Information & Security: An International Journal

Rademaker & Gauw, vol.32, 2015 http://dx.doi.org/10.11610/isij.3202

TRUSTED NETWORKS INITIATIVE: THE NETHERLANDS' RESPONSE TO DDOS ATTACKS

Michel RADEMAKER and Marc GAUW

Abstract: Cybercrime is on the rise and distributed denial of services attacks are among the most used by hacktivists, criminals, and even states. This article focuses on a Dutch solution to that problem, namely the Trusted Networks Initiative. The initiative aims at a global trust concept that provides website operators with a last resort option in case a large or long-lasting DDoS attack cannot be mitigated by other anti-DDoS means. The paper describes the foundational principles of the initiative, and more specifically the intended solution via the trusted routing concept.

Keywords: cybercrime, DDoS attacks, cluster, trusted routing, Internet exchanges.

Introduction

Cyber security in modern societies is more and more handled as an issue of national priority to guarantee the unhampered functioning of society as a whole and enable private enterprises and governments, as well as the public to optimise the use of their information and communication technologies and systems. However, the pervasive nature of the technologies utilised in the everyday life of businesses, individuals and public organisations requires constant attention and innovative approaches. Not only to harvest opportunities but also to mitigate the threats that inherently come from misuse and abuse of the cyber domain by script kiddies, hacktivists, criminals and even states for a thrill, economic or political reasons. Cybercrime as a Service (CaaS) is on the rise. Distributed Denial of Service (DDoS) attacks, among others, are often used by these players. And it is reported that DDoS attacks are getting stronger, last longer and are here to stay. In the Netherlands, the cyber security research and innovation community is actively engaged in finding solutions and tools to help mitigate these threats.

As a private initiative, welcomed by the business and governmental communities, a new solution is developed called the *Trusted Networks Initiative* (TNI). The initiative

is made possible by The Hague Security Delta[1] and NLnet[2] foundations. The initiative came to fruit because of the urgency to institute mitigation measures against DDoS attack on the one hand and the opportunity The Hague Security Delta provided in being an independent cluster of businesses, knowledge institutions, government bodies and educational organisations. Being independent, trustworthy and highly visible helped getting organisations convinced that the TNI solution is feasible, non-partisan, does not hamper net neutrality and is allowed by legal standards. TNI also fits perfectly the ambitions outlined in the most recent National Cyber Strategy of the Netherlands,[3] which stresses the importance of enhanced cooperation between governments and businesses and declares that The Netherlands is resilient to cyber attacks and protects its vital interests in the digital domain.

What is the Trusted Networks Initiative?[4]

The Trusted Networks Initiative aims at a global trust concept that provides website operators with a last resort option in case a large or long-lasting DDoS attack cannot be mitigated by other anti-DDoS means.

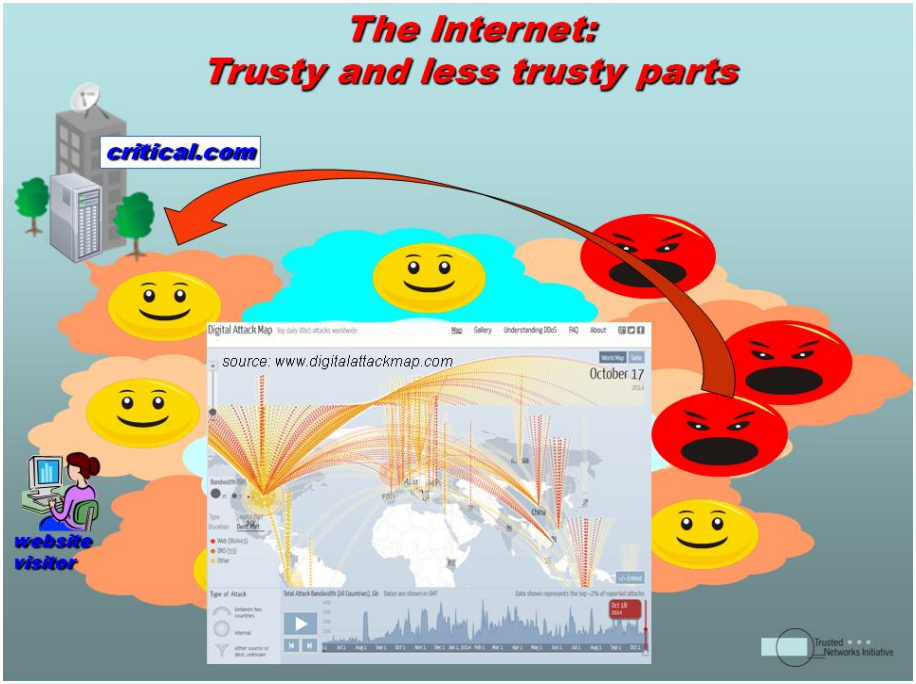

Figure 1: Some DDoS-attacks may become too big to handle.

The project is launched in The Netherlands[5] by a group of critical-website operators like financial institutions, access networks, internet exchanges, governmental organisations and supporting institutes, who recently kicked off the initial Trusted Routing concept that currently operates in beta mode.

The principles of the solution are simple. Each participating network at its sole discretion can step to "trusted internet only" if an emergency situation requires to temporarily disconnect from the global internet. In practice, this means that an organisation under heavy DDoS attack can decide to disconnect and have only traffic within the trusted parts on the internet. Initially, the trusted part of the Internet will primarily be The Netherlands. So, for example, when a person with a Dutch bank account on holiday at the Caribbean island Curacao via his personal computer orders a pair of shoes via an e-shop and pays digitally via his bank account, while at the same time the bank is under heavy DDoS attack and disconnected from the untrusted parts of the internet, he will not be able to pay. However, while doing the same in The Netherlands, he will still be able to perform this transaction. Consequently, instead of a complete stop of any internet traffic, the bank is still up and running in limited access mode.

Any network, content or access provider can participate in the trusted domain as long as they commit to a certain minimum of:

- DDoS preventing technology;
- Sufficient organisational response to DDoS events; and
- Respect to common laws.

Trusted Routing Concept

It should be noted that the Trusted Routing is not a new alternative for existing mitigation and scrubbing solutions to clean internet traffic, but specifically developed as an additional last resort solution on top of these existing services. Current initiatives as the Nationale Wasstraat NAWAS[6] (Dutch for "National Scrubbing Centre") may already work well for the majority of the DDoS attacks, and allowed this project to be of identical success in The Netherlands. However, none of the available solutions can secure a 100 % protection, and that created the demand for an additional last resort option.

Within the Trusted Routing concept the participating networks use existing anti-DDoS services, but route their internet connectivity via both "the global Internet" as well as the "trusted domain" of the Trusted Networks Initiative.

Currently, joining parties are primarily Dutch websites and operators. However, the solution is implemented at two of the largest Internet exchanges on the globe: AMS-IX (www.ams-ix.net) and NL-ix (www.nl-ix.net). Over 1000 connected international

hosters and networks are connected to these exchanges, and can therefore easily connect to the trusted routing upon being qualified.

The "trusted domain" is available via a dedicated VLAN-112 and a dedicated route server, as configured at both exchanges.

Parties interested to join the "trusted domain" can qualify at the independent Trusted Networks Initiative for meeting the Trusted Network policy requirements and then get connected to these exchanges, to activate the Trusted Routing to other participants.

The Trusted Routing route server is configured in standby-mode, and is only to be used in the case of emergency. Participating networks should first try to solve the DDoS attacks with their own generic mitigation solutions; however, they have the last-resort option to reroute to the trusted domain if the attack becomes too big or too long to handle generically. The Trusted Routing to other "Trusted Networks" is activated independently by each individual network. There is no "central authority."

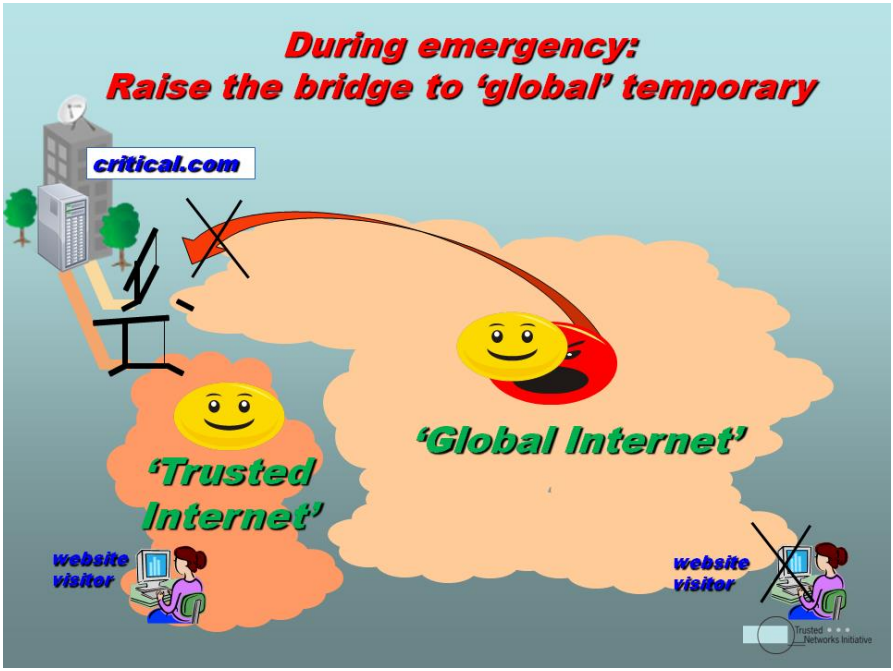

Figure 2: As a last-resort: Raise the bridge for attacks.

The Trusted Networks Initiative is focusing at content operators with (critical) websites using their own AS, IP and BGP4 routing facilities. Additionally, the initiative is focusing at fixed and mobile access networks with a significant number of subscribers that should always be able to visit the (critical) websites.

Conclusion

The Trusted Networks Initiative[7] is at the moment developed to be used for the Netherlands. It is a technical concept, and the certification procedures are not limited to the Netherlands alone. The internet exchanges NL-ix and AMS-ix have many international members already, and are also present in multiple countries. From this perspective, The Netherlands turns out to be an ideal country to bring this initiative further abroad, since it is just "a click of the buttons" to get many other internationally trusted parties to join the initiative as well. Moreover, other internet exchanges may join as well to expand the concept even further. So, in due time this solution could be a globally rolled out option to bring the Internet a step further in being safeguarded against DDoS-attacks.

Notes:

1 The Hague Security Delta (HSD) is the largest security cluster in Europe. The security cluster aims to stimulate economic development and innovation in security. The foundation acts as a driving force, responsible for the implementation of the strategic direction and the international promotion of the security cluster through trade missions, communication and acquisition of companies, institutions and conferences.

2 The foundation "Stichting NLnet" stimulates network research and development in the domain of Internet technology. The articles of association for the NLnet foundation state: "to promote the exchange of electronic information and all that is related or beneficial to that purpose." NLnet does not directly benefit from the undertaken projects, and all developments are published as Open Source.

3 Interested readers can find further information at https://www.ncsc.nl/english/current-topics/news/new-cyber-security-strategy-strengthens-cooperation-between-government-and-businesses.html.

4 For more information see https://www.trustednetworksinitiative.nl.

5 A similar project called FENIX is developed in the Czech Republic. The FENIX project was created by the Czech peering node NIX.CZ primarily as a reaction to intense DoS attacks targeting Czech internet services, media, banks and operators in March 2013.

6 Information on the Nationale Wasstraat NAWAS is available on: http://www.nbip.nl/diensten/nawas-demand-beveiliging-tegen-ddos/.

7 For more information on the concept of the Trusted Networks Initiative of The Netherlands see www.trustednetworksinitiative.nl or send an email to info@trustednetworksinitiative.nl.

Michel RADEMAKER is the Deputy Director of The Hague Centre for Strategic Studies (HCSS), www.hcss.nl. He has a degree in Transport and Logistics, obtained from the University of Tilburg. He gained fifteen years of hands-on experience as an officer of the Netherland Royal Army, where he held various military operational and staff posts and served a term in former Yugoslavia. After leaving the armed forces, Mr. Rademaker went on to work at TNO, The Netherlands as a project and programme manager and senior policy advisor for ten years. At the HCSS Mr. Rademaker is responsible for business development. He is particularly interested in setting up multi-stakeholder projects on new and upcoming security and political economic themes. He is one of the initiators of the Hague Security Delta (HSD), the largest security cluster in Europe, and leads projects for this cluster. His fields of expertise include security strategy, policy, concepts and doctrines, technology surveys and assessments, and serious gaming techniques. Mr. Rademeker is a Guest Lecturer at Webster University and the University of Amsterdam.

Marc GAUW is general director at NLnet foundation. He brings a wide range of experience from the internet and telecoms industry to NLnet. Between 2008 and 2014 he was Commercial Director at NL-ix, in which period it grew to become the fifth largest Internet Exchange on the planet. Prior to that, he worked at Priority Telecom, AUCS, Unisource and KPN International. He was Chairman of the Executive Board of Amsterdam Internet Exchange for four years, and executive member of the Board of COIN for three years.