Some Thoughts on Community, Responsibility, and Standards

Ten (rather obvious) claims

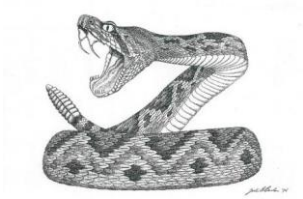
Phillip Rogaway
University of California, Davis, USA

AWACS 2016
(A Workshop about Cryptographic Standards)
Vienna, Austria
8 May 2016


2011

2016

Once bitten, twice shy



Comments
draft-rogaway-ipsec-comments-00.txt

P. Rogaway
UC Davis
April 3, 1995

Problems with Proposed IP Cryptography

From ipsec-request@ans.net Fri Jun 30 07:29:06 1995
To: Phil Rogaway (Phil Rogaway -rogaway@cs.ust.hk-)
Subject: Re: response to Last Call on: IP Authentication using Keyed MD5
Date: Fri, 30 Jun 1995 10:08:58 -0400
From: **Perry E. Metzger** ("Perry E. Metzger" -perry@imsi.com-)
… Phil, do I have to spell it out yet again? … ESP is *not* the "encryption mechanism". The architecture defines it simply as the the way to encapsulate opaque IPSP packets. Thats why the "E" doesn't stand for "encrypton".
> Either DES CBC encryption is architecturally non-compliant (and so the mechanism has to be changed), or else all of the above statements about the encryption buying you integrity need to be changed.
There is a third possibility, which I will leave to people's imaginations. …

From ipsec-request@ans.net Fri Jun 30 15:15:33 1995
To: Ron Rivest (rivest@theory.lcs.mit.edu (Ron Rivest))
Subject: Re: Some comments on IPSEC proposals
From: **Perry E. Metzger** ("Perry E. Metzger" -perry@imsi.com-)
It appears that by failing to be as vicious as possible about Phil Rogaway's lack of understanding of the architecture of IPSP that I have inspired people to take him seriously. It also appears that Phil has been lobbying people to have them comment. I can understand how even an intelligent reader, going through his comments, could become confused about the architectural issues here. However, let me say that I found his comments to be almost completely without merit. Other than a few comments about places where the text used ambiguous language …**I found almost nothing of value in what he had to say.**

From ipsec-request@ans.net Thu Oct 12 20:33:55 1995
Date: Fri, 13 Oct 95 02:53:56 GMT
From: **William Allen Simpson** ("William Allen Simpson" -bsimpson@morningstar.com-)
To: ipsec@ans.net (ipsec@ans.net)
Subject: Re: Photuris generality
>What cryptographers want and expect of a protocol like Photuris is that it works under the assumption that each of its primitives is instantiated to meet the (standard) definition of the goal of that primitive. … You do not facilitate analysis >by saying that Photuris is only required to work when its primitives are drawn from a certain concrete set of possibilities; >exactly the opposite-- you render cryptographic analysis impossible.
It gladdens my heart to hear that self-described cryptographers find that analysis is impossible! I was worried that there would be some subtle flaw that would facilitate cryptanalysis. Now that you have assured us that it is not possible, that makes Photuris the only protocol that has ever come to perfection!

2. Cryptographic standards are <u>important</u>

- Enable interoperability
- Codify best-practice
- Provide cryptanalytic targets
- Discourage roll-your-own crypto
- …

Code is Law

The **character** of that law is tied to the **cryptography** it employs; and that cryptography is set forth in **standards**.

[C]ode, or architecture, sets the terms on which life in cyberspace is experienced. It determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. It affects who sees what, or what is monitored. In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates. …

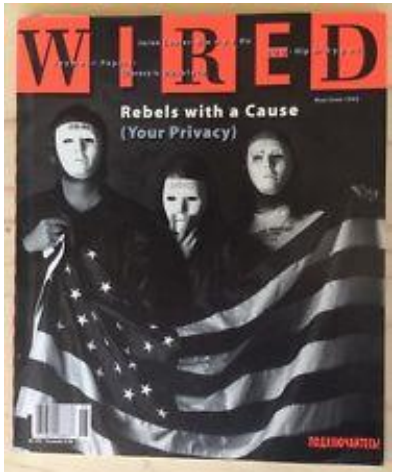
The code of cyberspace is changing. And as this code changes, the character of cyberspace will change as well. Cyberspace will change from a place that protects anonymity, free speech, and individual control, to a place that makes anonymity harder, speech less free, and individual control the province of individual experts only. …

The architecture of cyberspace is not given. **Lawrence Lessig, 1/1/2000**

3. Cryptographic work has a moral character

The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a `chilling effect,' causing people to alter their observable activities.

David Chaum: *Security without Identification: transaction systems to make big brother obsolete. CACM 1985*



Tim May – Eric Hughes – John Gilmore
S. Levy, "Crypto Rebels", *Wired*, 1993

But we discovered something. … A strange property of the physical universe that we live in. The universe believes in encryption. It is easier to encrypt information than it is to decrypt it. We saw we could use this strange property to create the laws of a new world.

***Julian Assange**, 2012*

In words from history, let us speak no more of faith in man, but bind him down from mischief by the chains of cryptography. ***Edward Snowden**, 2013*

4. We need to minimize intelligence agency and law-enforcement influence on standards and practice

But how?

a) Greater vigilance, attention to what is happening with systems and standards. Not just DUAL_EC_DRBG. Consider GSM encryption, for example.

b) Need to minimize undue influence. [BLN: Dual EC: A Standardized Backdoor] emphasizes that not only was NIST subverted, but so was ANSI and ISO

c) People working for or with the NSA—and other intelligence agencies with a SIGINT mission—should not hold leadership roles on standards bodies. As with Kevin Igoe (CFRG)

d) One might establish rules for this ↖, but social norms may work best.

e) Pledges might help
Eg: "The designer/designers have not hidden any weaknesses in this cipher" (DJB's CAESAR language). One can go further: No COIs, using all my knowledge/expertise, …

f) Ignore what “they” say

Background

IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

g) NIST contributions are suspect ☹

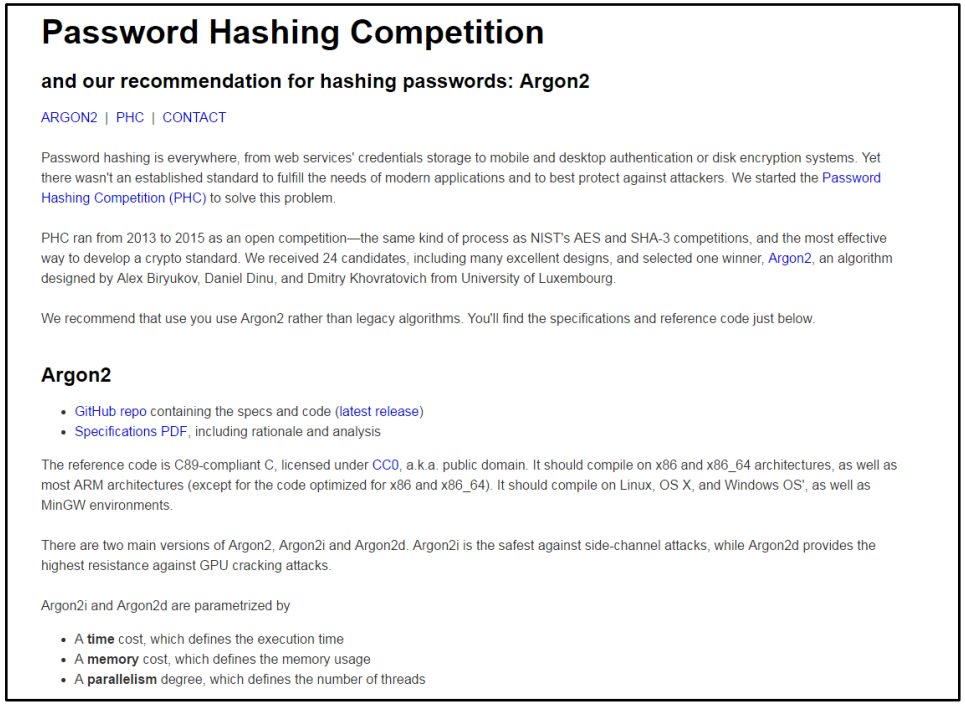
Subverting one cryptographic standard calls into question all cryptographic standards by the same organization

"NIST (and the public) should know whether there are any other current NIST cryptographic standards that would not be acceptable as standards if everyone knew what the NSA knows about them. These standards should be identified and scheduled for early replacement. If NSA refuses to answer such an inquiry, then any standard developed with significant NSA input should be assumed to be "tainted," unless it possesses a verifiable proof of security acceptable to the larger cryptographic community. Such tainted standards should be scheduled for early replacement."

*Individual report from **Ronald Rivest** contained with the **NIST** Cryptographic Standards and Guidelines Development Process: Report and Recommendations of the **Visiting Committee** on Advanced Technology of the National Institute of Standards and Technology. **July 2014***

5. Standards can come too early or too late

It is **too early** for work on post-quantum standards.



Password Hashing Competition

and our recommendation for hashing passwords: Argon2

ARGON2 | PHC | CONTACT

Password hashing is everywhere, from web services' credentials storage to mobile and desktop authentication or disk encryption systems. Yet there wasn't an established standard to fulfill the needs of modern applications and to best protect against attackers. We started the Password Hashing Competition (PHC) to solve this problem.

PHC ran from 2013 to 2015 as an open competition—the same kind of process as NIST's AES and SHA-3 competitions, and the most effective way to develop a crypto standard. We received 24 candidates, including many excellent designs, and selected one winner, Argon2, an algorithm designed by Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich from University of Luxembourg.

We recommend that use you use Argon2 rather than legacy algorithms. You'll find the specifications and reference code just below.

Argon2

- GitHub repo containing the specs and code (latest release)
- Specifications PDF, including rationale and analysis

The reference code is C89-compliant C, licensed under CC0, a.k.a. public domain. It should compile on x86 and x86_64 architectures, as well as most ARM architectures (except for the code optimized for x86 and x86_64). It should compile on Linux, OS X, and Windows OS', as well as MinGW environments.

There are two main versions of Argon2, Argon2i and Argon2d. Argon2i is the safest against side-channel attacks, while Argon2d provides the highest resistance against GPU cracking attacks.

Argon2i and Argon2d are parametrized by

- A **time** cost, which defines the execution time
- A **memory** cost, which defines the memory usage
- A **parallelism** degree, which defines the number of threads

6. Simple is good

- Complexity is friends with (many … but not all) standards
- Complexity is friends with intelligence agencies

7. It's easy to screw up

ISO/IEC 19772, Mechanism 5 (Encrypt-then-MAC)

Information Security – Security Techniques – Authenticated Encryption

The originator shall perform the following sequence of steps to protext a data string D.

a) A Starting Variable S for use with the selected block cipher mode of operation shall be selected. This variable shall be distinct for every message to be protected during the lifetime of the key, and must be made available to the recipient of the message. Further possible requirements for S are described in the appropriate clauses of ISO/IEC 10116.

b) Let $C' = \varepsilon_{K_1}(D)$.

c) Let $T = f_{K_2}(C')$.

The output of the above process, i.e., the authenticated-encrypted version of D, shall be the bit string $C = C' \| T$.

CBC, CFB, OFB, CTR (ISO 9797)

CBC MAC variants (ISO 10116)

– The SV is not included in the MAC
– Nor is the SV required to be random
– Nor are the underlying encryption modes and MACs total

8. Standards want to be free

as in “free beer”

- The sale of crypto standards is inappropriate
- Proprietary crypto standards are inappropriate
- Leak them or
  post them or
  pressure those organizations or
  don’t work for the organization …

9. Challenge the narrative:

~~NOBUS~~

"You look at a vulnerability through a different lens if even with the vulnerability it requires substantial computational power or substantial other attributes and you have to make the judgment who else can do this? If there's a vulnerability here that weakens encryption but you still need four acres of Cray computers in the basement in order to work it you kind of think "NOBUS" and that's a vulnerability we are not ethically or legally compelled to try to patch – it's one that ethically and legally we could try to exploit in order to keep Americans safe from others."

Michael Hayden, 2013

9. Challenge the narrative:

~~Going Dark~~

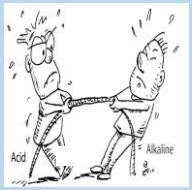
James Comey, FBI Director
Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?
2014

Law-Enforcement Framing

Privacy is a **personal good**

Security is a **collective good**

Inherently in **conflict**



Encryption has destroyed the **balance.** Privacy wins

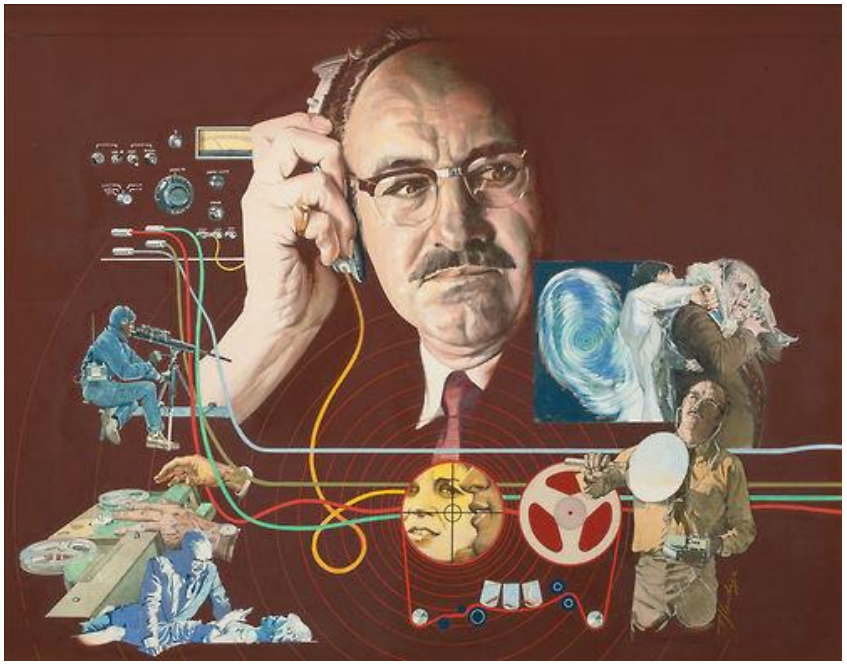
The **bad guys** may win

Risk of **Going Dark**.

9. Challenge the narrative:

~~≠ Robotic Surveillance~~

Collection =



10. It's easy to be misunderstood

Silly

- I ridicule FHE and iO
- and want to strangle them at birth.
- I say that that it's immoral/amoral to work in such areas
- and generally engage in inappropriate theory-bashing.
- It's all because I'm trying to market my own work
- by asserting (how arrogant and uncollegial!) that the work of others is amoral

Paraphrase of
Chatterjee, Koblitz,
Menezes, and Sarkar
(2016)

1. Cryptography is a social process
2. Cryptographic standards are important
3. Cryptographic work has a moral character
4. Minimize intel agency / law-enforcement influence on standards
5. Standards can come too early or too late
6. Simple is good
7. It’s easy to screw up
8. Standards want to be free
9. Challenge the narrative
10. It’s easy to be misunderstood