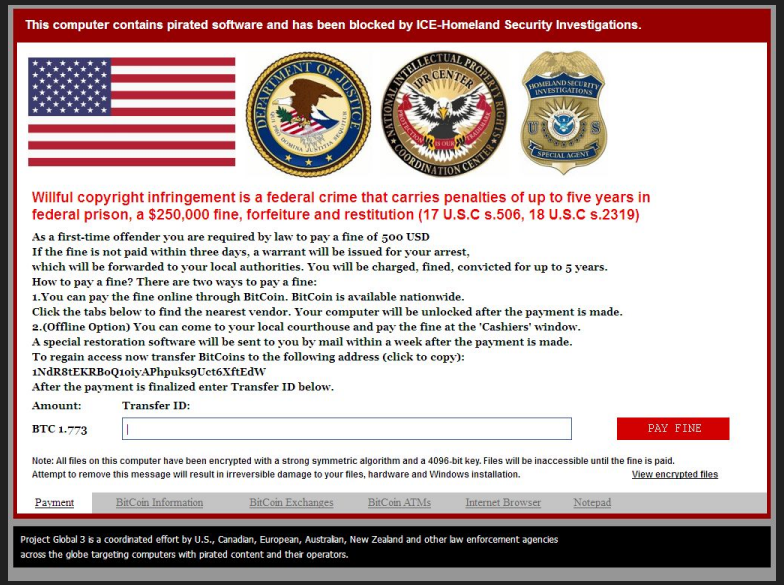


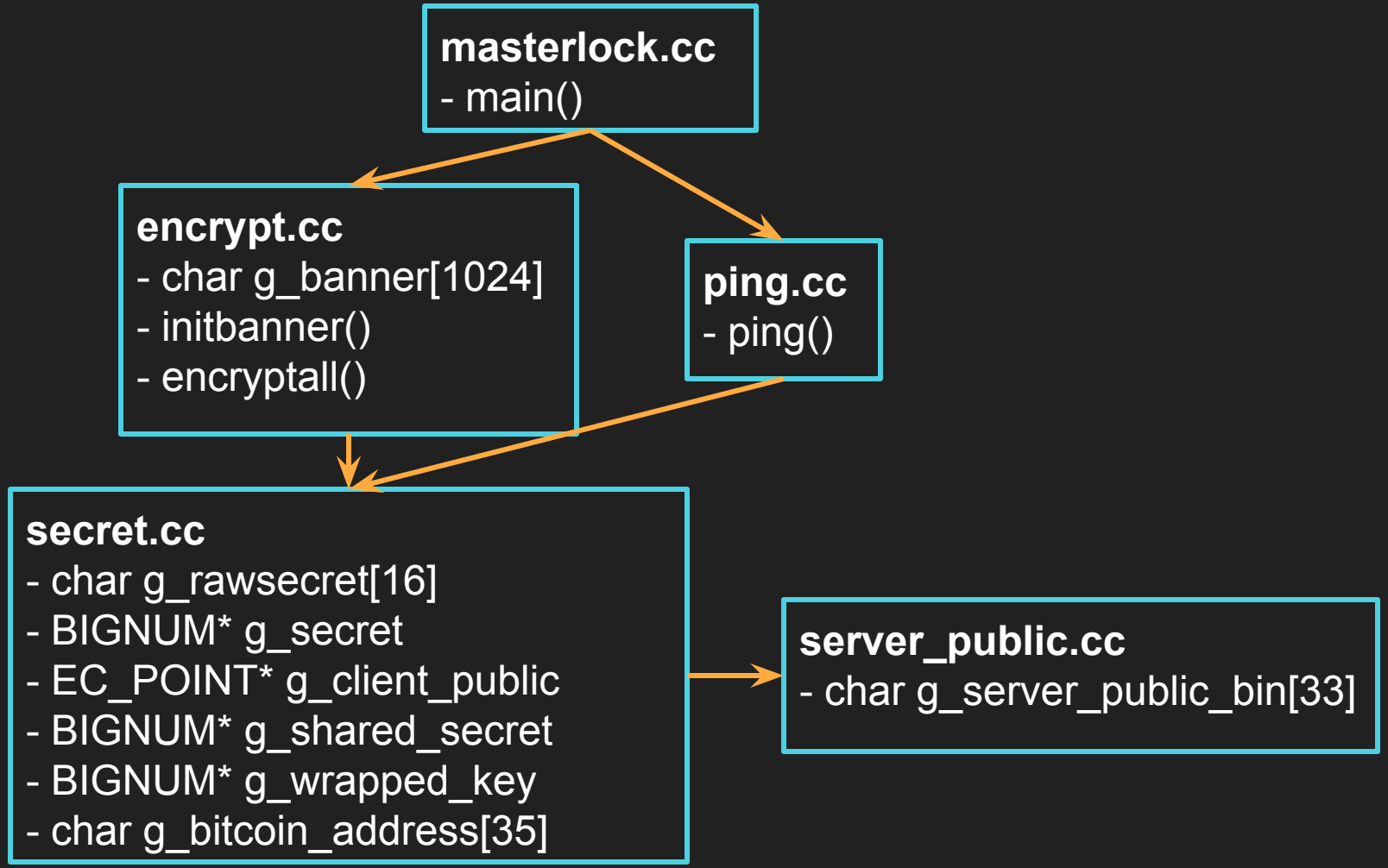
ECCryptolocker

Montréhack 2015/10/19

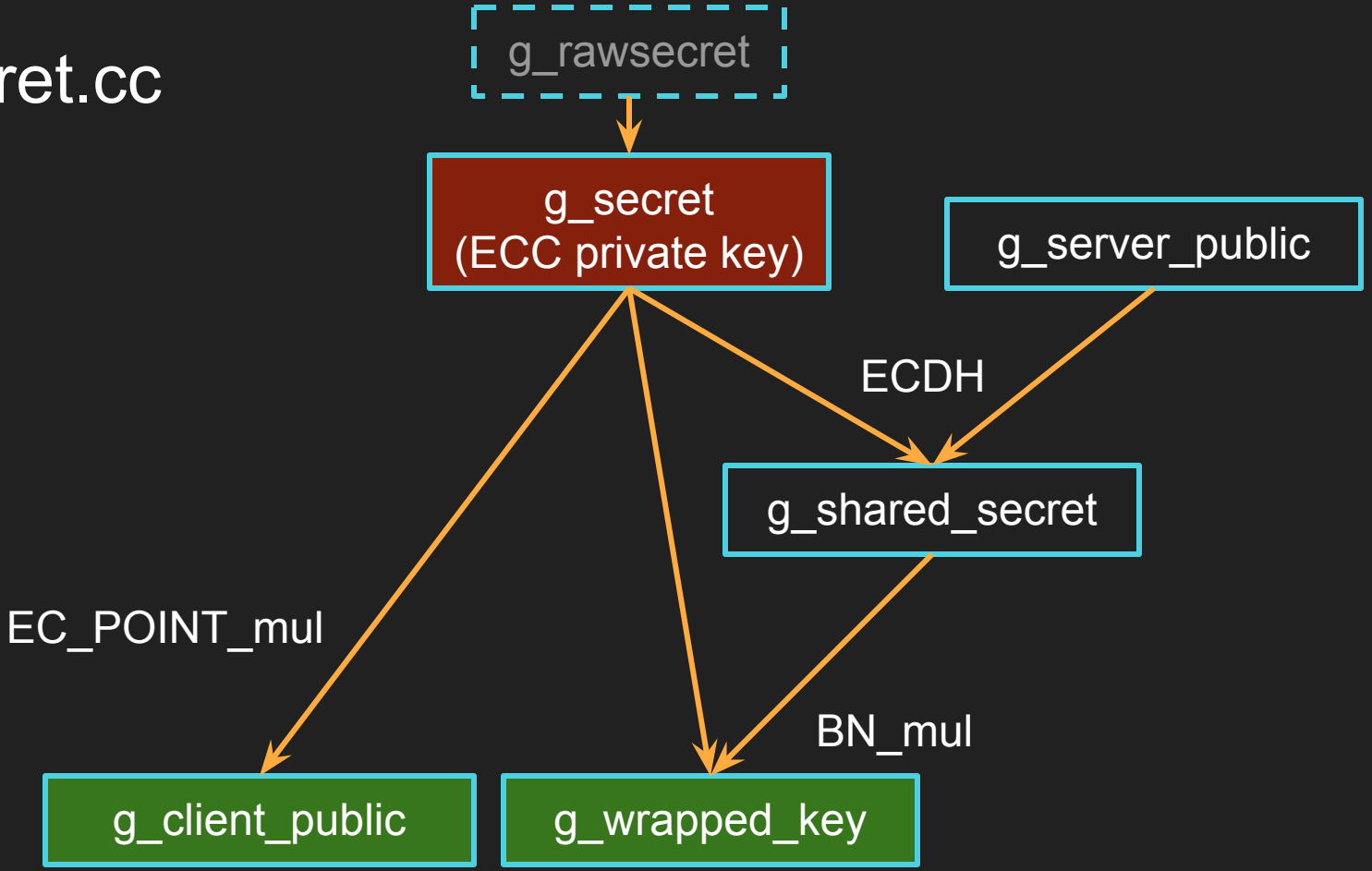
Catalin Patulea
http://github.com/cpatulea

http://tinyurl.com/montrehack-20151019

< 5 minutes de calcul


masterlock.cc
- main()
encrypt.cc
- char g_banner[1024]
- initbanner()
- encryptall()
ping.cc
- ping()
secret.cc
- char g_rawsecret[16]
- BIGNUM* g_secret
- EC_POINT* g_client_public
- BIGNUM* g_shared_secret
- BIGNUM* g_wrapped_key
- char g_bitcoin_address[35]
server_public.cc
- char g_server_public_bin[33]

secret.cc


g_rawsecret
g_secret
(ECC private key)
g_server_public
ECDH
g_shared_secret
EC_POINT_mul
BN_mul
g_client_public
g_wrapped_key

g_wrapped_key

```
g_secret * g_shared_secret = g_wrapped_key

128 bits * 256 bits        = 384 bits

a        * b               = 0x0636...61BC

p0p1p2p3…                  = n

ex. a = p0p2p3  b = p1p4p5p6
```

Factorisation

Techniques

Pollard’s rho (ρ): $< 2^{64}$ (38 chiffres)

Lenstra elliptic curve factorization (ECM): < 80 chiffres

Quadratic sieve (MPQS): < 100 chiffres

General number field sieve (GNFS): > 100 chiffres

Outils

GNU factor (ρ)

Python primefac (ρ, ECM, MPQS)

pyecm (ECM)

msieve (MPQS, GNFS)

ggnfs (GNFS)