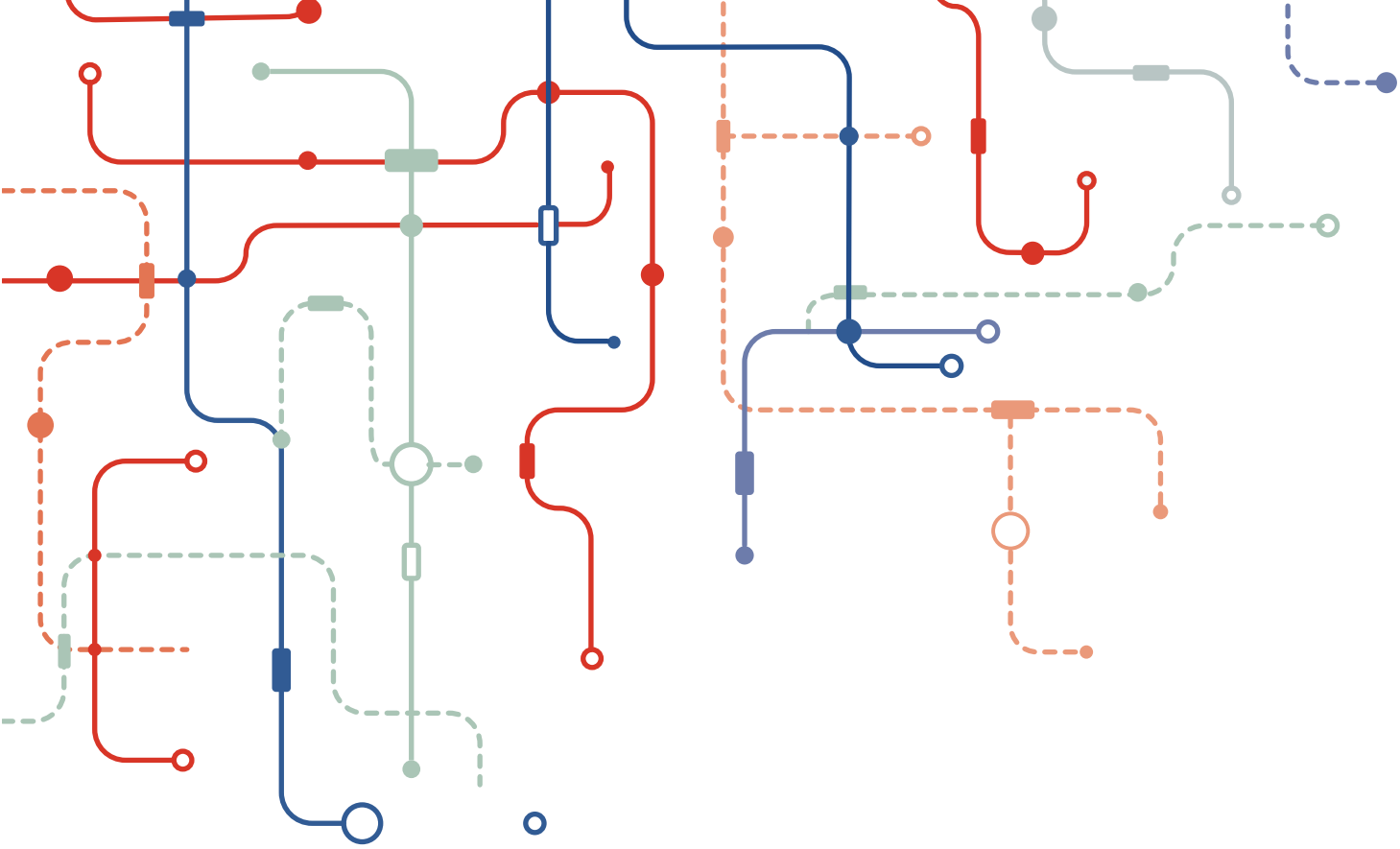
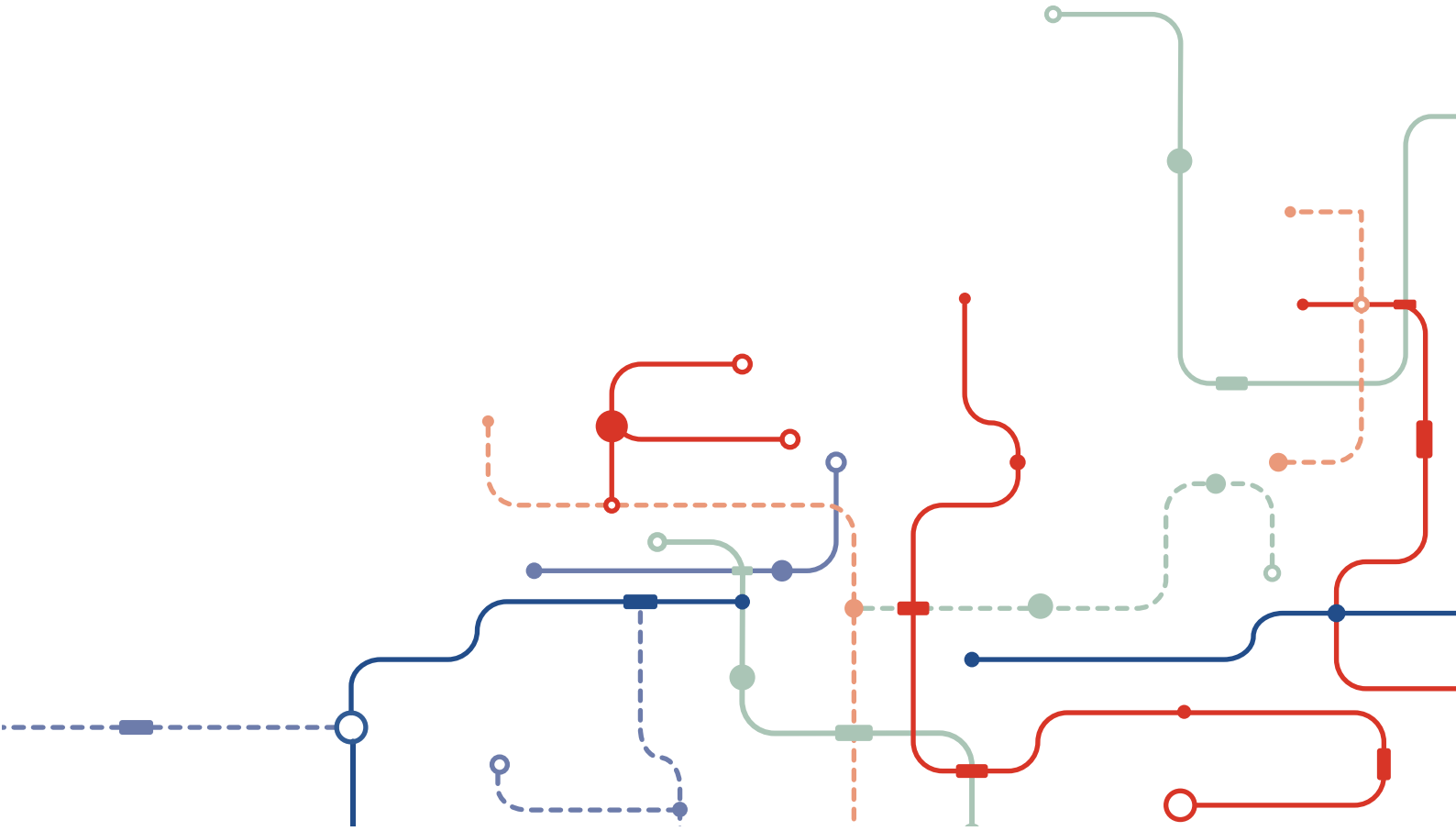


Solutions to prevent IoT devices to be used for DDOS attacks

WISeKey General Business Use



Solutions to prevent IoT devices to be used for DDOS attacks

WISeKey General Business Use

Contents

TMP_PRD_003 v6.1

The 18th of September, OVH, “the number 3 internet hosting company in the world” has been faced the most massive DDOS attack. It has been resolved on the 23rd of September.

https://www.ovh.com/us/news/articles/a2367.the-ddos-that-didnt-break-the-camels-vac

DDOS attack is more and more common on the internet, on the 21st of October Dyn experienced a similar attack scenario. The issue was resolved 10 hours later. Dyn is providing web site name to dynamic IP address translation. If you want to access a network from internet, you need to translate the URL into an IP address which may change from time to time. This is what Domain Name System is solving.

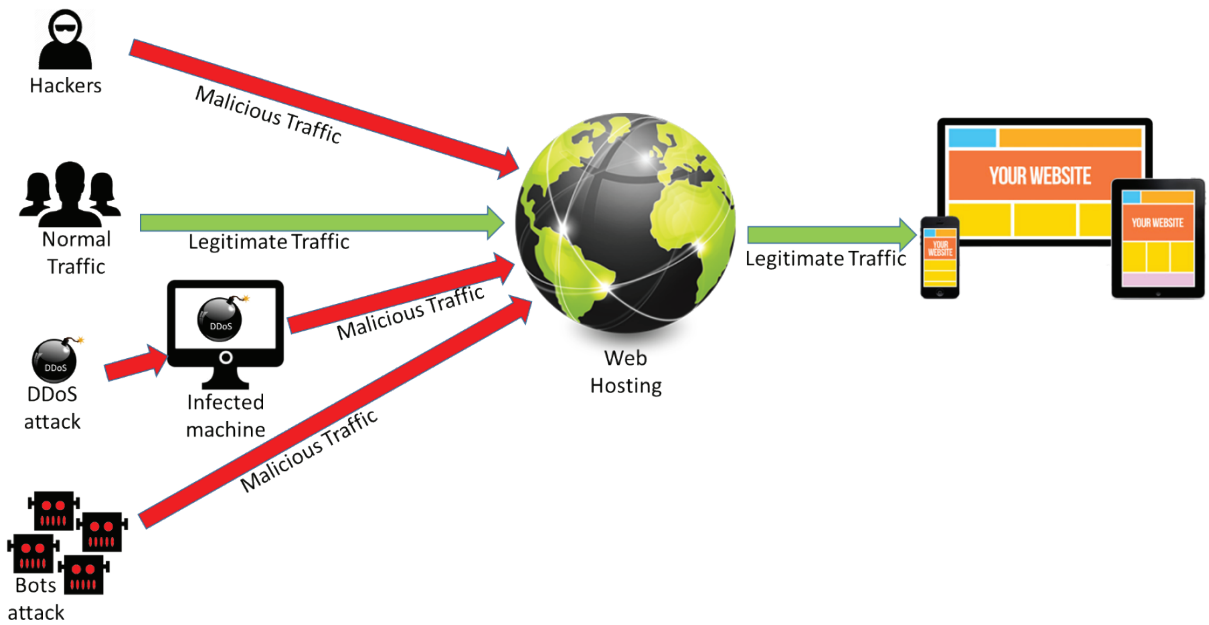
http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

These attacks are the largest ones reported so far.

What is Distributed Denial of Service attack?

There are 3 types of Cyber-attacks: those making service unavailable, those to steal/disclose content and finally those to alter content.

Distributed Denial of Service attacks aim to make a service unavailable to intended users, accomplished by criminal perpetrators. The common attack path is to flood the targeted victim with superfluous traffic to overload the victim's bandwidth, bringing the service down. The superfluous traffic is generated by hundreds to thousands of infected devices, all controlled by a central malicious source.



The figure above shows the difficulty to filter legitimate traffic vs malicious traffic. In fact, all this traffic will arrive at the targeted victim, where a fire wall would filter out the illicit traffic. But using standard protocols with correctly formed messages, the malicious traffic coming at vast quantities will eventually clog the bandwidth of the filter and block out the service.

The criminal perpetrators goal for the massive DDOS attacks mentioned above, was to make services down: the hosted websites were unavailable during the attack and during the time to recover backups.

Even though the service (like OVH in the first case) was not the final target, but its customers, it brings a very negative image to the service and can destroy public confidence in a brand as a whole.

DDOS attacks are commonly used to gain financial gain for the perpetrators, by blackmailing or extortion of the victim. They are easy to implement, and sometimes attackers can even rent botnets preinstalled on devices by a criminal organization.

The report published by Europol: "IOCTA The Internet Organised Crime Threat Assessment 2016"
https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf
clearly highlight DDOS attacks as key cyber threats, which can cost a company up to billions of dollars in losses, while 8 out of 10 companies suffer one or several DDOS attacks per year, as Kapersky states in their Q3 DDOS Intelligence report.

https://securelist.com/analysis/quarterly-malware-reports/76464/kaspersky-ddos-intelligence-report-for-q3-2016/

There are three types of DDOS attack paths:

1) **Volume based DDOS:** As the name implies, this type of attacks depends on volume. The attacker employs a basic tactic, using a maximum number of infected devices to send messages to and overload your resources. The strength of volume based attacks is measured in bits per second (bps). The strength of these 2 attacks was in the range of 1 Tera (10^{12}) bits per second.An easy way to decrease the risk for such an attack is to share hosts and environments in the small tiers and configurations.
2) **Protocol Based DDOS**: The internet is all based on protocols (e.g. TCP), getting messages across. A Protocol based Denial of Service attack uses the basic protocols to bring a service down. Ping of Death, SYN (Synchronization) Flood, Packet modifications and number of other variations. These attacks are difficult to counter because of the fact that the used protocols are normally very low in the total protocol stack of the service.
3) **Application Layer**: This is highest layer of Open Systems Interconnection standard model for network communication. Most common attack path is HTTP (layer 7) flooding queries. It happens when an attacker makes use of standard GET/POST requests in an effort to overload your web server response ability. This attack is also known as a volumetric attack, it doesn't require malformed packets, spoofing or any variation of reflection techniques. The mentioned OVH and Dyn attacks were operated using this attack path.

To increase the amount of requests, to increase the chance to overload the targeted victim and also to hide themselves, attackers are using infected computers (also called zombies): they manage to install a piece of software that they remotely control. In a synchronous way, the attack occurs against the same targeted victim.

To deploy a DDOS attack you need:

- A victim;
- A botnet: piece of software enabling remote control;
- Zombies: machines infected with botnet;
- Remotely trigger the attack in a synchronous way.

Why are these DDOS attack experiences different from previous ones?

These attacks have been conducted against the same victim, using zombies flooding the victim with HTTP requests in a synchronous way.

These attacks are different from previous because:

- IOT devices are involved instead of standard computers. Enabling the massive attack.
- The number of zombies is enormous: 150.000 CCTV cameras and other IOT devices, all connected to internet without bandwidth limitation (30Mbps), giving a potential 150.000 x 30.000 = 4.5Tbps attack.
- Complexity of the attack is high: IOT devices (zombies) infection is very smart, based on sophisticated botnet software called Mirai, executed on multiple platforms (ARM, X86, MIPS). Also the way to infect the IOT device is smart, exploiting the IOT device low password security level. Mirai is capable to execute a password brute force attack on 2 protocols (SSH and Telnet) with 60 combinations of name and password. Most of CCTV were manufactured by Hangzhou Xiongmai Technology, with a very weak default password. This CCTV manufacturer is now recommending customers to update firmware and to change the password. The Mirai source code has been published on the internet one month ago.

Which protections on the IOT device?

Security should be evaluated as an integral component of any network-connected device. While there are exceptions, in too many cases economic drivers or lack of awareness of the risks cause businesses to push devices to market with little regard for their security. But, even though the networks devices might not be the prime victim of DDOS attacks, failing to design and implement adequate security measures in the device, might result in liability cases in front of a court of justice.

The analysis of the attack shows following threats and possible solutions:

a) Door opening: IOT device connection protocols are weak by default, RFC 2941 proposes a solution for authentication over Telnet but this is optional. Easiness is increased thanks to the use of a weak login and password.

   Solutions:

   - Force user to change password as a minimal solution
   - Implement mutual authentication based on a secretly held private key and a root of trust.

b) Get into the house: package/application installation is not controlled by IOT device operating system by default. As soon as you are logged in, Botnet can be installed.

   Solutions:

   - Disable firmware update/package installation
   - Enable only authenticated and integrity verified firmware update/package installation, thanks to trusted 3rd party (certificate Authority) public key stored into a root of trust.

c) No bandwidth limitation: botnet has access to full internet bandwidth, enabling enormous malicious traffic against victim.

   Solutions:

   - Limit bandwidth by default
   - Enable bandwidth change only for authenticated users, controlled with root of trust

Which protections on the potential victim?

The challenge with a Layer 7 DDoS attack lies in the ability to distinguish legitimate traffic from bot traffic, which can make it harder to defend against the volumetric attacks. As Layer 7 attacks continue to grow in complexity with ever-changing attack signatures and patterns, organizations and DDoS mitigation providers will need to have a dynamic mitigation strategy in place.

Possible Solutions, depending on, the type of attack, include:

- Use a Content Delivery Network
- Cloud operated Firewall protection: applicable to web site protection
- DNS providers usage is another protection
- Temporary block sensitive part of an application

What can WISeKey offer against DDOS attacks?

WISeKey, the Swiss based provider of secure authentication means, based on a Public Key Infrastructure, deploys large scale IoT digital identities for devices using its Cryptographic Root of Trust. The device identity and related private key and certificate are securely stored in a tamper proof chip that makes it very difficult if not almost impossible for an attacker to access this secret data. The device will use this secret data to securely authenticate to the network, verify the authenticity and integrity of firmware upgrades, and limit access to sensitive information to authentic users.

The flexible Certificate Management System from WISeKey can control the emission, use, prolongation and revocation of the certificates and thus control the IOT system's integrity from a central point of administration.

Depending in the required security level, targeted market or local regulations, WISeKey offers a range of hardware and software solutions, protection the sensitive information of your devices, of which the secure tamper proof chip is the highest level.

WISeKey is a one shop stop solution for a complete and secure control of your devices. Your devices will not become a target for botnets and DDoS attacks cannot be perpetrated from your system.

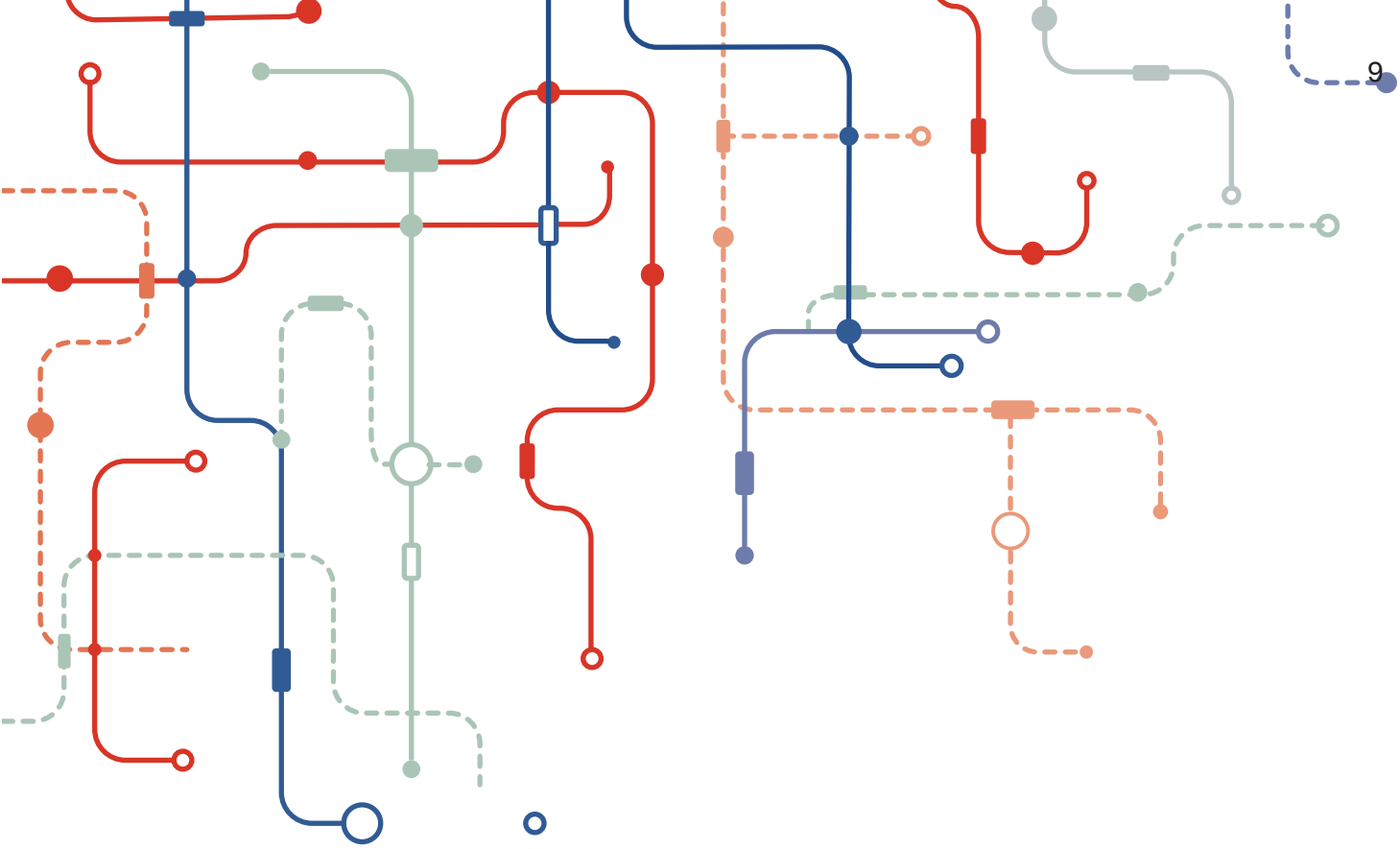
Additional, your devices equipped with the state of the art certificate based security means, will be protected against cybersecurity treats like:

- Illegitimate installation of firmware: for example firmware from third party sources that modify the behaviour of the device, change the level of service provided, open backdoors for eaves droppers or greyware that spy on the behaviour of the device owner. Think of jailbreaking an iPhone or rooting an Android device;
- Capture of sensitive data: Consumption data that is sent periodically by an electricity meter could be an indication for a criminal of the absence of the home owners to plan a burglary. The images from a video surveillance system, when captured by a hacker can be used for the same reason, or for blackmailing a victim (http://www.networkworld.com/article/2844283/microsoft-subnet/peeping-into-73-000-unsecured-security-cameras-thanks-to-default-passwords.html);
- Repudiation: An unprotected data stream from a device can be recorded and replayed by an attacker, it can be modified, it can be intercepted, and finally the data cannot be trusted. A legitimate owner of a device could always repudiate the data if it's integrity or authenticity is not granted;
- Counterfeiting of the device: If not protection is present, a third party could sell compatible devices with different characteristics, putting your revenue stream, your installation of even the life of people at risk.

The bottom line is that when securing your IOT devices with WISeKey's state of the art PKI system it will protect the internet against DDOS attacks, as well as give additional, but not less important protection against for instance theft, spoofing, eaves dropping, modification, counterfeiting, and protect your revenue stream, your image and your intellectual property.

Glossaire

CCTV	Closed Circuit Television
DDOS	Distributed Denial of Service Attack
DNS	Domain Name System
HTTP	Hypertext Transfer protocol
IOT	Internet Of Things
Mbps	Megabits per second
PKI	Public Key Infrastructure
Tbps	Terabits per second
TCP	Transmission Control Protocol



Contact

WISeKey SA

Mob: + 41 (0)79 946 00 89
Tel: + 41 (0)22 594 30 40
www.wisekey.com

WTC II • 29, route de Pré-Bois
1215 Geneva • Switzerland

Stay connected with @WISeKey

WISeKey Semiconductors

Arteparc Bachasson • Bât A
Rue de la carrière de Bachasson
13590 Meyreuil • France

TMP_PRD_003 v6.1