ERNW
Living Security.

Burning Asgard – An Introduction to the Tool *Loki*

Rene Graf, Daniel Mende, Enno Rey
{rgraf, dmende, erey}@ernw.de

Who we are

- **Old-school network geeks.**
- **Working as security researchers for Germany based ERNW GmbH.**
- **Fiddling around with devices and protocols makes the majority of our days.**

Some of our colleagues at this year's TROOPERS

ERNW GmbH

- **Heidelberg based security consulting and assessment company with currently 18 employees (as of july 2010).**
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate
- **Blog: www.insinuator.net**
- **Conference: www.troopers.de**

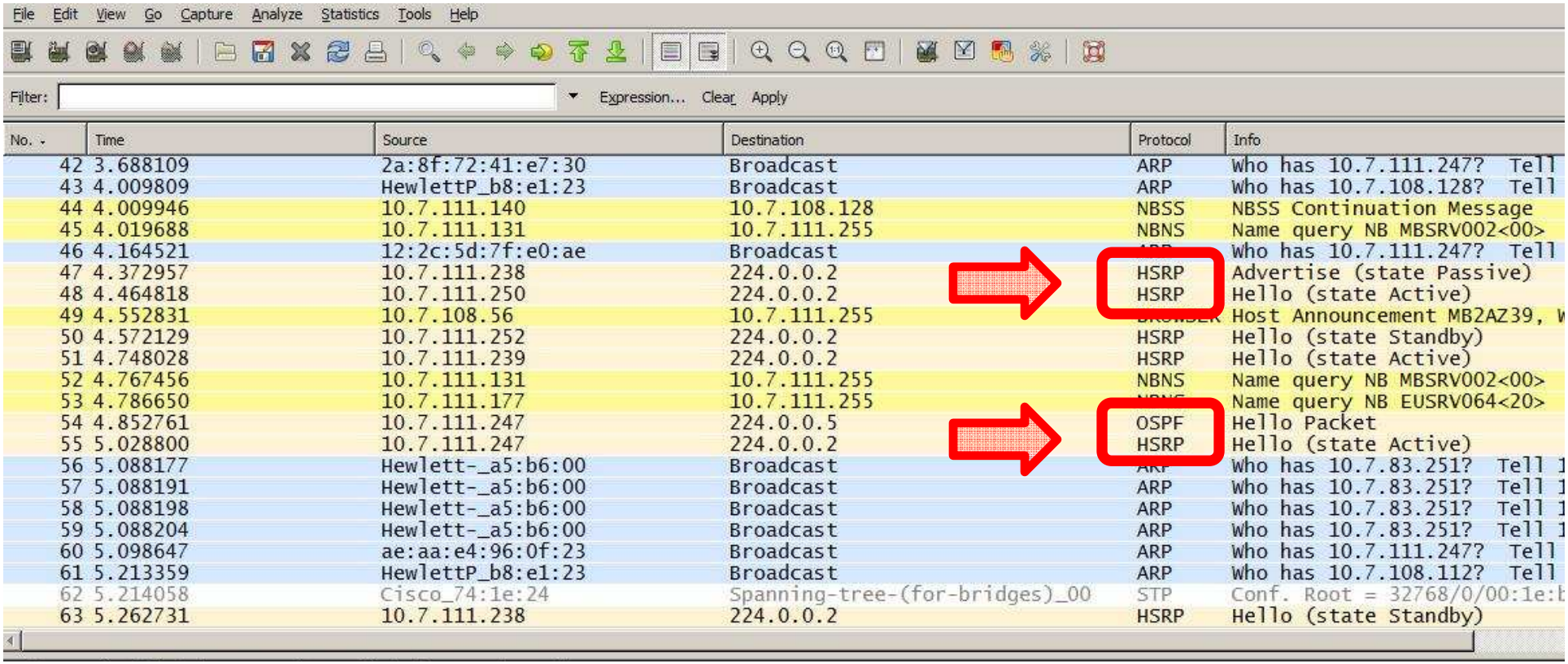
Agenda

ERNW Living Security.

- **Why LOKI** 
- **The Tool** 
- **Advanced Stuff** 

What do you see here?

ERNW Living Security.

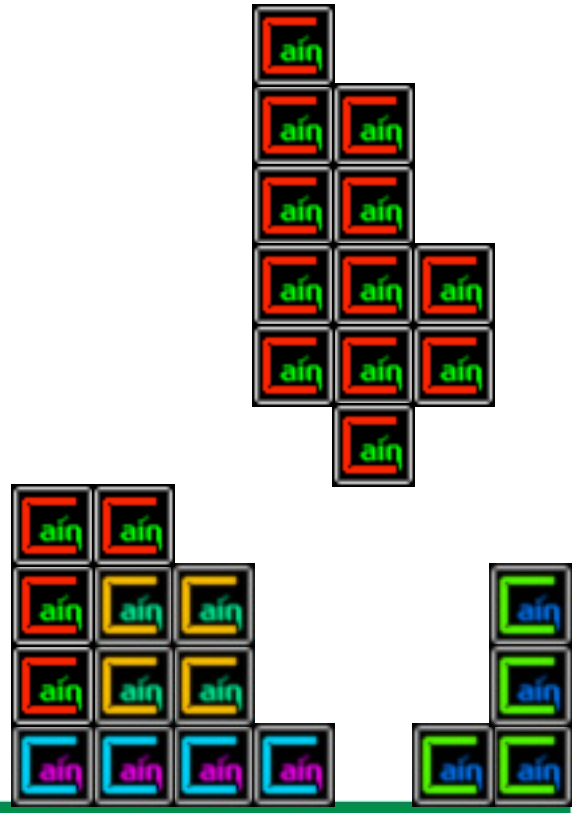


No.	Time	Source	Destination	Protocol	Info
42	3.688109	2a:8f:72:41:e7:30	Broadcast	ARP	Who has 10.7.111.247? Tell
43	4.009809	HewlettP_b8:e1:23	Broadcast	ARP	Who has 10.7.108.128? Tell
44	4.009946	10.7.111.140	10.7.108.128	NBSS	NBSS Continuation Message
45	4.019688	10.7.111.131	10.7.111.255	NBNS	Name query NB MBSRV002<00>
46	4.164521	12:2c:5d:7f:e0:ae	Broadcast	ARP	Who has 10.7.111.247? Tell
47	4.372957	10.7.111.238	224.0.0.2	HSRP	Advertise (state Passive)
48	4.464818	10.7.111.250	224.0.0.2	HSRP	Hello (state Active)
49	4.552831	10.7.108.56	10.7.111.255	BROWSER	Host Announcement MB2AZ39, W
50	4.572129	10.7.111.252	224.0.0.2	HSRP	Hello (state Standby)
51	4.748028	10.7.111.239	224.0.0.2	HSRP	Hello (state Active)
52	4.767456	10.7.111.131	10.7.111.255	NBNS	Name query NB MBSRV002<00>
53	4.786650	10.7.111.177	10.7.111.255	NBNS	Name query NB EUSRV064<20>
54	4.852761	10.7.111.247	224.0.0.5	OSPF	Hello Packet
55	5.028800	10.7.111.247	224.0.0.2	HSRP	Hello (state Active)
56	5.088177	Hewlett-_a5:b6:00	Broadcast	ARP	Who has 10.7.83.251? Tell 1
57	5.088191	Hewlett-_a5:b6:00	Broadcast	ARP	Who has 10.7.83.251? Tell 1
58	5.088198	Hewlett-_a5:b6:00	Broadcast	ARP	Who has 10.7.83.251? Tell 1
59	5.088204	Hewlett-_a5:b6:00	Broadcast	ARP	Who has 10.7.83.251? Tell 1
60	5.098647	ae:aa:e4:96:0f:23	Broadcast	ARP	Who has 10.7.111.247? Tell
61	5.213359	HewlettP_b8:e1:23	Broadcast	ARP	Who has 10.7.108.112? Tell
62	5.214058	Cisco_74:1e:24	Spanning-tree-(for-bridges)_00	STP	Conf. Root = 32768/0/00:1e:b
63	5.262731	10.7.111.238	224.0.0.2	HSRP	Hello (state Standby)

Now…

ERNW Living Security.

- **This ends up in sec_assessment-reports like “can theoretically be attacked, should be cured”.**
- **Is it going to be cured?**
- **Well… it’s only theoretical, isn’t it?**



Do we need a game changer again?

ERNW Living Security.

- **Would they care (more) if it wasn't just theoretical? ;-)**
- **Did *Cain&Abel* change the way "theoretical vulnerabilities" were perceived?**
- **Sure, it did…**

Here comes…

ERNW
Living Security.

For completeness' sake

ERNW Living Security.

- **What's currently out there**
  - *IRPAS* (only "discovery" for routing protocols)
  - *Yersinia* (mainly Layer 2)
  - *Hping*
  - *Nemesis* (OSPF module was never implemented)
  - *Scapy* (very powerful, still requires quite some $PROT knowledge)

Back on track

ERNW Living Security.

- **What does LOKI provide?**

- **GUI**
- **Written in Python**
- **Modular architecture**
- **Lots of protocols implemented (already) that none of the other tools have.**

- **Also a new version of the *mplstun* is included.**

LOKI – Overview / Introduction

ERNW Living Security.

- **Architecture**
- **(Main) Modules**
- **GUI**

Loki as depicted on an
18th century Icelandic manuscript
© Wikipedia

Architecture

ERNW Living Security.

The main program:

- **The module API**
- **Library extensions**

Legerdemains *LOKI* has learned so far

ERNW Living Security.

- **Protocols**
  - ARP
  - HSRP, HSRPv2
  - RIP
  - BGP
  - OSPF
  - EIGRP [not-yet-to-be-released due to legal blur]
  - WLCCP [not-yet-to-be-released due to legal blur]
  - VRRP, VRRPv3
  - BFD
  - LDP
  - MPLS (re-labeling, tunnel interface)

Attacks

ERNW Living Security.

- **Attacks implemented so far**
  - ARP
    - Arp spoofing
    - Arp scanning
    - Arp flooding
  - BFD
    - DoS of existing BFD session
  - BGP
    - NLRI injection
  - EIGRP
    - EIGRP TLV injection
    - Authenticated / Unauthenticated DoS
  - HSRP, HSRPv2
    - IP address take-over

Attacks – 2

ERNW Living Security.

- **Attacks implemented so far [cont]**
  - LDP
    - Injection of label mapping messages
  - MPLS
    - Rewrite of MPLS labels
    - MPLS-VPN enabled network stack
  - OSPF
    - Injection of LSAs
    - MD5 authentication cracking
  - RIP
    - Route injection
  - TCP-MD5
    - RFC2385 authentication cracking

Attacks – 3

- **Attacks implemented so far [cont]**
  - VRRP, VRRPv3
    - IP Address take-over
  - WLCCP
    - Winning the WDS master election
    - Sniffing and cracking of infrastructure authentication (asleap)
    - Sniffing and generating of CTK nonce and key
    - Sniffing and decryption of client PMK

GUI

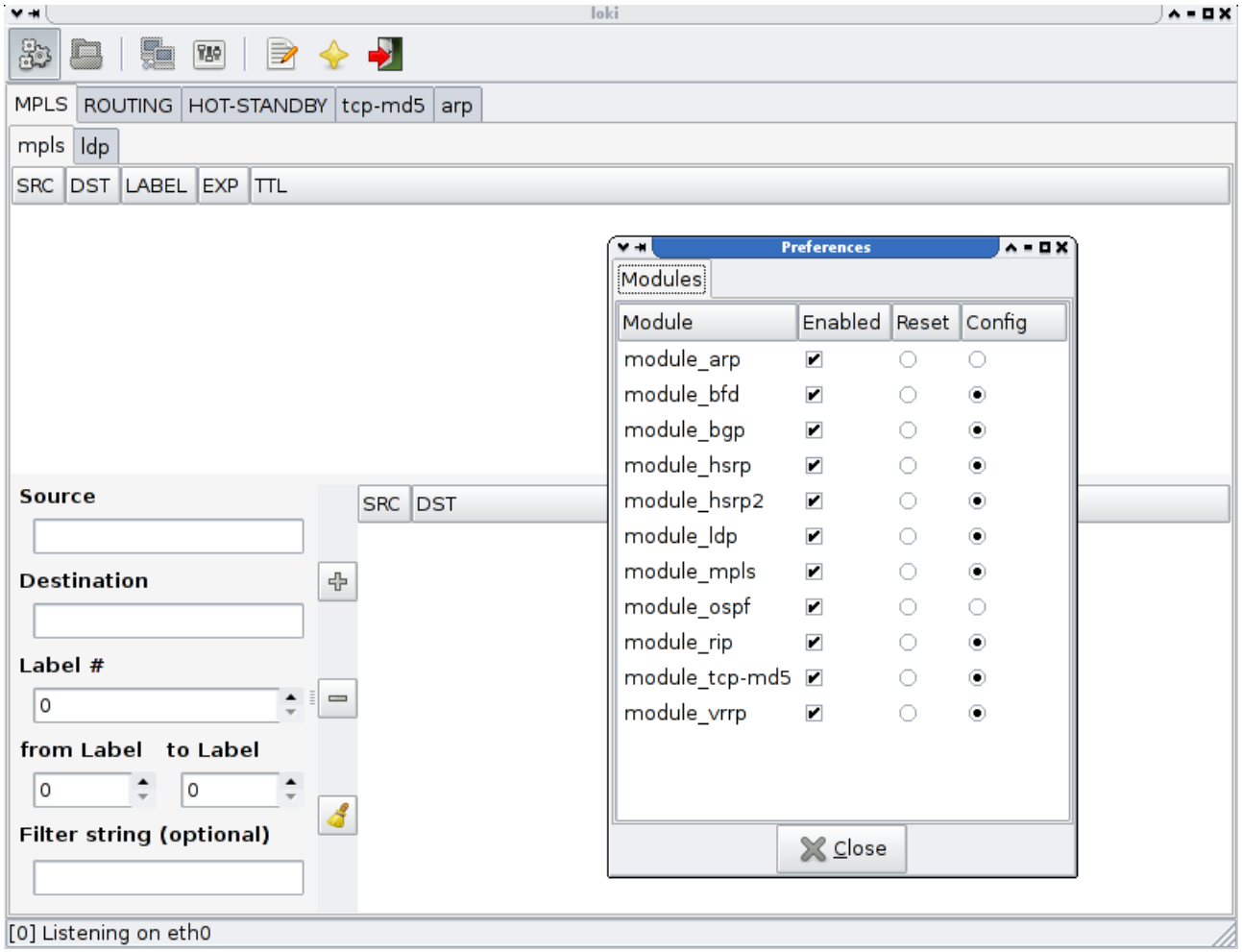
ERNW Living Security.

- **Based upon GTK.**
- **Main program implements main- and preference window.**
- **Module GUIs based on GLADE files and are parsed on load.**

With the increasing adoption of Macs, we thought a GUI might me a good idea ;)

GUI

ERNW Living Security.



Ok, so what can we do with it?

ERNW Living Security.

- **Simple answer: attack infrastructure protocols ;-)**
- **To give you an idea, some short discussion of attacks against routing protocols.**

Routing protocols

ERNW Living Security.

- **Different flavors**
  - Interior gateway protocols (“within an AS”)
    - RIP, EIGRP, OSPF, IS-IS
  - Exterior gateway protocols (“between different ASs”)
    - BGP
- **Different ways to perform their work**
  - Distance vector protocols
    - RIP, EIGRP
  - Link state protocols
    - OSPF, IS-IS
  - Path vector protocols
    - BGP

Attacking routing protocols

- **In the past quite some discussion of attacks against BGP**
  - DEF CON 2008 (Kapela/Pilosov)
  - Black Hat Europe 2009 (Mende/Rey)
    - See: http://www.ernw.de/content/e7/e181/e1309/download1357/ERNW_BlackHatEurope09_all_your_packets_ger.pdf
  - Youtube / Pakistan incident
  - China Telecom incident (March 2010)

- **Not too much discussion of attacks against IGPs**
  - RFC 4593 (Oct 2006) *Generic Threats to Routing Protocols*
  - IETF Draft (Jun 2006) on *OSPF Security Vulnerabilities Analysis*
  - Presentation (Roecher/Auffret) at IT Underground 2007
    - See: http://www.ernw.de/content/e7/e181/e520/download523/ospf-sec_02_dr_ger.pdf
  - IETF working group on *RPSec* concluded work some time ago.

Attacking IGPs – Impact

ERNW Living Security.

- **RFC 4593:**

  "We assume that the most common goal of an adversary deliberately attacking routing is to cause inter-domain routing to malfunction. A routing malfunction affects data transmission such that traffic follows a path […] other than one that would have been computed by the routing protocol if it were operating properly[…]
  As a result of an attack, a route may terminate at a router other than the one that legitimately represents the destination address of the traffic, or it may traverse routers other than those that it would otherwise have traversed. In either case, a routing malfunction may allow an adversary to wiretap traffic passively, or to engage in man-in-the-middle (MITM) active attacks, including discarding traffic (denial of service)."

- **So it's basically about**
  - Large scale traffic redirection/interception
  - Denial-of-Service

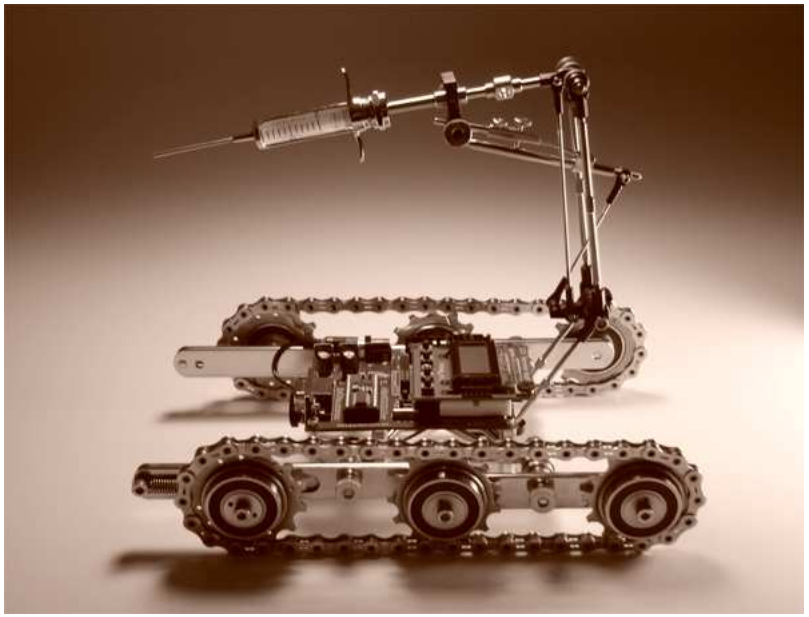
OSPF – Route Injection

ERNW Living Security.

- ***Open Shortest Path First***
- **Most widely deployed routing protocol in large networks**
- **Link state protocol (“tell world about neighbors”)**

- **Impact of route injection might depend on exact design/config.**

- **Has some built-in protection (“OSPF fight back”). Which does *not* protect against attackers (only against misconfig).**



EIGRP – Route Injection

ERNW Living Security.

- ***Enhanced Interior Gateway Routing Protocol***
- **Distance Vector Protocol ("tell neighbors about world")**
- **Cisco proprietary**
  - Hence our concerns as for release of the module.
- **Quite some deployment in enterprise networks ("Cisco shops")**
  - Mostly "fire+forget" implementations.
- **Some security discussion back in 2005.**
  - Nothing more happened since then as for EIGRP attacks.

OSPF – Attacking Authentication

ERNW Living Security.

- **MD5 key based authentication part of standard.**
- **Some cleartext auth variants can be found (Windows 2KSRV…)**
- **Overall good protection… if deployed correctly**
  - We know one very large corporate network with OSPF key "*highsecure*"…

- **Can be attacked/cracked… ;-)**

DEMO

Mitigating Controls

ERNW Living Security.

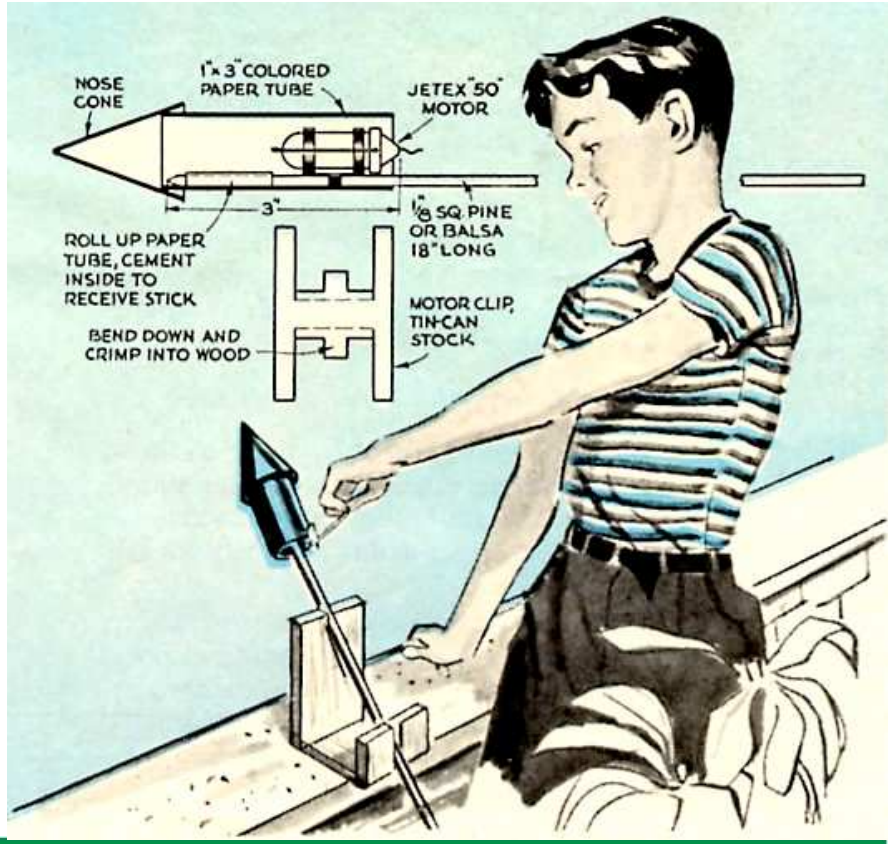
Category	Mitigating Control	Security Benefit	Operational Feasibility
Access Control	Authentication (MD5)	5	3
	Static Peers	4	2
	Passive-Interfaces	3	5
Isolation	Different RPs	2	1
	Routing config	2	2
Restriction	Route filtering	2	1
	IP based (peer) filtering	3	2
Encryption	IPsec for $RP traffic	5	1
Visibility (monitoring & logging/log-analysis)	Logging of adjacency changes	2	2

Going with (only) authentication and *passive-interfaces* provides “good enough security” for <u>most</u> networks!

You can contact us for config templates…

ERNW
Living Security.

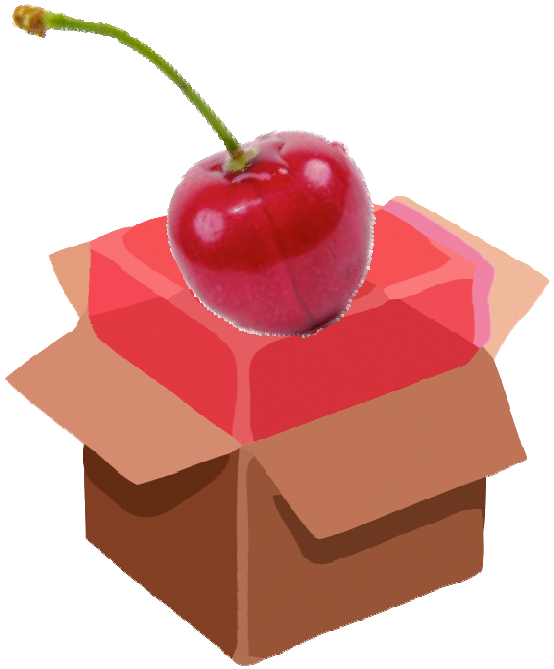
Advanced Stuff



Some more sophisticated modules

ERNW Living Security.

- **VRRP**
- **BFD**
- **LDP**



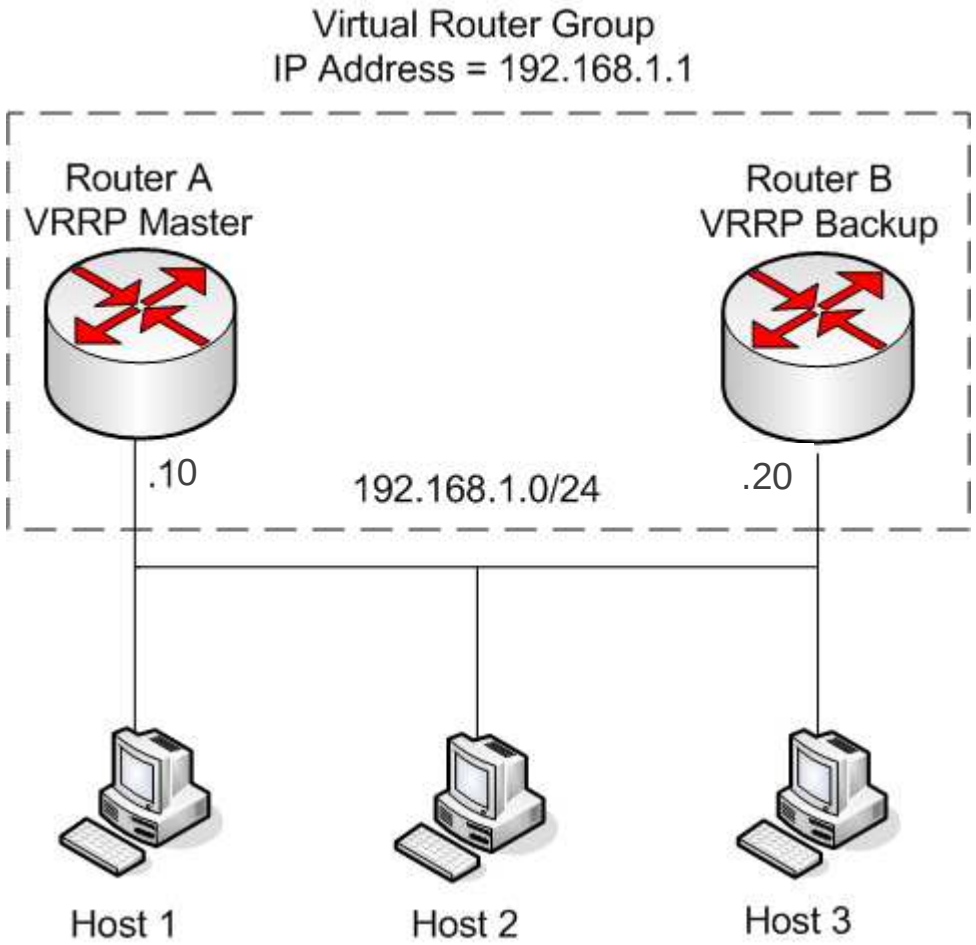
VRRP – Overview

ERNW Living Security.

- **“First hop redundancy protocol”**
  - Standardized (in contrast to Cisco-proprietary *HSRP*)
  - First described in RFC 2338, updated in RFC 3678.
  - In the interim (IPv6 capable) VRRPv3, specified in RFC 5798.

- **Initially gained some ground in *Firewall-1_on_Nokia_boxes* deployments some years ago.**

VRRP overview



VRRP – Some additional notes

ERNW Living Security.

- **From RFC3768:**

  The priority field specifies the sending VRRP router's priority for the virtual router. Higher values equal higher priority. This field is an 8 bit unsigned integer field.

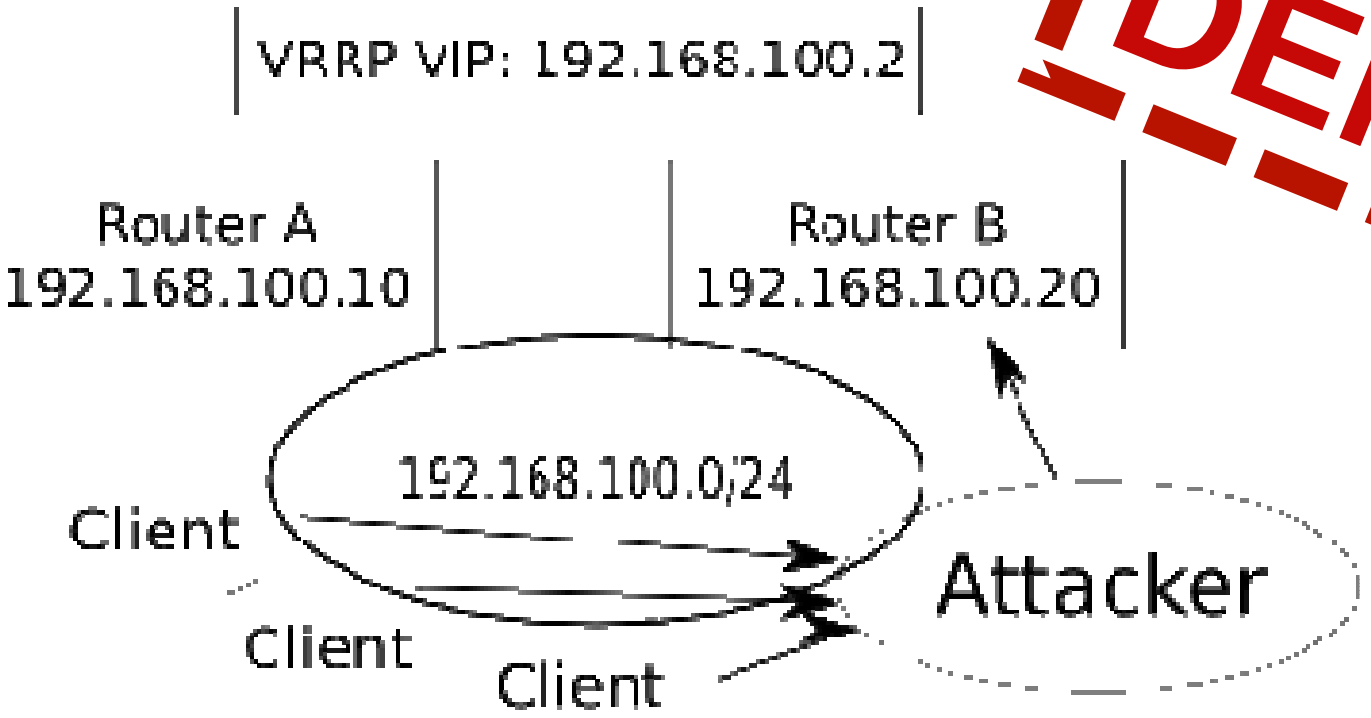
  The priority value for the VRRP router that owns the IP address(es) associated with the virtual router MUST be 255 (decimal).

→ **a priority of 255 is not available (at least on Cisco devices)…**

- **Really? ;-))**

Demo

ERNW Living Security.



Mitigating Controls – Remarks

ERNW Living Security.

- **VRRP Auth**
  - From RFC3768:

    VRRP does not currently include any type of authentication. Earlier versions of the VRRP specification included several types of authentication ranging from none to strong. Operational experience and further analysis determined that these did not provide any real measure of security.

BFD – How it works

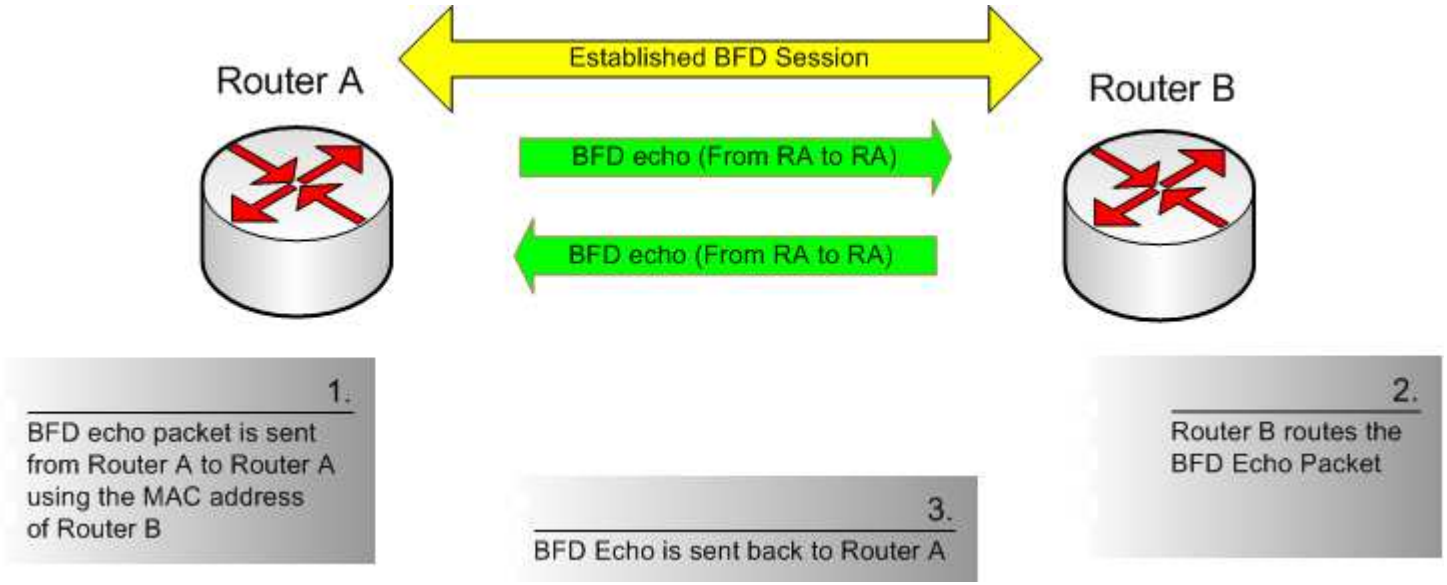
- **From RFC5882:**

  The Bidirectional Forwarding Detection protocol provides a liveness detection mechanism that can be utilized by other network components for which their integral liveness mechanisms are either too slow, inappropriate, or nonexistent.

- **Yet another keep alive mechanism**
- **Uses IP and UDP (on port 4784) for transport.**

- **Provides failover detection in about 100ms.**

BFD


Router A
Established BFD Session
Router B
BFD echo (From RA to RA)
BFD echo (From RA to RA)
1.
BFD echo packet is sent from Router A to Router A using the MAC address of Router B
2.
Router B routes the BFD Echo Packet
3.
BFD Echo is sent back to Router A

LOKI is “work in progress”

ERNW Living Security.

- **Upcoming features**
  - ISIS (Intermediate System Intermediate System)
  - GLBP (Gateway Load Balancing Protocol)
  - SNMP – Our SNMP framework will be integrated
- **To complete the suite:**
  - VTP, DTP, STP, DHCP [albeit already present in *yersinia*]
  - Maybe other infrastructure protocols
  - Direct suggestions to: dmende@ernw.de
- **Bug Fixes (of course ;-)**

Ragnarök begins…

ERNW Living Security.

- **LOKI project page**
  - https://c0decafe.de/loki.html
  - After BH also available for download at www.ernw.de
  - Current version: 0.2.4

- **Available as**
  - Source c0de
  - Ubuntu 10.04 (current) packages
  - Gentoo eBuild

Conclusions

ERNW Living Security.

- **There's a new kid in the infrastructure attack block. "From theoretical to practical, once more."**

- **Protect your infrastructure!**

- **When implementing controls, always think about "security benefit vs. operational impact ratio".**
  Do *not* do everything some smart whitepapers tell you / recommend.

- **Go out & write your own *Loki* modules**
  - … and have fun at Black Hat, of course ;-)

There's never enough time…

ERNW Living Security.

THANK YOU…

...for yours!

Credits

ERNW Living Security.

- **Olli for contributing to WLCCP research and module**
- **Flo for all the awesome eye-candy**

Additional Info

ERNW Living Security.

- **Download slides and tools later this day at www.ernw.de**
- **Subscribe to our blog www.insinuator.net**
- **Visit www.troopers.de or follow @WEareTROOPERS to stay up-to-date on TROOPERS conference**

Your next TROOPERS boot camp is scheduled for 14-18 March 2011 @ Heidelberg, Germany.

Final Wisdom

ERNW Living Security.

Whatever you do... always remember the following two:

- **Ross Callon in *RFC 1925*:**

  “Some things in networking can never be fully understood by someone who neither builds commercial networking equipment nor runs an operational network.“

  → If really interested in this stuff get your hands on some devices ;-)

- ***Simplicity Principle* from RFC 3439**