Karl Koscher (@supersat)
University of Washington

Shattring Your Secrets:

Coercion-Resistant Full Disk Encryption, and More!

The Problem

- DHS: "In the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information encountered at the border"


ACLU

AMERICAN CIVIL LIBERTIES UNION

BECAUSE FREED

KEY ISSUES ACTION

HOME › KEEP AMERICA SAFE AND FREE › SURVEILLANCE & PRIVACY

Court Rules No Suspicion Needed for Laptop Searches at Border

The Problem

CNET › Security › Researcher detained at U.S. border, questioned about Wikileaks

Researcher detained at U.S. border, questioned about Wikileaks

Jacob Appelbaum, who volunteers with Wikileaks, is questioned for three hours and has mobile phones confiscated on his way back to the United States for a hacker show.

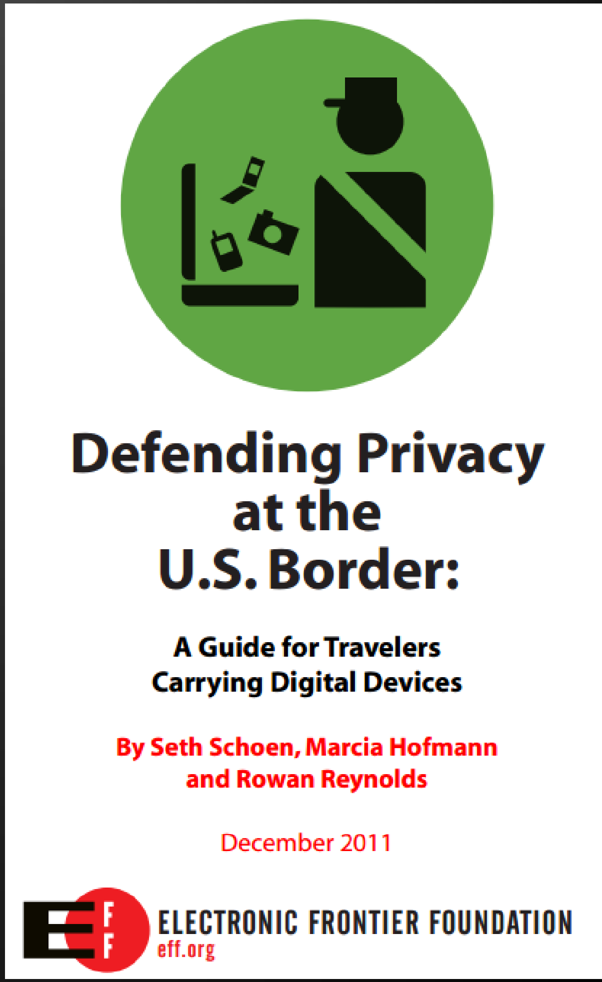
by Elinor Mills @elinormills / July 31, 2010 4:16 PM PDT

© DPA

- Hired by our lab on work on Tor
  - Would we suddenly be harassed too?
- Not just a US issue – economic espionage abroad

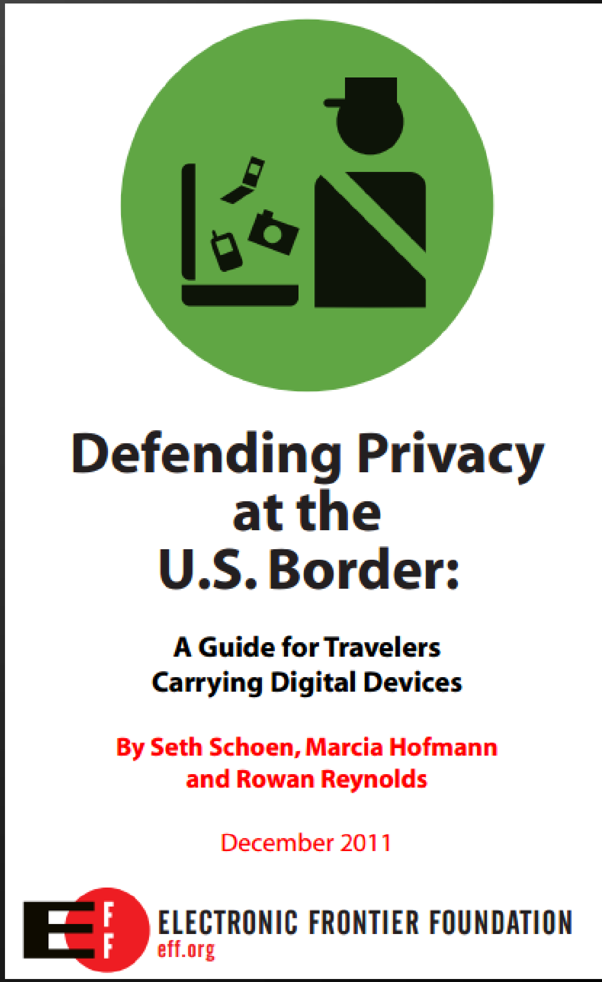
What does the ~~Fox~~ EFF say?

- Full Disk Encryption "… is the most fundamental security precaution for computer users who have confidential information on their hard drives and are concerned about losing control over their computers … "



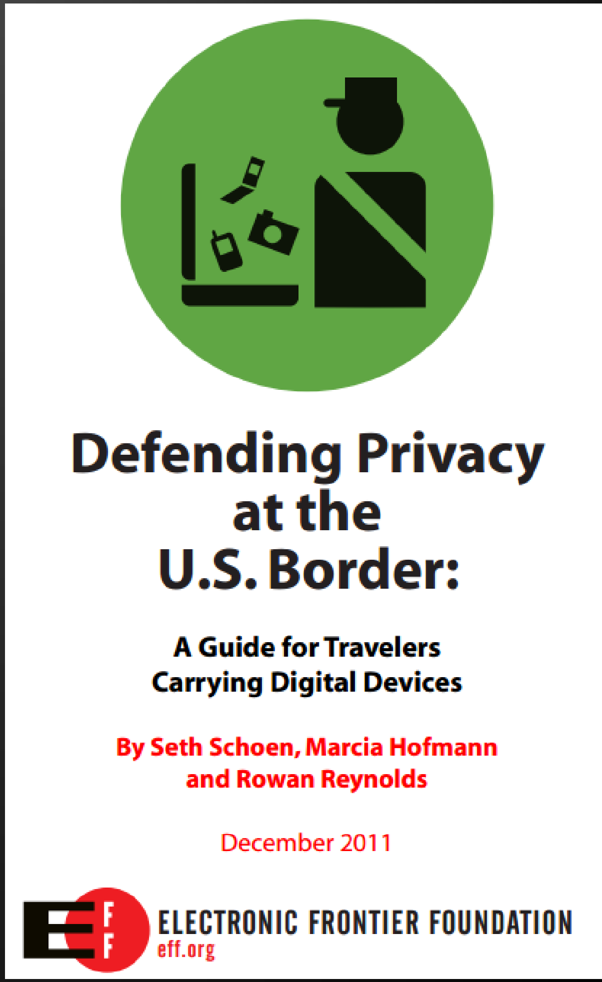
What does the ~~Fox~~ EFF say?

- "If a border agent asks you to provide an account password or encryption passphrase or to decrypt data stored on your device, you don't have to comply"



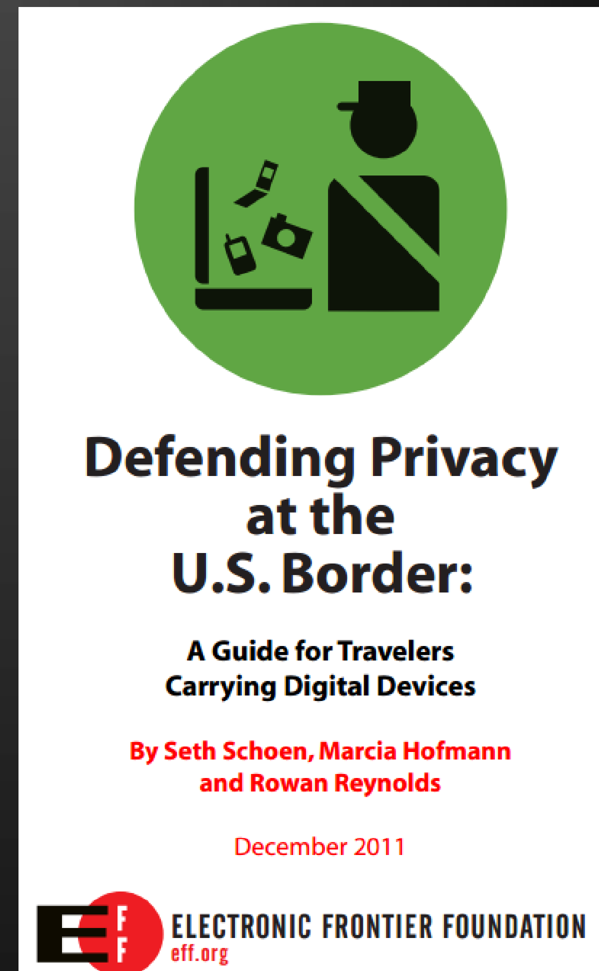
What does the ~~Fox~~ EFF say?

- "However, if you refuse to provide information or assistance upon request, the border agent may seize your device for further inspection or consider you uncooperative"



What does the ~~Fox~~ EFF say?

- "Another option is to generate a long and not-very-memorable encryption password before your trip, and then have someone else hold onto it and send it to you later, after you've crossed the border. This might be especially practical with a work computer if you have support from an IT department at your workplace, because the IT department could hold onto the password for you and let you know it when you check in with them again."



Defending Privacy at the U.S. Border:

A Guide for Travelers Carrying Digital Devices

By Seth Schoen, Marcia Hofmann and Rowan Reynolds

December 2011

ELECTRONIC FRONTIER FOUNDATION
eff.org

What about personal devices?

- Bitlocker allows multiple “protectors”
  - TPM storage (w/ or w/o PIN)
  - USB drive
  - Smart cards (for removable devices)
  - Recovery keys
- One solution:
  - Use TPM for everyday use
  - Clear the TPM before crossing
  - Retrieve recovery key after crossing

Options for Storing the Key

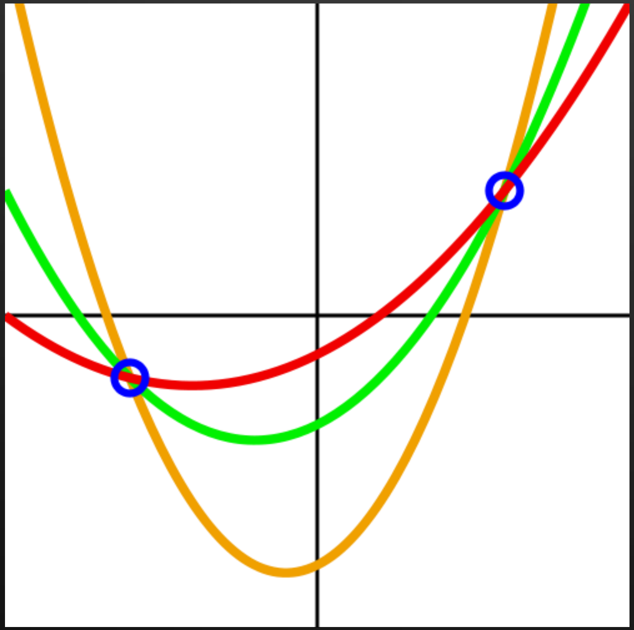
- A file and/or printout at home
  - Can be obtained with a warrant
    - Encrypting with a password helps
- An encrypted file in the cloud
  - In certain situations, you may still be compelled to provide access to the key (c.f. RIPA in the UK)
- Giving the key to a friend
  - But legally, they can be compelled a lot easier

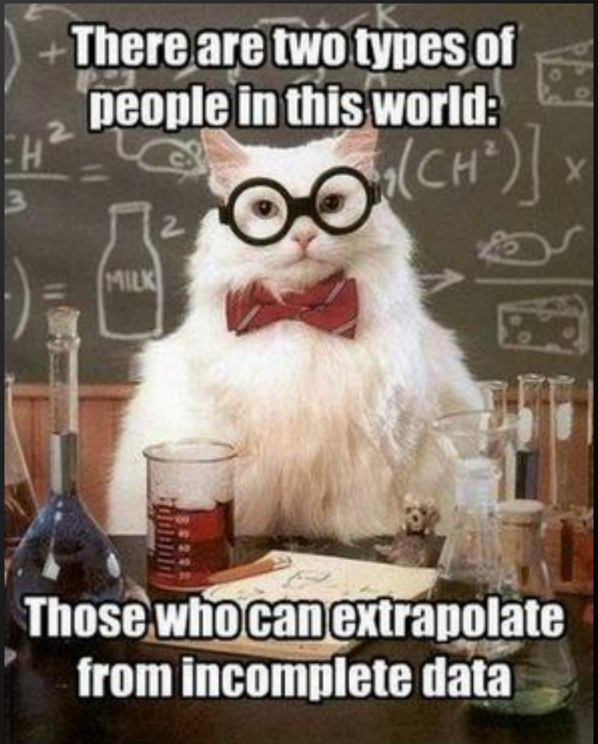
This talk: Splitting the key

- Split the key into several “shards” and distribute then to friends across the world
- Require several of them to reconstruct the key
  - E.g. It would be hard to simultaneously compel people in Russia and Germany to provide their shards

Shamir Secret Sharing

- Proposed by Shamir (the "S" of RSA) in 1979
- Idea: To find determine a polynomial of degree *n*, you need *n* + 1 points





Shamir Secret Sharing

- Suppose you want to require *m* of *n* shards
- Generate a polynomial of degree $m - 1$ with random coefficients and $f(0) = key$
- Generate *n* points along the polynomial
- Use Lagrange Interpolation for efficient recovery with sufficient shards

Shamir Secret Sharing

- Some pitfalls when using “normal math”:
  - Some information about the key can be determined if you have some of the shards
  - Arbitrarily high levels of precision are needed to recompute the exact key
- Instead, we perform these computations in a finite field

Galois Fields

- A field has
  - A set of elements
  - A definition of addition over the elements
  - A definition of multiplication over the elements
  - Operations must:
    - Be associative E.g. $(a + b) + c = a + (b + c)$
    - Be commutative E.g. $(a + b) + c = a + (b + c)$
    - Have an identity element E.g. $a + 0 = a$
    - Have an inverse element E.g. $a + b = 0$
  - Distributivity E.g. $a \times (b + c) = (a \times b) + (a \times c)$

Galois Fields

- Galois Fields are finite fields
  - i.e. there are a finite number of elements

- Example: integers modulo 7
  - $1 + 1 = 2$
  - $2 \times 3 = 6$
  - $5 + 3 = 1$
  - $3 \times 6 = 4$
  - $3 \div 6 = ???$

Multiplication in Galois Fields

- We find a generator
- Exponentiate it (i.e. multiply it repeatedly)
  - $1 \times 3 \equiv 3 \pmod 7$
  - $3 \times 3 \equiv 2 \pmod 7$
  - $2 \times 3 \equiv 6 \pmod 7$
  - $6 \times 3 \equiv 4 \pmod 7$
  - $4 \times 3 \equiv 5 \pmod 7$
  - $5 \times 3 \equiv 1 \pmod 7$

Multiplication in Galois Fields

- We build a table (or two) as we go
- Now we can do logarithms and antilogs!

0	1	2	3	4	5	6
1	3	2	6	4	5	1

- A useful property: a x b = $e^{\ln(a) + \ln(b)}$
  - Works in finite fields too!
  - $a \times b = g^{\log_g a + \log_g b \pmod 6}$
  - $a \div b = g^{\log_g a - \log_g b \pmod 6}$
- $3 \div 6 = 5$ and $2 \times 6 = 5$

Useful Galois Fields

- A Galois Field exists for any prime number raised to the power of any positive integer
  - $GF(2^x)$ is commonly used
- Elements are polynomials
  - $x + 1$
  - $x^6 + x^2$
- If we just write down the coefficients of polynomials in $GF(2^8)$, we get a byte!
  - E.g. $x^6 + x + 1$ => 01000011

Useful Galois Fields

- Addition: Add polynomials modulo 2
  - E.g. $(x+1)+(x^2+x)=(x^2+0x+1)=(x^2+1)$
  - In binary: 00000011 + 00000110 = 00000101
    - This is just XOR!
- Multiplication: Multiply polynomials, but divide by a reducing polynomial if degree is too great
  - E.g. $(x+1)\times(x^6+1)=(x^7+x^6+x+1)$
  - $(x^7+x^3+1)\times(x^2+x)=$
    $(x^9+x^8+x^5+x^4+x^2+x)$???

Useful Galois Fields

- We can't represent $(x^9 + x^8 + x^5 + x^4 + x^2 + x)$
- Use long division w/ an irreducible polynomial
  - Let's use $x^8 + x^4 + x^3 + x + 1$
- Let's represent as binary:
  - Product: 1100110110
  - Reduction Polynomial: 100011011

Useful Galois Fields

```
          __________
100011011 | 1100110110
```

Useful Galois Fields

```
                 1
           __________
100011011 | 1100110110
            100011011
            ---------
             100000000
```

Useful Galois Fields

```
                11
           ____________
100011011 | 1100110110
            100011011
            ---------
             100000000
             100011011
             ---------
             000011011  <= Remainder
```

- These are just bit shifts and XORs!
  - Really fast, especially in hardware
  - We can also use log/antilog tables

Putting it all together

- "Oh god why did you subject me to that much math?"

- Galois Fields underlie a LOT of technologies
  - Error correction (Reed-Solomon)
  - Diffie-Hellman key exchange
  - Elliptic curve cryptography
  - AES (aka Rijndael)
  - Shamir Secret Sharing

Putting it all together

- With Galois fields:
  - All operations are always defined (except division by zero)
  - We never have to deal with large numbers
  - All we need are XORs and table lookups
- This makes implementing Shamir Secret Sharing straight-forward

Putting it all together

- We are doing byte-wise Shamir Secret Sharing over $GF(2^8)$

- For each byte *k* of the key:
  - Choose $m - 1$ random bytes as coefficients
  - For each shard *(x):*
    - Compute $c_{m-1}x^{m-1} + \cdots + c_2x^2 + c_1x + k$
    - Now that we can do Galois field math, this is easy!

Putting it all together

- To reconstruct the key, we use Lagrange Interpolation
  - We want to build a polynomial that precisely equals y_i at x_i for each shard i
  - Intuition: We can do this by summing several polynomials, each that evaluate to 0 at every point except at x_i, where it is equal to y_i

Putting it all together

- How do we make such a polynomial?
- Simple: $(x - x_1)(x - x_2)\ldots(x - x_m)$
  - Exclude the x_i for that shard
  - At each x_i, the product will be 0
  - Normalize to 1 by dividing by $(x_i - x_1)(x_i - x_2)\ldots(x_i - x_m)$
  - Multiply by y_i
  - Since we are only interested in $x = 0$, we can simplify…

Putting it all together

- $y = \sum_{j=0}^{k} \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{-x_m}{x_j - x_m}$
- Or in Javascript:

```
for (var b = 0; b < len; b++) {
    var sum = 0;
    for (var i = 0; i < shares_x.length; i++) {
        var num = 1;
        var denom = 1;
        for (var j = 0; j < shares_x.length; j++) {
            if (i != j) {
                num = gf_mul(num, gf_sub(0, shares_x[j]));
                denom = gf_mul(denom, gf_sub(shares_x[i], shares_x[j]));
            }
        }
        sum = gf_add(sum, gf_mul(shards[i][b], gf_div(num, denom)));
    }
    output[b] = sum;
}
```

Introducing Shattr

- A web app for splitting your secrets
- Supports raw hex keys and Bitlocker keys
- Also lets you encrypt and sign data without exposing the raw key

Shattr

- "A web app? Are you NUTS?" Well… no.
- The entire app is a single HTML file, works completely offline, and is always served over HTTPS using HSTS
- Shattr will be on the DEFCON CD, and the file will never change
  - Anyone can audit the web site to ensure it hasn't
  - Please audit the code before July 15th!
- Uses the Web Crypto API for secure random number generation and non-secret sharing crypto

Using Shattr with Bitlocker

- Bitlocker encrypts your hard drive with a key
- This key is encrypted with keys provided by other protectors
  - This lets you add and revoke protectors without re-encrypting the entire drive

Using Shattr with Bitlocker

- Typical usage: TPM with recovery key
  - TPM releases its if the OS hash verifies
    - This requires an attacker to go through the standard Windows login process
  - If any boot parameters change, the TPM will not release the key
    - Which ones are checked can be set via Group Policy
  - A recovery key can also be used

Using Shattr with Bitlocker

- If you're using Windows 8 with a Microsoft account, make sure your recovery key ISN'T backed up: https://onedrive.live.com/RecoveryKey

- Optionally change your recovery key
  - manage-bde -protectors -get c:
  - manage-bde -protectors -add c: -rp
  - manage-bde -protectors -delete c: -id {…}

Using Shattr with Bitlocker

Shattr. Distributing Trust.

Home Shattr Combine Technical Details

I want to Shattr a Bitlocker key

465278 - 276892 - 023265 - 478555

296417 - 615813 - 495935 - 463045

Total Shards: 5 Minimum Threshold: 3

Compute shards

284064-379203-123596-178508-654853-538374-490568-197638

686466-200981-363374-532730-375025-666591-673521-188597

Using Shattr with Bitlocker

- Shattr your recovery key and give pieces to trusted third parties (preferably all over the world)
- Before crossing the border, remove the TPM protector and/or clear your TPM
  - manage-bde -protectors -delete c: TPM
- TURN OFF YOUR COMPUTER. ALL THE WAY.
  - Run memtest if you're super-paranoid

Using Shattr with Bitlocker

- Once safe, contact enough trusted third parties OVER A SECURE CHANNEL to reconstruct your recovery key
  - Video conference over ZRTP lets you have a high degree of confidence in the secrecy and integrity without access to any private keys (like with OTP)
- Re-enable the TPM protector:
  - manage-bde -protectors -add c: -tpm

Using Shattr with Bitlocker

- Once safe, contact enough trusted third parties OVER A SECURE CHANNEL to reconstruct your recovery key
  - Video conference over ZRTP lets you have a high degree of confidence in the secrecy and integrity without access to any private keys (like with OTP)

- Re-enable the TPM protector:
  - manage-bde -protectors -add c: -tpm

Using Shattr with Bitlocker

- "What if I'm worried about my friends colluding and accessing my drive?"
  - Or being compelled to hand over their shards
- Either encrypt the recovery key before giving it to Shattr OR generate shards for yourself!
  - E.g. if you require two out of three friends:
    - Generate seven shards
    - Set the threshold to six
    - Keep four shards for yourself (and encrypt them)

DEMO

Extra details

- File encryption uses AES-128-GCM, which gives you authenticity as well as confidentiality!
  - (Subject to browser support. As of April, only Chrome Canary supports file encryption.)
- Bitlocker-style keys take groups of 16 bits and multiplies them by 11
  - A simple checksum for Bitlocker
  - We extend this by encoding the shard ID (the x value)
  - First group of four have the first digit, second is 2^{nd}…

Other Applications

- Anything where you want the explicit cooperation of multiple parties
  - Encrypt your "digital will" – the keys to accounts
  - Digital signatures
  - Wikileaks "insurance" file?

Try it yourself!

https://shattr.it/