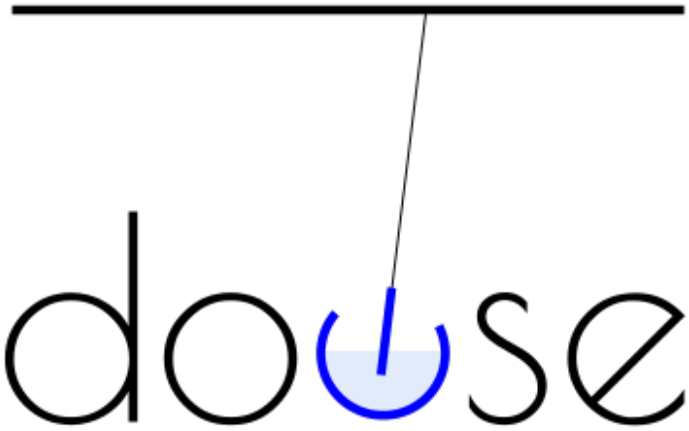
Dowse Whitepaper

Dyne.org Foundation

March 28, 2017

Contents



1 Introduction to Dowse

1.1 Scenario: the Internet of Things

Running a network in the age of the Internet of Things means hosting the connectivity of multiple devices owned by a diversity of subjects. Often such devices have full access to private, common and public information about humans operating them. Furthermore, devices can talk to each other without humans being consulted, and such interactions are not even manifest. This situation raises issues that are not just technical, but socio-political, about the way **connections happen without human consent**, within local networks and towards the outside, to and from the Internet.

The risks of *unconscious* abuse and exploitation of information asymmetry are growing tremendously. As **things initiate on the behalf of users**, we are making a major leap towards a world that provides us with contexts that we may not want at all. Getting insight on such situations is crucial for societies at large.

1.2 Problem: opaque gateways

As the concentration of network-connected devices and applications increases, so does the volume and complexity of network activity. While these network actors communicate on ever greater scales, the central device which interconnects them has remained basically the same. The so-called gateway or router is usually provided and programmed by an ISP, and meant to be largely ignored by the 'user.'

The gateway is opaque in terminology, and an engineering of disempowerment in practice. By making the gateway an esoteric device, a closed device, a device which hides under the couch, opportunities to create, distribute, and use software which properly govern the small-scale network are lost.

1.3 Opportunity: the hub

The centrality of the gateway device in the home/office puts it in a position of unique power and future opportunity. It is the locus of discovery, communication, and regulation between connected devices. It forms the fundamental structural matrix for the Internet of Things at the most basic scale.

We see an opportunity to create a hub which is a part of the experience of the networked person, the networked household, the owner of devices, the Internet participant. While the term "hub" belonged to the

era of 10Base-T, it seems appropriate to revive the term now, as we seek a new set of generic non-authoritarian terminology to talk about the device which joins the other devices in our local network.

1.4 Concept: de-militarization

Dowse is not only a functional tool, but a symbolic operation proposing a different linguistic approach to networking. In conceptualizing and documenting Dowse, all references to military traits are removed: there is no use of "defense", "shield", "guardian" or "firewall" words.

Privacy awareness (rather than protection) is envisioned and presented to its users not as a violent process, but as a responsible, natural act — one in search of harmony among those things connecting the inside and outside of a person's private, common, and public aspects of life.

1.5 Idea: responsible networking

In the IoT paradigm, having a clear overview of what goes in and out of the network becomes of crucial importance for home users and professionals. The ultimate question of responsibility for whatever happens within a network cannot be easily answered, considering the way *things can autonomously decide to initiate communications*.

Dowse is a smart digital network appliance for home based local area networks (LAN), but also small and medium business offices, that makes it possible to **connect objects and people in a friendly, conscious and responsible manner**.

Dowse aims to be a critical engineering project, abiding to the principles stated in the Critical Engineers Manifesto.[1]

1.6 Solution: context awareness

By bridging the outdated proprietary ISP 'gateway' with an open and user-visible device, Dowse creates a new platform that leverages its topologically unique access and influence in the domain of the local-area network. It introduces a visible, malleable, knowable communications hub to the language of the small network.

Dowse seizes on the power of the technologically/topologically necessary gateway/hub role to create development opportunities which cannot exist on other platforms. Dowse becomes the locus of a specific new class of end-user-visible applications which are able to perceive and affect all devices in the local sphere, whether they are open or closed.

Moving above the platform of Dowse, it is in touching upon the Internet of Things that a glimmer appears of what may be Dowse's killer app(s). These are the applications of Dowse in which human opportunities appear to interactively define the Internet of Things at a high level. The entrance or departure of a device from the local IoT ecosystem is accompanied by audiovisual interactive aspects. Such interactions extend to the new presence or absence of a communications channel, for example between an electrical meter and a corporation. The software explorations that can appear in this domain, enabled by the Dowse platform, can bring individual awareness, preference, and empowered influence to the network/IoT as its own organ.

[1] Berlin, October 2011, see: `http://criticalengineering.org`

2 Features

2.1 User cases

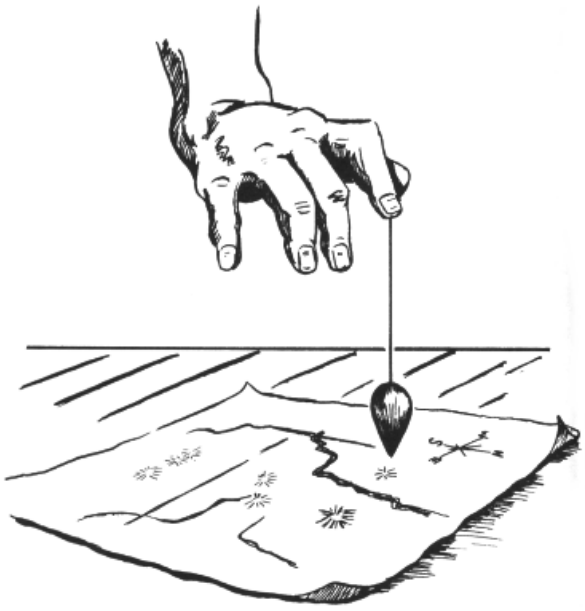
Imagine running a network whose password is known to several people: while one would desire lax security in order to enable people to connect, one could then never be sure about unknown devices on the network. Dowse actively monitors network events to alert the users of significant changes: whenever a device joins the network, an audible signal is produced with a welcome message and/or light signals.

Dowse grants default network access to guests while the presence of newcomers and unusual connection patterns is signaled. **Users can then mark guest devices as known** (white-listing) to grant wider or fine grained access to them, as well grant known users the right to welcome more guests. Devices can also be assigned a name which will make them reachable on the LAN via human readable URLs, as well customized audible signals like a warm "*welcome back*" for dear guests.

In a highly connected home environment, Dowse will provide an easy to use interface on which proper user-centric design has been done (LEAN UX approach). Inhabitants will be able control exactly which flows of data go in and out of their private LAN space, being enabled to make decisions about new devices when they appear: from a new electricity meter to a mobile phone or computer.

From a legal perspective, **Dowse clearly separates the leased network device by the network carrier (ISP) from user owned LAN devices**, making them opaque to each other.

Dowse helps **removing undesired advertisements and browser malware** to make Internet surfing less distracting and less dangerous. Dowse filters all cleartext web traffic to avoid advertisements, and also applies IP block-lists to avoid known malware distributors and botnet connections. It helps to avoid damages and complaints in case a tainted device brought in by a guest connects from inside the network.



Dowse enhances the privacy of people surfing the Internet in cases where **confidentiality and integrity of research is important**. For example, in the case of journalists and activists, the profiling of DNS resolution queries can be a delicate point of vulnerability to all kinds of covert operations: not just passive tapping, but also active deception. Dowse alleviates the risk in such situation by relying on the connection to a few trusted and authenticated DNS services, encrypting all traffic (UDP port 53) and avoiding the most widespread practices of covert user profiling. In case of Internet censorship, Dowse also facilitates access to parallel networks that let users circumvent limitations imposed by a connectivity carrier. Access to parallel networks like Tor, I2P, GNUnet or Netsukuku is granted without requiring users to install any software.

Finally, Dowse can enable **responsible parents** to address the freedom of their kids to browse the Internet, by preventing aggressions by malware, phishing and other kind of intrusions into their experience.

2.2 Architecture

Dowse is a **transparent proxy** facilitating the awareness of ingoing and outgoing connections, from, to, and within a local area network.

Dowse provides a **central point of soft control for all local traffic**: from ARP traffic (layer 2) to TCP/IP (layers 3 and 4) as well as application space, by chaining a firewall setup to a trasparent proxy setup. A core feature for Dowse is that of **hiding all the complexity** of such a setup.

Dowse communicates with users in various ways: via a web interface, but also pushing messages via audio (synthesized speech), Bonjour and simple apps interfacing with personal mobile devices.

Dowse can implement this with a complex of open-source, well established technical tools, simplifying their integrated setup: specific directives read by daemon applications are generated from a central configuration point. The configuration options visible to users are reduced to the minimum, while adopting **automatic guessing mechanisms in most cases**. Both the implementation and the user interface for Dowse are extremely minimal.

Dowse is also a **highly extensible platform**: interoperability between modules is available using Socks4/5, UNIX pipes, local TCP/IP sockets and port redirection, conforming to specific daemon implementations. At the core of Dowse is a very portable shell script codebase implementing a modular plugin architecture that isolates processes and supports any executable written in any language: Shell, C, Perl, Python etc.

At last, **Dowse also acts as a gateway to the future proliferation of parallel networks**, mostly based on particular content niches or on different levels of privacy granted, like Tor and GNUnet. Using Dowse, is possible to access such opaque networks without installing anything on any device, just stepping into an home or office.

2.3 Technical design

At least from its first appearance on the market, and in people's home/office setups, the **Dowse box should be visible device** to virally spread its image which indicates that the local network in a particular environment is taken care of responsibly. This will involve an industrial design project of the exterior of the object at a later stage.

In its software form, Dowse will be a free and open source application bundle: OS independent and hardware independent. A reference implementation will be distributed as a ISO, ready to be flashed on SD cards and run on RaspberryPI and other common devices running Debian and OpenWRT.

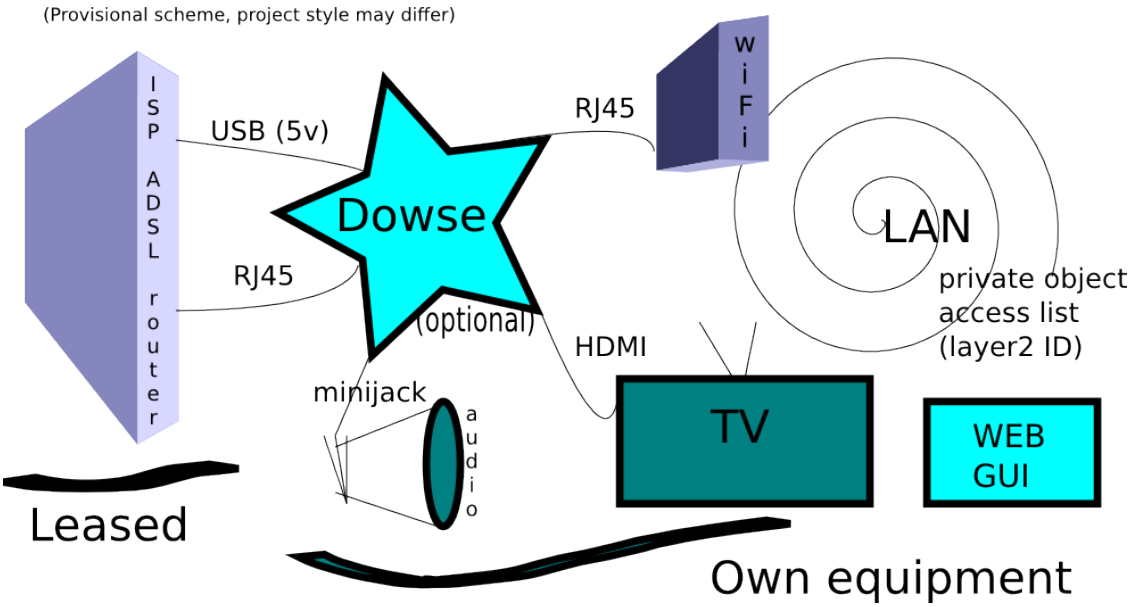
In general, and considering especially the success of modular design products like RaspberryPi or Arduino, modularity should be a key feature for the final hardware box design, adopting an **add-on architecture that allows the community to make modules and distribute them autonomously**.

The Dowse box should operate on low power (USB 5v, 2.5W) and two ethernet network connectors (RJ45). It is **made to sit between the broadband network router and the rest of the internal network**, therefore it can be simply connected to the USB and Ethernet ports of the router box using short cables for a complete installation.

For a first prototype, the second network interface can be realized using an additional USB adapter which can also be an Ethernet (RJ45) or WiFi adaptor, eventually turning the Dowse into a wireless access point for small areas.

For a dual-ethernet prototype platform, the *Olimex A10* so far matches best our requirements (company in Bulgaria, well distributed in Benelux) running both a stable Debian GNU/Linux based distribution or OpenWRT. The bare cost for such hardware, all included, amounts to approx 50€.

2.4 Overview of functions



Dowse takes control of a LAN by becoming its DHCP server and thereby assigning itself as main gateway and DNS server for all clients. It keeps tracks of assigned leases by MAC Address. DNSMasq is the DHCP and DNS daemon.

All network traffic is passed through NAT rules for masquerading. All HTTP traffic (TCP port 80) is filtered through a transparent proxy, using an application layer chain of Squid2 and Privoxy.

All DNS traffic (UDP port 53) is filtered through DNSCrypt-proxy and encrypted using AES/SHA256 before being sent to DNSCrypt.eu or other configurable servers supporting this protocol.

In the future, traffic of all kinds may be transparently proxied for monitoring, filtering, and transformation by other applications loaded on the Dowse device.

All daemons are running as a unique non-privileged UID. The future plan is to separate them using a different UID for each daemon.

When running on a single physical network interface Dowse will require users to deactivate manually the DHCP daemon on the ADSL router. But the hardware prototype will be based on devices with at least two RJ45 ethernet and/or a WiFi AP in order to enforce physical segmentation and isolate the broadband router into a DMZ. So far the best possibility to realize this in a modular fashion is to add USB modules that provide an extra ethernet RJ45 (~5€) and a WiFi interface (~10€).

2.5 Proof of concept

Dowse already comprises of a proof of concept implementation as free software visible on [`http://www.dyne.org/software/dowse`].

This proof of concept is OS and hardware independent. It currently supports only one physical network interface, and is being tested on Debian. Also see [`http://freecode.com/projects/dowse`] and [`http://ohloh.net/p/dowse`].

Dowse 0.4 can only be operated from a terminal, and it has a rudimentary implementation for modules, including working instances of DNSCrypt-proxy and Tor as gateway to the .Onion network.

3 Motivation

The goals for Dowse are in first place ethical: our priorities go far beyond the sustainability of the project itself, ultimately aiming at the production, enhancement and distribution of responsible and free/libre software.

In the long term there is a business model that we envision, and it should make this initiative well sustainable. It is the business scheme adopted by most succesful **free software** and **open hardware** bundles that bring to market a product for which there is high demand by virtue of viral adoption and de-facto simple standards.

In order to achieve such a success, the ambition we put forward is that of following a *LEAN* approach to the design of this project, and therefore we invite all recipients of this document to be involved in a user-centered design process. In order to have results, we will **defer long-term research tasks in favor of rapid achievements** that will enable developers and designers to have a close-knit feedback loop with use cases.

In the medium-term we will seek alliances with existing hardware producers and utility distributors to adopt Dowse as a well documented, minimal and solid platform for generic development. We envision a win-win situation for the adoption of Dowse by specific utility distributors, on national and regional scales, that will benefit from a **shared, community driven, decentralized and peer reviewed R&D process**, insuring the long term sustainability of devices embedded in domotic installations and running crucial network operations.

We do hope for the network effect and high demand for this product to be driven by recent events which have woken up the world to the importance of privacy and integrity, and also by the fact that existing devices of this kind (routers, switches, wifi access points) offer a sub-optimal and hardly usable set of functions for **awareness in the age of the Internet of Things**, which currently in the best case are designed to be operated by specialized engineers and security experts.

In the longer term, high quality, low production, adaptability and resilience are key to the business model of Dowse, which configures itself as a design intensive project with low hardware requirements.

4 Acknowledgments

In 2014 Jaromil has conceived the Dowse plan, proof of concept and the making of this whitepaper. Earliest contributors to the whitepaper drafting process are Hellekin O. Wolf, Anatole Shaw, Juergen Neumann, Federico Bonelli, Julian Oliver, Henk Buursen, Tom Demeyer, Mieke van Heesewijk, Floris Kleemans and Rob van Kranenburg.

4.1 About Dyne.org Foundation

Dyne.org is a digital born organization committed to research and development of free and open source software and services. Dyne.org acts in support of artists, creatives and engaged citizens in the digital age with tools, practices and narratives for community empowerment. Since its birth in 2000 several radio makers, humanitarian organisations, artists, medics, activists and educators employed and redistributed Dyne.org software worldwide and free of charge.

Dyne.org is constituted by an international network of experts syndicating and contributing to diverse technological developments for their quality and role within societies. Among its peers Dyne.org shares mutual support and resources for peace and equal rights, operating outside the logic of profit and competition. The mission of Dyne.org is to supports cooperation within social contexts to leverage on-line and on-site community values, to empower people with the hacker attitude to re/think, re/mix and re/design to circumvent limitations and find ways out from economies based on scarcity and privilege.

At the origin of Dyne.org are several BBS and in particular the Freaknet, which is now an on-line and on-site medialab and computer museum based in the Mediterranean island of Sicily, surviving since 1994 the hostile environment of South Italian criminal administration and cultural repression. Dyne.org members regularly gather in the Italian Hackmeeting which is, since 1998, the annual gathering of many computer and reality hackers, an auto-organized TAZ inspired by people and projects at CCC, 2600, GNU and EFF.

In 2001 Dyne.org started developing the dyne:bolic GNU/Linux distribution, 100% free multimedia operating system that works well on recycled computers, endorsed and promoted by the Free Software Foundation. Further on Dyne.org has been developing and documenting a variety of empowering tools made by and for digital natives around the world, running workshops and putting in contact artists and practitioners, providing a public and common space for on-line interactions. Among the others, Dyne.org creations have been redistributed by:

Free Software Foundation	(USA)
Montevideo / Time Based Arts	(NL)
Ircam, Centre Pompidou	(FR)
Providence Univ. Taichung	(TW)
Tecnhische Univ. Ilmenau	(DE)
Netherlands Unix User Group	(NL)
Instituto de Computação Uni de Campinas	(BR)
Heraklion University Crete	(GR)
Ibiblio public library	
UNESCO	

In 2013 Dyne.org became an European research organization, partner of the D-CENT project (FP7/CAPS).

4.2 License of this document

5 Appendix appendix

5.1 Lean Canvas prospect