

Everyday Cryptography



John Kristoff
jtk@cymru.com



Revealed at FIRST 2014!

- Novel new amplification and reflection threat
- ...and network information disclosure vulnerability

D'OH! Not accepted! :-(
See you at NANOG 62



Agenda

- The crypto we have
- Bootstrap issues
- Email and PGP
- WWW (HTTPS), SSL/TLS, X.509 and DANE
- Routing
- The crypto we don't have



Challenge, Instructor to Student

-----BEGIN PGP MESSAGE-----

Comment: How many RFC 1918 addresses are there?

jA0EAWMC2vuGtFvCpx9gyevRifsVMzSE33SNeX0ZyjCiyNnGgpW0cQJ4d2FtcIpF
ULgl++5RD30OULb8RbmEYP25iT2LuY8kNcD8bV3k+fU/X47KE+EvQ7RWhq2RaLzY

...




Student Often Ends Up Here

- <https://www.google.com/#q=pgp+decrypt>



First Search Result



Trade without Bureaucracy™


About iGolder Buy Gold Sell Gold Join Now! Contact Home

PGP Decryption Tool

This tool is simple to use: enter your private PGP key, your PGP passphrase, and the PGP-encrypted message you wish to decrypt, then click on the **Decrypt Message** button. If you supply the proper PRP private key and passphrase/password, then you will be able to read the decrypted message, otherwise you will see an error message the tool is unable to decrypt the message.

iGolder respects your privacy and does not log nor monitors any activity (decryption) done on this web page.

PGP Private Key (paste your private key - you also need to supply your PGP passphrase to unlock your private key)

PGP-Key Password / Passphrase: 

PGP-Encrypted Message (paste the PGP-encrypted message you received)

Related Pages

- [PGP Freeware Tools](#)
- [PGP Key Generator](#)
- [PGP Encrypt Message](#)
- [PGP Email Encryption](#)



Crypto Advice From Dilettantes

- From: businessinsider.com

Dylan Love, JUN 17 2013 4:18

EDWARD SNOWDEN: How To Make Sure The NSA Can't Read Your Email

“ [...] You can generate PGP keys to your heart's content using the free tool at iGolder and a number of other services around the web.” [...]

- #OpNSA – PGP Encryption TuT

“ [...] The NSA needs to know the people are waking up. [...] generate you're Public and Private key. You can do this at [igolder]



Bootstrapping

- Web of trust
- Trust anchors
- Trust on first use

```
ssh-keygen -l ssh_host_*_key.pub
```

```
openssl x509 -nout -in cert.pem \  
-fingerprint
```

```
gpg -keyserver pgp.example.org \  
-send-key DEADBEEF
```



Usability

- Digital keys are not a concept the mass market gets
 - Nor asks for
 - Nor fits well with closed devices and clouds
- Individual certificates require maintenance if not cost
- Secret protection, recovery and revocation
- End-to-end security is desirable, but challenging
- Software integration and compatibility often tenuous
 - PGP is notoriously troublesome
 - S/MIME has advantages but inherits CA/PKI issues



Pretty Good Privacy (PGP)

- Use a GnuPG or Symantec version if possible
- Other options include
 - Android Privacy Guard (APG)
 - iPGMail, oPenGP
- Use packages if possible
 - GPGTools (Mac), Gpg4win (Win)
- MacOS point releases have history of integration issues



PGP Algorithms, Keys and Email

- Encryption and signing algorithm choice is academic
 - Modern defaults should be fine
- 2048-bit key is the modern default
 - I've used 4096-bit for years without complaint
- Protect your private keys, duh
- MUA integration is user dependent
- I use Claws Mail, has nice PGP integration
 - With a GnuPG agent, I can search encrypted emails
- Inline versus MIME



Group with PGP Communication

- Shared key
 - Best for small groups and teams
 - FIRST, DRG and various IRTs
- Encrypt to list, exploder to individual keys
 - This is probably the path forward
 - ops-trust, SELS



I Asked...

- `first-teams@first`
- `general@ops-trust`
- `discuss@ren-isac`

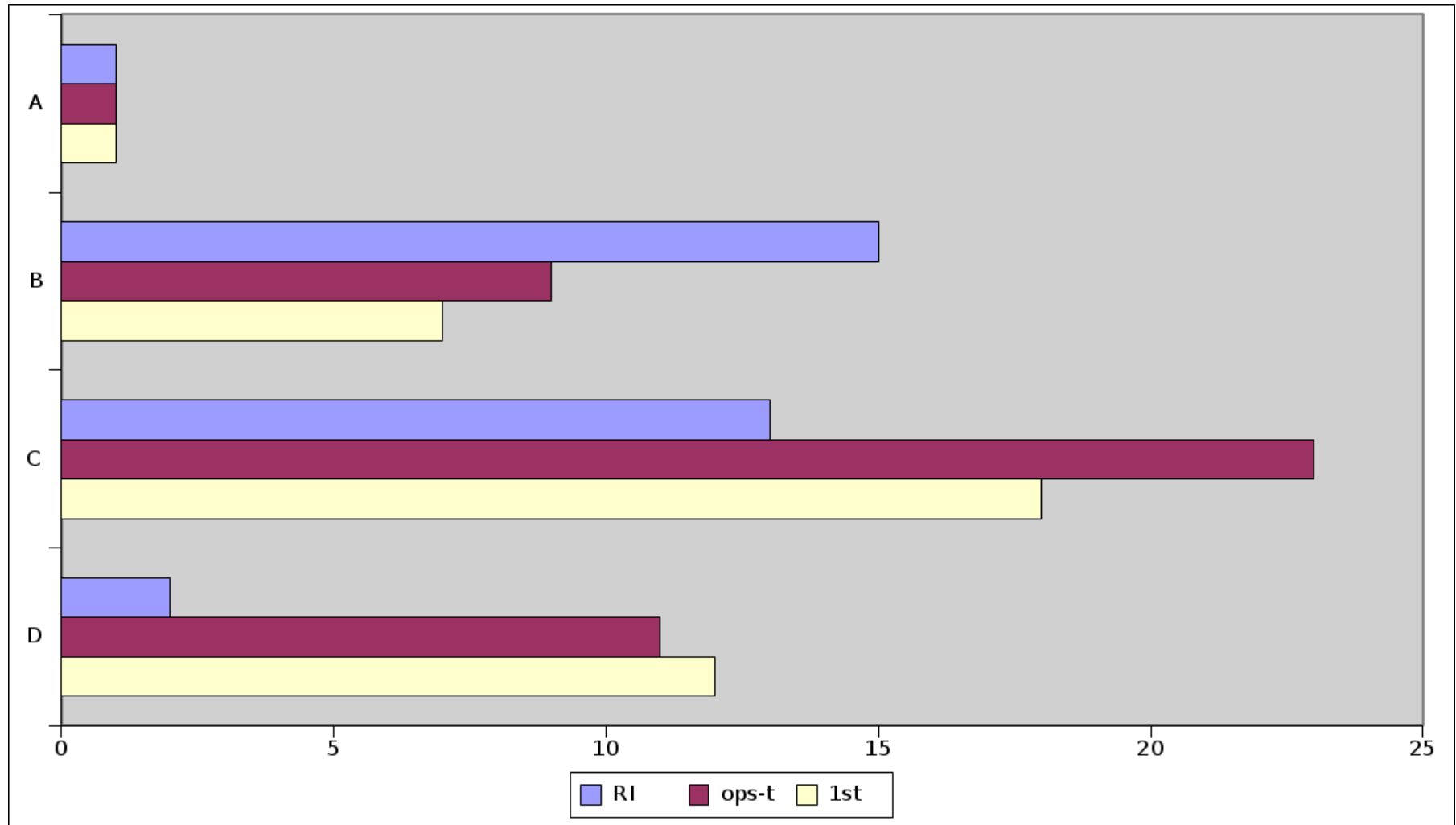


Value of PGP for Email Survey

- A. Practically of no value / it is failed technology
- B. Some value, but limited / niche technology
- C. Important technology, wish it was more widely used
- D. Critical / couldn't live without it



PGP for Email Survey Results



PGP for Email Verdict and Notes

- Our colleagues are all over the board on best practices
- Many have never signed a key or had one signed
- A few sign all messages by default
- A few regularly receive or send encrypted messages
- While pessimism is high, usage is also
 - 2/3 have signed or encrypted a message recently
 - More than 75% have had their key signed



PGP Key Considerations

- Subkeys or new keys?
- Do you validate and sign all uid's on the key?
 - Our friend Ian Cook has at least 16!
- Keyserver uploads
 - Anyone can create a jtk@cymru.com key
 - Then proceed to sign keys and upload updated keys
 - Will the fake jtk key get any signatures back?
- Why bother signing keys?!

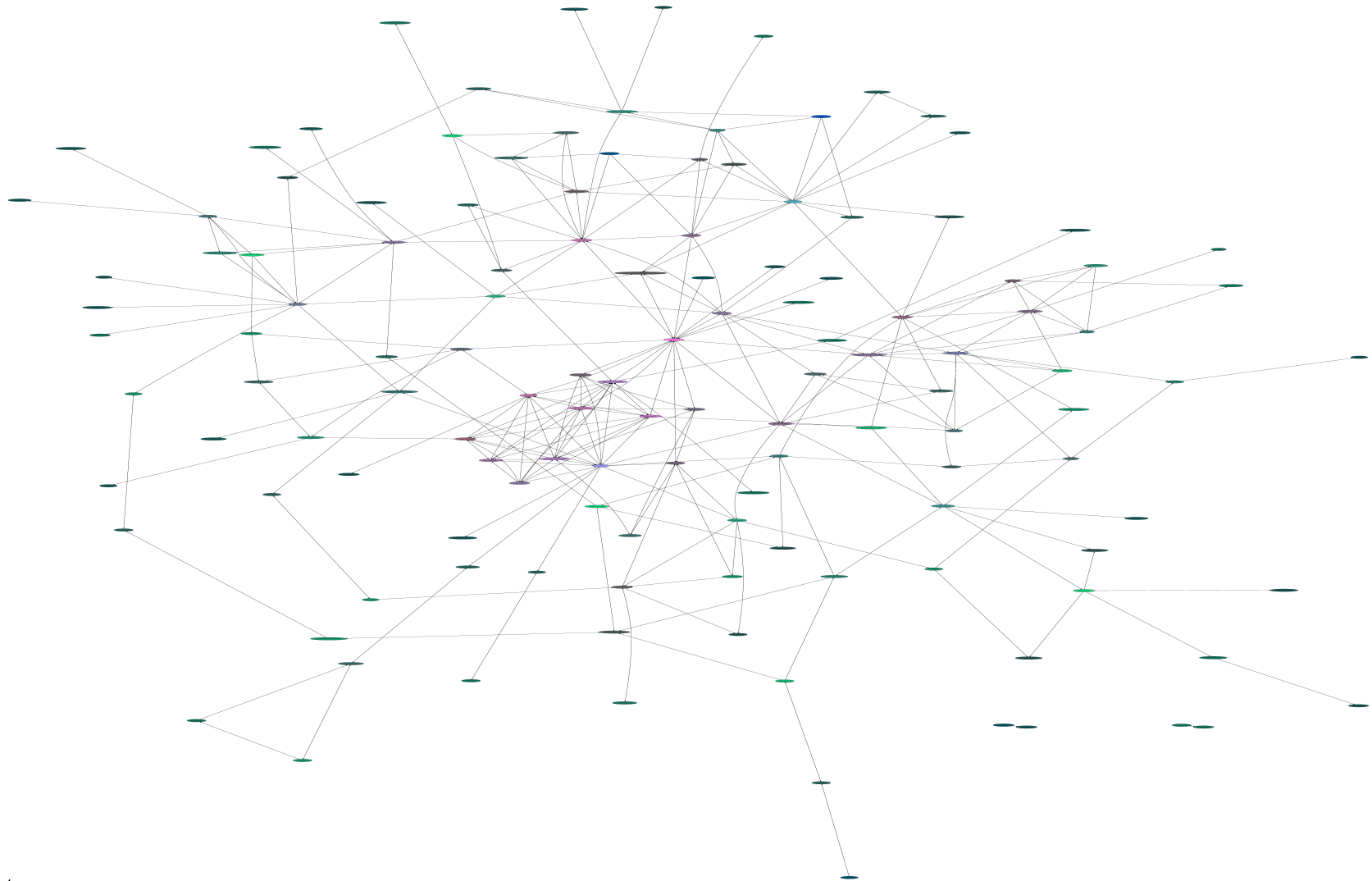


Key Signing Party Challenges

- Key ring collection
- Same-day, on the job key creation and training
- Physical ID validation
- Unverified email IDs



PGP Web of Trust



PGP Key Liveliness

- From which the preceding graph was based
 - A few hundred keys analyzed
 - 29 expired keys
 - 1 revoked
 - 3 due to expire within 30 days



If You Want My PGP Signature

- Put your public PGP key on the FIRST 2014 keyring
<http://biglumber.com/x/web?keyring=1628>
- Introduce yourself to me, show me some ID (haha)
- A business card with your fingerprint on it is ideal
- I will do the same
- I will send you an encrypted email with my signature
- If you had signed my key prior to today, bonus!



I was asked about Heartbleed

- This was my original reaction when it was announced
- Consider how it was presented:
 - Grammatical and spelling mistakes
 - How often has a vulnerability gotten its own .com?
 - Why? Who? What is to be gained?
- Nonetheless, fascinating vulnerability
- Attackers don't know what they will get
 - This is actually helps dampen people's concerns
- Not easily weaponized, requires significant analysis



Heartbleed Notwithstanding

- Client/Server SSL/TLS and X.509 very successful
- Flexibility as a boon and scourge
 - In that way similar to traditional DNS, pay attention
 - This (ab)use will probably never go away
- CA lapses are a relatively tiny part of the problem
- Delegated root authority uncommon, but not impossible



X.509 Certificates

- EFF Observatory lead the way in active analysis
- Notary services
- Flexibility as a boon and scourge
 - In that way similar to traditional DNS, pay attention
 - This (ab)use will probably never go away
- CA lapses are a relatively tiny part of the problem
- Delegated root authority uncommon, but not impossible



DANE

DNS-based Authentication of Named Entities

- Tie X.509 data to the DNS
- Cynic or optimist? Depends on your perspective
 - How can we disrupt the CA market?
 - How can we promote DNSSEC and DNS ops?
 - How can we overload the DNS?
 - How can we eliminate unwanted shared fate?
- Note: DNSSEC deployment status is pretty dismal



DNSSCurve

- This is probably a better solution than most will admit
- DNSSEC does not do encryption
- DNSSCurve does encryption on a per-DNS-hop basis
- Traditionally DNS data was considered public
 - Queries probably shouldn't be
 - Some zones probably shouldn't be
- Sometimes theology trumps technology
 - Dan Bernstein versus the world
- Passive DNS as currently implemented won't work



Routing

- No encryption in BGPSEC
- Practically no one encrypts routing messages
- Next slide



The encryption we don't have

- Bootstrap, discovery and zeroconf protocols
 - Apple's MDNS and Microsoft's NetBIOS NS, blech
- Automated, background, tray applications
- Games
- Social media
- Management and control traffic
- No heartfelt “encrypt everything” movement
 - Notwithstanding the EFF HTTPS everywhere project
 - Some key WWW sites still redirect HTTPS to HTTP



Thank You!

- My active PGP keys:

```
pub      1024D/FFE85F5D 2008-07-31
         57D8 14C3 A644 200C 3ACE
         46B3 7118 0AF1 FFE8 5F5D
John Kristoff <jtk@cymru.com>
```

```
pub      1024D/C85CCA46 1999-11-16
         C594 D57F 9538 CFE5 4F06
         549F 207C C968 C85C CA46
John Kristoff <jtk@depaul.edu>
```

