secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

# IPv6 Security: Attacks and Countermeasures in a Nutshell

J. Ullrich, K. Krombholz, H. Hobel,
A. Dabrowski, E. Weippl

SBA Research, Vienna, Austria

bmvit Bundesministerium für Verkehr, Innovation und Technologie

bmwfj Bundesministerium für Wirtschaft, Familie und Jugend

Christian Doppler Forschungsgesellschaft

FFG

wirtschaftsagentur wien

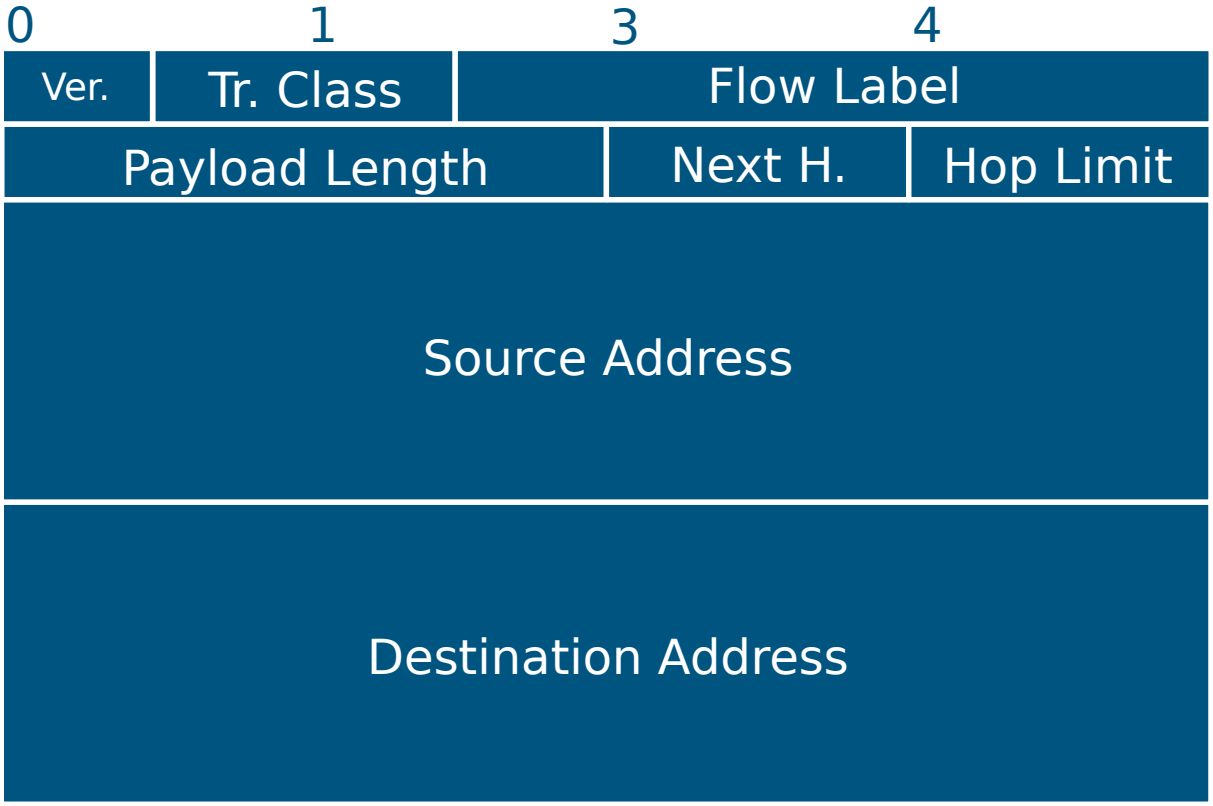
zit Die Technologieagentur der Stadt Wien

secure
sba-research.org

# Motivation

- Variety of sources
  (RFCs, blogs, ...)
- Systematization
  of attacks and countermeasures
- Identification of challenges

# IPv6 Header Format



# Systematization

- Vulnerabilities
  - action, object, target, result, origin, and modification
- Countermeasures
  - action, object, and activity level
- Evaluation
  - on vulnerabilities and adequate countermeasures

# Future Challenges

- Address assignment and structures
- Securing the local network
- Reconnaissance

# Addressing

- Stateless Autoconfiguration
  - Modified EUI-64 format
  - Privacy Extension
- DHCPv6
  - DHCP unique identifier
- Manual address assignment

# Securing the Local Network

- IPsec
  - Bootstrapping problems
  - Manual key assignment
- Secure Neighbor Discovery (SeND)
  - Cryptographically Generated Addresses
  - Signation of packets

# Reconnaissance

- Vast address space
- Alternatives
  - DNS querying
  - Messages to multicast addresses
  - Eavesdropping
- Active probing still promising
  - Address selection
  - Patterns?

# Conclusion

- Generation next – generation best?
  - Not less secure than IPv4
  - Transition technologies
- Challenges for the future remain ...