IPv6 Intrusion Detection Research Project

Carsten Rossenhövel, EANTC AG

Sven Schindler, Universität Potsdam

Co-Financed By:

Bundesministerium
für Bildung
und Forschung

Project Goals

Independently assess the true, current risks of IPv6 attacks

Develop intrusion detection tools for IPv6

Assess the readiness of commercial firewalls to cope with intrusion attempts

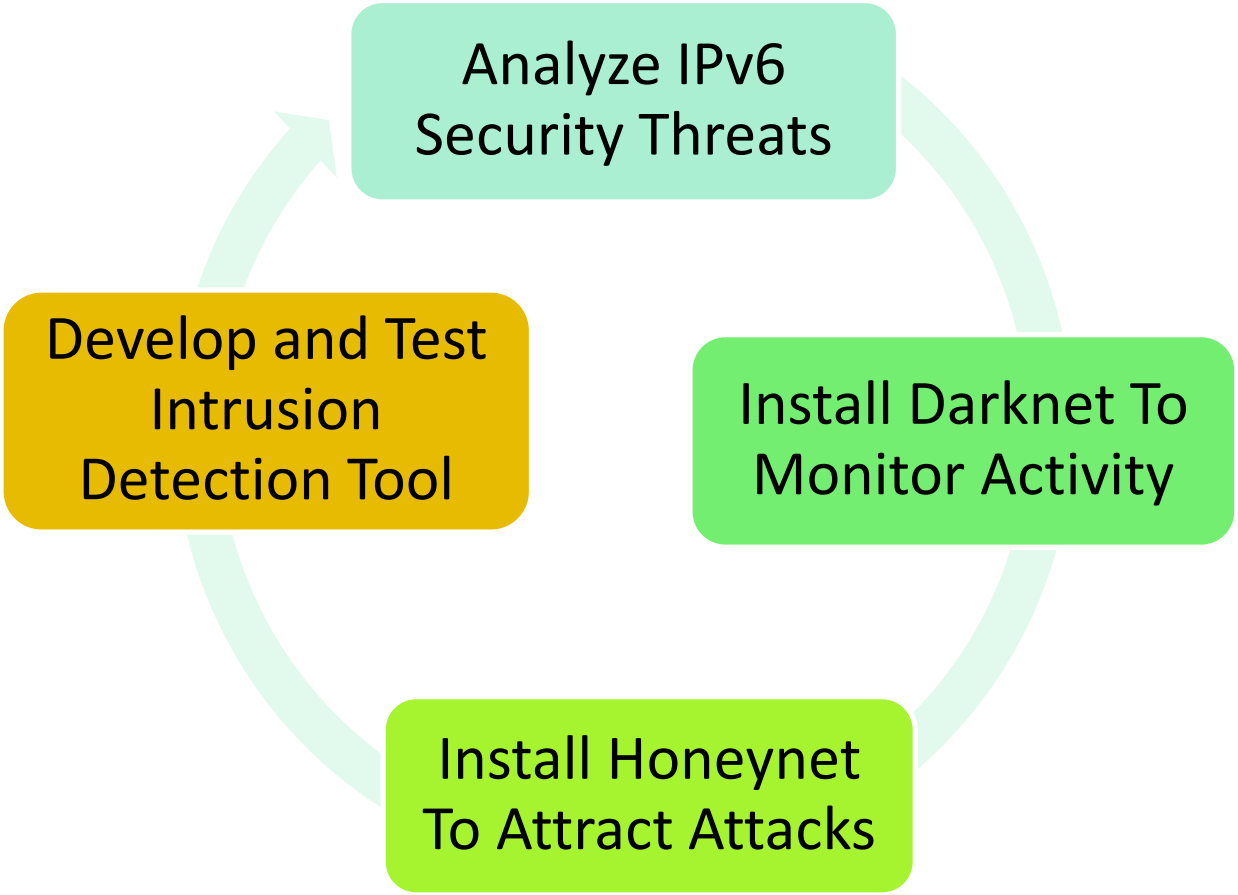
Jointly conducted by Beuth University of Applied Sciences, Berlin; University of Potsdam; Strato AG and EANTC AG.

Co-funded by German Federal Ministry of Education and Research

Testing and Consultancy services for the service provider network life cycle

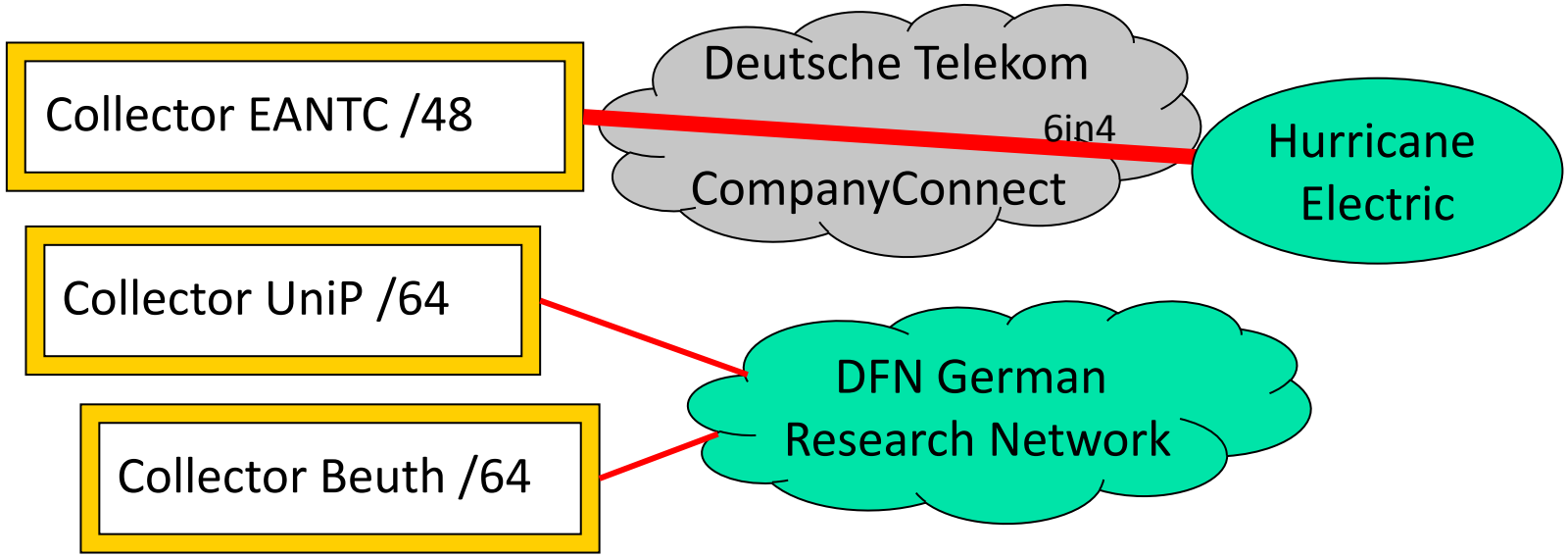
- Network design consultancy and proof of concept testing
- RfP support, acceptance testing and network audits
- Vendor neutral technology seminars

Project Steps 2011-2013



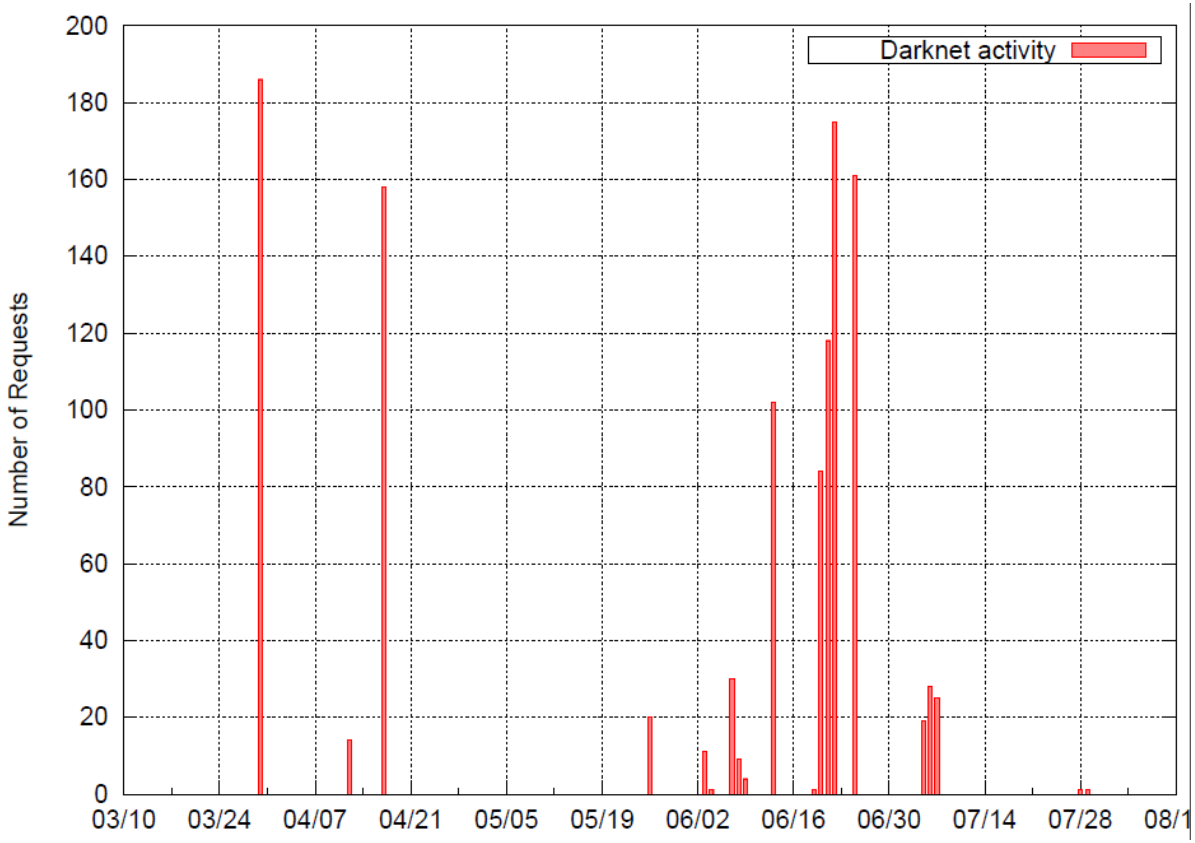
IPv6 Darknet

- Live since February 2012, 99.90 % availability
- Set up two directly attached darknets, one via tunnel broker
- Completely passive – no routes announced; darknet did not respond in any case
- Should receive only backscatter traffic or attacks



IPv6 Darknet Results

- Received only 1,145 packets in five months!
- Mostly TCP backscatter (SYN/ACK-bits set)
- No ICMP or DNS requests
- Example: 186 backscatter packets arrived from one IRC server in Cape Town – probably a victim of a DDOS attack



IPv6 Darknet Results (2)

- How to crawl address spaces in IPv6?
  - Incremental address search infeasible in IPv6
  - Possible solution: Distribute new prefix for IPv6 address autoconfiguration, triggering Duplicate Address Detection responses
  - Possible solution: Send ICMPv6-echo request to the AllNodes multicast group
- No attacker used smart methods like the above;
  Result matched expectations

- With advertised routes, things change:
  Sandia.gov received 70 packets/s on a /12 darknet in 2012
  http://www.caida.org/workshops/dust/1205/slides/dust1205_cdeccio.pdf

IPv6 Honeynet (*honeydv6*)

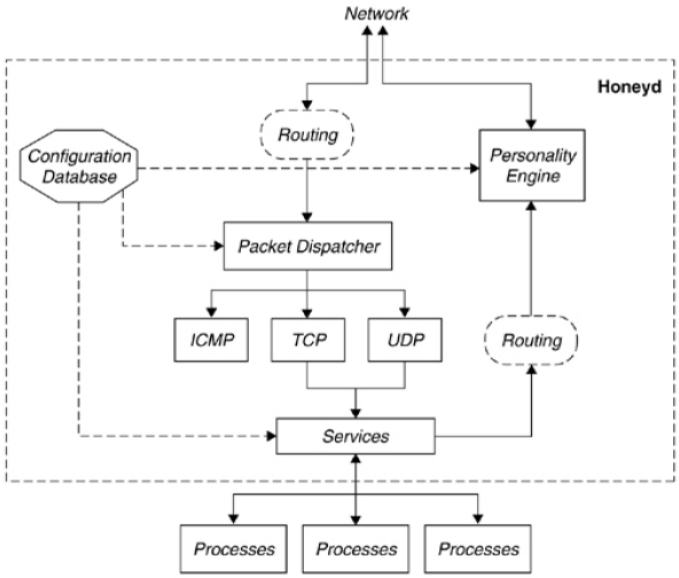
- Project team extended low-interaction open source *honeyd* to support IPv6 (original author: Niels Provos)

What is standard *honeyd*?

- Emulates a complete network
- Uses nmap fingerprints to mimic a range of operating systems
- Captures packets via *pcap* library

We:

- Added IPv6 extension header, fragmentation, ICMPv6 support



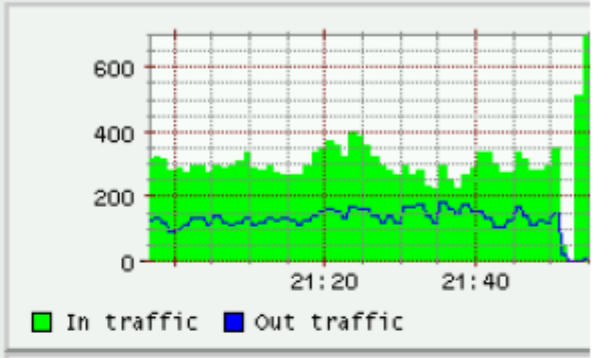
Honeyd Administration Interface

Welcome to the Honeyd Administration Interface.You are visitor 4.

Interface Information

This table shows the interface that Honeyd has been configured to listen to.

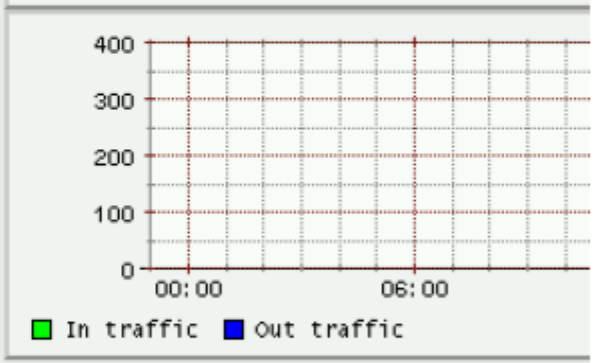
Name	Address	MTU	Link Address
em1	192.168.2.101	1500	08:00:27:39:ee:f0



Honeyd Statistics

This table shows current statistics collected by Honeyd.

Variable	Minute	Hour	Day
Output Bytes	148.75 B/s	0.00 B/s	0.00 B/s
Input Bytes	343.43 B/s	0.00 B/s	0.00 B/s



Active TCP Connections

This table shows the currently active TCP connections

Src IP	Src Port	Dst IP	Dst Port	Received	Sent	Op
2001:db8::3	60907	2001:db8::6	23	66	1030	⊗
2001:db8::3	41194	2001:db8::5	23	67	1031	⊗

Honeyd Test with OpenVAS

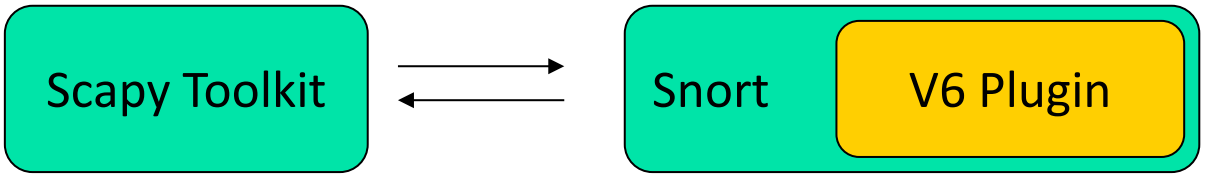
We validated the implementation with OpenVAS (free vulnerability assessment tool)
Honeydv6 detects all newly introduced attacks

Next: Install honeyd at large-scale data center site of the associated project partner (www.strato.de)

Security Issues for Host 2001:db8:1:0:a00:27ff:fe0c:8131

Low NVT: Checks for open tcp ports (OID: 1.3.6.1.4.1.25623.1.0.900239)	general/tcp
Open TCP ports are 22	
Low NVT: Services (OID: 1.3.6.1.4.1.25623.1.0.10330)	ssh (22/tcp)
An ssh server is running on this port	
Low NVT: SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)	ssh (22/tcp)
Remote SSH version : SSH-2.0-OpenSSH_5.5p1 Debian-4ubuntu5 Remote SSH supported authentication : publickey,password	
Low NVT: SSH Protocol Versions Supported (OID: 1.3.6.1.4.1.25623.1.0.100259)	ssh (22/tcp)
Overview: The remote SSH Server supports the following SSH Protocol Versions: 1.99 2.0 SSHv2 Fingerprint: db:1b:d1:ad:b1:11:bc:5c:27:a4:9c:27:c6:7e:35:66 Risk factor : None	

Development of New/Extended IPv6 Attacks



- Open source flexible packet generation toolkit for IPv4/IPv6 packets with arbitrary headers
- Project created GUI to simplify Scapy use without programming knowledge

- Open source intrusion detection tool
- Project extended it for special IPv6 attacks detection beyond trivial basics

The Hacker‘s Choice (THC) IPv6 Attack Toolkit

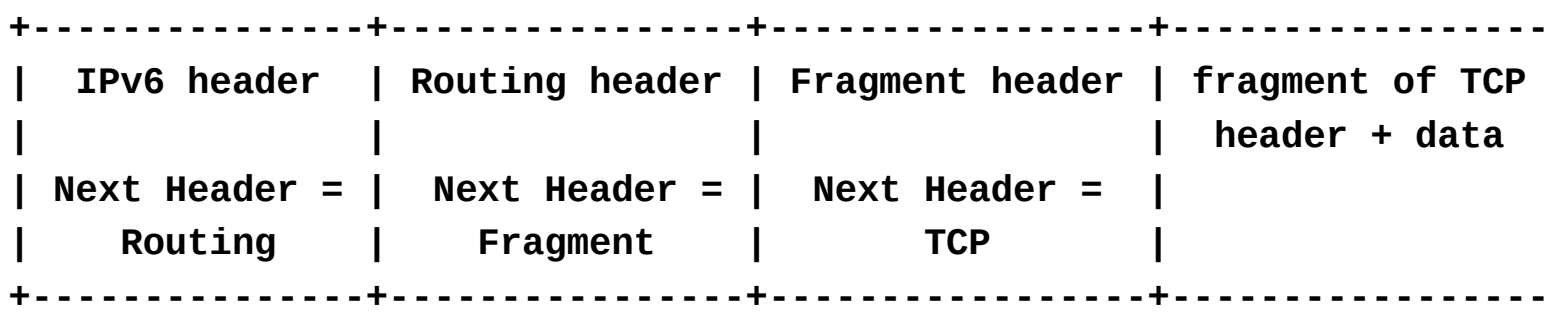
Project based IPv6 attacks on THC‘s tool

- Tools/Attacks/Test Suite initiated by van Hauser
- **Parasite6**: icmp neighbor solicitation/advertisement spoofer
- **Fake_router6:** Announce yourself as a router with the highest priority
- **dos-new-ipv6**: Detect new IPv6 devices and tell them that their chosen IP collides on the network
- **Flood-router6:** Flood a target with random router advertisements
- …

http://thc.org/thc-ipv6/

IPv6 Extension Headers

- IPv6 extension headers are a source of potential attacks
- Variety and complexity challenging for any implementation
- Some headers are to be inspected on each hop, some only at destination

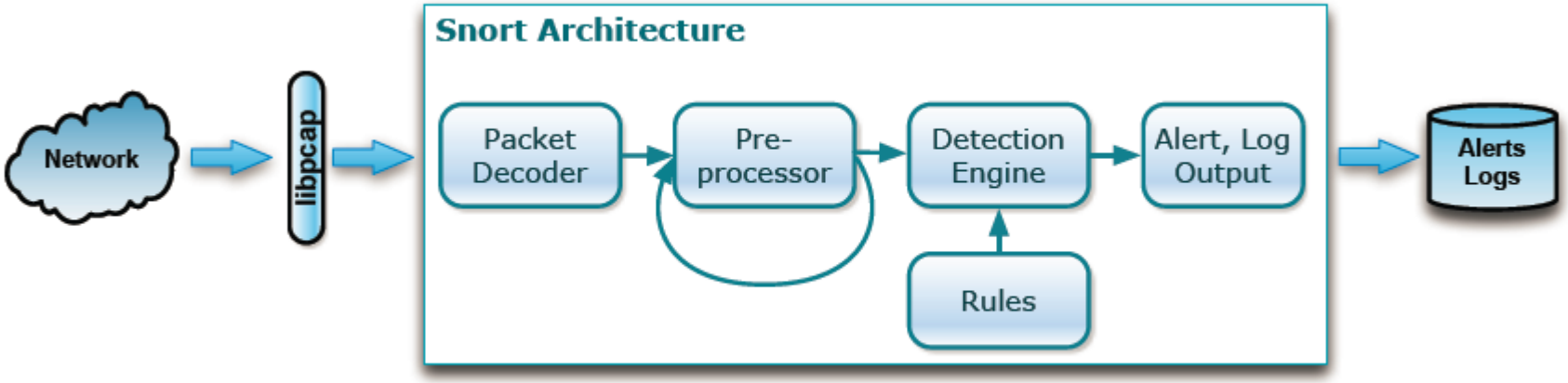


Hop-by-Hop and Destination Options

- Router Alert – RFC 2711
- Padding – Pad1, PadN
- „IPv6 Jumbograms”– RFC 2675
- Tunnel Encapsulation Limit – RFC 2473
- IP Mobility – Home Address – RFC 6275

- Action to take when option is not recognized is encoded in the option type.

Detection of Attacks With Snort



- Free lightweight network intrusion detection system
- Open source; rulesets maintained by Sourcefire
- IPv6 extensions available at http://www.idsv6.de

Attacks Included in Test Plan

1. ICMPv6 Filtering
2. Type 0 Routing Header
3. IPv6 Header Chain Inspection
4. Overlapping IPv6 Fragments
5. Tiny IPv6 Fragments
6. Excessive Hop-by-Hop Option
7. PadN Covert Channel
8. Address Scopes
9. Spoofed Neighbor Discovery
10. Duplicate Address Detection
11. Spoofed Redirect Message
12. Spoofed Zero-Lifetime Router Advertisement Message
13. Router Advertisements Flooding
14. Neighbor Advertisements Flooding

Outlook

- Project nears completion
- Honeydv6 evaluation pending
- Project partners in the process of publishing tools (under GPL) to ease attack testing for SPs and enterprises
- EANTC is going to publish an open source IPv6 firewall test plan with functional attacks and performance test cases
- EANTC may publish firewall test results in the future

Thank You For Your Interest!

For further information, please contact us:

EANTC AG
Salzufer 14
D-10587 Berlin
Germany

Phone: +49.30.318 05 95-0
Fax: +49.30.318 05 95-10
E-mail: info@eantc.de
www.eantc.de