphor that it is “like managing a code-signing key” doesn’t hold water: look up “Stuxnet”
- “Hardware security modules” (HSMs) have also shown vulnerabilities.
- Protection against secret surveillance by bricking phone probably won’t work either: see *Cellebrite* and *Grayshift*.

The debate continues...

- Congress introduces bill to ban backdoor access...

  https://9to5mac.com/2018/05/11/secure-data-act/

The debate continues...

- Congress introduces bill to ban backdoor access...

  https://9to5mac.com/2018/05/11/secure-data-act/

- FBI can’t count... (7800 locked phones → 1000-2000 at most)

  https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/30/

  the-fbi-blunder-on-phone-encryption-explained/?utm_term=.3a7875569952