Alert system retirement

You are now Building on Bitcoin

Bryan Bishop <kanzure@gmail.com>

0E4C A12B E16B E691 56F5 40C9 984F 10CC 7716 9FD2

2018-07-03

Talk outline

- History and background
- Vulnerabilities
- Alternatives
- Key disclosure

What alert system?

- Well, it was removed a long time ago.
- Used bitcoin's p2p network messaging layer
- Node peers would relay alert messages between each other on a flood network
- Public-key cryptography (public-private key pair)
- Alert key (private key) was given to a number of developers for safekeeping and it was to be used in the event of extreme emergencies

Alert message fields

```
int32_t nVersion;
int64_t nRelayUntil;      // when newer nodes stop relaying to newer nodes
int64_t nExpiration;
int32_t nID;
int32_t nCancel;
std::set<int32_t> setCancel;
int32_t nMinVer;           // lowest version inclusive
int32_t nMaxVer;           // highest version inclusive
std::set<std::string> setSubVer;  // empty matches all
int32_t nPriority;
```

- Alert message is a serialized object consisting of the above + vchSig
- Identified by sha256(serialize(alertmessage))

Conceptual and actual problems with the alert system

- Surprisingly a lot of problems and issues in something so simple
- Somewhat at odds with the idea of a decentralized p2p network
- Caused confusion and misconceptions
- Requires secure storage of the key proportional to the value of the key (e.g. potential for market disruption...). Becomes a target for thefts.
- Altcoins copying the public key (both intentionally and unintentionally)
- Alert + partition attacks etc...

Version history

- bitcoin v0.3.11 introduced alert system (2010)
- bitcoin v0.10.3 and later had -alerts=0 to disable or opt-out of the alert system
- bitcoin v0.12.1 disabled the alert system
- bitcoin v0.13.0 removed alert system completely
- bitcoin v0.14.0 final alert "Alert Key Compromised" hardcoded

Original implementation

- Satoshi introduced the alert system in August 2010, bitcoin v0.3.11
- https://github.com/bitcoin/bitcoin/commit/401926283a200994ecd7df8eae8ced8e0b067c46

Early DoS vulnerabilities

- Two alert system vulnerabilities reported by Sergio Lerner (August 2012) (CVE-2012-4684)
- https://github.com/bitcoin/bitcoin/commit/d5a52d9b3edaae6c273b732456d98e6b28ed7b31
- https://en.bitcoin.it/wiki/CVE-2012-4684
- Malleable BER/DER-encoded signatures
- Solutions:
  - Exclude signature from hashing
  - Check setKnown before checking signatures
  - Disconnect peers that are spamming alerts

Final alert concept (2012)

- Maximum sequence final alert such that other alerts cannot override the message
- Meant to be a permanent final alert...
- https://github.com/bitcoin/bitcoin/ea2fda46c3d12a17ebba07c139b4cd65ea0b63d9

Removal proposed (June 2015)

- Removal was proposed in https://github.com/bitcoin/bitcoin/pull/6260 but was not merged
- Instead, alert system was made opt-out option https://github.com/bitcoin/bitcoin/pull/6274

Removal (March 2016)

- Self-explanatory
- https://github.com/bitcoin/bitcoin/pull/7692

Completing the retirement of the alert system (late 2016)

- https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2016-September/013104.html
- https://bitcoin.org/en/alert/2016-11-01-alert-retirement
- Pre-final alert broadcasted
- Final alert: Max sequence Alert to disable the alert system ("Alert Key Compromised")
- Eventually, final alert was hardcoded https://bitcoin.org/en/release/v0.14.0#final-alert
- Alert key disclosure postponed

Infinitely sized map (CVE-2016-10724)

- Attacker spams a node with a large number of alerts
- No limit on size of the map structure in memory
- Node runs out of memory and dies
- basic Denial of Service (DoS) attack

Infinitely sized alerts

- Alert system used bitcoin p2p network messages, imposing a limit of 32 megabytes on the size of messages
- setCancel field (list of integers, spam with many integers)
- setSubVer field (lits of std::string values, no length limit per string)
- bitcoin prior to v0.10.0 did not length limit on a handful of other fields (strComment, strStatusBar, and strReserved)
- DoS attack

Multiple final alerts

- Alerts are identified by H(serialize(alertmessage))
- Final alert definition is missing a few fields of the message structure
- Multiple final alerts can be generated by varying the value of some of the fields not required in the final alert definition
- Each final alert gets stored in memory
- See https://github.com/bitcoin/bitcoin/commit/ea2fda46c3d12a17ebba07c139b4cd65ea0b63d9
- Another DoS attack

Final alert cancellation (CVE-2016-10725)

- Final alert was meant to be uncancelable, but it is in fact cancelable
- Alerts are checked in the following order:
  - Check whether this alert cancels any other alerts
  - Check whether any other alerts cancel the current alert
- Attacker can cancel a final alert by another alert allowing a node (with the alert system) to again be vulnerable to these disclosed vulnerabilities

Alternative alert system proposals

- Building on p2p layer is an okay idea, didn't require consensus rules... but there are other designs that could have done better.
- "Todd-lerts": OP_RETURN + burn BTC on different forks of the chain (proof-of-burn?)
- n-of-m multisig alerts, ring signatures, certificate authority, …
- Just use traditional news outlets, mailing lists, twitter, etc.

Alert key disclosure (announcements)

- IRC, twitter, email, etc.
- Looked through other source code of altcoins etc.
- Asked around for any concerns etc.
- https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-June/016123.html
- https://www.coindesk.com/long-secret-bitcoin-key-finally-revealed/
- https://bitcoincore.org/en/meetings/2018/06/21/

Alert key disclosure

name	value
mainnet alert key (public)	04fc9702847840aaf195de8442ebecedf5b095cdbb9bc716bda9110971b28a49e0ead8564ff0db22209e0374782c093bb899692d524e9d6a6956e7c5ecbcd68284
mainnet alert key (private) (WIF)	5JTCEcgNthSUemCNERKp21MRxXD46RLq56St4VztDHQNM1NQytv
testnet alert key (public)	04302390343f91cc401d56d68b123028bf52e5fca1939df127f63c6467cdf9c8e2c14b61104cf817d0b780da337893ecc4aaff1309e536162dabbdb45200ca2b0a
testnet alert key (private) (WIF)	928KUNGSTZnL17VeBMCSwwKEWaVFdJD5Lq6joBFR4EuQgbrb4FP