Crypto News 2018

Bill Ricker
for BLU.org annual keysigning
Sept 19, 2018
0. Agenda

1. Crypto News Review
2. Annual Historical Vignette
3. How To Reminder for GPG/PGP Key-signing
4. GPG/PGP Key-signing
1. Crypto in the news since last year

- Crypto means Cryptography.
  - See previous rant about “crypto coins”
    http://blu.org/cgi-bin/calendar/2018-may
  - Crypto isn’t magic sauce. If you haven’t studied the flaws in prior cryptography, you shouldn’t be inventing new crypto.
    (And if you have, how about you give this talk next year?)
  - Tony Arcieri @bascule commend
    Eventually the cryptocurrency space will come to understand Kerckhoff’s Principle
    retweeting @Haaroony
    Cryptokitties Ethereum contract genetic algorithm cracked by Erays
News – WPA2 Krack

• "Key Reinstallation Attacks"
• 10 CVE’s - one per protocol problem, not per vendor. *uh oh.*
  – **generic protocol flaw**
  – found TEN instances of different WPA1/WPA2 protocols.
  – A reply attack on a specific step.
  – That should have been checked to prevent replay but ... the implementors have frequently failed to test for reply there.
  – Possibly because using standards proof of concept code unthinkingly ...

• Links
  – *
  – * https://www.krackattacks.com/
    • "KRACK works by targeting the four-way handshake that’s executed when a client joins a WPA2-protected Wi-Fi network. Among other things, the handshake helps to confirm that both the client and access points have the correct credentials. KRACK tricks the vulnerable client into reinstalling an already-in-use key. The reinstallation forces the client to reset packet numbers containing a cryptographic nonce and other parameters to their initial values. KRACK forces the nonce reuse in a way that allows the encryption to be bypassed."
  – * "Android 6 & Linux particularly vulnerable"; macOS & OpenBSD easier than in paper w/new bits.

• * Side note: what can be compromised before VPN connect by built-in clients https://arstechnica.com/information-technology/2015/06/even-with-a-vpn-open-wi-fi-exposes-users/*
News: Prepare for (post)Quantum Crypto

- 2001: factored the composite integer 15 with 7 qubits (NMR)
- 2011: same algo factored 21. (on optics)
- 2011: factored 143 using 4 qubits (big enough for ONE factor; NMR) [arXiv-quant-ph-1111.3726-quantum-factoring.pdf]
- 2011: D-Wave selling 128 qubit openly
- 2013: NASA/Google got two 512-qubit machines
- 2017: Google has announced a separate 72-qubit design "Bristlecone;"
- 2018: D-Wave claims to be selling a 2kqubit computer D:Wave 200Q for "only" $15M.
- 2019: plans for 4kqb ...

uh oh

good news is NIST has been planning ahead ... RFC 2016 ...

MS released https://github.com/Microsoft/PQCrypto-VPN which is OpenVPN-on-SSL with Frodo/SIKE/Picnic based on post quantum safe maths.
News: Quantum Key Distribution

- Works somewhat but not nearly as concerning as Quantum computing
- GCHQ on Quantum Key Distribution (via Schneier )
- 2018.08.01 The UK’s GCHQ delivers a brutally blunt assessment of quantum key distribution:
  - QKD protocols address only the problem of agreeing keys for encrypting data. Ubiquitous on-demand modern services (such as verifying identities and data integrity, establishing network sessions, providing access control, and automatic software updates) rely more on authentication and integrity mechanisms -- such as digital signatures -- than on encryption.
  - QKD technology cannot replace the flexible authentication mechanisms provided by contemporary public key signatures. QKD also seems unsuitable for some of the grand future challenges such as securing the Internet of Things (IoT), big data, social media, or cloud applications.
  - Bruce: "I agree with them. It's a clever idea, but basically useless in practice. I don't even think it's anything more than a niche solution in a world where quantum computers have broken our traditional public-key algorithms. Read the whole thing. It's short."
- https://www.ncsc.gov.uk/whitepaper/quantum-key-distribution
News: More Vulns / attacks

- Sidechannel
  - Changes for libgcrypt20:i386 version: 1.6.5-2ubuntu0.5
  - SECURITY UPDATE: memory-cache side-channel attack on ECDSA signatures
  - CVE-2018-0495
  - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0495

- SPECTRE Variants continue to appear
  - e.g. Add Spectre Variant 2 protection for family 17h AMD processors (CVE-2017-5715)
  - Backport to xenial. THIS IS A FIRMWARE CHANGE !!!

- Huge Dirty Cow CVE-2017-100405
  - The Dirty COW patch was itself broken for THP (transparent huge pages)
  - http://www.theregister.co.uk/2017/12/04/dirty_cow_sequel_huge_dirty_cow_patched/

- BT privancy commonly vulnerable to intentionally weak device
  - https://www.kb.cert.org/vuls/id/304725
  - Vulnerability Note VU#304725
  - Bluetooth implementations may not sufficiently validate elliptic curve parameters during Diffie-Hellman key exchange
  - CWE-325: Missing Required Cryptographic Step http://cwe.mitre.org/data/definitions/325.html
  - CVE-2018-5383
  - variant of the “Invalid Curve Attack”
  - @XorNinja 11:58 AM - 24 Jul 2018
  - https://twitter.com/XorNinja/status/1021786823524110336
  - Why only checked x? Maybe the designers thought that because the y-coordinate of the shared point is discarded, it’s fine not to check the y-coordinate of the public keys. A subtle misunderstanding leads to total collapse of an otherwise secure protocol
  - Matthew Green @matthew_d_green 24 Jul 2018
  - https://twitter.com/matthew_d_green/status/1021805830886015603

- Contributory behavior is such a common requirement in Diffie-Hellman based protocols that I rarely see real-world protocols that don’t break due to bad point/pubkey validation.
- Roughly speaking, there’s “classical Diffie-Hellman”, which assumes that the contributors’ key share contributions are authenticated somehow. In these protocols, you can usually trust the key shares, because if you don’t — it means one of the endpoints is evil.
- But then there’s a whole class of protocol that does retrospective authentication. That is, they don’t authenticate the key shares — but use the output of the DH exchange to authenticate things after the fact.
- So for example, Bluetooth pairing codes or ZRTP shared authentication words, or TLS finished messages when used for channel binding (including the triple handshake attack). All require contributory behavior.
- In these protocols, if an attacker can inject a bogus keys/are that results in a known shared DH secret, then they can often break the crap out of the protocol. And it keeps happening.
2. Crypto History
One time Pad (OTP),
BRIDE/BOURBON/VENONA,
Russian Spies,
Vint Hill Station
Signage
In June 1942 the U.S. Army established a top-secret post at Vint Hill Farms to intercept enemy radio transmissions. These barns housed the monitoring station. The Signal Corps' cryptographic school, which taught personnel to encode, decode, and translate messages, was moved here. Pvt. Leonard A. Mudloff is credited with intercepting a message here from Oshima Hiroshi, the Japanese ambassador to Germany, on 10 Nov. 1943. It described German coastal fortifications in western France, troop strengths, and contingency plans. The "Oshima Intercept" was a crucial contribution to the planning for D-Day, the Allied invasion of Europe. The post operated through the Cold War, closing in 1997.
Vint Hill Farms Station
The Listening Post

In 1942, Vint Hill Farms was purchased by the Department of the Army for $127,500, as a quiet and secure place for the Signal Intelligence Service. By July of that year, Vint Hill Farms Station began operations and officially took over the role, directives and name of “Monitoring Station No.1” as the first soldiers of the 2nd Signal Service Battalion arrived.

The Barns in 1940
The original large barn, former home to Shorthorn cattle, was selected to be the home of signal intelligence operations. Vint Hill Farms Station was engaged in communications intelligence and served as a cryptologic installation providing support to the National Security Agency and to the Army.

Japanese-American Soldiers
Diverse companies of translators were stationed at Vint Hill during the war. It was a Vint Hill Morse Code operator who intercepted a coded transmission between Tokyo and Berlin indicating the location of fortifications along the French coast, contributing to the success of the Normandy invasion.

This map illustrates the Army’s original plans for development of Vint Hill Farms Station.
In 1942, Vint Hill Farms was purchased by the Department of the Army for $127,500, as a quiet and secure place for the Signal Intelligence Service. By July of that year, Vint Hill Farms Station began operations and officially took over the role, directives and name of “Monitoring Station No.1” as the first soldiers of the 2nd Signal Service Battalion arrived.
The Barns in 1940

The original large barn, former home to Shorthorn cattle, was selected to be the home of signal intelligence operations. Vint Hill Farms Station was engaged in communications intelligence and served as a cryptologic installation providing support to the National Security Agency and to the Army.

Women Working for Victory

The formation of the Women’s Army Corps (WAC) offered a golden opportunity to solve the manpower shortage created by male operators being sent overseas. The art of Morse interpretation, or “bitty bop,” required intelligence and patience, not muscles.

In 1943, WAC’s reported to Vint Hill Farms Station to attend classes. The women’s presence produced a noticeable change in the enlisted men. They no longer had to be reminded to shave, and the sale of after-shave quadrupled at the PX. Men and women worked side-by-side on shifts, called “tracks,” which were eight hours long and were rotated to provide round-the-clock coverage.
Arlington Hall Station in the 1940s
One Time Pad

Multiple discovers, multiple uses
  Vernam Mauborgne, 1917-1919, teletype tape first!
Post ww1 (into WW2)
  super-encipherment pads
  German Foreign Office & USSR dip, GRU/KGB
WW2
  Marks/ SOE & GCCS/BP pads
  SIGSALY voice, Sturgeon tape
Coldwar
  Shannon proof
  SIGTOT & Hotline
  pads in Cuban stores on Grenada
  Pocket OTP – Unix, Brit Forces
http://en.wikipedia.org/wiki/One-time_pad
Unbeakable?

Theory vs Practice
   Implementation flaws
Public Key
   Moore's lap, time = factors
Software bugs
Session key protected, but is session cipher safe?
Block Ciphers
   computationally, practically
Software Bugs
Sophisticated structural & statistical attacks

OTP
Russians and Germans dupped One Time Pads in WWII (VENONA, GEE)
German GEE OTP
   mechanically non-random
Machine key-stretching
   computationally, practically
Indicator group / Nonce key
Complications can be simplifications
On-air training with simplified procedures
Slowly tightening practice

RERUN 2009
Cribbing works with any key system ... if trial key can be extended which can signal if crib was matched for real.
OTP Applications

- **Clear Text**
  Single encipherment of text (letter pad)
  - SOE replacement for poems, “Between Silk & Cyanide”

- **Cipher Text**
  Super-encipherment of cipher
  - Straddling Checkerboard (number pad)
  - Transposition, Playfair, etc (letter pad)

- **Code Groups**
  super-encipherment of code groups (Encicide)
  - Number pad common, letter less so
Soviet OTP Usage

- Illegals – OTP, miniature, with Straddling Checkerboard
- Diplomatic cables – Codebook & OTP
  - GRU (Sov. Army MI)
  - NAVAL GRU
  - Trade (ZET)
    - Low intrinsic interest but stereotyped, voluminous, and weakened further
  - Diplomatic (ZDJ)
  - NKVD/KGB Station Chief under legal cover
  - All 4-number, single-part codes, with spell ciphers and garbleproof numberals
• Vint Hill stayed open after WW2 to monitor Soviet radio teletype and morse code

• But most of the messages we’re discussing were sent by Cable as Diplomatic traffic and copied by ASA at WU DC&NYC cable offices

• SIS/SSA/ASA Arlington Hall in sorting messages discovered some OTP messages reused OTP pages!
Soviet Practice

• Russian Copulation – stereotypes harder
  – Split message randomly and swap halves, with separator

• Encipher indicator in message
  – As with Enigma, this was added later, after break, oops
Unbreakable in theory but ...

• OTP must be ONE TIME
  – If not … find the dups!
  – 1942 cheat.
    • Carbon paper?
  – Voluminous ZET cheat
    • RED REVERSE
• codebook’s spell cipher
• Single-part code weaker than 2-part
How Found?

- Keypunch leading $16 \times 5 = 80$ figures on cards
- Search for coincidences or common differences
- Looking for common prefixes of message (or simple short additive tables)
  - Found common additive OTP pages instead!
- Noticed long Trade messages reused sheets immediately, Top to Bottom then Bottom to Top
Book Breaking

- First find codes for parts of message; Numerals; Letters for spelling.
- In One Part Code, the code values are in numeric order as the words/phrases are in alphabetic order: HINT!
Who

- “Gene” Gabreel - 1st analyst on BRIDE/VENONA
- LT R Hallock - “Depth” and pattern in Trade code
- Frank Lewis expands break for first partial decryption in 1943
- Genevieve Feinstein – pad indicator finds depth
- Cecil Phillips - patterns in KGB encidode
- Lucille Campbell – KGB
- Meredith Gardner – book breaker
- Robert Lamphere - FBI CI
More Hidden Figures?

In the spring of 2018, Angeline Nanni revisited Arlington Hall, where the Venona team got cracking. It is now on the National Register of Historic Places. (Maggie Steber / VII Photo)

From Smithsonian article ...
Meredith Gardner (left)
... true context
Featured in NSA Venona history ...

Mildred Hayes
VENONA linguist/analyst for more than twenty-five years. She closed the VENONA effort on 1 October 1980.

Joan Malone Callahan, the first U.S. VENONA analyst/linguist to serve at GCHQ 1949 to 1954. She became project supervisor and principal customer interface in 1954 when Meredith Gardner replaced her in the United Kingdom.

Gloria Forbes (left) She began processing Soviet diplomatic messages in mid-1943 and continued to supervise this and related activities for

Arlington Hall bowling team of cryptanalysts ca. 1947. Standing (left to right): Ottil Phillips, Bill Ludwick, Paul Denthick. Below (left to right) Frank Lewis, Louise Denthick. (All except Louise worked at some time on VENONA-related...
Gene Grabeel, 1st Analyst

Gene Grabeel (right) 
She began work on 
Soviet diplomatic 
messages on I 
February 1943 and 
continued working the 
problem until the late 
1970s.
Computer History (1)

SIS “Slide Run”
- IBM 405 Tabulator +
- Relay circuits
- Counters
- Plugboards (PROM)
- Telephone crossbar relays
- Statistical tests
- Conditional print
Computer History (2)

• Many other special purpose devices
• General purpose electronic computers late 40s early 50s
  – ERA ATLAS, a von Neumann machine, 16k words = 64kB (huge for the day!)
    • Interlacing on drum!
  – ABNER – general purpose plus special instruction sets
    • arbitrary-base carryless-add
    • crib-dragging
    • block transfer and block loop operation;
    • stream operations.
Public Release


1. Soviet atomic bomb espionage
2. New York KGB messages of 1942 and 1943
3. New York and Washington KGB messages of 1944 and 1945
4. San Francisco and Mexico City KGB messages; GRU New York and Washington messages; Washington Naval GRU messages
5. KGB and GRU messages from Europe, South America, and Australia
6. Messages inadvertently left out of the previous five updates of previously issued translations. Updates some translations by restoring names that had been protected for privacy reasons in the original releases.

Also, UK GCHQ released COMINTERN messages 1934-37 (MASK) and 1943-43 (ISCOT).
3. GPG/PGP Key Signing

• A quick HOW TO

PKI / PGP Primer:
- Public Key
- Private Key
- Message

encrypted + key = locked
encrypted + key = decrypted
message + key = signed
message + key = authenticated
4. Key Signing

Key#3 on the list is RSA **2048** with expiration date in **2030**.
This key is not considered safe. We do **NOT** recommend signing it.

<table>
<thead>
<tr>
<th>Seq</th>
<th>Key ID</th>
<th>Owner</th>
<th>Fingerprint</th>
<th>Size</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5640D33F</td>
<td>John Abreau (Personal email)</td>
<td>87B1 6063 9962 0824 0406 8893 B184 3049 5640 D33F</td>
<td>4096</td>
<td>RSA</td>
</tr>
<tr>
<td>2</td>
<td>C9039A2B</td>
<td>Braullo Carreno (Sep 2018)</td>
<td>1357 E187 E888 412B 99E0 ABA2 AE18 9974 C903 9A2B</td>
<td>4096</td>
<td>RSA</td>
</tr>
<tr>
<td>3</td>
<td>7493DAEC</td>
<td>James R. Doyle</td>
<td>F0B5 2E03 C626 DF05 BA2D 7491 FB35 AF40 7493 DAEC</td>
<td>2048</td>
<td>RSA</td>
</tr>
<tr>
<td>4</td>
<td>4340F598</td>
<td>Andrew Holden</td>
<td>F218 F449 0895 29A5 7A46 F094 3114 7708 4340 F598</td>
<td>4096</td>
<td>RSA</td>
</tr>
<tr>
<td>5</td>
<td>87145445</td>
<td>Elliott Mitchell</td>
<td>8A19 5802 7E3D DDF4 7BA6 41D1 B375 37D9 8714 5445</td>
<td>3072</td>
<td>DSA</td>
</tr>
<tr>
<td>6</td>
<td>6FA9E1F9</td>
<td>George Mitchell</td>
<td>35D3 3864 792D B095 B990 A657 C111 12DE 6FA9 E1F9</td>
<td>4096</td>
<td>RSA</td>
</tr>
<tr>
<td>7</td>
<td>41936952</td>
<td>William Ricker (Boston)</td>
<td>090F 3675 F519 C3D3 A508 E763 9CD4 CB6D 4193 6952</td>
<td>4096</td>
<td>RSA</td>
</tr>
<tr>
<td>8</td>
<td>6E0D8E7D</td>
<td>Goh Wei Zhong (non-primary email address)</td>
<td>090F FC0C CIFD 31EC 2C54 B6B1 DCC1 B708 6E0D 8E7D</td>
<td>4096</td>
<td>RSA</td>
</tr>
</tbody>
</table>

Instruction email said,

* We will **NO LONGER** sign RSA or DSA 1024b keys (or shorter). Obsolete.
* We will **NOT** sign RSA 2048b keys without expiration dates or with expiration dates beyond 2020.
* Use RSA 4096 or ed25519 for gpg2 –gen-key

(Alas the keyserver or signup utility doesn't have new enough GPG2 to do ed25519 yet. I tried.)