Australian Government

Department of Defence

Defence Science and Technology Group

# OSPF Cryptographic Authentication

Chris Wiren, Engineer

Communication Networks Research Group

Defence Science Technology Group

Email: chris.wiren@dsto.defence.gov.au

Office: +61 8 7389 6572  Mobile: 0421 708 753

DST GROUP Science and Technology for Safeguarding Australia

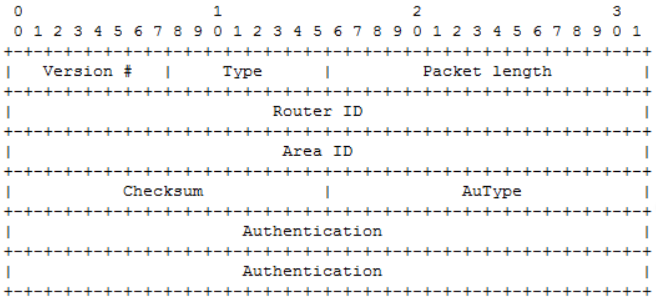
# OSPF Cryptographic Authentication

Hashing Function

+

Key Id + Sequence Number

RFC 2328 Appendix D



```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Version #   |     Type      |         Packet length         |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                          Router ID                            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                           Area ID                             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |           Checksum            |             AuType            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                       Authentication                          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                       Authentication                          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

HMAC
Hashed Message
Authentication Code

OSPF

+

Shared Secret

> *"A simple risk analysis would suggest that an ideal attack target of minimal cost but maximal disruption is the core routing infrastructure."*
> RFC4948 – August ***2007***

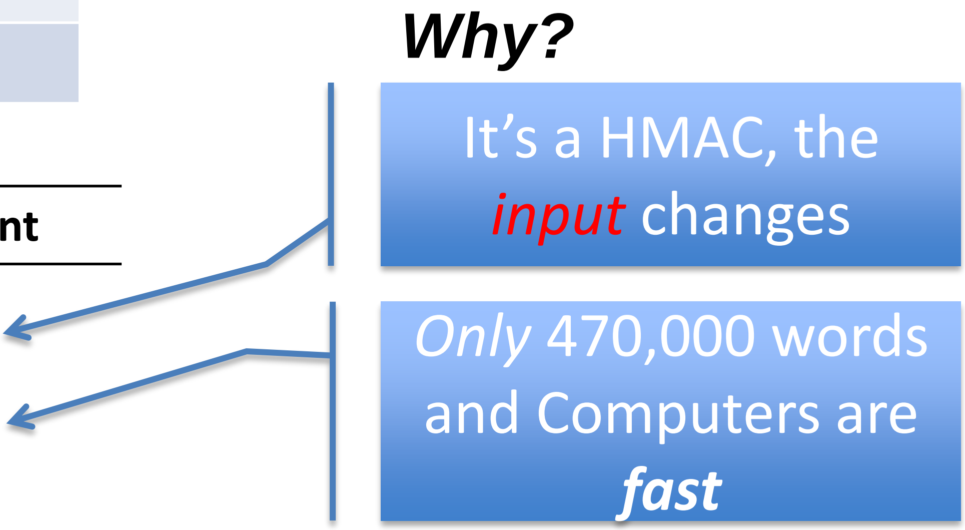
Confidentiality ✗
**Integrity** ✓
**Availability** ✓

# OSPF Cryptographic Authentication

| OSPF MD5 Key Recommendation | |
|---|---|
| **Character Set** | **Length** |
| Alphabetic | 14 |
| Alphanumeric | 14 |
| Printable | 13 |
| Binary | 10 |

> *"It is a common misconception that because OSPFv2 specifies MD5 as the hashing function, it is fundamentally insecure."*

| **Shared Secret Complexity is Important** | |
|---|---|
| Complex with sufficient length | 1 Year |
| Dictionary word | 1 Second |



***Why?***

It's a HMAC, the *input* changes

*Only* 470,000 words and Computers are ***fast***

Chris Wiren, Engineer
Communication Networks Research Group
chris.wiren@dsto.defence.gov.au
Office: +61 8 7389 6572 Mobile: 0421 708 753

Witty, B, Wiren, C., Nagy, S. '*Cryptographic Security of Pre-Shared Keys in OSPFv2*', DSTO-TR-0508