DHCP Security Considerations

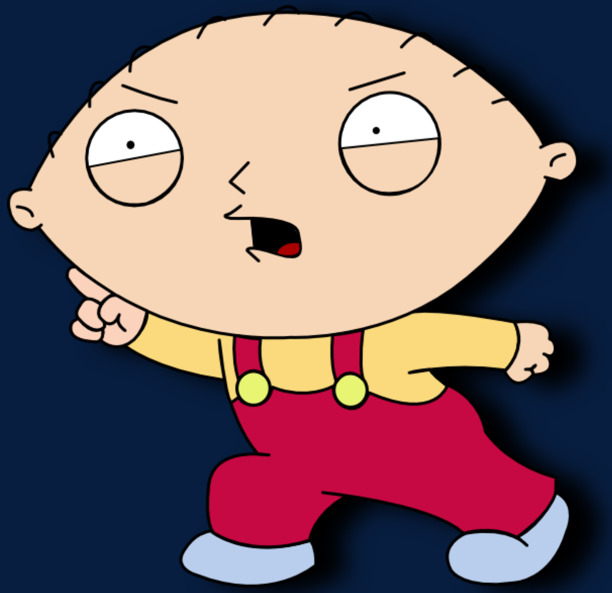
N3K Expert Webinar Series

Andreas Taudte
Principal DDI Consultant

Last updated December 2023

Housekeeping

- Timing, Schedule, Q&A Session
- Online Etiquette (microphones, distracting activities)
- Recording and Privacy



DDI’s Sandwich Child

DNS

Security

DDI’s Sandwich Child

Automation

Integration

Compliance

Visibility

DDI’s Sandwich Child

DHCP Stability, Reliability & Security at Risk

- Rogue (unauthorized) DHCP Servers
- DHCP Exhaustion Attacks (denial-of-service for legitimate clients)
- DHCP Snooping Evasion (bypass snooping mechanisms)
- DHCP Message Tampering (manipulate messages for unauthorized access or traffic redirection)
- Unauthorized DHCP Options (distribute malicious configurations or redirect traffic)

DHCP Security Considerations

Disaster & Human Error Defences

- Geographic Provisioning of DHCP against natural & unnatural Disasters (earthquakes, hurricanes, floods, terrorist attacks, acts of war)
- Periodic User Trainings & Communication
- Roles & Responsibilities clearly enumerated and understood
- Change Control Meetings among relevant Stakeholders
- IPAM System to identify & correct potential Config. Errors
- Audit Logging to enable Review

DHCP Security Considerations

Hardware & Operating System

- Physical Access (unplug, disconnect, console access)
- Updates & Patches for known Vulnerabilities (OS & Service)
- Protect Control Channel from unauthorized Access
- Permissions to Servers, Directories & Files containing DHCP Config.
- Monitoring of Logs (OS & Service)

DHCP Security Considerations

DHCP Monitoring

- Monitoring of the Service itself
  (status, version, patch level, connectivity, utilisation, probe, failover, etc.)
- Syncing Logs into Security Management Platform
  (further Investigation of single and groups of DHCP requests)

DHCP Security Considerations

DHCP Configuration

- Host Declaration (known & unknown clients)
- Class-based Address Allocation (user, vendor, vendor-specific, fingerprint)
- Zone Declaration for direct dynamic DNS Updates
- OMAPI Port & Key (if used)
- Monitoring of Configuration Changes

DHCP Security Considerations

First-Hop Security

- DHCP Snooping validates & filters `DHCPOFFER`/`DHCPACK`/`DHCPNAK` Messages from untrusted Sources
- IP Source Guard validates & filters Sources of DHCP Client Traffic
- DHCPv6 Guard blocks `Reply`/`Advertisement` Messages from unauthorized Servers and Relay Agents
- RA Guard blocks or rejects unwanted or rogue Router Advertisements
- Integration with NAC can enforce Policies and ensure Compliance for authorized Devices

DHCP Security Considerations

DHCP Fingerprinting

- Identify and categorize Network Devices based on unique Set of DHCP Options requested
- Recognize Device Type without manual Intervention
- Apply Security Policies based on Device Type
- Permit or deny Network Access to Devices based on NAC Integration
- Backtrack Network Activity to specific Device Types in forensic Analysis

DHCP Security Considerations

DHCP Lease Policy

- Define Lease Times based on Network Size, Device Turnover and Usage Patterns
- Aggressive Renewal Times for mobile/transient Devices to ensure frequent Check-ins & Policy Compliance
- Utilize reserved Leases for critical Infrastructure to guarantee Availability & consistent Network Configuration
- Plan for DHCP Failover Scenarios to maintain Service Continuity
- Purge unused Leases to reclaim IP Addresses and reduce the Chance of IP Conflicts
- Ensure Lease Assignments & Renewals are logged for Auditing, Troubleshooting & Security Monitoring

DHCP Security Considerations

DHCP Forensics and Incident Response

- Monitor DHCP Logs for unusual Patterns (rapid lease requests, unexpected lease denials, unexpected MACs)
- Examine DHCP Lease History to identify suspicious Activities (e.g. multiple leases to the same MAC)
- Correlate DHCP Logs with other Security Events (cross-reference DHCP data with other security tools)
- Map IP Addresses to MAC Addresses for Device Identification during an Investigation
- Analyse Lease Timestamps to establish Timelines of Events (understanding sequence of an attack)
- Ensure DHCP Logs are preserved in secure Manner
- Develop Profiles of normal Network Behaviour to identify Anomalies easier

DHCP Security Considerations

Legislation and Compliance

- Ensure DHCP Logs are managed in Compliance with Privacy Regulations that govern Personal Data Handling
- Adhere to Industry Security Standards which require secure Network Systems (e.g. PCI-DSS[1])
- Follow Cybersecurity Frameworks like NIST[2] Guidelines
- Periodic Assessments of DHCP Configurations to ensure ongoing Compliance
- Have an Incident Response Plan that includes DHCP-related Breaches (e.g. CIRCIA[3])
- Integrate DHCP Security into the Risk Management Framework (e.g. ISO/IEC 27001[4])
- Ensure DHCP Practices meet Requirements of international Regulations (e.g. ITU-T X-series[5])

[1] Payment Card Industry Data Security Standard
[2] National Institute of Standards and Technology
[3] Cyber Incident Reporting for Critical Infrastructure Act
[4] International Organization for Standardization and International Electrotechnical Commission
[5] Telecommunication Standardization Sector of the International Telecommunication Union

DHCP Security Considerations

Authentication

- Authentication Option[1] for DHCP Messages (RFC 3118)
- Authenticate Identity of DHCP Participants
- Verify that Content of DHCP Message hasn't been changed during Delivery
- Backward Compatibility with existing Clients, Servers & Relay Agents
- Authentication via Kerberos, Token (plain text) or shared Secret (per client)
- DHCP Server and Relay Agent Authentication Suboption (RFC 4030)

[1] https://kb.isc.org/docs/aa-01323

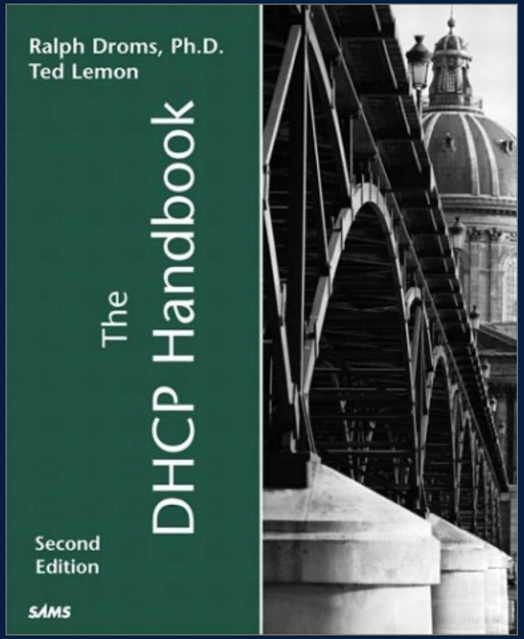
DHCP Security Considerations

DHCPv6 Security

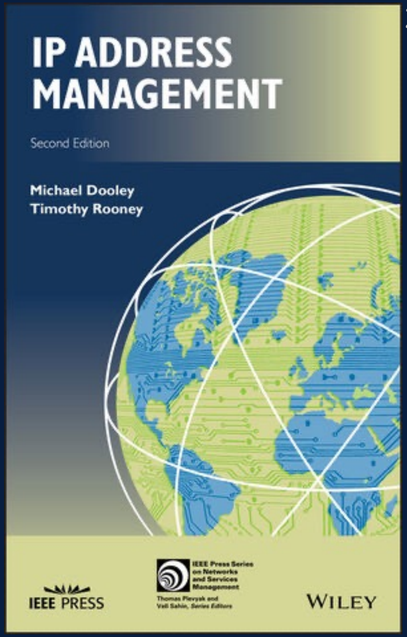
- DHCPv6 Security Considerations (RFC 8415 Section 22)
- IETF Draft for end-to-end Encryption of DHCPv6[1]

[1] https://datatracker.ietf.org/doc/html/draft-ietf-dhc-sedhcpv6-21

Greedy for more?



[1]



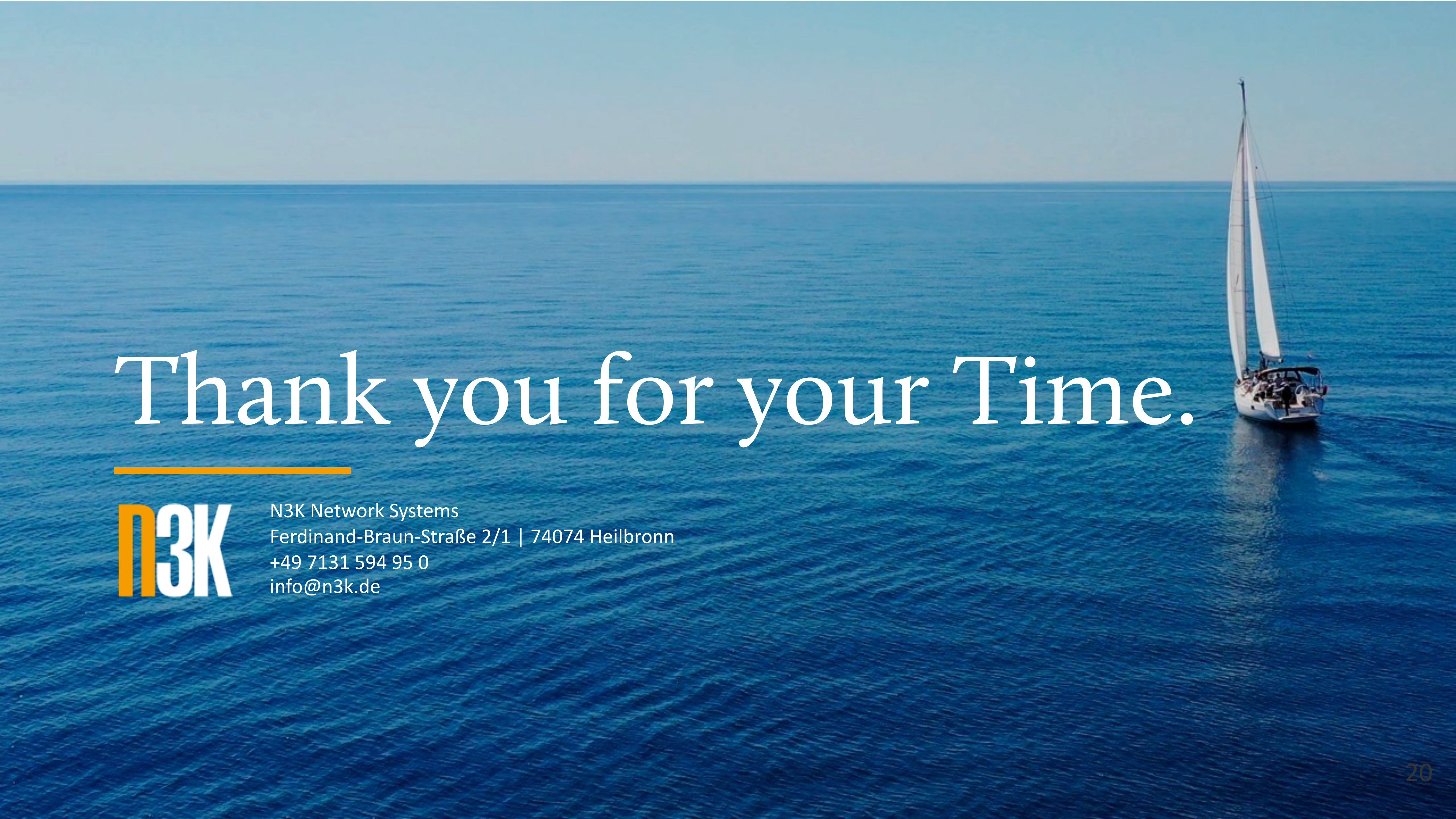
[2]

[3]

[1] https://www.pearson.ch/Informatik/SamsPublishing/EAN/9780672323270/DHCP-Handbook-The
[2] https://www.wiley.com/en-us/IP+Address+Management,+2nd+Edition-p-9781119692270
[3] https://www.n3k.com/experten-webinar-reihe-mit-andreas-taudte-mr-ddi

What’s next?

> *Thank You for Your Participation!*
>
> *Looking forward to more exciting Webinars in 2024.*



Thank you for your Time.

N3K Network Systems
Ferdinand-Braun-Straße 2/1 | 74074 Heilbronn
+49 7131 594 95 0
info@n3k.de