Crypto Update for BLU annual keysigning – Bill n1vux

NEWS

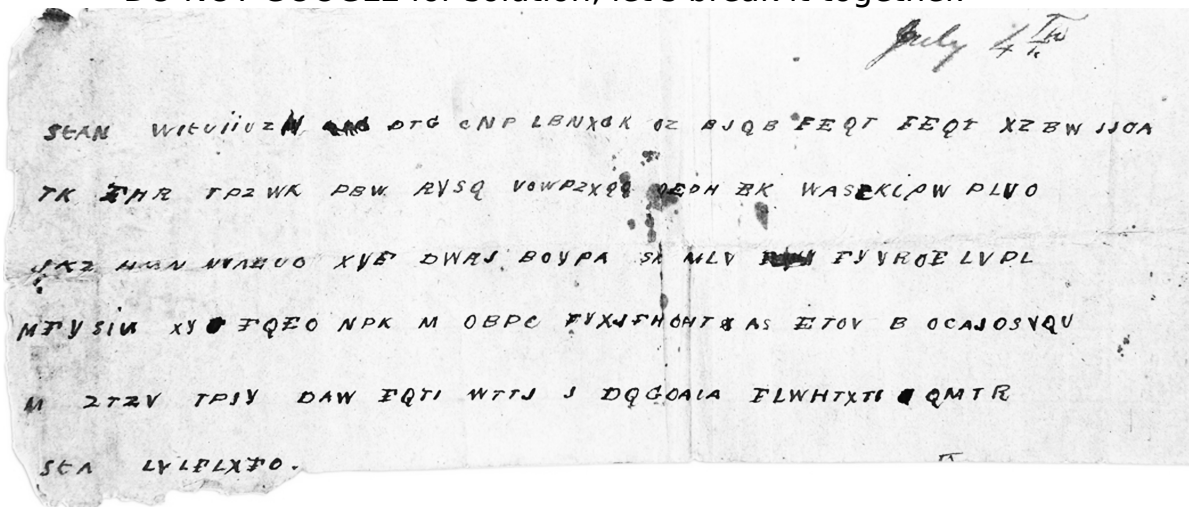
- RSA token break https://www.schneier.com/blog/archives/2011/08/details_of_the.html
- Mac OSX Lion Security Flaw Permits Non-Root PWD Hash Views http://www.infosecurity.us/blog/2011/9/20/lion-security-flaw-permits-non-root-pwd-hash-views.html & http://feedproxy.google.com/~r/ChetBlog/~3/yhsFzOo7PNE/
- **Comodo/Diginotar** CA breaks & MITM
  - http://www.schneier.com/blog/archives/2011/09/domain-in-the-m.html as way to use comodo/digitnotar universal certs without subverting /owning an ISP (http://isc.sans.edu/diary.html?storyid=11608&rss etc)
  - & http://isc.sans.edu/diary.html?storyid=11590 & http://www.us-cert.gov/current/index.html#fraudulent_diginotar_ssl_certificate
- **BEAST - SSL/TLS exploit - paypal trojan horse** sortof MITM
  - http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/
  - & http://news.ycombinator.com/item?id=3015498 & http://isc.sans.edu/diary.html?storyid=11611
  - http://blog.eset.com/2011/09/20/ssl-threatened-by-a-beast-of-prey
  - http://feedproxy.google.com/~r/HurricaneLabsEngineeringNotes/~3/ECD4KeKF6gs/
  - http://isc.sans.edu/diary.html?storyid=11611
  - "Users: Don't bank using someone else's wifi."
  - Friday updatets - http://www.schneier.com/blog/archives/2011/09/man-in-the-midd_4.html ; Chrome and the BEAST http://www.imperialviolet.org/2011/09/23/chromeandbeast.html ; https://blog.torproject.org/blog/tor-and-beast-ssl-attack ; Saturday https://isc.sans.edu/diary.html?storyid=11635&rss
-

Historical & theoretical topics

- Breaks in systems
  - most breaks are procedural errors -- human operator or protocol design or implementation, not core crypto math flaw. (exceptions for Moore's law and math breakthrough.)
    - Why RSA encryption padding is critical
      http://rdist.root.org/2009/10/06/why-rsa-encryption-padding-is-critical/
      - Ref'd at http://www.blu.org/pipermail/discuss/2009-October/033898.html
    - RSA token break was network break-in, looting of secret keys
    - OTP misuse
    - Enigma misuse
    - SIGABA misuse was aggressively prevented
  - recent theoretical but impractical attacks
    - importance: attacks never get worse
    - P=NP ?
  - smarts beats exhaustive search
    - which modern law do those classic ciphers violate
    - branch and prune search (SIGABA)
    - divide & conquer. Bayesian and automation at BP (Enigma & Fish).
    - Hill climbing for classical ciphers
    - space vs time, precompute dictionaries/rainbow tables
- Manual ciphers
  - Solitaire
  - Off the Grid (Security Now podcast c/o Twit.tv http://twit.tv/sn) A work in progress, not quite ready https://www.grc.com/OffTheGrid.htm http://www.google.com/search?s?pq=off-the-grid+grc . (His “how big is your haystack” password strength meter https://www.grc.com/haystack.htm disagrees with XKCD https://m.xkcd.com/936/ , and on grounds that safety is conservative, I side with Randall not Steve, so am holding my endorsement of OtG for now.)
  - OTP : Unbreakable except.
    - Bellovin/Miller – yet another and earlier discovery of the one-time-pad
      - *Frank Miller*: Inventor of the One-Time Pad *https://mice.cs.columbia.edu/getTechreport.php?techreportID=1460* . Steven M. *Bellovin*. Department of Computer Science. Columbia University
      - *http://www.cs.columbia.edu/~smb/papers/crypto_abstracts.html*
      - *For a memoire of a later discovery by first principles in WW2, see http://isbn.nu/work/between_silk_and_cyanide*
    - Venona & GEE
      - perfect cipher cracked by imperfect use

    - https://secure.wikimedia.org/wikipedia/en/wiki/Venona
    - http://findarticles.com/p/articles/mi_qa3926/is_200010/ai_n8903631/pg_4/ “American solution of a German one-time-pad cryptographic system (G-OTP), The from ... 240 printing wheels were set in a single bed with one digit on each wheel ... 1A copy of the redacted NSA technical report entitled "The Gee System."
- treasure cipher shown to be a hoax: THE *BEALE CIPHER*: A DISSENTING OPINION *members.fortunecity.com/jpeschel/gillog3.htm*
  This paper reports a statistical anomaly in B1 which suggests that it my be a *hoax*.

- **Civil War message recovered**
  - BRIEFING - Confederate officer was taking message in a bottle by boat into besieged city of VICKSBURG, on the MISSISSIPPI RIVER. Vicksburg is surrounded by UNION troops under GEN GRANT (USA), defended by recently promoted LT GEN PEMBERTON (CSA), who reports to MAJ GEN JOHNSTON (CSA).
  - Another message was captured and read contemporaneously, this one was neither captured nor delivered. Had it been delivered or captured, would if have prevented the surrender?
    DO NOT GOOGLE for solution, let's break it together.



    - More context can be had at ... https://secure.wikimedia.org/wikipedia/en/wiki/John_C._Pemberton#Vicksburg
    - Hill climbing program could crack this automagically
-

PGP How To

Keysigning

- [**Best**] **Joe Abley - *PGP Key Signing*** *www.nanog.org/meetings/nanog34/presentations/abley.**pgp**.pdf* Trust Reflection. A distributed approach to *PGP key signing* at multi-day events. Joe Abley, ISC. NANOG 34. Seattle, WA, USA …
- [short] PGP keysigning *www.terena.org/activities/tf-csirt/pre-meeting3/cormack-**keysigning**.pdf*
- PGP Keysigning *dougbarton.us/**PGP**/**PGP**-**Keysigning**.pdf* Doug Barton dougb@dougbarton.us. *PGP Keysigning*. ∎ Suggested verification procedure. • Once the control of the private key is verified … *a bit overdone !*

Other How To

- ***PGP* Command Line Guide** *ftp://ftp.**pgp**i.org/pub/**pgp**/6.5/docs/english/**PGP**CmdLineGuide.pdf*
- **The *PGP* Trust Model** netresearch.ics.uci.edu/Previous_research.../abdul-rahman-***pgp***-*trust.pdf* by A Abdul-Rahman - 1996 -One of the major problems of *PGP* has to do with *key* distribution and management**...** which everybody trusts, but instead, individuals *sign* each other's *keys* and …
- **Howto use *PGP*** *www.sindominio.net/metabolik/alephandria/txt/Boer_**pgp**-howto.pdf* By following this document, a reader should be able to set up his or her own *PGP key* **...**
- **Exchanging Files with *PGP*** http://www.nsa.gov/ia/_files/factsheets/I73-FS-035-09.pdf *PGP* by the *PGP* Corporation offers public *key* file encryption
- **Using *PGP* to Verify Digital Signatures** *www.cert.org/archive/pdf/**PGP**sigs_paper2.pdf* *PGP keys*. *PGP* is based on *keys*, a public *key* and a private *key*. For example, the CERT/CC has a private *key* for *signing* documents. We protect our private *key* **...**
- ***PGP* – How to do it.** users.ox.ac.uk/~aesb/***pgp***.*ppt* Sending plain text E-mail is little more secure than sending a postcard – PGP **...**involve just this;
- **An Introduction to How *PGP* Works** < *www.metrowestchess.org/.../**PGP**/.../**PGP**_An_Introduction_to_How_**PGP***>
- PGP <*www.cs.huji.ac.il/~sans/students_lectures/**PGP**.ppt*> *Web* Of *Trust*. Pretty Good Privacy. First released in 1991, developed by Phil Zimmerman, provoked export control and patent infringement controversy. *PGP***..** [PPT technical, academic student presentation] **.**
- ***PGP Web* of *Trust*** *www.cc.gatech.edu/classes/AY2001/cs8803g_spring/crypto20.ppt* *PGP Web* of *Trust*. Validity of *pgp* keys may be verified by its fingerprint; *Pgp*uses: Meta introducer. Root CA's; Not only validity of keys but also the **...**
- **Mutt-i, GnuPG and *PGP* Howto** *tldp.org/HOWTO/pdf/Mutt-GnuPG-**PGP**-HOWTO.pdf*

For further study

- **Military Cryptanalysis- NSA/CSS** PART I – IV . 1938 Declassified 2005. **http://www.nsa.gov/public_info/declass/military_cryptanalysis.shtml**
- **Intro to *Cryptanalysis*** www.cs.sjsu.edu/~stamp/crypto/PowerPoint_Windows/0_Intro.ppt C very introductory
- **Breaking Stuff: *Cryptanalysis* and Protocol Failures** http://www.winlab.rutgers.edu/~trappe/Courses/AdvSec05/Breaking_Analysis.ppt **2005 Real** examples of DES busted by Moore's Law; RSA with small exponents attack that doesn't scale (unless P=NP or fast factoring breakthrough)
- **Recovering a private key with only a fraction of the bits** http://rdist.root.org/2011/09/20/recovering-a-private-key-with-only-a-fraction-of-the-bits/