Security Now! #460 - 06-17-14

Authenticated Encryption

Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

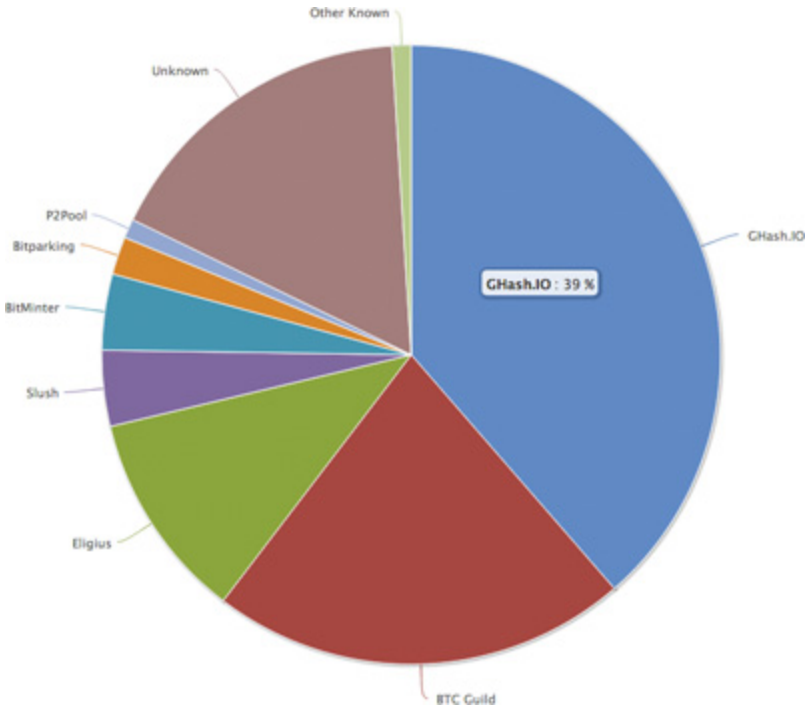
This week on Security Now!

- A dubious and worrisome milestone for Bitcoin,
- An interesting tweet worm,
- The Kung Pow credit card breach,
- Microsoft feels the IPv4 squeeze
- Sci-Fi and other Miscellany
- SQRL client development update

Security News:

Ghash.IO: A single Bitcoin mining pool operation approaches 51% majority:

Concerns first surfaced back in January 2014Ghash.IO:



- What's the problem? The "51% Attack"
- Bitcoin is a "decentralized" virtual currency… but what's "decentralized" is the Proof of Work (PoW) processing power required to evolve the blockchain.
- If a single entity controls more than half of the entire network computing power, it **could** (not that it would, but it could) misbehave and break some of the assumptions inherent in the network's decentralization.

- "Hacking, Distributed" blog, Friday the 13th, 2014: (two Cornell University researchers) http://hackingdistributed.com/2014/06/13/time-for-a-hard-bitcoin-fork/
- A Bitcoin mining pool, called GHash and operated by an anonymous entity called CEX.io, just reached 51% of total network mining power today. Bitcoin is no longer decentralized. GHash can control Bitcoin transactions.

  Is This Really Armageddon? Yes, it is. GHash is in a position to exercise complete control over which transactions appear on the blockchain and which miners reap mining rewards. They could keep 100% of the mining profits to themselves if they so chose.

  Some people might say that this is a sensational claim. It's not. The main pillar of the Bitcoin narrative was decentralized trust. That narrative has now collapsed. If you're going to trust GHash, you might as well store an account balance on a GHash server and do away with the rest of Bitcoin -- we'd all save a lot of energy.

- There's only a couple things someone with 51% of the network hashrate could do:
  - They could prevent transactions of their choosing from gaining any confirmations, thus making them invalid, potentially preventing people from sending Bitcoins between addresses.
  - They could also reverse transactions they send during the time they are in control (allowing double spend transactions).
  - They could potentially prevent other miners from finding any blocks for a short period of time.

- Upon hearing this news, Peter Todd, a very well known Bitcoin evangelist and developer honored a solemn promise he'd made to himself and sold off half of his bitcoins at $650 USD per BTC. This was somewhere in the five-figures, presumably Canadian. (BTC dropped to about $550 but has since rebounded to ~$600.)

- GHash.IO statement: https://t.co/xSMFKFDMJr
  Headline: Bitcoin mining pool GHash.IO is preventing accumulation of 51% of all hashing power

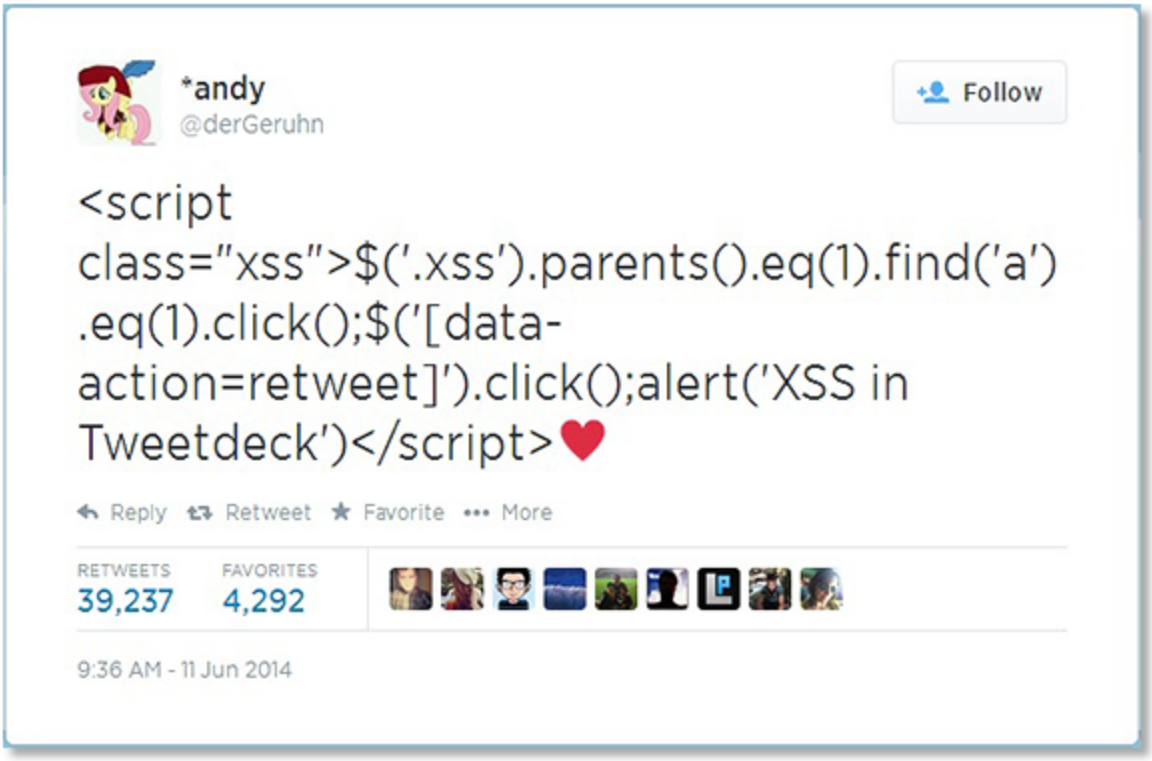
  GHash.IO, the worlds largest and most powerful mining pool, has entered 2014 with overall hashing power of over 40%, making it the #1 pool currently in the Bitcoin network.

  The pool has gained significant hashing power due to the 0% pool fee, merged mining of alt coins, excellent real-time data presentation as well as quality 24/7/365 support service.

The hashing power of GHash.IO consists of:
• ~45% BitFury ASIC based miners
• ~55% independent miners

Although the increase of hash-power in the pool is considered to be a good thing, reaching 51% of all hashing power is serious threat to the bitcoin community. GHash.IO will take all necessary precautions to prevent reaching 51% of all hashing power, in order to maintain stability of the bitcoin network.

A Tweet Worm? A Twitter flaw enables a self-retweeting tweet.



- <script class="xss">
  $('.xss').parents().eq(1).find('a').eq(1).click();
  $('[data-action=retweet]').click();
  alert('XSS in Tweetdeck')
  </script><3
  - Finds and clicks the retweet button,
    Clicks 'yes' to confirm,
    Pops up a polite dialog saying: "XSS in Tweetdeck."

- An Austrian teenager, who goes by the name Firo online, was experimenting with Tweetdeck, trying to get the service to display the unicode ♥ character. In the process, he found that anything in a tweet ending with the heart symbol would be treated by Tweetdeck as though it was HTML code, which could be used to change the formatting of tweets, or put an alert on users' screens. Just 14 minutes after discovering the flaw, Firo told Twitter of its existence, but by then it was too late: the vulnerability was in the wild.

Ninety minutes later, the first worm – the name given to a computer attack which is self-replicating – was created using the flaw, by German IT student @derGeruhn. The tweet uses the same vulnerability to make any user of an affected version of Tweetdeck retweet it automatically. At publication time, it has 81,500 retweets.

- (Later 85k+ retweets.)

- Twitter briefly took TweekDeck services down while assessing the problem. They later wrote: The flaw leads to vulnerable versions of Tweetdeck (3.7.1-19002e5) running javascript code contained in tweets from other sites. Most attacks using the vulnerability are no more than irritations, opening warning dialogues on users' computers - though one version created a retweet of itself, and spread 38,000 times in two minutes, and another changed the font on Tweetdeck itself to Comic Sans.

- https://www.youtube.com/watch?v=zv0kZKC6GAM

Microsoft Windows Azure Blog: "Microsoft Azure's use of non-US IPv4 address space in US regions"

- Quoting from the Blog:
  Some Azure customers may have noticed that for a VM deployed in a US region, when they launch a localized page on a web browser it may redirect them to an international site. The following explains why this may be happening.

  IPv4 address space has been fully assigned in the United States, meaning there is no additional IPv4 address space available. This requires Microsoft to use the IPv4 address space available to us globally for the addressing of new services. The result is that we will have to use IPv4 address space assigned to a non-US region to address services which may be in a US region. It is not possible to transfer registration because the IP space is allocated to the registration authorities by Internet Assigned Numbers Authority.

  At times your service may **appear** to be hosted in a non-US location.

  Service and Data are located where deployed: It is important to note that the IP address registration authority does not equate to IP address physical location (i.e., you can have an IP address registered in Brazil but allocated to a device or service physically located in Virginia). Thus when you deploy to a U.S. region, your service is still hosted in U.S. and your customer data will remain in the U.S.

  We are currently working with a few major IP geo-location database companies to update the location of these IPs which should help alleviate the issues this may be causing.

- ***Related Note:*** PC World, in covering this story, noted that there have been corporate acquisitions driven specifically by one company wanting another's IPv4 allocation.

P.F.Chang's Chinese restaurant confirms massive credit card breach:

- First early reports from Brian Krebs.
  - https://krebsonsecurity.com/2014/06/banks-credit-card-breach-at-p-f-changs/
  - Brian saw thousands of newly-stolen cards appearing for sale on one of the underground stolen-card-selling sites he monitors.
  - Unclear how many branches may have been affected.
  - P.F. Chang's has 204 restaurants. United States, Puerto Rico, Mexico, Canada, Argentina, Chile and the Middle East. Banks contacted for this story reported cards apparently stolen from PFC locations in Florida, Maryland, New Jersey, Pennsylvania, Nevada and North Carolina.
  - The advertisement on Rescator's shop for cards sold under the Ronald Reagan batch does not list the total number of cards that are for sale currently. Instead, it appears to list just the first 100 pages of results, at approximately 50 cards per page. The cards range in price from $18 to $140 per card. Many factors can influence the price of an individual card, such as whether the card is a Visa or American Express card; similarly, Platinum and Business cards tend to fetch far higher prices than Classic and Standard cards.

- Then Rick Federico, CEO of P.F. Chang's:
  - http://pfchangs.com/security/
  - States that they were informed by the U.S. Secret Service.
  - Since they can no longer trust their systems, and do not know where the trouble lies, all restaurants have switches to old-school manual Credit Card Imprinters.

Miscellany:

Cover of TIME Magazine, June 23, 2014: Eat Butter
Health / Nutrition / "Ending the War on Fat"
http://time.com/2863227/ending-the-war-on-fat/

Sci-Fi

- Falling Skies Season #4 begins next weekend.
- Season #3 Marathon all day leading up to it.

Fiction

- No program has ever been better named than: “Halt and Catch Fire”.
- It’s NOT about computer tech. It’s not “for us”. It’s just an awful drama.

SQRL:

- Conversation with Ralf who is doing his masters thesis on SQRL and implementing an Android client.
    - Trouble with the ‘C’ code / liked GCM / worried about the patent question.
- Decided to switch from OCB to GCM…
- Then spent seven days implementing the new mode in portable 'C' and writing a full NIST test vector validation test... 47,250 tests passed perfectly.

SpinRite:

Bruce Behrens
Location: VA Beach
Subject: Testimonial/comment
Date: 20 Mar 2014 20:56:21

Hi Steve,

I wanted to let you know that I finally bought a copy of SpinRite. My wife's old Vista desktop was intermittently crashing and giving her the blue screen of death. I decided SpinRite was worth a try (and I've enjoyed the podcast since 2006!). I ran SpinRite, I think on level 2 first and then on level 4, and it didn't report any problems or miraculous recoveries at all... but, on the other hand, there has been not a single problem since. My wife suspects a "wasted" purchase, which wouldn't bother me in the least, since, as I said, I've enjoyed the podcast since 2006. But I'm not sure. What do you think?
Regards,
Bruce

= Authenticated Encryption =

Why Authenticated Encryption?

- Privacy with a passive versus an active attacker: ONLINE vs Offline.
- Attacker can tweak the ciphertext, observe results… and tweak some more.
    - Error message feedback, time taken to respond, etc.
- Necessary to ABSOLUTELY detect any modification and NEVER act upon any change.
- A traditional Message Authentication Code (MAC) is very similar to a hash, but is keyed by a secret key…
    - Otherwise an attacker could tweak the ciphertext, recompute the simple hash to fix the signature.
    - Therefore… we need one secret for the cipher and another for a keyed hash.
- So…
    - Do we encrypt the plaintext and then apply an authentication code to it?
    - Or apply the authentication code to the plaintext, then encrypt it?
    - Does it matter?
    - What about doing BOTH the encryption and MACing at the same time?

The history of "Focused Cryptographic Competitions":

- http://competitions.cr.yp.to/
- AES -> Rijndael
    - NIST announcement: Jan, 2nd, 1997
    - "Block cipher supporting a block length of 128 bits, key lengths of 128, 192, and 256 bits."
    - Security:
        - Actual security compared to challengers
        - Comparison to random
        - Soundness of its mathematical basis
        - Any other security factors which may arise
    - Cost:
        - Licensing requirements ("AES shall be available on a worldwide, non-exclusive, royalty-free basis.")
        - Computational Efficiency
        - Memory requirements
    - Algorithm & Implementation Characteristics
        - "Flexibility" -- other key sizes, other block sizes, suitability for other applications such as stream cipher, MAC, PRNG, hash, etc.
        - Hardware and software implementation suitability.
        - Simplicity.
- Timeline:
    - Series of deadlines and conferences
    - NIST announces selection: October, 2, 2000

- **Other Crypto Competitions:**
  - eStream: Stream ciphers. Opened in 2004, still underway.
  - SHA-3:
    - Jan 23, 2007 NIST announces SHA-3 competition
    - Deadlines and conferences.
    - Round 1: 51 submissions accepted
    - Many withdrawn, many broken
    - Round 2: 14 remain.
    - Finalists: 5
    - October 2nd, 2012, NIST announces selection of SHA-3: "Keccak"

  - "PHC" -- Password Hashing Competition
    - https://password-hashing.net/
    - "The Password Hashing Competition (PHC) is an effort organized to identify new password hashing schemes in order to improve on the state-of-the-art (PBKDF2, scrypt, etc.), and to encourage the use of strong password protection. Applications include for example authentication to web services, PIN authentication on mobile devices, key derivation for full disk encryption, or private keys encryption."

    - Motivation:
      - The poor state of passwords protection in web services: passwords are too often either stored in clear (these are the services that send you your password by email after hitting "I forgot my password"), or just hashed with a cryptographic hash function (like MD5 or SHA-1), which exposes users' passwords to efficient brute force cracking methods.
      - The low variety of methods available: the only standardized construction is PBKDF2 (PKCS#5, NIST SP 800-132), and there are mainly just two alternatives: bcrypt and scrypt.
      - A number of new ideas discussed within the security and cryptography communities, but which have not yet led to a concrete proposal.

    - Timeline/ provisional (subject to change) for the PHC:
      - 2013 Q1 call for submissions published on the website of the competition
      - 2014 March 31 submission deadline
      - 2014 Q3 selection of finalists ("tweaks" will then be permitted)
      - 2015 Q2 selection of one or more password hashing schemes

    - 24 submissions have been accepted.

  - "CAESAR": Competition for Authenticated Encryption: Security, Applicability, and Robustness.
    - Competition announcement, Jan 15th, 2013.
    - Deadline for 1st round submissions: March 15th, 2014
      - 57 initial entrants -- a handful already withdrawn or modified
    - **Tentative final announcement: December 15th, 2017**

We MUST have AE today: The "Chosen Ciphertext Attack" is REAL.

Traditional two-phase schemes are provably secure, but they can be:

- Complex and thus slow to operate, introducing too much overhead into the process.
    - Today's systems must operate at "line speeds" -- many gigabytes per second.
- Complex and thus expensive to implement on "The Internet of Things" constrained devices.
    - Today's consumer products need to have this too!

To solve these problems we have "AE" modes (Phil Rogaway coined: AEAD) adding "Associated Data.:

- Handle both encryption and authentication at the same time.
- Requires a single key, rather than one key for each phase.
- Many can be run "in parallel" hardware for increased acceleration.

So how do we choose from among the many different AE modes?

- How fast is encryption and decryption?
- How complicated is the implementation?
- Are there free implementations out there?
- Is it widely used?
- Can hardware parallelize it?
- Is it 'on-line', *i.e.,* do I need to know the message length before I start encrypting?
- Is it patented or otherwise license encumbered?
- Does it allow us to include Associated Data (like a cleartext header)?

OCB - Offset Code Book // Simple, blindingly fast… but patented.
GCM - Galois/Counter Mode
EAX - 'e' and 'a' presumably stand for encryption and authentication (2-pass)
CCM - Counter Mode with CBC-MAC (also 2-pass, and not "online" - length must be known.)
...and…
XCBC, IAPM, CWC… and scores more coming from the CAESAR competition.

Details:

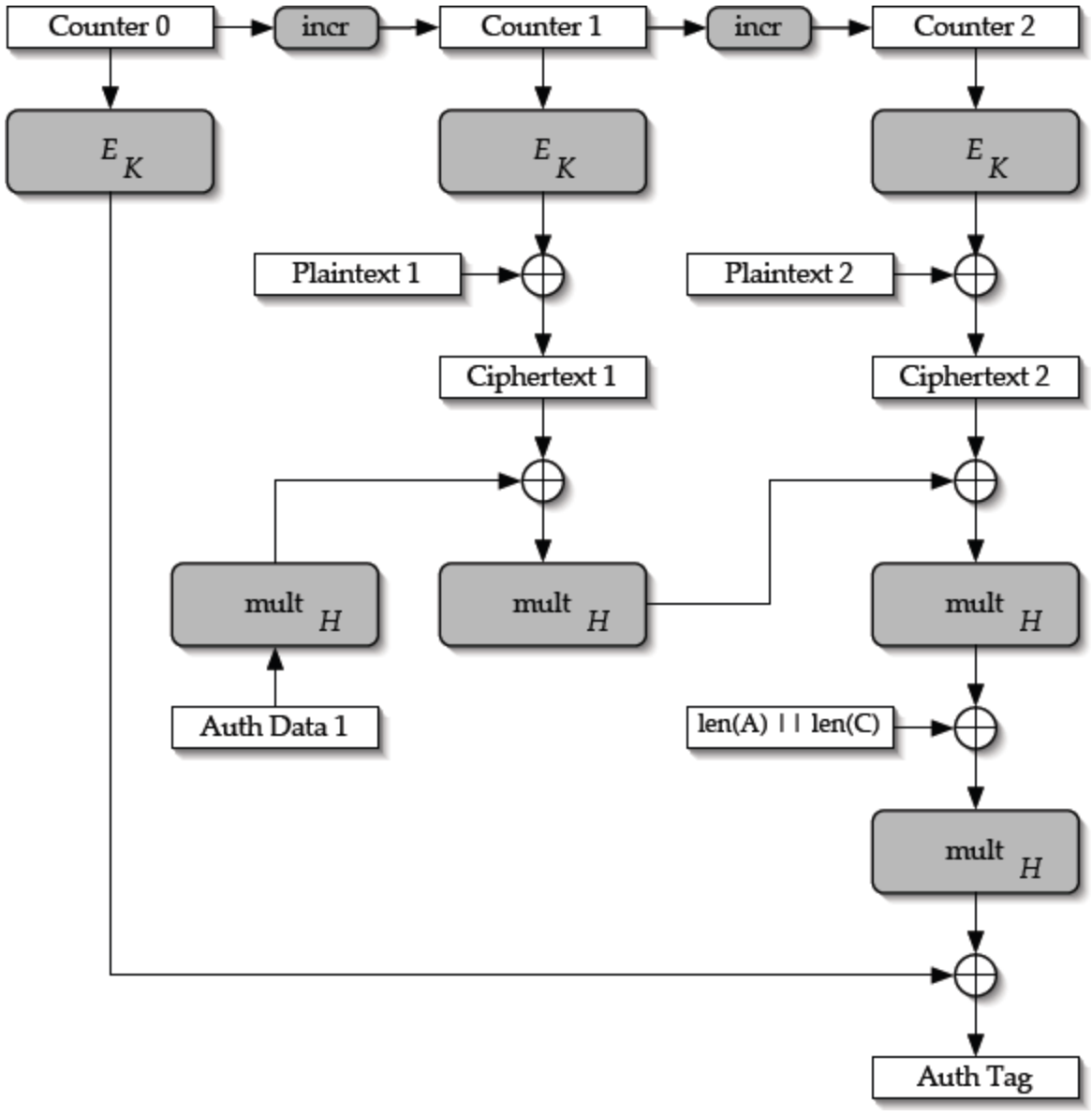
- Single or multiple keys
- "Online" or "Offline" -- Need to know the plaintext length before beginning?
- Ciphertext block-size expansion
- Single-pass
- Flexible Tag-length choice

OCB:

- Killed by its patents.
- GRC received explicit permission from Phil Rogaway to use OCB for CryptoLink and anything we did… but that doesn't mean it's okay for SQRL.
- The rest of the industry kept looking at OCB, but deciding not to implement it… solely due to its unclear intellectual propery.
- OpenSSL did decide to put it in, but required a special explicit licence from Rogaway.

AES-GCM:

- http://en.wikipedia.org/wiki/Galois/Counter_Mode
- Galois/Counter Mode
- "Galois: Finite Field" → GF(2^128)
- Intel 64x64->128 instruction since 2010
- Can be moved into hardware
- Counter-Mode, thus NO padding NOR ciphertext block-size expansion
- Standards:
  - In TLS v1.2 (RFC 5288) - Supported by Firefox, Chrome, OpenSSL
  - IPSec (RFC 4106 & 4543)



Only two major operators: AES Encryption and the GHASH GF(2^{128}) multiplication, plus incrementation and XOR.

GRC's implementation of AES-GCM passes the NIST validation vector test suite of 47,250 individual test vectors.