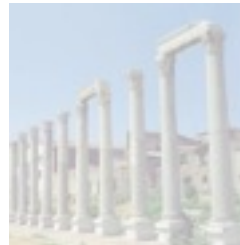


our darknet and its bright spots



building connections for spaces and people



Overview

- Who are we?
- What are we talking about?
- Why should you care?
- Where are we going with this?
- When can I join?

Who are we?

- Eric Michaud - TOOOL US, HacDC, PS:One, hackerspaces.org
- aestetix - OpenAMD/Sputnik, Noisebridge
- mc.fly - ChaosVPN, CCCHH
- equinox - dn42, sublab

The Usual Suspects

- Who do we have here in the audience?

What are we talking about?

- Double fudge cookies?

What are we talking about?

- Double fudge cookies?
- Long walks in the rain?

What are we talking about?

- Double fudge cookies?
- Long walks in the rain?
- Raiding the Saturn with TV-B-Gones?

What are we talking about?

- Double fudge cookies?
- Long walks in the rain?
- Raiding the Saturn with TV-B-Gones?
- Oh right!?! Networks!

What are we talking about?

- NETWORKS!

Why should you care?

- Do you find it hard to connect your friends?
- Test new protocols?
- Your bandwidth being squeezed?
- Just have fun? CTFs?
- Basic Research?

Community is just good.

- It's great to share, it's how we all grow.
- We also stand on the shoulders of giants.

So to sum it up

- We need a way to share with each other.
- Networks are a great way to do this.
- Very little setup and maintenance.
- Free collaboration for everyone involved.

So let's get technical!

Networks Involved

- dn42
- ChaosVPN
- Agora Link (Beta)

Targets and requirements

Our project has several goals:

- Privacy – no one looking in our traffic
- Community – connect with friends
- Availability – solid uptime
- Speed – as fast as possible
- Easy to use – maintenance is simple
- Neighborly – join our friends, block our enemies

Privacy

Some projects aren't ready yet, research takes time!

Community

We want to be able to share ideas and projects with our friends.

Availability

- The network needs to be available.
- The best way to reach that is to avoid single points of failure.
- That means if a node fails not the whole network shall fail.

Speed

A fast paced society demands a fast paced network.

Fast in network terms can be

- Bandwidth

Multimedia requires high bandwidth

- Latency

Voice communication and games require low latency

→ everyone talks to everyone → mesh

Easy to Use

- The network should be easy to configure.
- Nodes should be able to join or leave the network without a sysadmin
- This requires an automated update solution.

Neighborly

- To be with our friends, we need to connect
- Targets are hackerspaces, community zones, clubs, shared apartments...
- Abstracted they can be seen as networks of different sizes.

An idea about solutions

- So we want a mesh based encrypted and authenticated private network that administrates itself.
- Easy right?!?!

Solutions that won't work

- OpenVPN
 - Classical client/server model
 - Centralized

Solutions that won't work

- Tor - The Onion Router
 - Too slow, encryption/decryption at every hop
 - We are not concerned with anonymity within the darknet, as we already trust everyone

Solutions that won't work

- Freenet – Decentralized network
 - mainly focused on anonymity and filesharing
 - Good for filesharing, but what about irc, skype, and new protocols we want to integrate?

Solutions that won't work

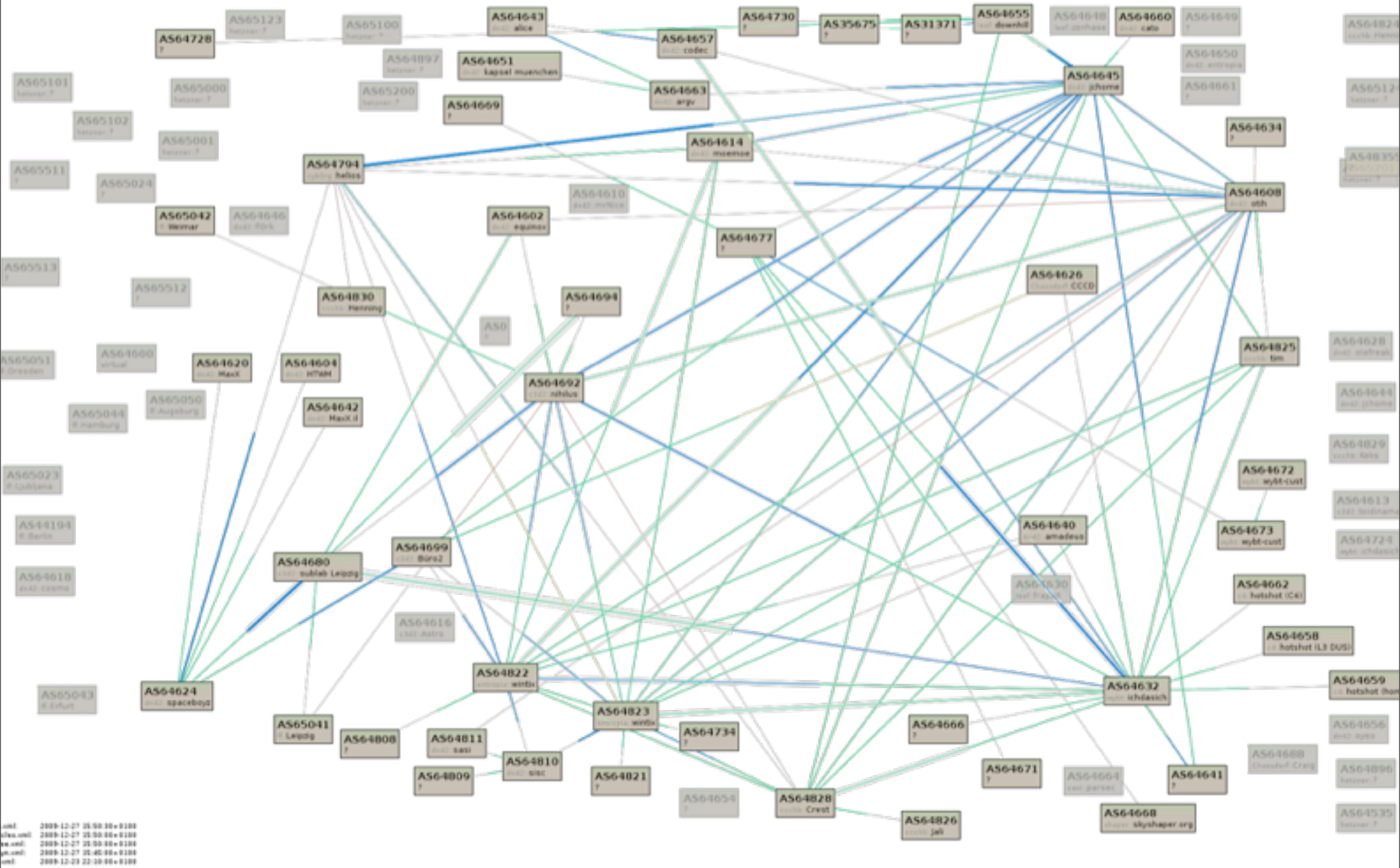
- MRN VPN
 - OpenVPN Server Mode
 - SPOFs, sub-optimal routing
 - unreliable
 - down

the dn42 approach

- “Started as a BGP playground, now it’s being used to connect people”
 - use point to point links
 - openvpn, IPSec, ...
 - put BGP on them, do dynamic routing

shaken, not stirred

- ca. 55 entities on the list
 - that's people and spaces
- 70 IPv4 prefixes, 40 IPv6 prefixes
- around 140 tunnels



.uml 2009-12-27 05:50:00+0100
 alice.uml 2009-12-27 05:50:00+0100
 be.uml 2009-12-27 05:50:00+0100
 ipn.uml 2009-12-27 05:40:00+0100
 .uml 2009-12-28 22:30:00+0100

participants grab

- an IP subnet from 172.22.0.0/15
- an IPv6 network from anywhere
- a private BGP ASN
- Some people have official numbers...
- also, the wiki is t3h rulez

peerings are made

- whenever two people agree to peer
- and they agree on the parameters
- and they set it up

most people follow a common scheme
-but why should anyone restrict anyone's choices?

we can haz network

- quite *social* network (take that, facebook)
- ask your peers for services
- bring you friends to the network

we can haz network

- quite *social* network (take that, facebook)
- ask your peers for services
- bring you friends to the network

damn, I forgot to embed a Ponzi scheme

we can really HAZ network

- founder dropped for half a year, nothing happened
- boxes went down and weren't rebuilt, nothing happened
- friends nag you to fix your connection

semantics

- a bit like IRC:
 - servers form *links*
 - participating *servers* agree on rules
 - *servers* tend not to die, but netsplits are possible

chaosvpn

- first setup by haegar @ hamburg . ccc . de
 - used tinc
 - mostly ccc based
 - haegar wrote perl based update script
 - works mostly fine
 - perl not available on most routers
- many nodes did not update → problems

update.pl

- download a configuration file from vpn.hamburg.ccc.de
- decode
- sanity checks
- generate tinc configs
- (re)start tinc

chaosvpn 2.0

- Rewrite of the perl update code in c with some improvements so it fits on routers
- Few requirements, dependency to keep lightweight
- Mostly done by ryd, hc and Haegar with more help from the USA, namely Cinus, Cheryl, John Doe

and further

Road map

- better authentication, certificate handling
- more pull nodes
- OpenWRT package
- one network on every of the 4 ports

Current Projects

- freifunk
 - no automatic updates
 - leading to network issues
- Agora Link / ChaosVPN
 - hackerspaces network
- warzone
 - research network between research groups
 - enter at your own risk

freifunk

- Used to connect the clouds inter-city like
- Usually runs on small routers
- The perl issue
- No automatic updates, leading to issues like netsplits
- Partly working

Agora

- North American hackerspaces involved:
 - NYC Resistor (NYC)
 - Noisebridge (San Francisco)
 - PS:One (Chicago)
 - CCCKC (Kansas City)
 - People / Academia
 - More to come

chaosvpn

- CCC Hamburg
- CCC Hanover
- Links to CCC Koeln and Berlin
- t42
- Used to transport Chaos Phone earlier
- hackint irc node
- people

Use Cases

- VOIP (Chaosphone)
- media broadcasting,
- talk streaming
- making HPC Accessible
- cloud computing
- Internal Sites/Services/Webpages

Warzone

- Playground for security groups:
 - CTFs!!1!
 - University groups
 - Security groups
 - Hackerspaces who want to play
 - Next generation research platform

Übermensch Recap

- We found a problem to communicate and we tackled it!
- The network IS UP!
- We need you!
- Have resources to share?
Contact us!

Outro

Projects in the future:

- Global VoIP
- HPC Computing
- Media Multicasting
- CTFs

THX

Many thanks to:

haegar, ryd, hc, winni,
OpenWRT

helios, jchome, ichdasich,
frapzzt, wintix, Crest



Where to Join

- www.agora-link.org - (BETA)North America
- dn42.net
- ChaosVPN - wiki.hamburg.ccc.de