The
Asymmetrical
Communication
Endpoint

A Computer system for the Internet usage, physically save against any types of attacks which are performed via the Internet.

27.10.2020, update August 2022
firewalls.feuerbach.info

What is it about?

- Physical data security based on Asymmetry, mathematically proven.
- Adding a Control-Layer 8 on top of the 7-layer-OSI-model.
- A new client package for Linux, under GPL v.3.0 or later and the related Hardware
- A completely new and systematic approach to secure data and the privacy of data – against all attacks performed via the internet while being online, including Ransomware attacks.
- A physical invention in data security and a new platform and framework.
- Security measures which are unreachable by any network attacker/attack.
- A new type of infrastructure to ensure privacy **and** communication at the same time;
  No need for isolation from the Internet anymore to reach the highest level of data privacy.

What is it NOT about?

- Asymmetry as different upload/download speeds
- Just another Proxy/Firewall
- Complicate system, which can’t be used in daily operations in office and privately
- A new type of Computer
- Something what needs different computer networks than we have nowadays
- Mixing-up the existing ISO-OSI layers of the well-known 7-layer-model

Why Asymmetry in Computing?

- Asymmetry gives us much more possibilities in technology.
  Examples: Asymmetrical Cryptography, separation of open/close functionality in car keys (two buttons instead of just one), separating source IPs from target IPs in TOR-routing, and many others.

- The “hackability“ of currently used networked computers results directly out of the *symmetry* of todays way communicating with the Internet.
  Symmetry of networking endpoints gives the **applications** the full control over the communication, not the **users**.
  A single system, which can send **and** receive in the same network connection, is a symmetrical communication endpoint or SCE. Such endpoint can communicate anytime without a user-interaction. Following that, the user lacks control over the own network communication.
  In comparison to that, an asymmetrical endpoint or ACE may communicate just and only via a **user-interaction**. Said that, technically all the current symmetrical endpoints are rather like server computers, which are used on-top as well as client computers.

The principles of proven Security

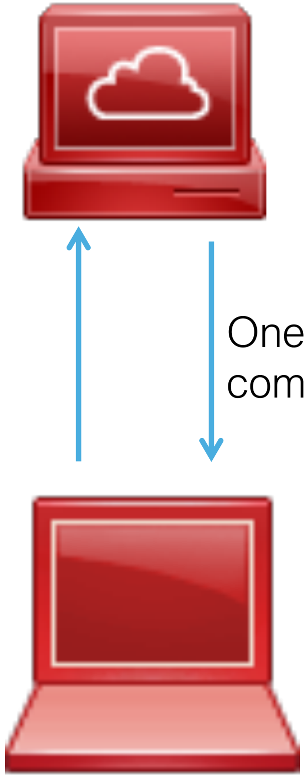
The ACE bases it‘s security on physical measures. Physical measures means:

- The measures are out of the reach of whatever Attacker/Attack
- It is based on Physics, so separate hardware working with its own software on it
- The measures are mathematically proven, providing a clear understanding of the level of security
- The effectiveness of these measures is independent of any software updates
- There is a clear and concise definition of ”what” is the security it gives to you (see „Security Matrix”)

In the following graphics colors are used to show the level of security with “red” as symmetrical unsecure, while “green” and “yellow” as asymmetrical physically secured. The Security Matrix and more detailed information can be found under firewalls.feuerbach.info.

Comparison SCE/ACE,1

Today's Use Case with SCE's:



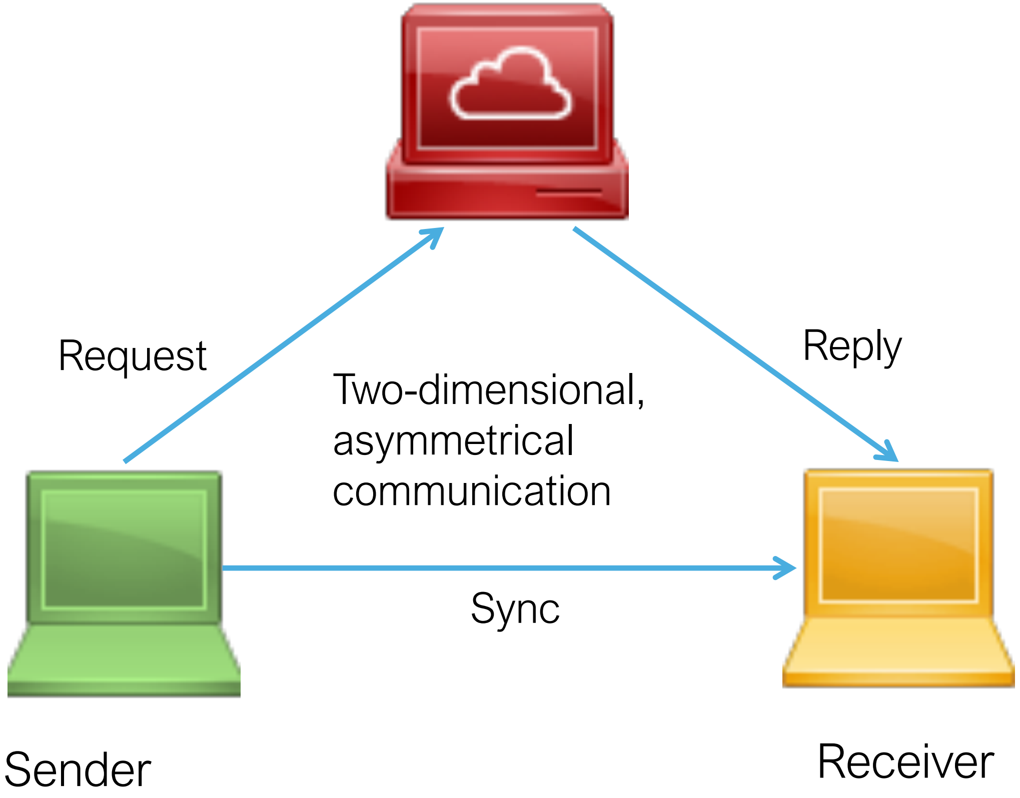
Server, eg. Web server

One-dimensional symmetrical communication

Client

Comparison SCE/ACE,2

Future Use Case with an ACE:



Request

Reply

Two-dimensional,
asymmetrical
communication

Sync

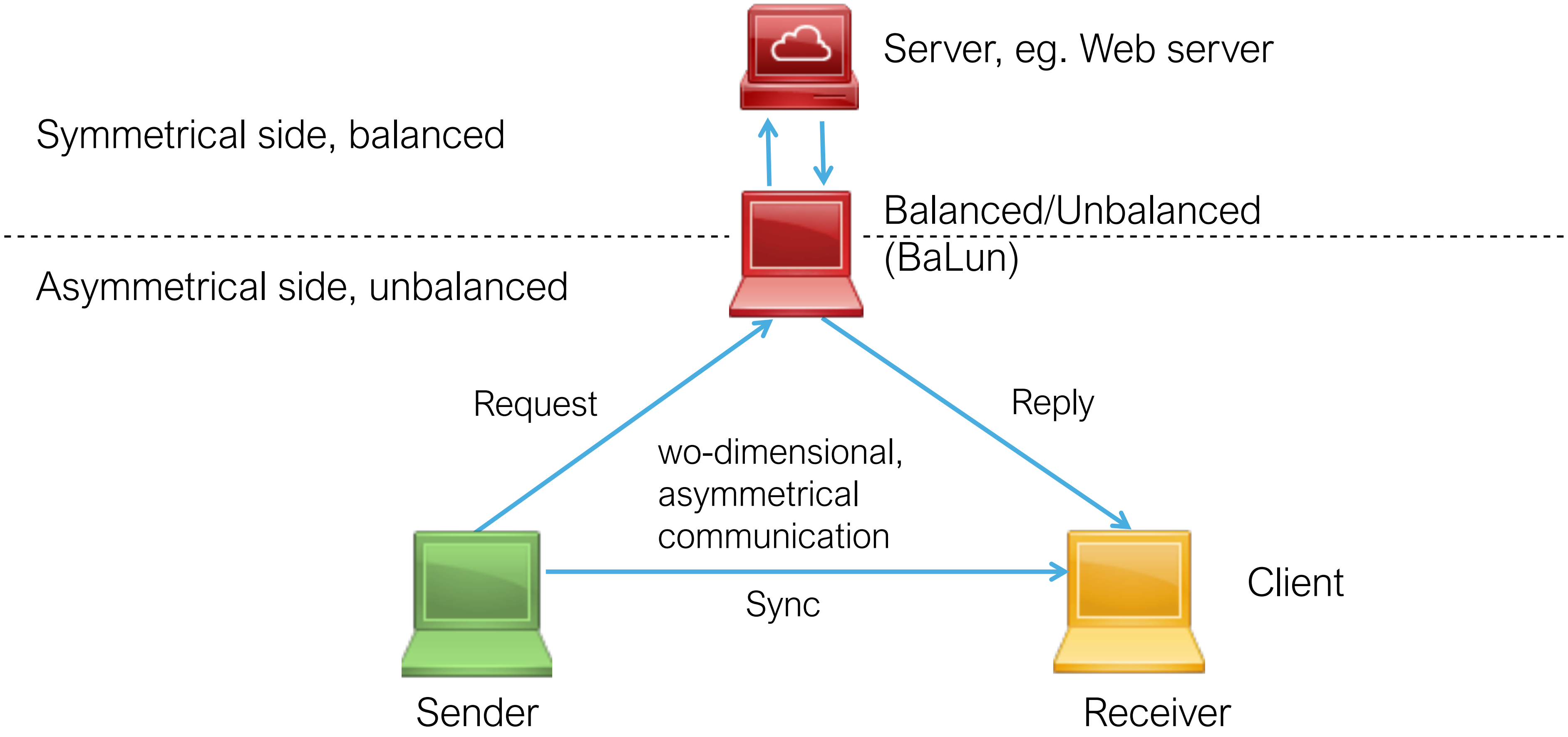
Sender

Receiver

Server, eg. Web Server

Client

ACE: How To Do It,1



Server, eg. Web server

Symmetrical side, balanced

Balanced/Unbalanced (BaLun)

Asymmetrical side, unbalanced

Request

Reply

wo-dimensional, asymmetrical communication

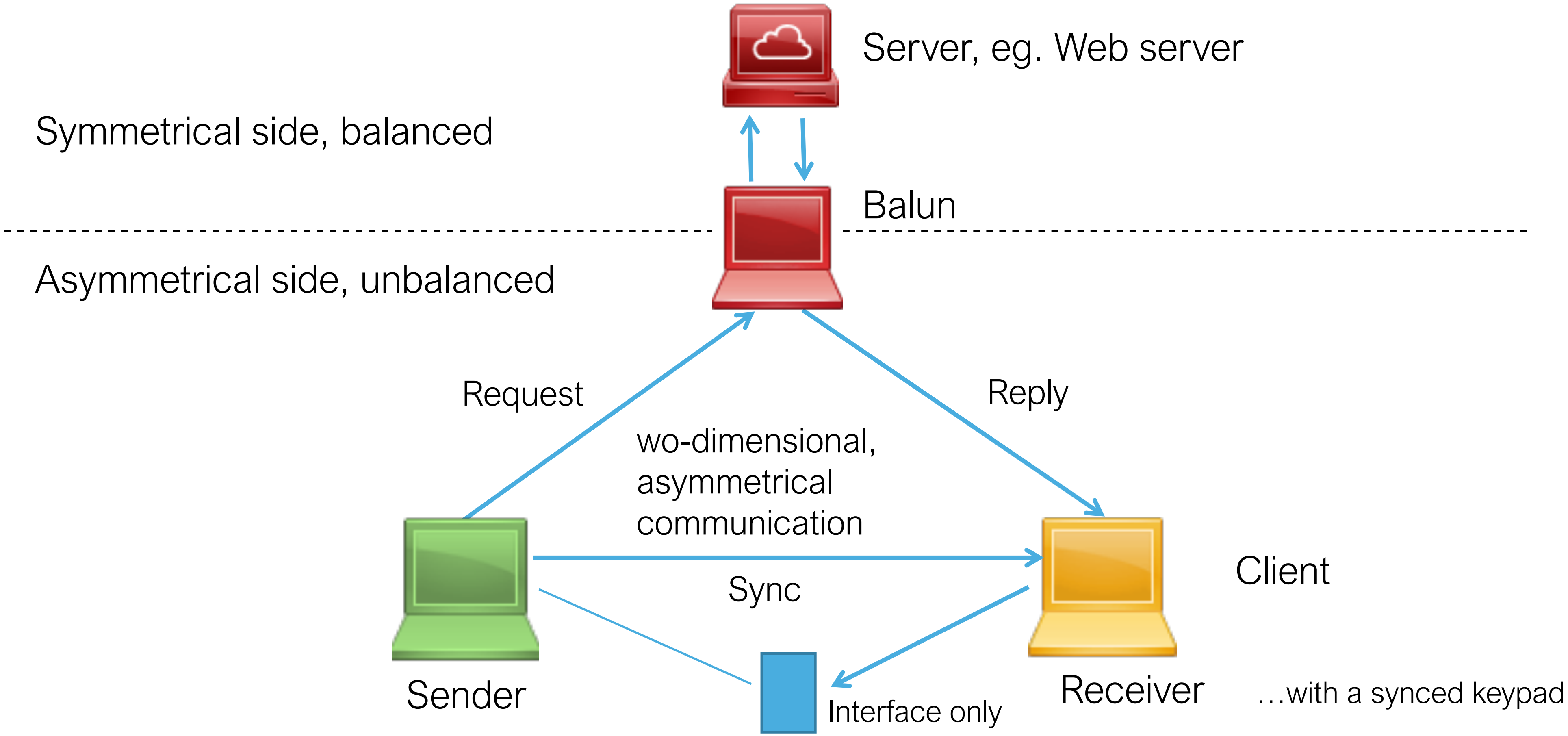
Sync

Client

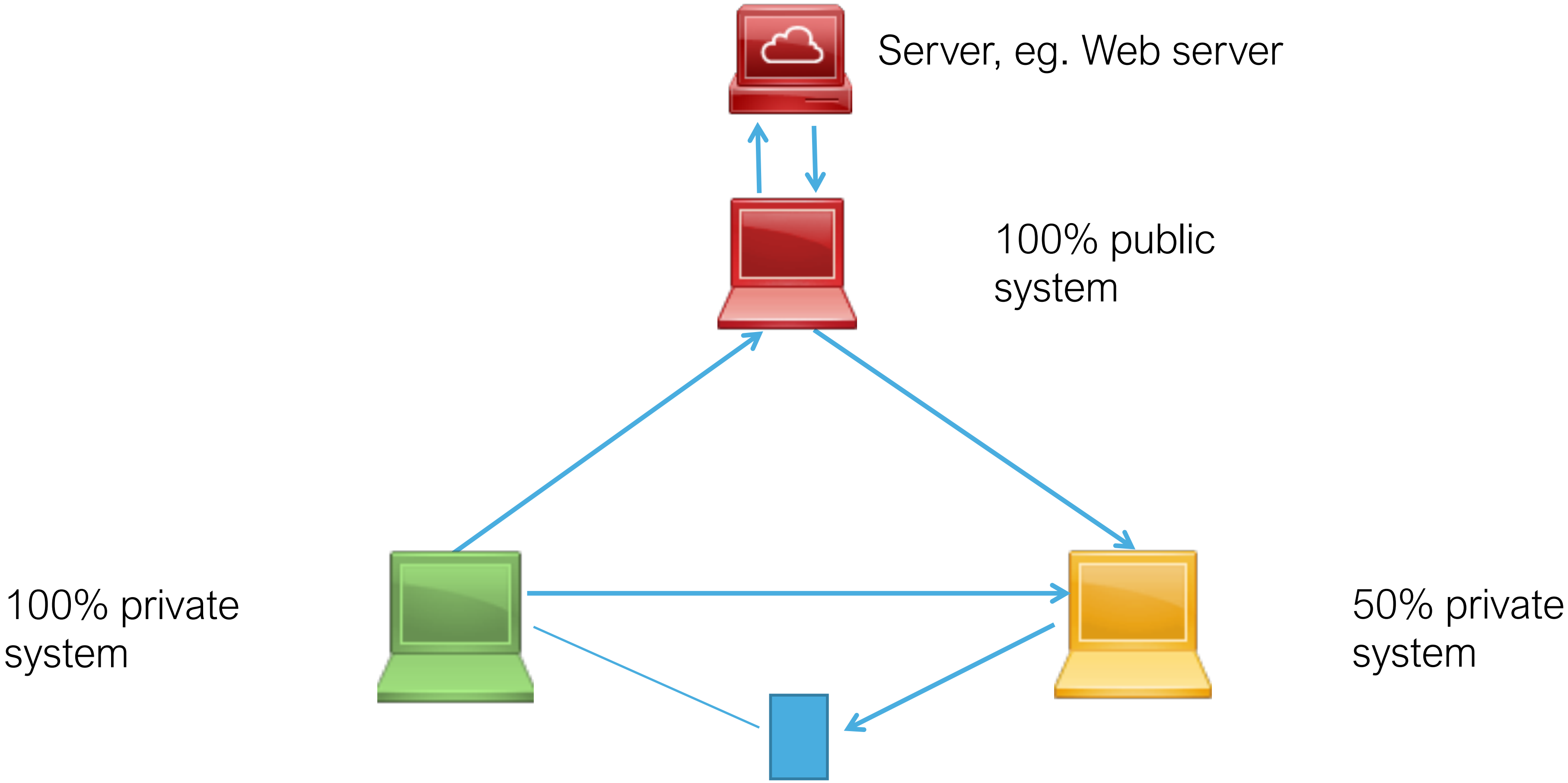
Sender

Receiver

ACE: How To Do It,2



ACE: About Levels of Privacy



ACE: The Software Needed

While the ACE is an invention on layer 1, the physical layer, there is of course programming needed to make it work.
Most work here needs to be done for each protocol by adding a related proxy program on red. Less programming is needed on the network- and local programs, like browsers, on green and yellow.
The layer 1 of the ACE is a foundational layer now, and it allows programs to be built on such a much more stable platform.
Programming is needed for an ACE, esp. to bridge the protocol gap.
Every application protocol can be applied to make it work on an ACE.

(All the software needed is under GPLv.3.0 or later and can be downloaded via links provided on the bottom of my web page: firewalls.feuerbach.info.
The files contain also precise instructions for installation. Currently only in German language.)

ACE: A Real Client Computer

The ACE is for the first time a pure and real client computer, as it interacts with the network just and only in case the user wants, and how the user wants.
This is physically ensured. That's why I call it a “Layer-8-Device”.
An attacker can’t change these security measures via the network because of its physical setup.
These security measures are fully out of the reach of attackers on the internet or local network.
Even if the software of an ACE will never be updated, the high level of security will be further given, as the security level is independent on software versions - and so on patches. That allows also to have much more stable systems. While security updates on SCEs are very often done and often without enough testing for side effects before, because of their urgency, making the patched systems unstable.

The security of an asymmetrical platform is easy to prove: Nevertheless, how long a user is online with an ACE and actively e.g., browsing with it, the sender shows for its network interface always zero Bytes received.
To test it on the command line in the sender: ifconfig command showing always 0 Bytes and 0 packets RX.

How does the ACE solve the issues? Part 1

- Ransom Ware

(*Encrypting all data on a given system. To pay a ransom for retrieving the own data or publishing data)*

In an ACE, the user types data automatically always synchronously into both sender and receiver, so all this data is continuously held on both computers, green and yellow. In case of a ransomware attack, it takes less than an hour to completely rebuild yellow by setting it up newly with an OS-Image and then with the data from green, the sender. Publishing of receiver's data is phys. not possible.

- Data Espionage

(*Reading out the data on a given system. Sending it to the internet)*

As the sender can‘t be reached from attackers, it can‘t be forced to send data outside.

The receiver can be reached from attackers over the network, but it can‘t send anything back.

How does the ACE solves the issues? Part 2

- Tracking of Users

(*User behavior is monitored and collected)*

Lot of the user-tracking is done by reference links in each webpage loaded. These reference links are then opened by the browser in the background and that way e.g., statistic servers are contacted and data about the user is transferred - without consent or even knowledge of the user. This data can be easily personalized. These cross connections to 3rd parties‘ servers are also delaying much the load process for the webpage the user wants to see. That‘s the reason why the ACE's browser loads much faster.

Result: because the cross connections in the webpage can‘t be followed by the browser in an ACE (all such requests are put into the Recycle-Bin, the „blue“ interface), all user-tracking will be blocked.

How does the ACE solve the issues? Part 3

- DDoS etc.

  (*Sabotage of systems)*

  An ACE can‘t send data in an automatically way into the outer network. So, in case the receiver got some malware related to DDoS, the ACE won‘t attack anyone else as it can‘t send requests to the world outside. That way ACEs help against DDoS Attacks by not taking part in bot nets.

- Viruses

  (*Infecting systems and spreading the infection through the network)*

  Even the receiver part of an ACE may get a virus by chance, the virus can‘t spread afterwards, as the receiver can‘t send anything back into the network. That way also the servers in the local network, often the main targets behind an attack on client computers, are safer.

How does the ACE solve the issues? Part 4

- Trojan horses
  (*Functionalities in programs of which the user is unaware and attacking from inside)*
  Like with viruses, a Trojan horse can‘t be spread from an ACE to other computers. All locally from the receiver by a Trojan Horse collected data can‘t be sent back into the internet to the attacker.

- Worms
  (*Infecting systems and spreading the infection through the network)*
  Same as with viruses.

- Built-in Malware
  (*Malware, which is already in the system (operating system, applications, BIOS…))*
  Pure asymmetry is here not enough. Here may help open hardware and open software as well as testing against unwanted and undocumented functionality etc. to avoid having built-in malware. Or to use in an ACE two senders and two receivers in parallel, comparing their sending- and other behavior (so a three-dimensional communication).

Private Computer Infrastructure(1/2)

Asymmetry in network communication may also be applied to servers, providing them as well with a much higher level of data protection in comparison to symmetrically communicating servers. An asymmetrical server would be further a Layer-7 system, as it must answer requests from clients in an automatically way. However, as of its asymmetry, it would be much more secure for its processes and data hosted on it, than any symmetrical server we use nowadays. Technically, the dummy interface of the ACE would be replaced by a fourth computer, like the red system, with a proxy on it, to control all requests before pushing them further to green. On green then is the real server, a database, fileserver or whatsoever service needed.

Private Computer Infrastructure (2/2)

Both asymmetrical servers and -clients together would establish the Private Computer Infrastructure or PCI. The PCI would allow applications which are nowadays not even thinkable because of the current lack of data protection.

Together with asymmetrical encryption (Public Key Infrastructure, or PKI) both the moving data and the data in rest will be save against all attacks over the network.
PKI and PCI together can eliminate their respective remaining weak points.
The weak point of PKI alone is the insecure encryption and signing process in SCEs.
The weak point of PCI alone is the receiver side. By using PCI and PKI, the processes for PKI are safe and the receiver side in an ACE will be safe against manipulation of data because of signing/verifying of files automatically always.

Backup

This backup shows current status of security issues and which of these would be fixed by an ACE.

Current Main Data Security Issues,1

- Data Manipulation

Ransom Ware. Encrypting all data on a given system. To pay a ransom to get back the own data

- Data Espionage

Reading out the data on a given system. Sending it to the internet

- Tracking of Users

Users' behavior is monitored and collected without their knowledge or agreement

- Sabotage of systems

DDoS Attacks etc.

Current Main Data Security Issues,2

- Viruses

Infection of systems and spreading the infection through the network

- Trojan horses

Functionalities in programs of which the user is unaware and attacking from inside

- Worms

Infection of systems and spreading the infection through the network

- Built-in Malware

Malware, which is already in the system (operating system, applications, BIOS…)

What are the ways of attacks?

- Direct attacks on the networked computer

eg. „Ping of Death”. Port scans. Attacks against open ports, once found…

- Indirect attacks on the networked computer

eg. Ransom Ware, Trojan Horses, tracking of user behavior, key loggers…

- Built-in attacks on the networked computers

eg. BIOS: direct network communication and attacks from the lowest level.
Operating system: every form of an attack, which can be programmed. Same for applications.

What are the attacks aiming at?

- Reading out the data/processes which are inside a computer.
- Manipulating the data/processes which are inside a computer.
- Disturbing the user or the system used (sabotage)

- (see also the Security-Matrix on my website)

What are the current counter measures applied (w/o ACE)?

- Firewalls: to stop all direct attacks from outside via network
- Antivirus: to find malware which has already been found the way into the computer
- IDS/IPS: to find unusual network behavior, network attacks beforehand.
- Backups: as a last resort if above has not helped as expected…

And how effective are they?

- Firewalls: to stop all direct attacks from outside via network

SW based, so can be exploited. FW rules can be the weak point. Updates needed. High cost.

- Antivirus: to find what has been already found the way into the computer

SW based, often not current enough to find attacks, not helpful against new forms of attacks.

- IDS/IPS: to find unusual network behavior, network attacks beforehand.

Same as with Antivirus. High Cost and effort.

- Backups: as a last resort if above has not helped as expected…

Never current data, often issues with the playback, taking a lot of time to play back. Can also be already infected with malware.