Policy-based Communication

- Communication in CES is policy controlled.
- Hosts define these reachability (or admission) policy in CES.
- CES negotiates policy elements on behalf of hosts that it serves.
- These policy elements are represented by CES as TLVs, in Customer Edge Traversal Protocol (CETP).
- We have defined number of these policy elements for CES, and they are *group*ed as *ID*, *RLOC*, *Payload* and *Control* elements.

- We identify these elements using TLV Group and Code values; the code identifies the exact policy element within each group.

Policy elements

Group	Code	Description
Control	cesid dstep terminate warning ack ttl ratelimit headersignature certificate	The CES ID The destination endpoint ID Contains the terminating information Contains the warning information The acknowledgement cookie The time-to-live for the session The rate limitation for the session CETP header signature CES-certificate
ID	fqdn maid moc	FQDN of the host Mobile assured-ID of the host Mobile operator certificate
RLOC	ipv4 ipv6 eth	IPv4 address of CES IPv6 address of CES MAC address of CES
Payload	Ipv4, ipv6, eth	Payload contains ipv4, ipv6 packet Payload contains eth frame

Policy-based Communication

- A policy in CES is defined by three vectors: *Offer*, *Requirement* and *Available*.

Outbound Policy represented in *Group.Code*

Offer	Id.fqdn, ctrl.cesid, rloc.ipv4
Require	Id.fqdn, ctrl.cesid, rloc.ipv4
Available	Id.fqdn, ctrl.cesid, rloc.ipv4

Inbound Policy represented in *Group.Code* format

Offer	{ }
Require	Id.fqdn, ctrl.cesid, rloc.ipv4
Available	Id.fqdn, ctrl.cesid, rloc.ipv4

- The operation field for these TLVs can be:
  - ***Info****:* indicates the value of an offered policy element.
  - ***Query***: is the request for a policy element;
  - ***Response****:* is mandatory operation to a query
    - Can be empty if no such element is supported

Policy-based Communication

- CES acts as connection broker for hosts that it serves, and it provides tools that attempt security at the level of interaction between hosts.
- CES facilitates network administrators by providing security mechanisms that are configurable by policy, to tackle classical Internet vulnerabilities: unwanted traffic, source address spoofing and DoS.
- By eliminating address spoofing, CES facilitates attributing the evidence of (mis)behavior against sender node, host or application.

Security Heuristics

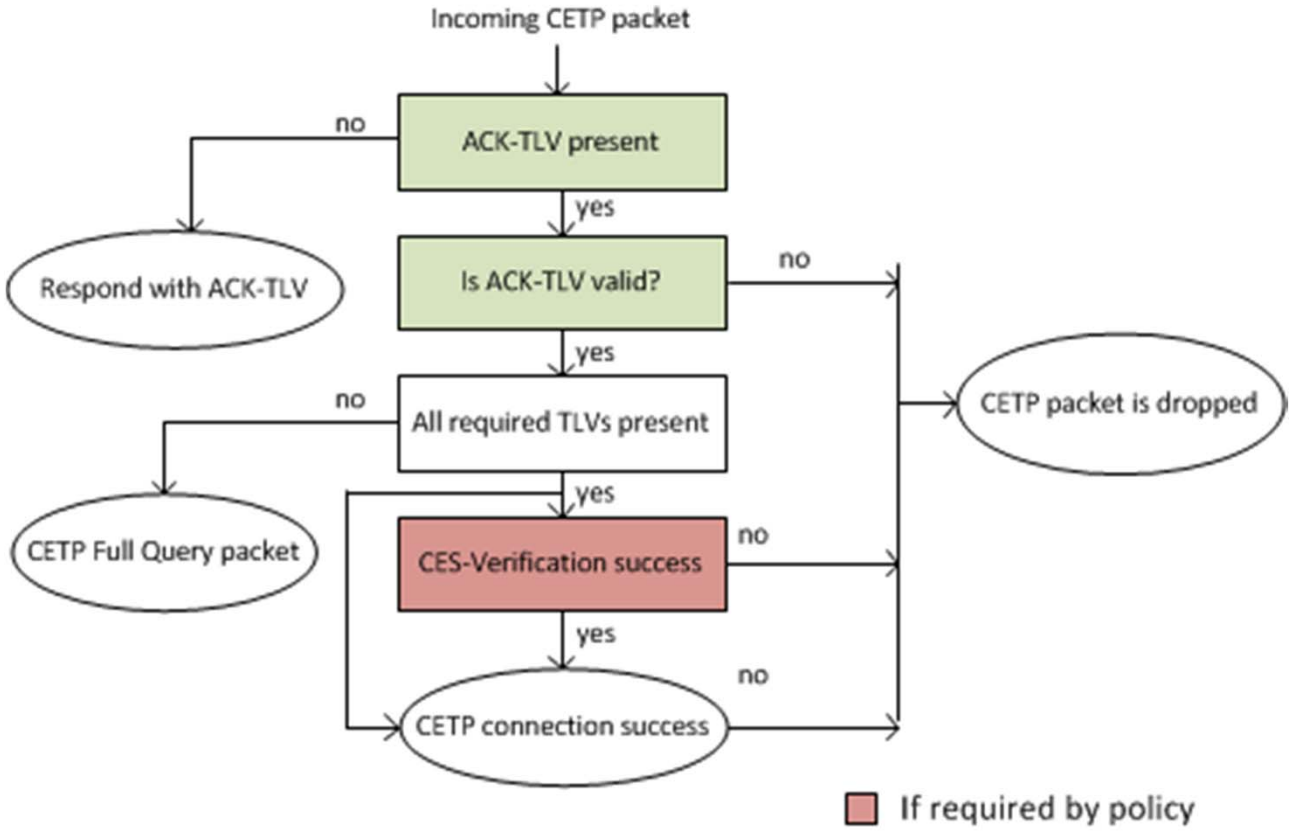
- ***ACKnowledge***: to eliminate spoofing in the inbound CETP packets. iCES delays connection establishment until the sender is determined non-spoofed.
- ***CES Verification*****:** to authenticate the remote node as CES and subsequently collect evidence on the sender-host.

- For CES verification, CES eliminates spoofing on admitted packet and subsequently requests the sender to present its CES certificate and sign the CETP header. Upon successful validation, sender node is admitted as CES.

CES Certificate

- We define "*CES Verification*" object identifier in the Extended Key Usage field of X.509 certificates in order to distinguish certificates issued to CES from legacy Internet certificates.
- The absence of this identifier in the legacy certificates prevents a certificate-bearing legacy host from imitating as CES, and sending forged signed CETP flows.

Security Heuristics



- Guarantees access to non-spoofed legitimate CES nodes

Security contributions

- We provide these security mechanisms as policy-control features for network administrators, that seek to step-up their network security against Internet attacks.
- Unlike other proposal for addressing Internet security, i.e. Accountable Internet protocol (AIP), CES does not require changes to end-hosts (or protocols).
- All the changes are limited to edge-nodes, to facilitate adoption of the technology.
- By eliminating unwanted or spoofed traffic towards private realm, it enables longer sleep cycles contributing to battery lifetime of wireless/mobile devices.

Security contributions

- CES enables collecting evidence on the sender behavior and start forming a reputation by aggregating the evidences under an Internet-wide trust management.
- CES nodes can seek *secure* identities and policy compliance from remote nodes; before admitting a flow, turning the traditional stateful firewalls into cooperative firewall.
- We argue that evidence collection by CES, when aggregated under an Internet-wide reputation system can potentially reduce threat levels (and bot lifetime) in the Internet, improving the overall Internet welfare.
- Trust management is another aspect of our research. We only refer to our research on trust management system here.

Security Testing

	Response duration	*Outcome*
CETP cookie for spoofing elimination	0.00373 msec	Respond with cookie
CETP cookie verification	0.00433 msec	Packet drop
CES-Verification (on first packet)	~ 2 msec	Accept/Deny

- Security processing delay to connection establishment is around 2 milliseconds, due to CES-verification on the first inbound flow from the sender. For the subsequent attempts, we re-use the existing verification results.