Crypto year in review
Sept 2014

Bill Ricker for BLU.org

Size matters

Current recommended key sizes.

RSA. 1024 is obsolete. 2048 is barely ok for short term use especially with legacy devices, 3072 is currently acceptable, but for long expiration, 4096 is now recommended.

> Because 4096 doesn't add significantly more strength,

Not exactly right, only approximately true today. These equivalences are date specific and rounded.
At current factoring speed, 3072 and 4096 have respective equivalent symmetric strengths that *round down* to the same power of 2 = 128. (Unlike between 56 and 128 they don't bother with values between 128 and 256, since 256 is the holy grail value. Might be useful but ...they don't. sometimes.)
As Moore's Law grinds on and number theorists continue to tune factoring shortcuts, 3072 bit RSA will drop below 128 equivalent symmetric bit strength much sooner than 4096 will.

So new keys generated today for long-term use should be 4096, but 3072 is effectively as good today so no urgency to upgrade from a 3k key to a 4k key yet.

sources.
http://danielpocock.com/rsa-key-sizes-2048-or-4096-bits
NIST SP 800-131A.

For Signature (only)
DSA: $|p| \geq 2048$ and $|q| \geq 224$;
RSA: $|n| \geq 2048$;
ECC: $|n| \geq 224$

(these are stronger than RSA Lab recommended http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/key-size.htm since time has passed.
Note that RSA2048 is still ok for signing but for secrecy it's legacy-use-only.)

Note on cipher suites.
SHA-1 no longer acceptable for DSA (exc legacy), but *is* acceptable for other uses*.
*[“HMAC, Key Derivation Functions (KDFs), Random Number Generation (RNGs and

RBGs), and hash-only applications (e.g., hashing passwords and using SHA-1 to compute a checksum".]

Note that ECC is only in GNUPG 2.1 Beta but not in 2.0 Prod. :-(
But you can create an ECC key now and start getting sigs on it, even if you can't yet rely on it as your primary key.

[Note. GPG's ECC is *not* affected by the presumed backdoor in Dual_EC_DRBG in FIPS 182-2 TLS. Same underlying EC Maths but, Different curves, Different use.]

Operational PGP: how to email securely

By “The Grugq”

> Parker Higgins @xor 9/1
>
> So you know how to use PGP. Now @thegrugq lays out how to take email security to the next level. https://gist.github.com/grugq/03167bed45e774551155 …

Or, Operational Security / Tradecraft with Email

Outline. (see full doc linked above!)

- **Metadata**
  - Email app/client
  - Subject. Empty, otherwise it leaks.
- **Safer Keys**
  - Don't lose it.
    - Plan to lose it – OOB compromised key alert signal.
  - Re key early and often.
    - Travel key
  - Key server not for high anonymity usage.
    - Deniable key exchange
    - (separate key/IP/client/... for hi anonymity traffic from 'normal')
- **Writing**
  - Security vs convenience tradeoff.
  - Don't save un-encrypted drafts
  - Attachments inside the main PGP
  - For anonymity don't tag message with which key to use, use –throw-keys.
  - “For more control and compatibility, use inline PGP” vs PGP/MIME
- **Sending**
  - Encrypt by default in the encrypting client (commandline wins)
  - Sign messages only explicitly, when needed. Think.
  - Store locally only & delete.
- **Receiving**
  - Delete. Delete. Delete.

Also, Patch early, Patch often. GPG & Enigmail plugins had potentially dangerous bugs recently.

News updates.

- Not news – rerun screensaver
  http://www.explainxkcd.com/wiki/index.php/177:_Alice_and_Bob

- If the NSA weren't tapping the internet to track our enemies, as a taxpayer I'd ask WHY NOT. Civilian control and protection of innocent citizens are a valid questions.
- **PGP or what** ?
  - http://blog.cryptographyengineering.com/2014/08/whats-matter-with-pgp.html Matt Greene.
  - Thomas H. Ptacek @tqbf Aug 13 There is a lot wrong with PGP! Unfortunately: PGP is the only trustworthy mainstream cryptosystem. The. Only. https://news.ycombinator.com/item?id=8174310
    - Thomas H. Ptacek @tqbf Aug 20 You can design an encrypted mail service that is trivial for users to adopt, or one that meaningfully resists courts. You can't do both.
    - Thomas H. Ptacek @tqbf Aug 13 If you're a college professor, sure, replacing PGP sounds like an AWESOME PROJECT. If you care about real-world OPSEC, not-so-sure.
  - http://www.theregister.co.uk/2014/08/14/pgp_viability/
  - https://pthree.org/2014/08/18/whats-the-matter-with-pgp/
  - http://thehackernews.com/2014/08/cryptography-expert-pgp-encryption-is_19.html
  - SN 471.
- SHA-3 / Keccak / FIPS 202 still not final.
  - Draft was 8 months late, May 2014. Public comment through 8/26. https://www.federalregister.gov/articles/2014/05/28/2014-12336/announcing-draft-federal-information-processing-standard-fips-202-sha-3-standard-permutation-based
  - Is tuning for performance … or (in)security? pp 44ff Likely perf but trust ... https://docs.google.com/file/d/0BzRYQSHuuMYOQXdHWkRiZXlURVE/edit
- SHA-1 retirement calendar set, Microsoft and Google put squeeze on CAs.
- **Acoustic & Groud-loop sidechannels**
  - **Acoustic** known-plaintext/ciphertext RSA4096 crack. http://eprint.iacr.org/2013/857
  - Ground loop/potential http://eprint.iacr.org/2014/626
  - Affected PGP e.g.,CVE-2013-4576, & CVE-2014-5270
  - http://www.cs.tau.ac.il/~tromer/handsoff/
  - http://people.canonical.com/~ubuntu-security/cve/2013/CVE-2013-4576.html & http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-5270.html
    - GnuPG 1.x before 1.4.16 generates RSA keys using sequences of introductions with

certain patterns that introduce a side channel, which allows physically proximate attackers to extract RSA keys via a chosen-ciphertext attack and acoustic cryptanalysis during decryption. NOTE: applications are not typically expected to protect themselves from acoustic side-channel attacks, since this is arguably the responsibility of the physical device.
Accordingly, issues of this type would not normally receive a CVE identifier. However, for this issue, the developer has specified a security policy in which GnuPG should offer side-channel resistance, and developer-specified security-policy violations are within the scope of CVE.

- (1.4.15-2ubuntu1 is back-patch of 1.4.16 fix)

- Recent patches affecting GPG
  - * SECURITY UPDATE: side-channel attack on Elgamal encryption subkeys (a different one?)
  - - debian/patches/add_gcry_divide_by_zero.patch: replace deliberate
  - division by zero with new _gcry_divide_by_zero().
  - - debian/patches/CVE-2014-5270.patch: use sliding window method for exponentiation algorithm in mpi/mpi-pow.c.

  - http://people.canonical.com/~ubuntu-security/cve/pkg/gnupg.html < updated
  - **Engmail** Thunderbird/GPG plugin – CVE-2014-5369 "`if a mail only had Bcc recipients, the mail was unexpectedly sent in plain text … fixed in Enigmail versions 1.7.1 and 1.8.0`". There are other plain-transmission problems. http://seclists.org/oss-sec/2014/q3/436
  -
-

- "Details of how the FBI found the administrator of **Silk Road**, a popular black market e-commerce site. It was bad operational security." (Schneier) http://arstechnica.com/security/2013/10/silk-road-mastermind-unmasked-by-rookie-goofs-complaint-alleges/ (somewhat related to Tor)
- Insecurities in the Linux /dev/random. http://eprint.iacr.org/2013/338.pdf
- "Ross Anderson liveblogged Financial Cryptography 2014. Interesting stuff" http://www.lightbluetouchpaper.org/2014/03/03/financial-cryptography-2014/

- **TACK**
  - not really news, 2012 proposal. http://blog.cryptographyengineering.com/2012/05/tack.html http://tack.io https://twitter.com/tqbf/status/504978650970603520 http://arstechnica.com/security/2012/05/ssl-fix-flags-forged-certificates-before-theyre-accepted-by-browsers/
  - Firefox 32 now implements (some sort of) pinning.

- **TrueCrypt** Audit & shutdown.
  - http://istruecryptauditedyet.com/ https://opencryptoaudit.org/reports/
  - shutdown https://www.schneier.com/crypto-gram-1406.html#7 & SN 451 458 459 & ISC https://isc.sans.edu/diary.html?storyid=18177

- Credit Card breaches are largely Point-of-sale malware, some server/DB cracks, not crypto breaches. Malware may be creeping from PCs to POS because networks aren't segregated ?!

- "At Eurocrypt this year, researchers presented a paper that completely breaks the discrete log problem in any field with a small characteristic. It's nice work, and builds on a bunch of advances in this direction over the last several years. Despite headlines to the contrary, this does not have any cryptanalytic application -- unless they can generalize the result, which seems unlikely to me." http://link.springer.com/chapter/... http://www.sciencedaily.com/releases/2014/05/140515163739.htm

- First review of the secure Blackphone. http://arstechnica.com/security/2014/06/... https://www.blackphone.ch/
- "Man-in-the-middle attack against a Brazilian payment system:"
  - http://krebsonsecurity.com/2014/07/brazilian-boleto-bandits-bilk-billions/.
  - "This is the sort of attack that bypasses any two-factor authentication system, since it occurs after all authentication has happened. A defense would be to send a confirmation notice to another device the account-owner owns, confirming the details of the transaction."
- **IoT** - "LIFX is a smart light bulb that can be controlled with your smart phone via your home's Wi-Fi network. Turns out that anyone within range can obtain the Wi-Fi password from the light bulb. It's a problem with the communications protocol."

  http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/
- "Brian Krebs is reporting on the risks of **keyloggers** on public computers in hotels"
  - https://krebsonsecurity.com/2014/07/beware-keyloggers-at-hotel-business-center
  - "It's actually a very hard problem to solve. The adversary can have unrestricted access to the computer, especially hotel business center computers that are often tucked away where no one else is looking. I assume that if someone has physical access to my computer, he can own it. This is doubly true if he has hardware access."
- Hold security 1.2B passwords? Maybe but …
- WhatsApp SSL bad. http://arstechnica.com/security/2014/02/crypto-weaknesses-in-whatsapp-the-kind-of-stuff-the-nsa-would-love/ (FB bought them; no pinning either.)
  -

- **Heartblead** april → vpn products patch in 2 days→ Hospital chain breached quickly
  - "Basically, an attacker can grab 64K of memory from a server. The attack leaves no trace, and can be done multiple times to grab a different random 64K of memory. This means that anything in memory -- SSL private keys, user keys, anything -- is vulnerable. And you have to assume that it is all compromised. All of it." (Schneier)
  - **Heartbleed Explained...**
    - **with Jelly Beans**: *Coding 101* #13 Twit.TV https://www.youtube.com/watch?v=-H0EnaFji9M
    - … as a joke. @dragosr
      "Would you like to hear an OpenSSL joke? It's 64k letters long and you can repeat it back to me when I'm done.

      It's "A".
  - patch http://pastebin.com/5PP8JVqA
    - Patch criricized as stiff … http://tstarling.com/blog/2014/04/ssl-implementations-compared/
  - Assume all affected servers private keys, user list, cleartext or hashed passwords, everything secret, are toast. http://mashable.com/2014/04/09/heartbleed-bug-websites-affected
    - https://www.schneier.com/blog/archives/2014/04/heartbleed.html & https://www.schneier.com/blog/archives/2014/04/more_on_heartbl.html
    - more links https://www.schneier.com/crypto-gram-1404.html#1
  - found to affect clients too
    - https://isc.sans.edu/diary/The+Other+Side+of+Heartbleed+-+Client+Vulnerabilities/17945
    - https://isc.sans.edu/diary/Reverse+Heartbleed+Testing/17957 => https://github.com/Lekensteyn/pacemaker
  - http://arstechnica.com/security/2014/04/**google-chrome-protection-for-heartbleed-hacked-sites-called-completely-broken/**
  - perils of monocultures
  - 6 additional patches in June for other issues. Keep up to date ! https://isc.sans.edu/diary/Updated+OpenSSL+Patch+Presentation/18219 youtube: https://www.youtube.com/watch?v=qeLsgtMOp-M pdf: https://isc.sans.edu/diaryimages/openssljune5th2014.pdf

- "**The Voynich Manuscript** has been partially decoded. This seems not to be a hoax. And the manuscript seems not to be a hoax, either."
  - http://www.medievalists.net/2014/02/20/voynich-manuscript-partially-decoded-text-hoax-scholar-finds/
  - http://www.youtube.com/v/fpZD_3D8_WQ?hl=en_US&version=3 (47 min; Feb.2014 paper)
  - http://stephenbax.net/wp-content/uploads/2014/01/Voynich-a-provisional-partial-decoding-BAX.pdf Feb.2014 paper
  - Informal talk April 10, 2014. http://www.youtube.com/watch?v=Gj3Bgih3LkI (73 min)
  - http://stephenbax.net/ has recent updates: other scholars suggest Syriac or Mandean origin; have found more plant matches, astronomical/astrological matches to diagrams.
  - Www.voynich.nu is the center of community.

- **Big Data & de-anonimization**.
  "New York City officials anonymized license plate data by hashing the individual plate numbers with MD5. (I know, they shouldn't have used MD5, but ignore that for a moment.) Because they didn't attach long random strings to the plate numbers -- i.e., salt -- it was trivially easy to hash all valid license plate numbers and deanonymize all the data."
  - https://medium.com/@vijayp/f6bc289679a1
  - http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/
  - https://news.ycombinator.com/item?id=7926358
  - "Of course, this technique is not news." http://techatftc.wordpress.com/2012/04/22/does-hashing-make-data-anonymous/
  - No, we knew in '80s that encrypthing small strings with a secret key was insecure and would leak privacy fast; hashing with a disclosed algorithm is obviously not better !
  - RELATED http://www.stanfordlawreview.org/online/privacy-and-big-data/three-paradoxes-big-data

Topics.

- Matasana challenges ?

Sources.

http://www.schneier.com/crypto-gram.html

http://twit.tv/sn https://www.grc.com/securitynow.htm https://www.grc.com/sn/

https://isc.sans.edu/ SANS Internet Storm Center – follow Handlers Diaries and/or Daily Podcast.

- 2014-08-12 Adrien de Beaupre Host discovery with nmap (2 Comments) https://isc.sans.edu/diary.html?storyid=18519
- 2014-08-11 Bojan Zdrnja Verifying preferred SSL/TLS ciphers with Nmap (8 Comments) https://isc.sans.edu/diary.html?storyid=18513
- 2014-06-02 Rick Wanner Using nmap to scan for DDOS reflectors https://isc.sans.edu/diary.html?storyid=18193
-