Aalto University
School of Electrical
Engineering

Cooperative Security for the Internet and 5G

Raimo Kantola
raimo.kantola@aalto.fi
Aalto University, Comnet, Finland

University of Cambridge – Computer Lab/FW26 - Thu, Sep 29th, 2016

Agenda

- Research Background
- Customer Edge Switching
- Realm Gateway
- Policy Management
- Privacy Preserving Trust Management for the Internet

www.re2ee.org & ResearchGate

Background

Current security attitude: I worry about my hosts and my network

- **I don’t care what other people do**
- **I cooperate with other people if forced to by the Regulator**
- **I don’t want to reveal any bad stuff that happened in my network if not forced to do so**

BUT…

State-of-the art in cooperative security

- **CERT – national cyber security…**
- **Vulnerability data bases**
  - CVE – Common Vulnerabilities and Exposures
- **Sharing of threat intelligence**
  - E.g. to combine cloud capabilities with host based security software functions
  - Vendor specific

Scattered developments/few standards/no ubiquitous deployment

Nrof security breaches/a is not going down!

What is a Customer Edge Switch?

- **Replacement and Generalization of NAT**
- **Cooperative Firewall**
  - Flows admitted by policy
- **An Address/ID split solution for the Internet**
  - Globally unique AND private addresses (IPv4, IPv6, Ethernet)
  - FQDN (or Service FQDN) for identification
- **Edge to edge tunneling endpoint**
- **Split to Control/Data plane**
- **Deployment: one customer network at a time**

Signaling Cases

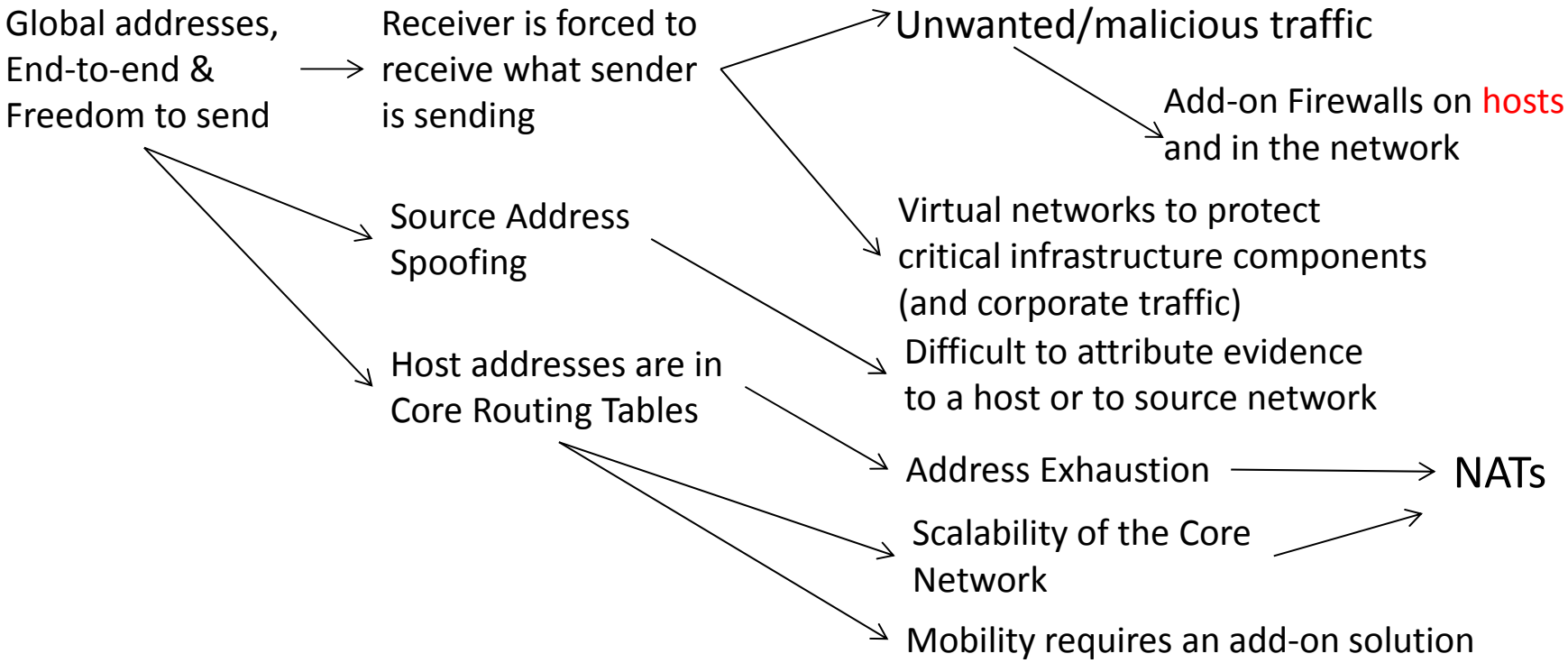
	Legacy receiver	Receiver behind CES
Sender Behind CES (new Edge)	CES acts as NAT	**Customer Edge Traversal Protocol** used To signal tunnels Thru the core
Legacy IP sender	Traditional Internet	Inbound CES acts as ALG/ **Private Realm Gateway** or server side NAT

Emerges from “Future Internet” research topic

- Exhaustion of IPv4 addresses
- Scalability of the core of Internet (large routing tables)
- Unwanted/malicious traffic
- IPv6 has been around for a long time but adoption is not taking place as expected by IETF
- Role of IP has been going down, add-on solutions like MPLS, Firewalls, NATs are playing an increasing role → deterioration of the Architecture
- Power consumption is becoming an issue
- Poor fit of IP to the needs of wireless battery-powered devices:
  - Internet has 3,5B users, AND 3.6B are using mobile broadband (by end of 2016)!

Hundreds of projects in the US, EU, Japan, China, Korea etc.

Causal relations of the problems(1)



Causal relations of problems (2)

Private addresses&
Network Address Translators
(or NATs)

→ Hosts with private addresses normally not reachable

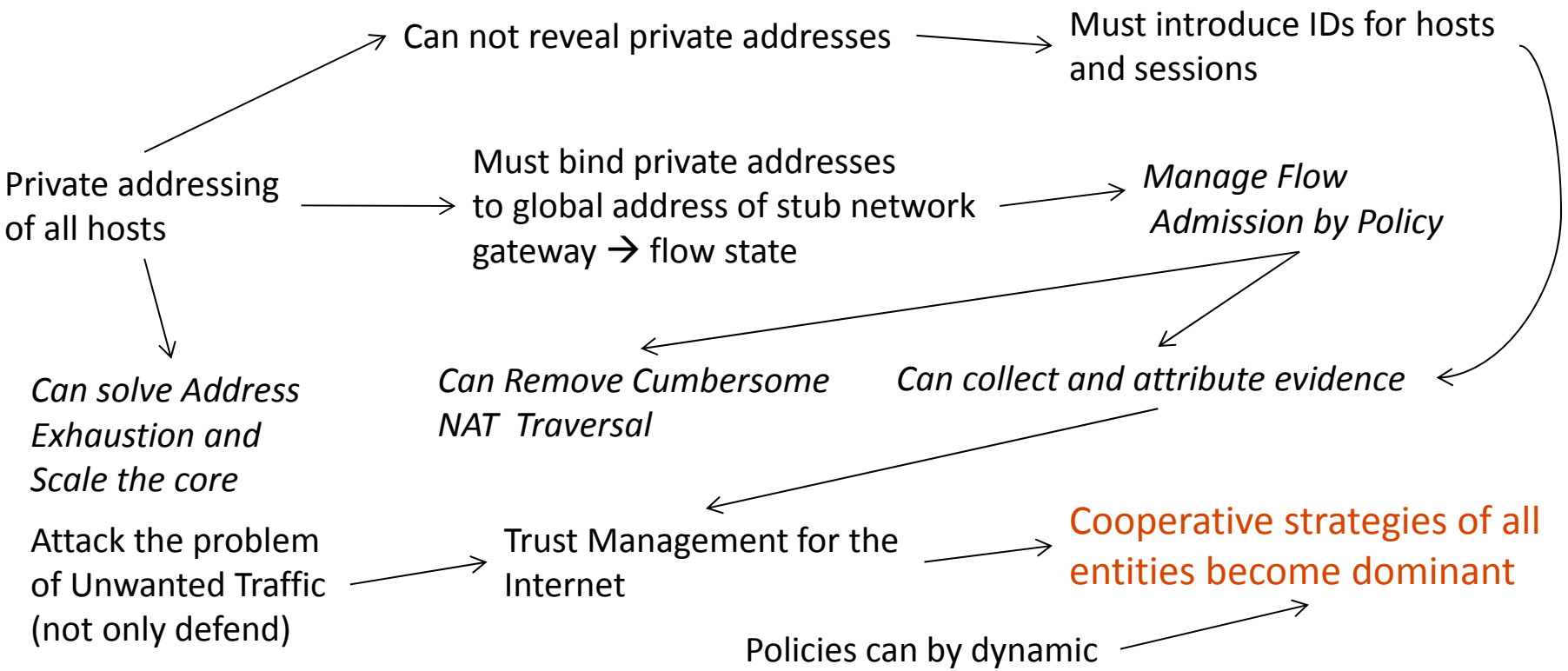
→ Cumbersome NAT traversal mechanisms (STUN, TURN, ICE):
- Overhead on air interface
- Slow session setup
- Battery consumption
- Application specific code
- Security?

IP over everything → Difficult to optimize using several criteria

Related work

- Proposals can be classified by where changes are required:
  - Hosts; network nodes; if network nodes, which?
  - It is critical for adoption that the investor gets his money back
- IPNL, TRIAD, MILSA, Pub/Sub, Shim6, HIP, PBS (permission based sending), Information Centric Networks
- Typical weaknesses
  - Most popular motivation: scalability of the core → where is the new revenue?
  - Have to make changes in many places
  - Investments and benefits are not perfectly aligned or for some proposals: start Melcalfe's law from zero!

Solution logic: reshape Internet based on IPv4

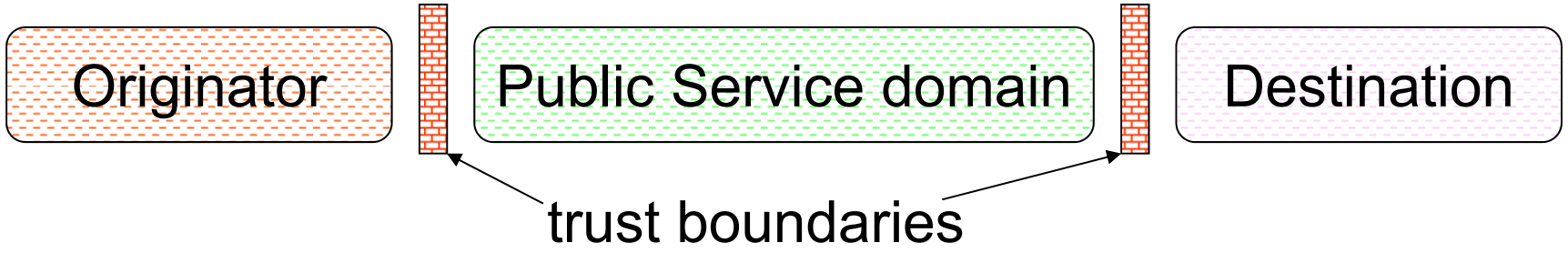


Business: makes sense to pay attention to where the growth is: mobile broadband!

Constraints on the solution

- Because we can not solve the problems of unwanted traffic and NAT traversal in hosts for battery powered wireless devices
  - → MUST change a network node
  - → MUST not require changes in hosts at all
- Changes only in one place at a time: must bring benefit to the adopter irrespective what other players are doing

Communication over Trust Domains

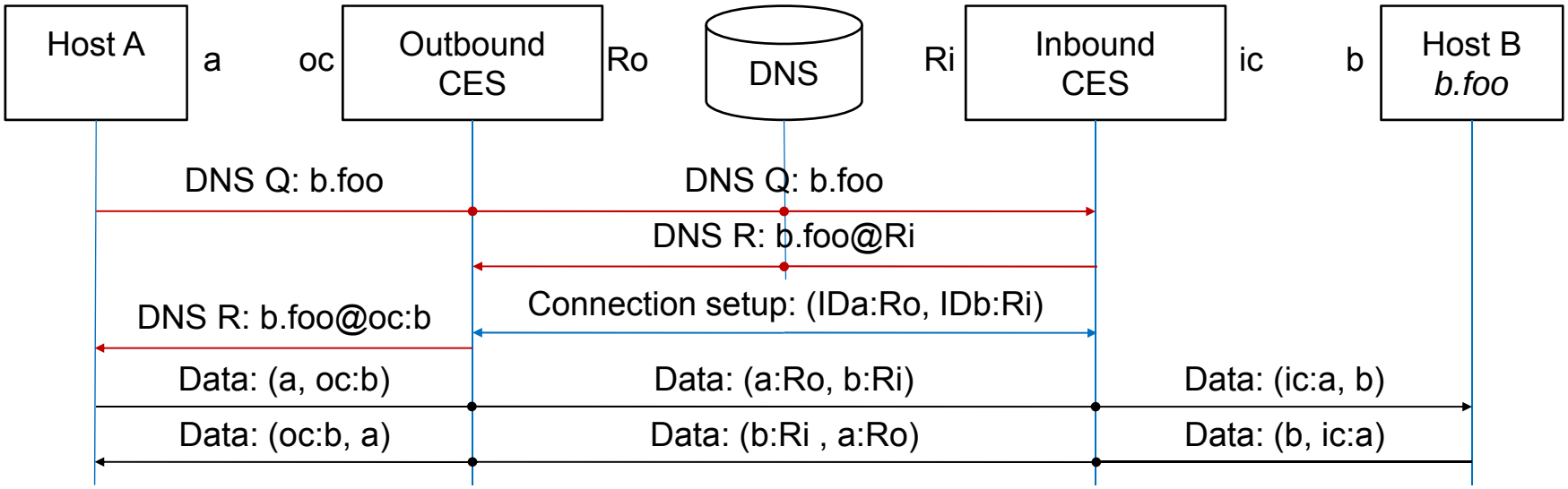


Originator and Destination are customer networks (stub networks in terms of IP routing)
+ each of them may have one or many private address spaces;
+ extreme case: mobile network addressing model: each user device is in its own address space and all communication takes place through the gateway or edge node connecting the user devices to the Internet

Trust Boundary == Customer Edge Switch == cooperative firewall

A CES has one or several RLOCs (routing locators) that make it reachable in the public service domain

Customer Edge Switching PoC



a – IP address of host a
b – IP address of host b
Ro – Routing locators of outbound CES
oc – Address pool of outbound CES
oc:b – IP address representing host b to host a
IDa:Ro – Representation of IDa in outbound CES
a:Ro – Representation of hosta in outbound CES

IDa – ID of host a
IDb – ID of host b
Ri – Routing locators of outbound CES
ic – Address pool of inbound CES
ic:a – IP address representing host a to host b
IDb:Ri – Representation of IDb in inbound CES
b:Ri – Representation of hostb in inbound CES

CES can…

- Switch between IPv4/IPv6/Ethernet – is agnostic to forwarding protocol
- Execute outbound AND inbound policy
  - –We separate CES policies from Host policies
  - –ASK for any types/values of IDs, certificates
  - –iCES can ask oCES to slow down

Experience from the first PoF Customer Edge Switching

In principle it works – Robot framework testing ongoing

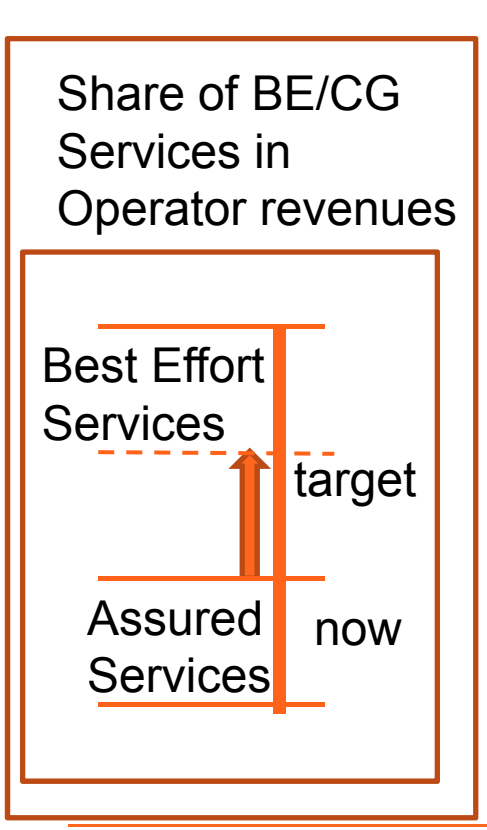
But

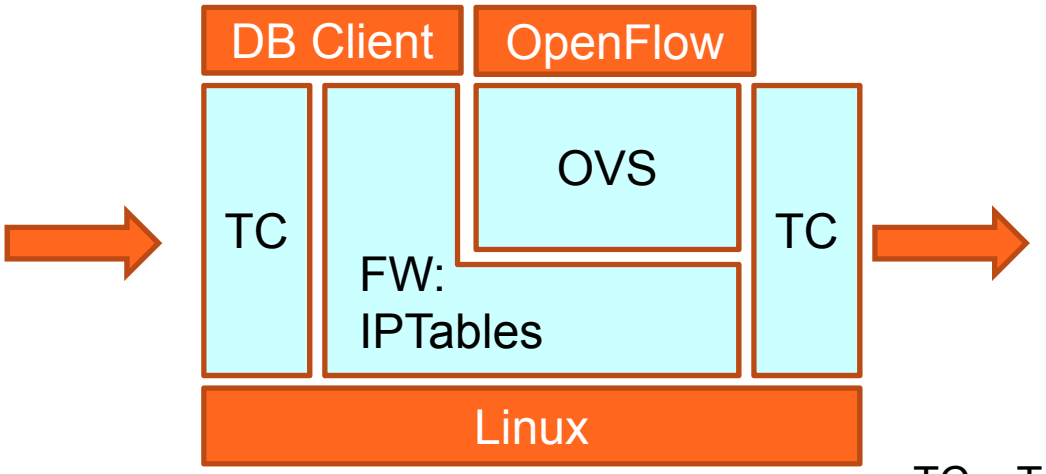
- **One can not implement a real FW with OpenFlow Switch, because**
  - *OpenFlow has limited set of operations for processing packets*
  - *No general purpose – packet level processing except send it to Control Plane*
  - *FW → must send **all** packets to CP*

Now moving to OVS + Linux dataplane node

- **Linux can do packet level processing in kernel: IPTables**

Practical Data Plane of Edge Gateway





TC – Traffic Control

Role of OVS: mangle packets/reformat forwarding formats

Role of IPTables: packet filtering, rate limiting of nrof new flows, rate liming of service flows, spoofing elimination

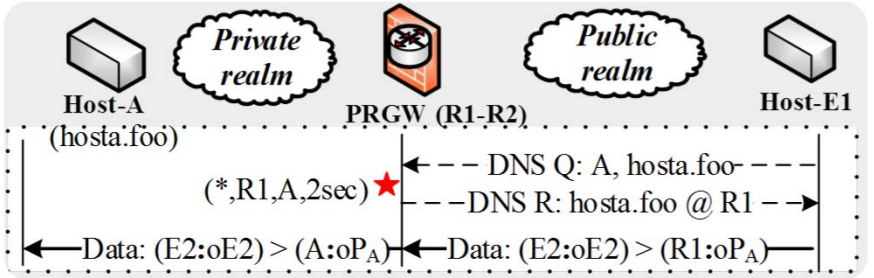
CP resides in the DC and will have rules DB, Flow level Firewalling logic with edge to edge signaling and Connection control

TC and IPTables use a common flow abstraction

Introduction to Private Realm GW

IFIP Networking 2016

- PRGW is a client and server-side NAT solution.
- Deployment:
  - *It can replace NATs at network edges, or can be part of a rich cooperative firewall.*
  - *Doesn't require changes in end-hosts or applications.*



- Operations (compared to NAT):
  - ***For outbound connections**, the behavior is same as NAT*
  - ***For inbound connections,** CPPA admits an inbound flow, following the reception of a domain query for Fully Qualified Domain Name (FQDN) of the private host.*
- Advantages:
  - *Scalable NAT traversal solution, optimal for mobile devices.*

PRGW solution

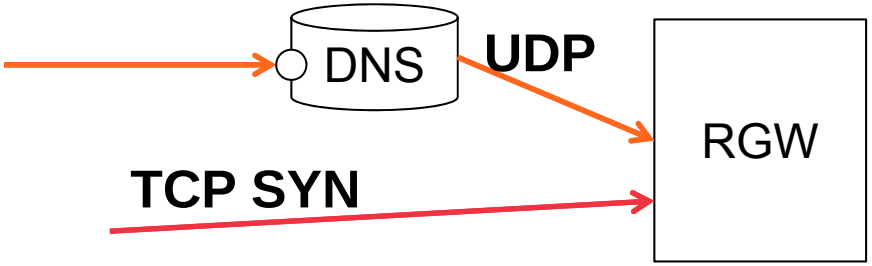
- Circular pool of public IP addresses (CPPA) enables unilateral initiation of connection towards the private hosts.
- Upon receiving a DNS query for FQDN of the private host, PRGW creates a temporary ***half connection state***, *which* allows forwarding of the subsequent inbound flow to the private host.
  - *It contains a public IP address from the pool to represent the host in the Internet.*
  - The half connection state applies ***endpoint independent filtering*** **relative to the client**
- Upon receiving the first inbound packet from the client, PRGW creates a ***full connection state*** for the flow and returns the allocated public address to CPPA for future allocations.
  - *Full connection state applies* ***address and port dependent filtering*** *relative to client.*

Principles of Security mechanisms

It is possible to take clean-slate approach to design new architectures free of any weaknesses, at the cost of a huge deployment difficulty. In our work, we take these deployment constraints in account.

1) To favor deployment, security algorithms and heuristics shall not require changes to end-hosts, protocols, or application.
2) Flow acceptance must be limited to verifiable sources, to tackle address spoofing and prevent resource exhaustion
3) UDP flow initiations are admitted only after a connection has been signaled through a secure channel e.g. SIP(s) → Now adding “loose UDP”
4) Under the network stress, resource access should be granted based on the source reputation.

Preventing DNS Abuse/Exploitation



Normally, DNS runs over UDP + initial requester info/path of the request
Is not present in the query

- **Spoofing → reflection attack**
- **There are DNS servers (e.g. Google) that respond to any host**

Run DNS over TCP → eliminate spoofing
SLA with ISP: use ingress filtering = serve only known hosts
→ Whitelisted/Grey/Black DNS servers
Rate limit/DNS server + Rate limit/destination FQDN

Preventing DNS Abuse/Exploitation (2)

- **DNS Relay front end:** implemented to protect PRGW from direct exposure to the Internet. This is to prevent the CPPA exhaustion from malicious domain resolutions, e.g. inbound DNS floods and spoofed requests. Under this model, PRGW is protected by virtue of delegating the DNS security to its ISP.
- The approach draws upon the use of DNS reverse proxies in ISP networks and cloud-based security solutions that aim to secure networks against DNS abuses.
- The delegation of security to a dedicated DNS-Relay element offers multiple benefits:
  1) *It lessens the load of executing the complex DNS security algorithms from PRGW.*
  2) *The dedicated relay element can independently leverage the existing state-of-the-art and future research in DNS threat detection, to serve the PRGW with legitimate traffic only.*

Preventing DNS Abuse/Exploitation.. (3)

Name Server classification

- *PRGW classifies the public DNS servers into: whitelist, greylist and blacklist. Servers on each list are treated differently in PRGW and are dynamically promoted/demoted, based on the influx of attack traffic.*
- *Whitelist servers are specifically configured in PRGW. By default, rest are greylisted*
- *Whitelisting can be based on business contracts and service level agreements (SLAs) between service providers, and may require networks to meet a set of pre-conditions.*
  - For example, Use DNS/TCP to forward domain requests, DNSSEC, ingress filtering

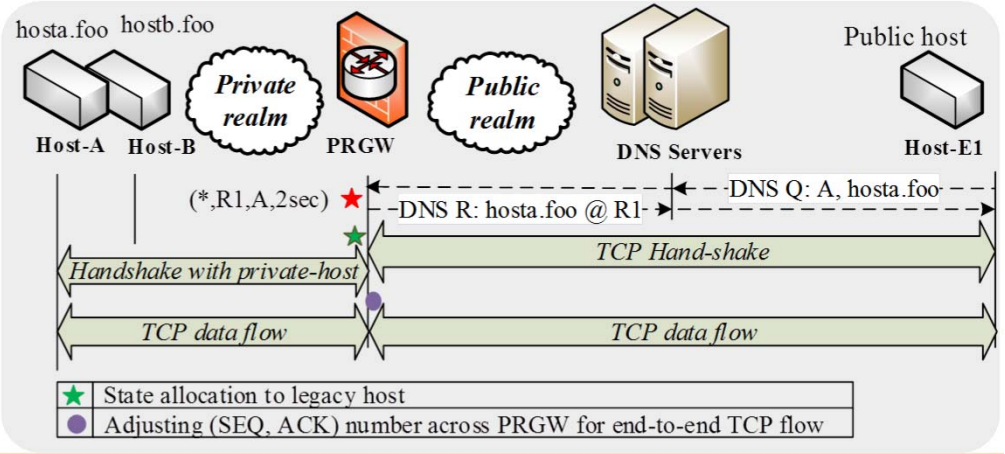
- **Circular pool address allocation model**
  - *Rate limits the number of simultaneous DNS queries from a DNS server.*
  - *Rate limits the number of simultaneous DNS queries to a private host/service.*
  - *Total CPPA allocations to greylist servers < a portion of the circular pool.*
    - Ensures that under the load situation, whitelist servers have preferred access to PRGW.

Filtering Malicious flows.. (1)

- TCP-Splice
  - *Ensures that resources (i.e. half-states) are only allotted to non-spoofed senders.*
  - *Use of the SYN cookie requires that TCP flow is relayed across PRGW. The relay itself must adjust the SEQuence and the ACKnowedgement number on both sides of the PRGW, to maintain the end-to-end semantics of the TCP connection.*

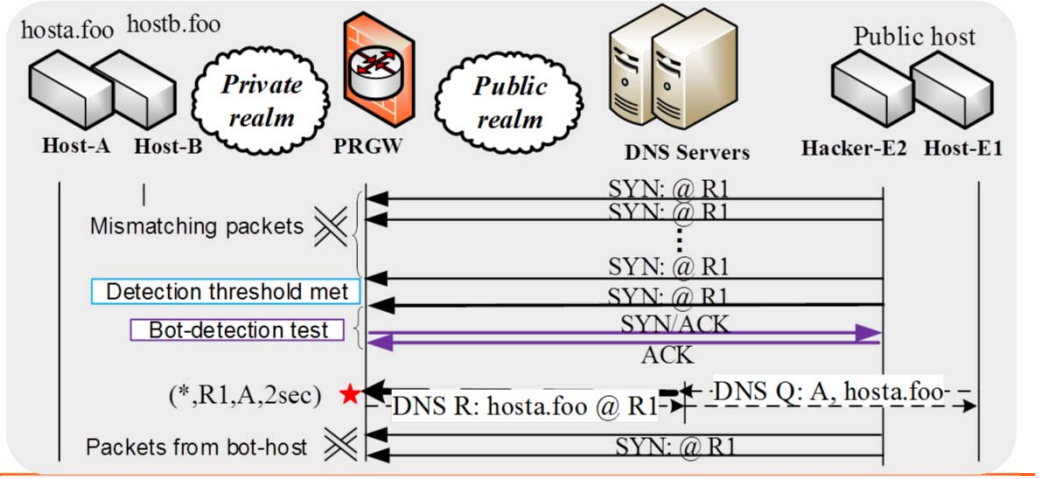
- Outcome:

  Eliminates spoofing in admitted flows



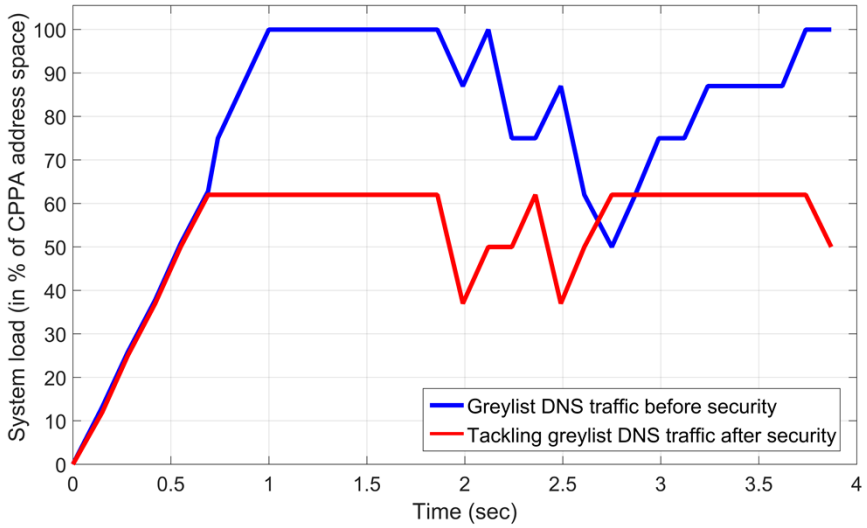
Filtering Malicious flows.. (2)

- Bot-Detection method
  - *Complements the limitations of TCP-Splice*
  - *Attempts to protect PRGW against SYN floods from botnets*
- Outcome
  - *Filters flows from aggressive non-spoofed sources.*



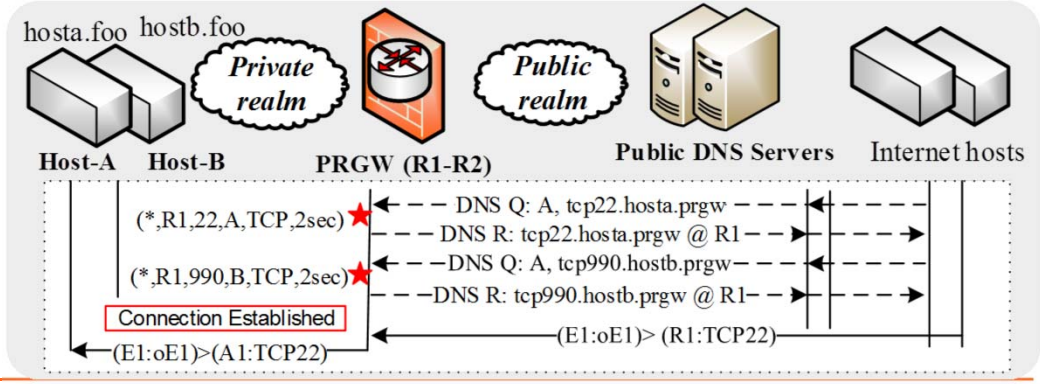
Security Evaluation: White/Grey DNS servers

- Protection against DNS floods
  - *Without heuristics*, DNS flood would reserve all the CPPA resources and force PRGW into DoS.
  - Address allocation model notes that the DNS source is greylist, and limits the resource allocations to a portion of the circular pool.
  - This ensures preferred access to whitelists servers, particularly under attack/load conditions.



Service FQDN

- New algorithm for allocating the public IP addresses of the circular pool.
- The underlying idea is to address the services and endpoints simultaneously.
  - *For example, an SSH service at Host A – a.foo can be represented as ssh.a.foo or it can be defined as combination of port number and transport protocol:* ***tcp22.a.foo***.
- Since it includes both the endpoint and the service, PRGW creates ***endpoint independent but port dependent filtering*** in the half state relative to the client.



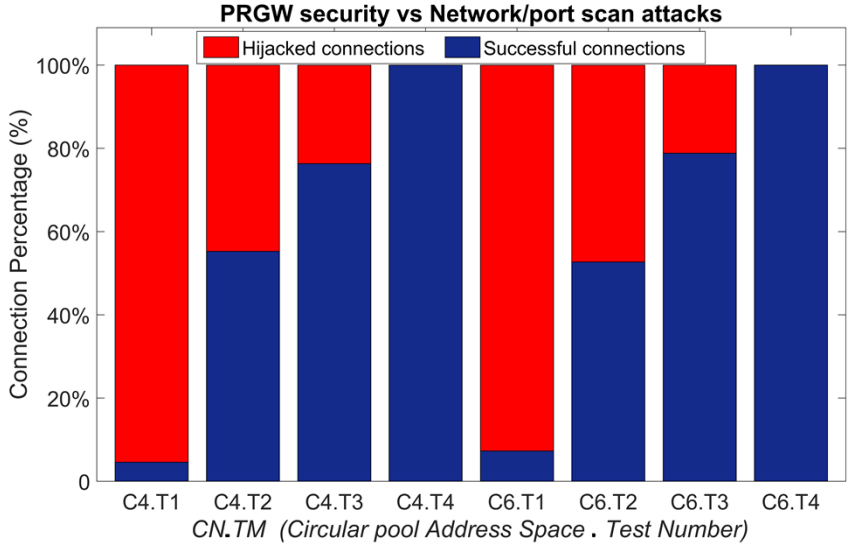
Advantages of Service FQDN

- *More specific half connection state,*
  - allows reusing a public IP address for several different services, improving the scalability of CPPA.
  - contributes to security, by increasing the attack surface for hacker i.e. Hacker must target the allocated port besides the public-IP → more difficult to force the blocking state.
  - Attacker will have more opportunities to meet the detection threshold, and get blacklisted.
- *Service-FQDN = key to incoming security policy*

Security Evaluation – Quantifying sFQDN

- **Contribution of Service-FQDN (SFQDN)**
- Stress the prototype with below traffic patterns, at network delay of 200 msec and a constant load of 4 connections per second.
  - *Connection load is distributed among private hosts. -> Exponentially distributed.*
  - *In parallel, a network scan attack at 40 SYNs/sec from public nodes targets PRGW.*

  - *Inbound traffic patterns:*
    - Test1: 100% FQDNs based inbound traffic.
    - Test2: 50% of the inbound traffic is FQDN.
    - Test3: 75% of inbound traffic is SFQDN; the rest FQDN.
    - Test4: 100% of the inbound traffic is SFQDN.



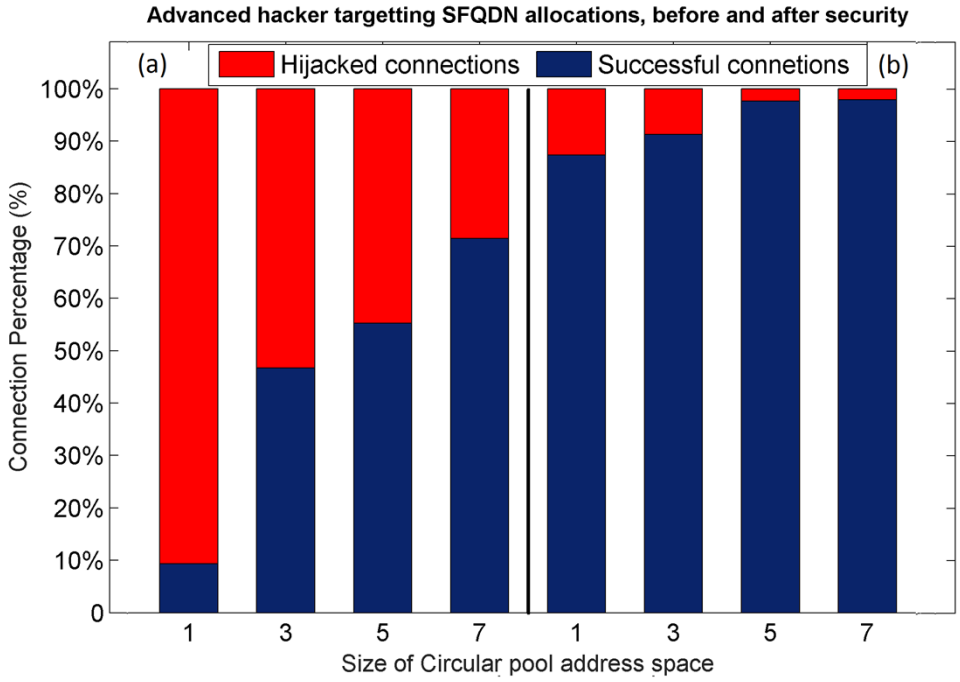
Security Evaluation: spoofing

- **Filtering of malicious flows**
- Due to TCP-splice mechanism, packets from spoofed addresses failed to claim any half connection states.
  - *TCP-splice obviates spoofing, at the cost of delaying claim to the connection state.*
  - *In terms of performance, this limits the reusability of the public IP address and the port combination by the same duration for the next inbound connection.*
- For non-spoofed (i.e. bot-controlled hosts)
  - *Bot-Detection would track the sender of repeatedly mismatching packets, and then performs a bot-detection test. When detected as non-spoofed, it is blacklisted.*
  - *Under this method, an attack with more active bots is filtered.*
  - *It is possible that a hacker stays below the Detection threshold and thus avoids Bot-Detection.*

Attack proficiency vs PRGW Security

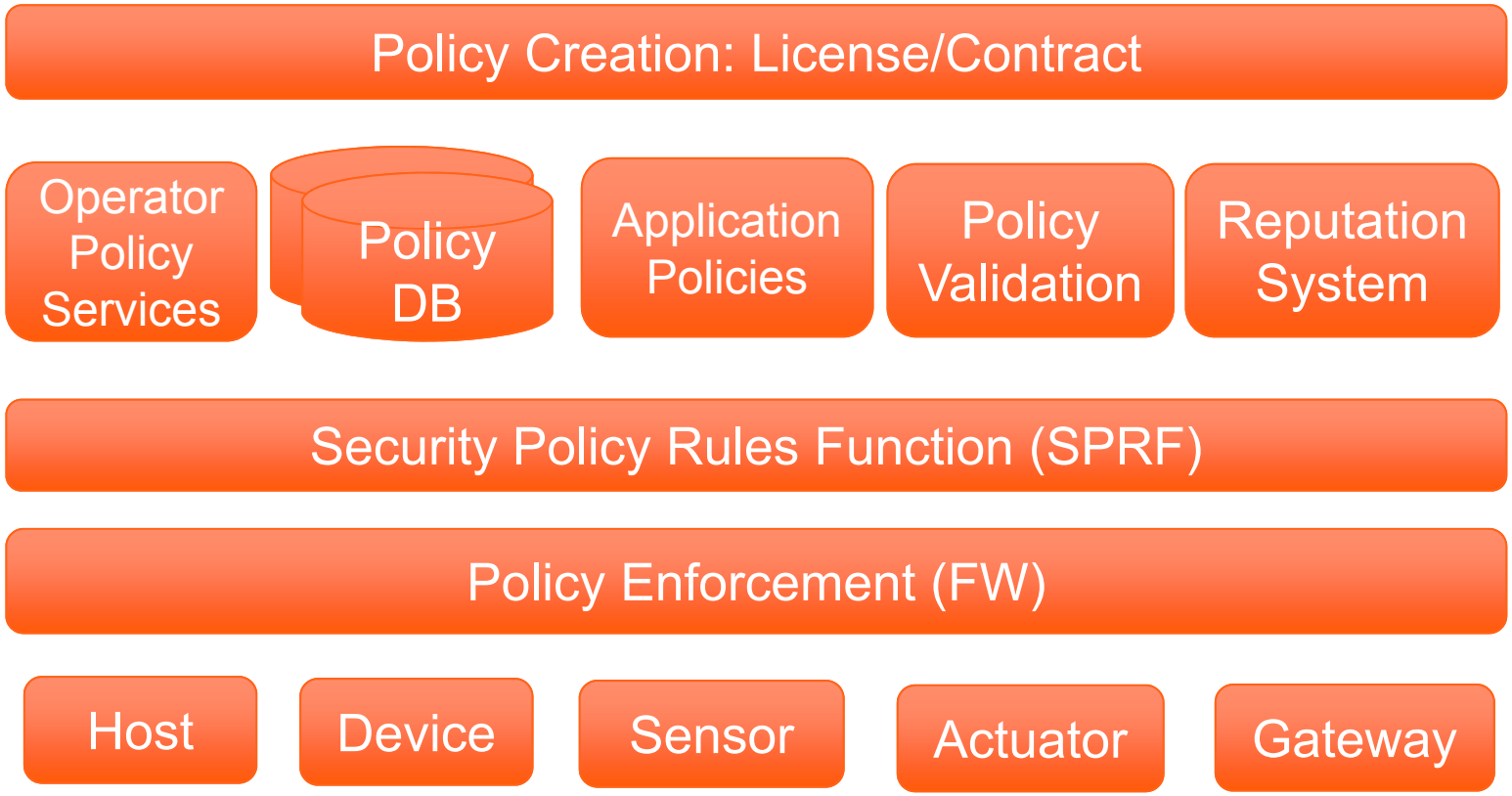
- Hacker proficiency
  - *a) Probing/scanning/amateur hacker*
    - A probing hacker scans the entire CPPA address space and port range to discover the available services, IP addresses or NAT mappings.
    - Such an attacker due to its limited victim's knowledge will fail to attack PRGW
  - *b) Advanced hacker*
    - may already know services/ports in the target network,
      via knowledge sharing among hackers or by consuming bots from bot-rental business or
      via first setting up legitimate flows thru RGW
    - As a result, the hacker can target the SYN floods to the specific service ports.

Attack proficiency vs PRGW Security



In case the same organization
Owns the network with servers
And the clients→
Device management can change
The ports used for services
→ Wider attack surface

Policy Architecture for CES networks



Privacy preserving unwanted traffic control based on trust management

Motivations:

- Many entities either refuse or are reluctant to share attack evidence
- Monitoring of traffic by ISP is not allowed because of privacy of communications without evidence of malicious activity

Our proposal → a privacy preserving unwanted traffic control based on trust management and homomorphic encryption.

Principles of Privacy Preserving Trust Management for the Internet

- Entities: Host/corporate network; ISP; Trust Operator
- Host/corporate network shares evidence in encrypted form – its Identity is anonymized by ISP
- ISP aggregates evidence using Homomorphic crypto
- Trust Operator processes → Trust and credibility value for each entity → Send Greylist to ISP=authorize ISP monitoring → ISP Decrypts suspect IDs → Monitored list by ISP → ISP monitors, gets conclusive evidence → containment + deliver black lists to all CES

References

1. www.re2ee.org
2. ResearchGate

Thank You
(Questions? )

A”