Cybersecurity and IoT

Overview of the security challenges for 6LoWPAN IoT

GIoTS Industry Forum III

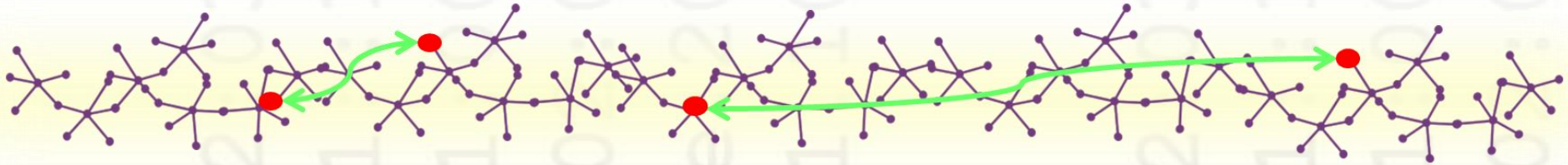
Dr David Holder CEng FIET MIEEE

david.holder@erion.co.uk

Erion

Cybersecurity and IoT

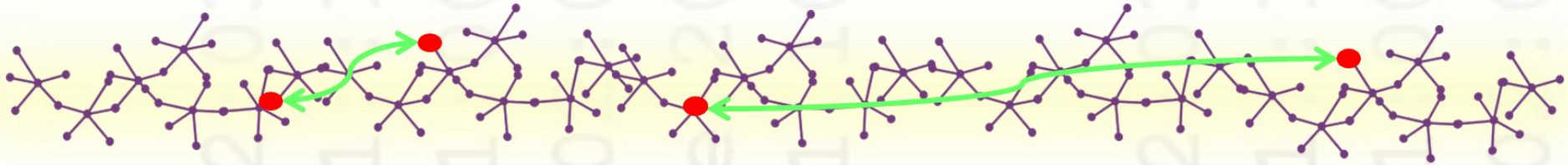
- IoT and 6LoWPAN
- Challenges for IoT Cybersecurity
- 6LoWPAN threats and vulnerabilities
- IPv6 and 6LowPAN security features
- IoT forensics



Erion

Cybersecurity and IoT

- **IoT and 6LoWPAN**
- Challenges for IoT Cybersecurity
- 6LoWPAN threats and vulnerabilities
- IPv6 and 6LowPAN security features
- IoT forensics

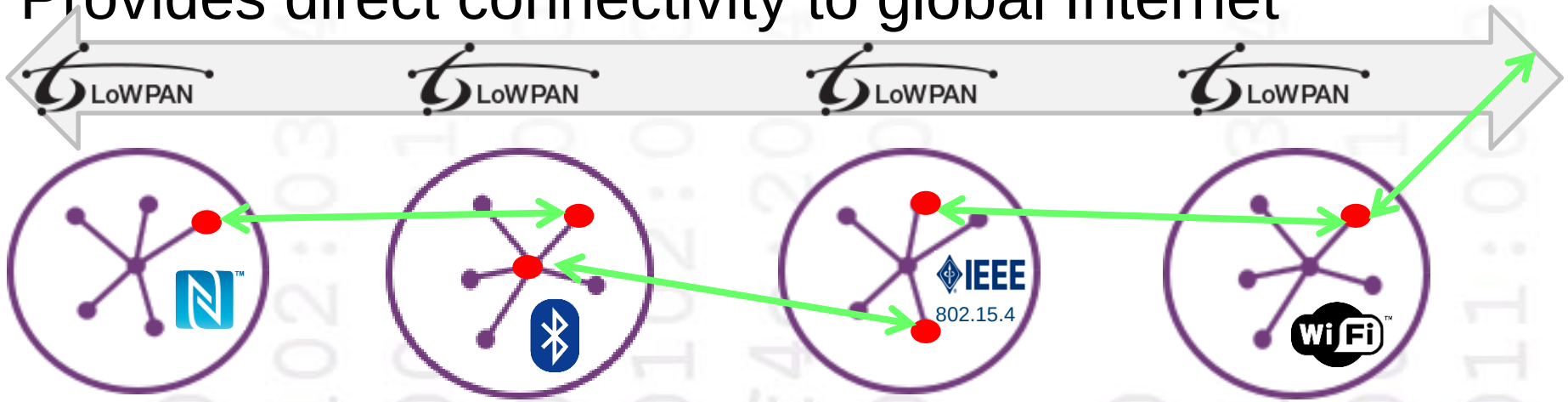


Erion

IoT and 6LoWPAN (IPv6 for IoT)

- ✓ Based on standard Internet Protocols
- ✓ Interoperates across many radio types
- ✓ Designed for Low-power, Lossy IoT networks
- ✓ Familiar APIs for software developers
- ✓ Allows direct connection between devices
- ✓ Provides direct connectivity to global Internet

IETF etc...



Internet (IPv6)

Erion

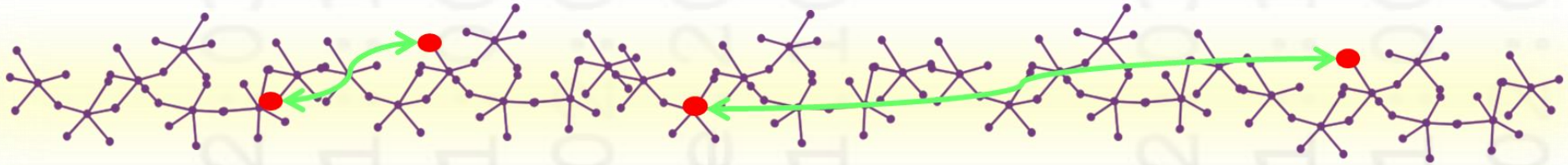
6LoWPAN – Fitting IPv6 into IoT

- **Compression**
  - Squeezing IPv6 (minimum MTU 1280) into IEEE 802.15.4 (127 bytes)
  - Compressing upper layer protocols including security protocols
  - Don’t keep network information that can be derived from link-layer
- **Reduced the number of frames**
  - E.g. A problem for key negotiation is the number of frames required
- **Modified core protocols**
  - E.g. Neighbor Discovery (NDP), Stateless Address Autoconfiguration (SLAAC) and routing (route-over/mesh-under)

Erion

Cybersecurity and IoT

- IoT and 6LoWPAN
- ➢ **Challenges for IoT Cybersecurity**
- 6LoWPAN threats and vulnerabilities
- IPv6 and 6LowPAN security features
- IoT forensics



Erion

Challenges for IoT Cybersecurity

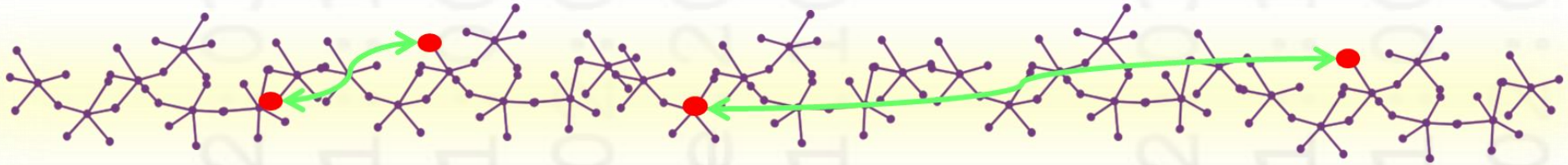
- IoT has additional cybersecurity challenges

- IoT is resource constrained
  - **Bandwidth** – low and **very** expensive (battery life)
  - **Computational power** – low and expensive (battery life)
  - **Visibility** – mesh and wireless networks mean not everything is visible
- IoT defence is more asymmetric than internet defence
  - Defenders are resource constrained
  - Attackers are **not** resource constrained
- Internet security techniques do not always map to IoT
  - They can be impractical, inappropriate or impossible in IoT

Erion

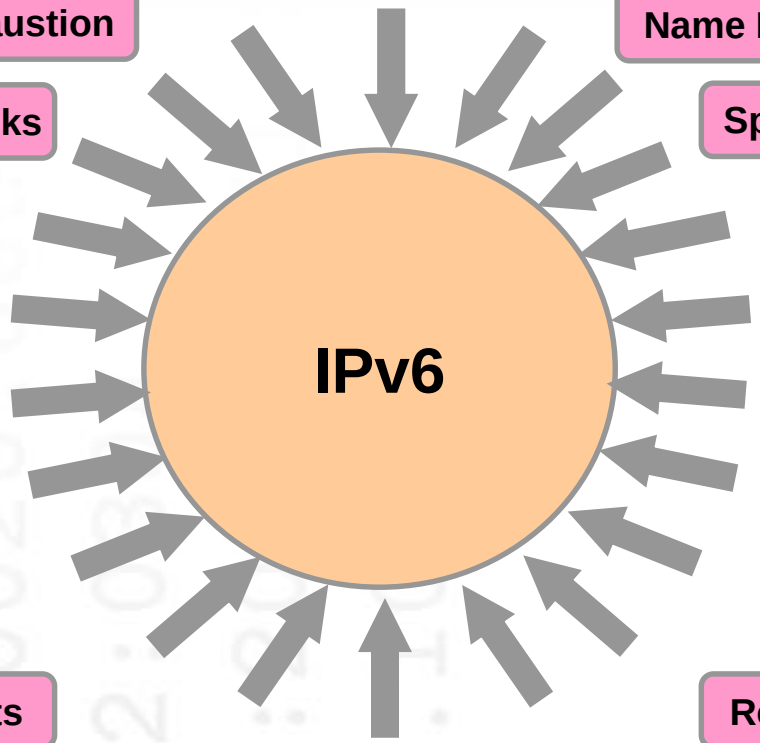
Cybersecurity and IoT

- IoT and 6LoWPAN
- Challenges for IoT Cybersecurity
- ➢ **6LoWPAN threats and vulnerabilities**
- IPv6 and 6LowPAN security features
- IoT forensics



Erion

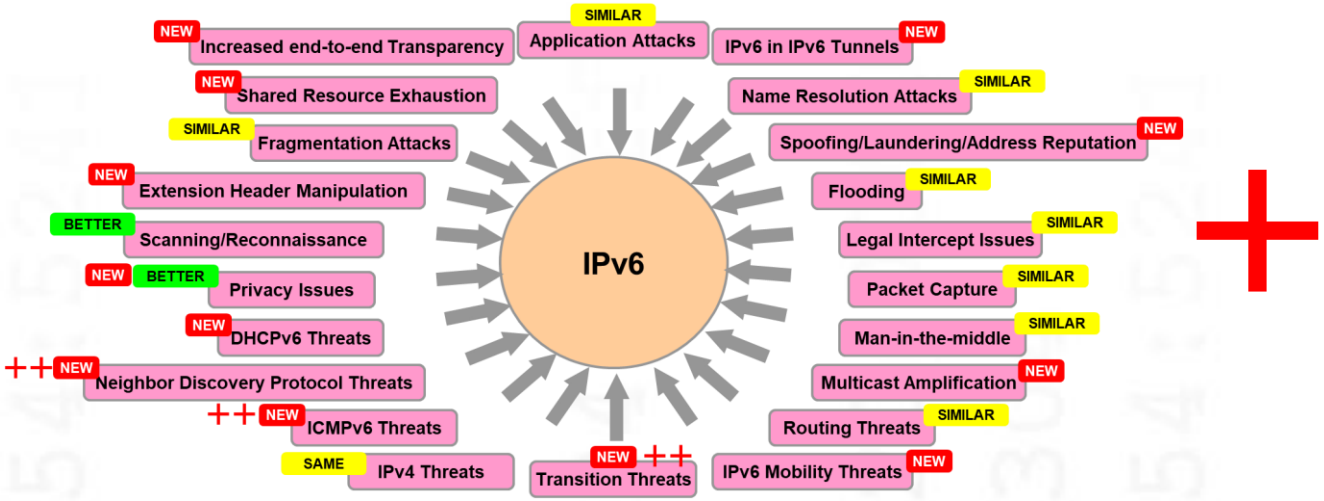
The IPv6 Vulnerability Surface



- NEW — Increased end-to-end Transparency
- SIMILAR — Application Attacks
- NEW — IPv6 in IPv6 Tunnels
- NEW — Shared Resource Exhaustion
- SIMILAR — Name Resolution Attacks
- SIMILAR — Fragmentation Attacks
- NEW — Spoofing/Laundering/Address Reputation
- NEW — Extension Header Manipulation
- SIMILAR — Flooding
- BETTER — Scanning/Reconnaissance
- SIMILAR — Legal Intercept Issues
- NEW BETTER — Privacy Issues
- SIMILAR — Packet Capture
- NEW — DHCPv6 Threats
- SIMILAR — Man-in-the-middle
- ++ NEW — Neighbor Discovery Protocol Threats
- NEW — Multicast Amplification
- ++ NEW — ICMPv6 Threats
- SIMILAR — Routing Threats
- SAME — IPv4 Threats
- NEW ++ — Transition Threats
- NEW — IPv6 Mobility Threats

Erion

The 6LoWPAN Vulnerability Surface



6LoWPAN

- Wireless attacks – e.g Jamming
- Physical security of nodes
- Bootstrapping and key distribution
- DoS due to constrained resources
- Wormholes
- Blackholes

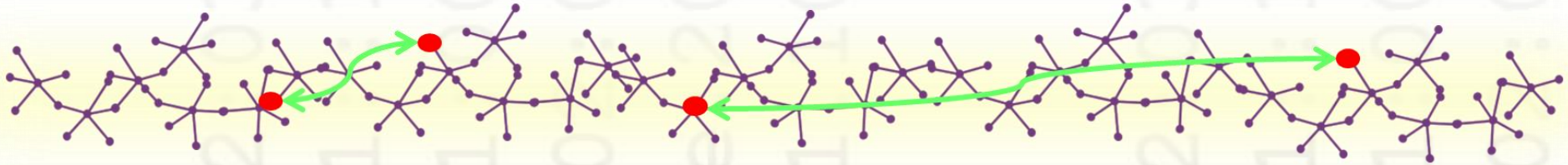
6LoWPAN

etc…

Erion

Cybersecurity and IoT

- IoT and 6LoWPAN
- Challenges for IoT Cybersecurity
- 6LoWPAN threats and vulnerabilities
- **IPv6 and 6LowPAN security features**
- IoT forensics

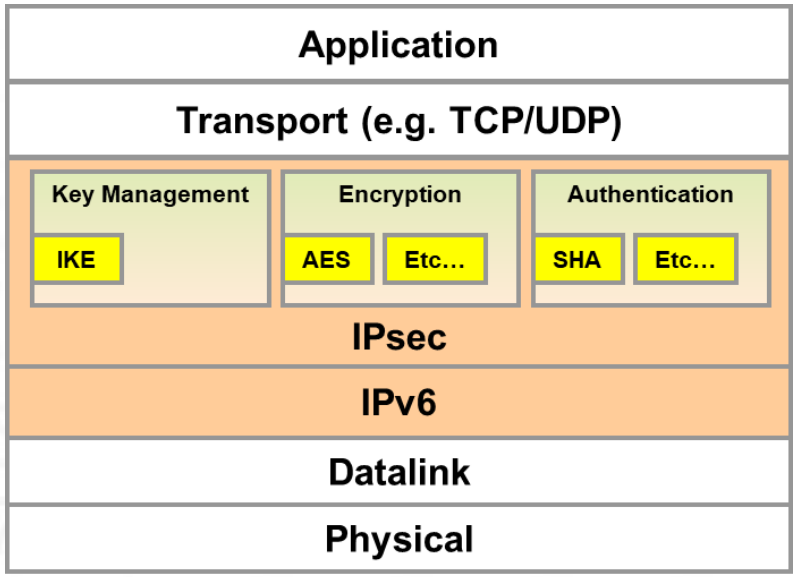


Erion

IPv6 Network Security (IPsec)

RFC 4301
RFC 4302
RFC 4303
RFC 4305
RFC 4306

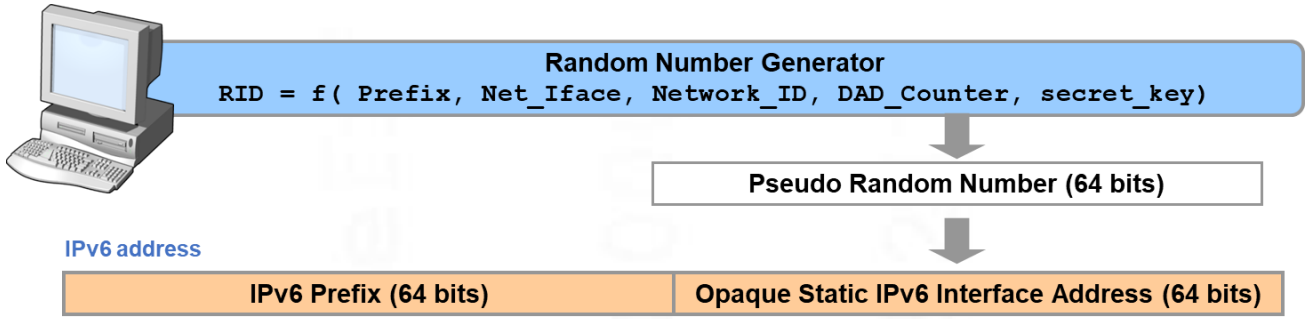
- Built into and protects the network layer
- Allows for different security mechanisms and is extendable
- Two extension headers
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Was mandatory feature in IPv6 stacks
- Compressed IPsec still too big
- Tunnel mode impractical in 6LowPAN
- Key management difficult in 6LoWPAN due to IKE chattiness
- Proposals for compressed IPsec have not been standardised



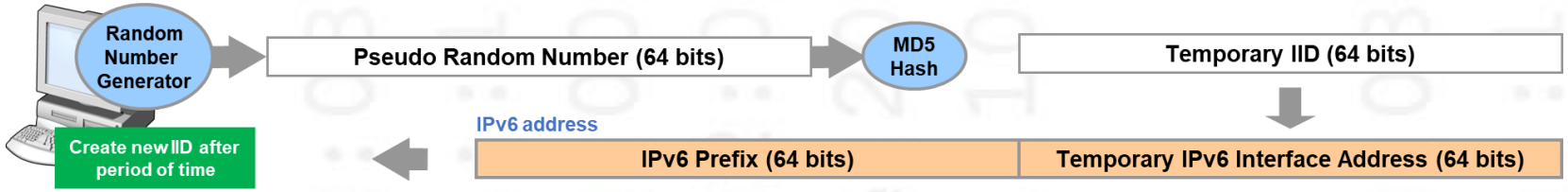
Erion

IPv6 Address Privacy

- **Opaque Static Addresses**
  - Avoids use of MAC address in IID (modified EUI-64)



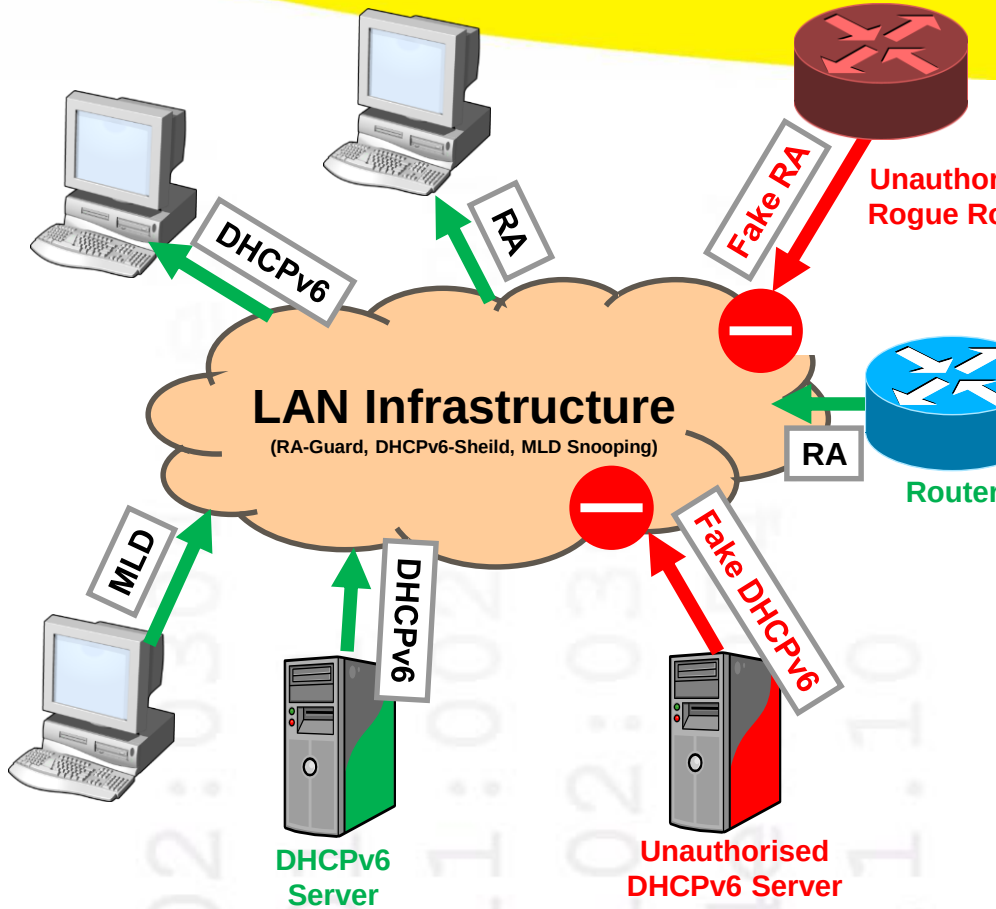
- **Privacy Addresses**
  - Temporary IID for client communications that changes with time



- Both addresses cannot be easily elided in 6LoWPAN

IPv6 Link Security Features

- **Cryptographically Generated Addresses (CGA)**
- **Secure Neighbor Discovery (SeND)**
  - Secures NDP messages (uses CGAs)
- **RA-Guard**
  - Validation and control of RAs
- **DHCPv6-Shield**
  - Validation and control of DHCPv6
- **Neighbor Discovery Inspection**
  - Validation of NDP messages
- **MLD Snooping**
  - Mitigates some multicast attacks



Security Approaches in 6LoWPAN

- Move the security to the datalink
  - E.g. IEEE 802.15.4 AES encryption & authentication
- Use different techniques
  - E.g. Datagram Transport Layer Security (DTLS)
- Compress existing techniques
  - E.g. TLS, SEND and possibly IPsec

- Challenges
  - Management
  - Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
  - Forensics

Erion

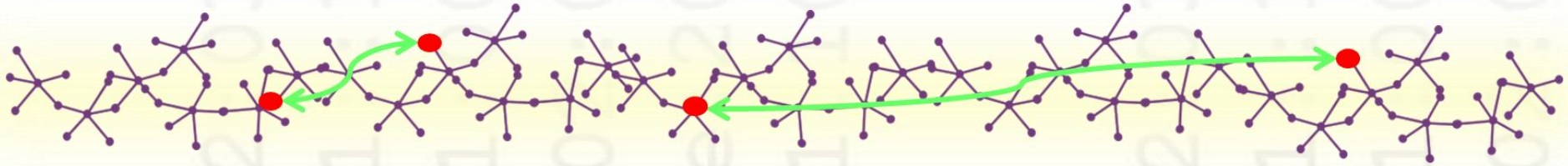
IPv6 vs 6LoWPAN Cybersecurity

Network Layer	IPv6	6LoWPAN (IEEE 802.15.4)	Comments
All	IDS/IPS/Firewalls	Firewall/IDS/IPS at edge	Difficult in IoT
Application	TLS	DTLS	End-to-end?
Transport	TLS	DTLS	Still large
Network			
Authentication/Encryption	IPsec	802.15.4 security	IPsec/IKE overheads
Address Privacy	Opaque/Privacy addresses	Cannot be elided	
Source address ownership	CGA	Cannot be elided	
Secure NDP	SEND ND Inspection	Lightweight SEND N/A	802.15.4/6LoWPAN E.g. 6LBR state
Secure Router Advertisements	RA-Guard	Problematic	
Secure DHCPv6	DHCPv6-Shield	Problematic	
Multicast protection	MLD Snooping	Problematic	
Link	Link specific	802.15.4 security	Key management

Erion

Cybersecurity and IoT

- IoT and 6LoWPAN
- Challenges for IoT Cybersecurity
- 6LoWPAN threats and vulnerabilities
- IPv6 and 6LowPAN security features
- ➢ **IoT forensics**



Erion

IoT Forensics

- Forensics requires the ability to obtain evidence
- In the case of digital evidence this is “best evidence”
  - Must be visible – vantage point is important
  - Must be collected automatically (avoid hearsay)
  - Must be stored/transmitted to “secure” location
- IoT presents additional challenges for forensics:
  - Mesh and wireless networks make visibility of traffic challenging
  - Automatic collection of potential evidence requires resources
  - Storing and transmitting evidence requires resources
  - Additional mappings (due to compression techniques) may be required to make sense of the evidence collected
  - Forensics tools generally do not support IoT (some don’t support IPv6)

Erion

Summary

- Cybersecurity in IoT is challenging
- Security techniques used on internet may not map to IoT
- Some security may be deferred to data link
- Additional techniques may be required
- IDS/IPS and other tools are limited or non-existent
- Forensics remains a significant challenge

Erion

Questions and Discussion

Thank you for listening

Further Information

Erion	http://www.erion.co.uk
IPv6 Training	http://www.ipv6training.com
IPv6 Consultancy	http://www.ipv6consultancy.com
IPv6 Blog	http://www.ipv6consultancy.com/ipv6blog

Erion

Profile: David Holder

- CEO and Chief Consultant Erion Ltd
- Author of numerous reports and whitepapers
- Chairman of IPv6 Task Force Scotland
- Regular speaker on IPv6
- Extensive experience of IPv6 spanning over 20 years

Erion