STIP:
A New Model of Trusted Network

Sara Bitan | Adi Molkho

NIPAA 2021

HUAWEI TEL-AVIV RESEARCH CENTER

Network5.0
ALL CONNECTED WORLD

Who Are We

Sara Bitan(*)

- Sara Bitan is world known Cyber-security expert, specializing in the design, implementation, and analysis of secure systems. Dr. Bitan is a senior security researcher at the Huawei Tel-Aviv Research Center, and the founder of CyCloak, a high-end Israeli cyber security consulting company, that provides vulnerability search and secure software/hardware design services to large international product companies. Previously she was a chair of the IPsec Remote Access working group in the security area of the IETF. Sara is also a senior researcher in the Hiroshi Fujiwara research center in the Technion, Israel's Institute of Technology. Recently she was part of a team that found and exploited a zero-day Siemens' S7-1500, which is considered the most secure PLC. She presented this work in the reputed BlackHat USA Cyber-Security conference. Her recent research in focused on intrinsic security and trustworthiness in IP networks. A first paper from this research will be presented in the 2nd Workshop on New Internetworking Protocols Architecture and Algorithms (NIPPA), part of the IEEE International Conference on Network Protocols (ICNP).

.

Adi Molkho(*)

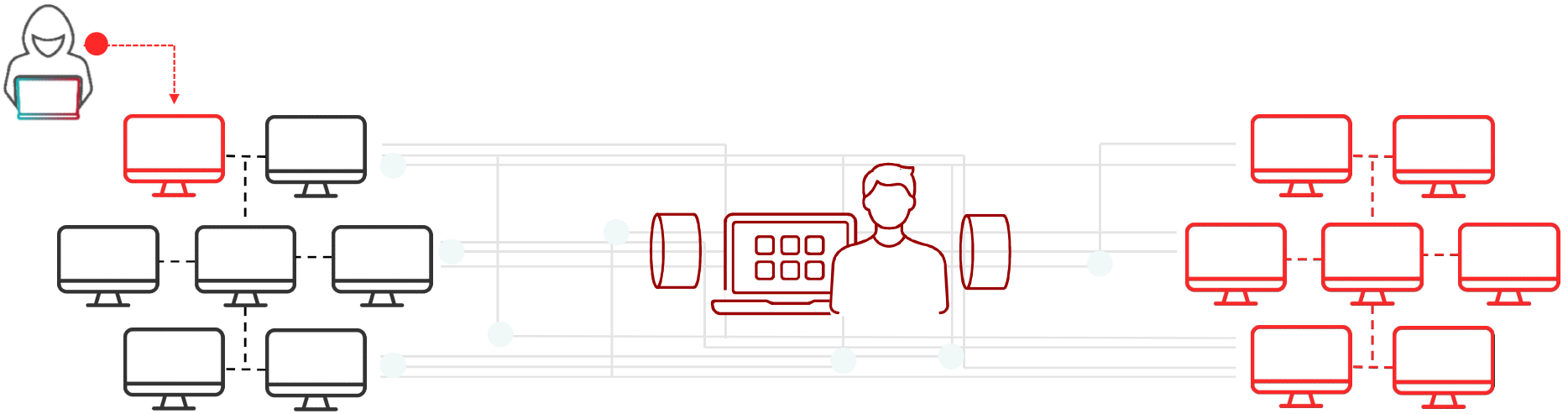
- Adi Molkho is a network veteran with more than 20 years of experience in networks on L1.5-L4. For the last 10 years Adi is involved in state of the art research projects in Huawei such as virtual STB and virtual Access Router. CTO of OPNFV project (Root Cause Analysis), Involved in NFV architecture, and was engaged with different POC with EU operators. His recent research together with Dr. Sara Bitan in focused on intrinsic security and trustworthiness in IP networks.

(*) Network 5.0 lab, based in Huawei Tel-Aviv Research center (TRC)

HUAWEI TEL - AVIV RESEARCH CENTER

Network5.0 ALL CONNECTED WORLD

The Network is not a Player in the Security Scene



IP network are designed to provide connectivity.

Application level and VPN security filled the security void.

Creating opaque connection, and leaving the network blind.

Protection in the network is possible only by MitM proxy and DPI.

Make the Network a Significant Security Player

Protect the network devices and the network from malicious traffic.

Provide continuous and complementary protection to the application layer.

Enforce localized security policies.

Provide value added security services.

Deliver reliable network level data.

Introducing STIP - Scalable Trusted IP networks

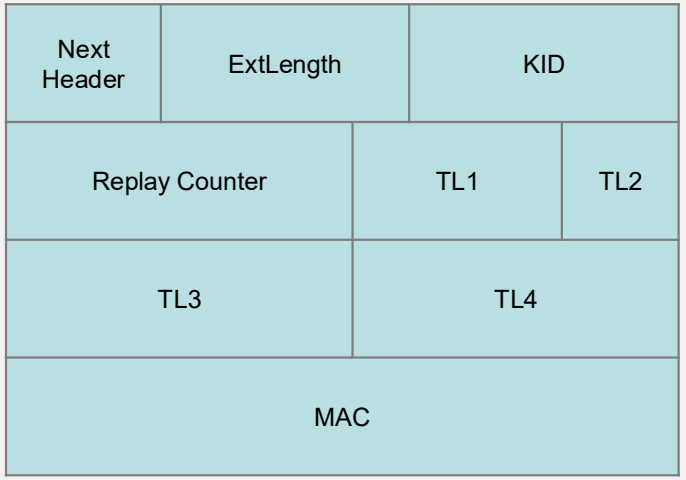
- **TE -** Trust extension is an integrity protected and authenticated virtual container in the packet, that is used to carry critical information between devices.
- **TW –** *TW (a)* is a quantity expressing the probability that network device *a* will act appropriately when handling traffic.

Will not tamper with the protected information.

Will not leak it to third party.

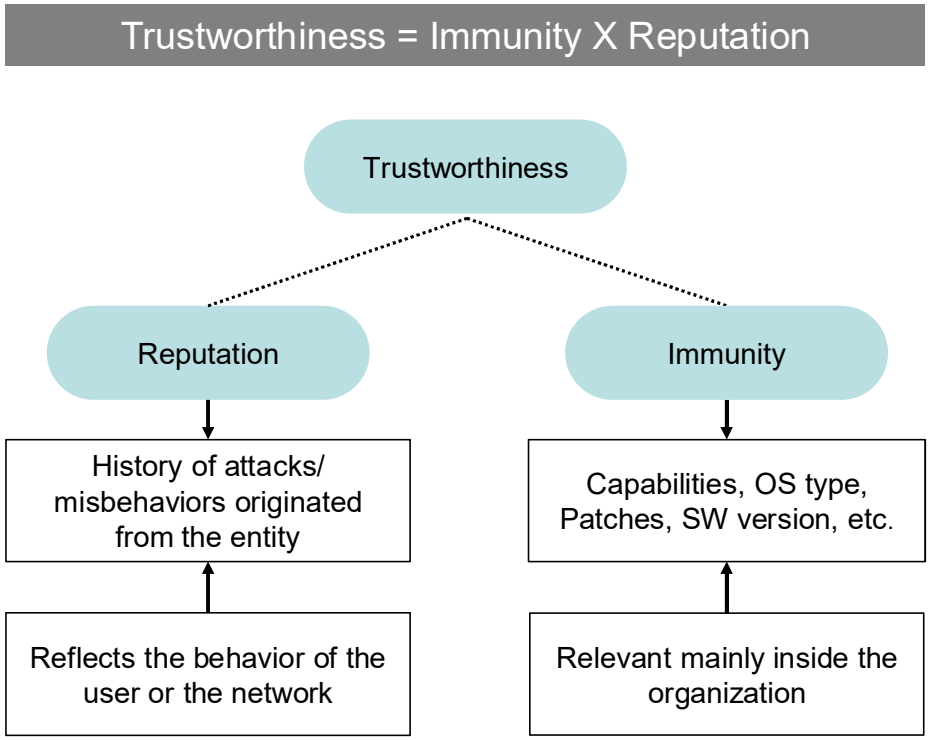
Will not create malicious data.

- The reliability of a TE issued by *a* depends on *TW(a)*



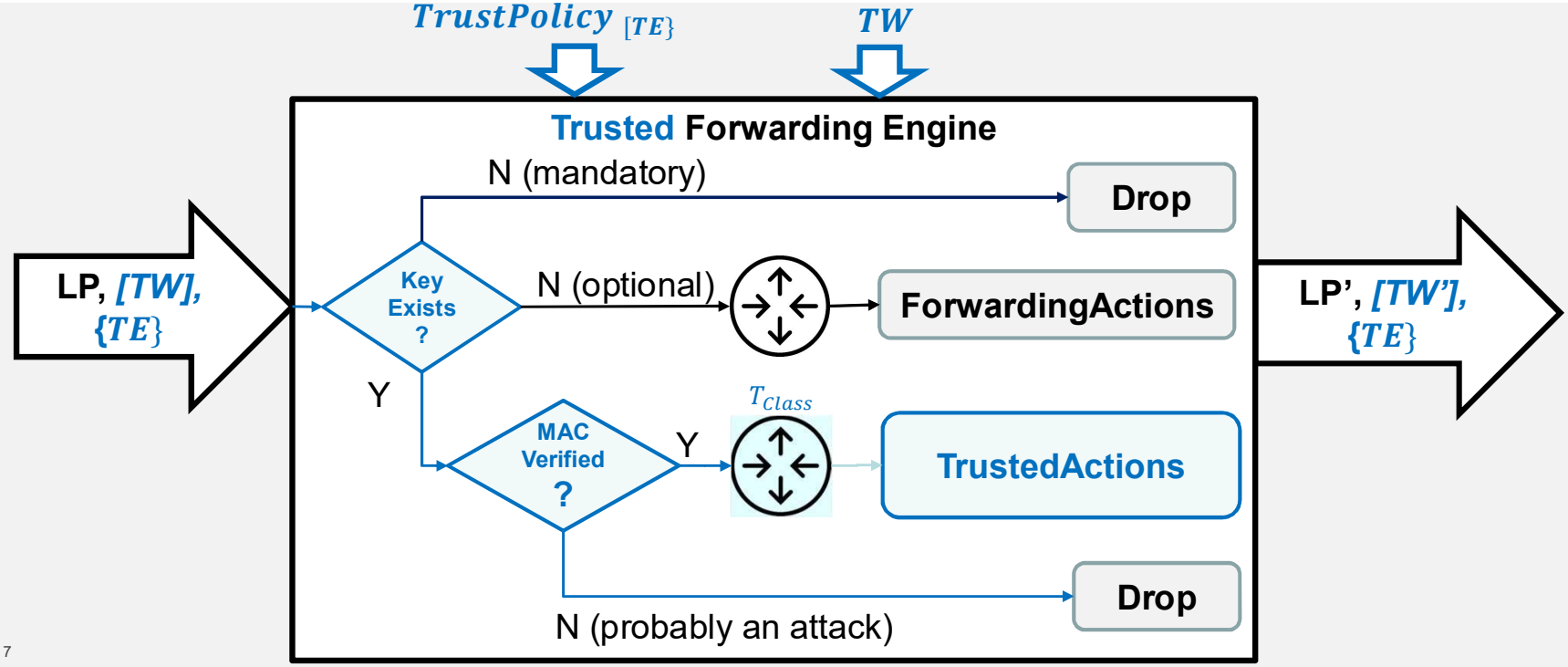
Trust Extension

Trust Worthiness – Immunity & Reputation



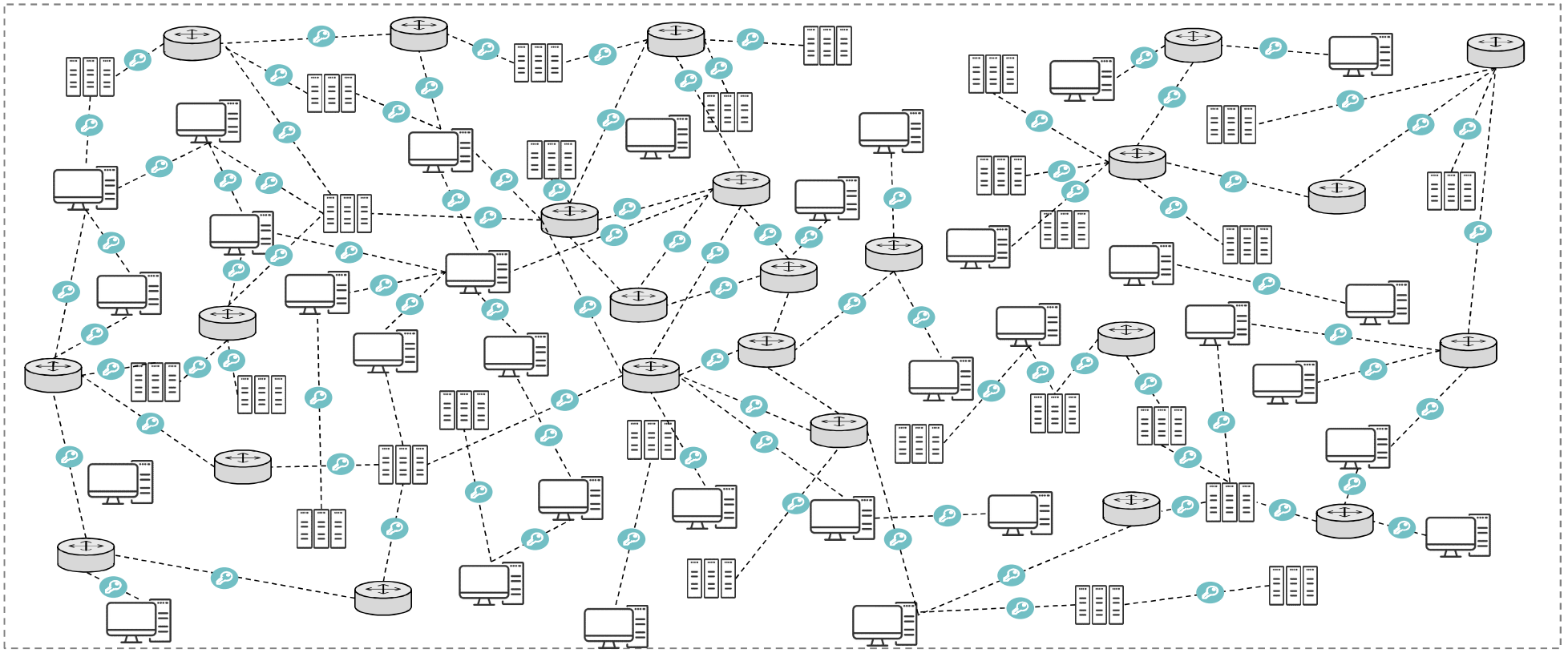
- Trustworthiness varies over time.
- Immunity is constantly polled to see that all patches are installed, no relevant zero day vulnerabilities were announced, etc.
- Reputation is constantly updated according to attacks on or from the entity.

The Trusted Forwarding Engine

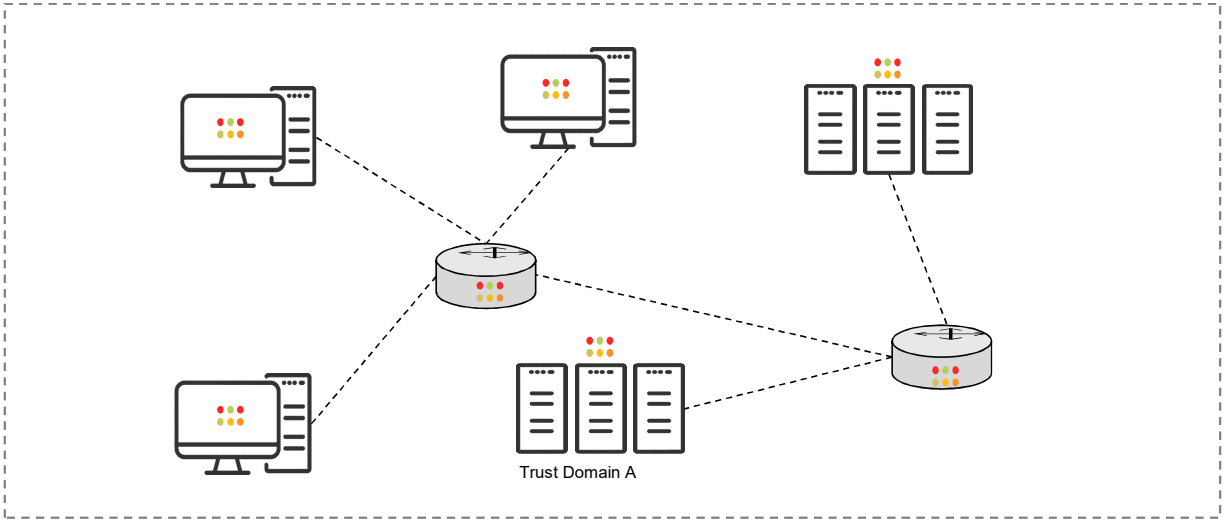


$$T_{Class}\,(TW(a), TE) = \{TrustedActions\}$$

Trust in an Internetwork



What is a Trust Domain?

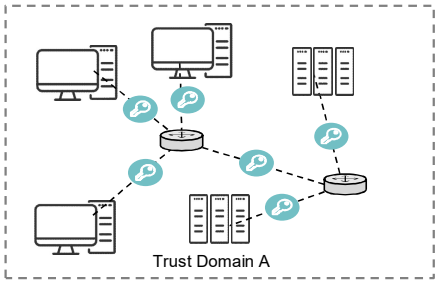


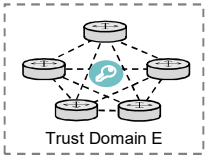
Trust domain is a group of hosts and network elements managed by a single organization.

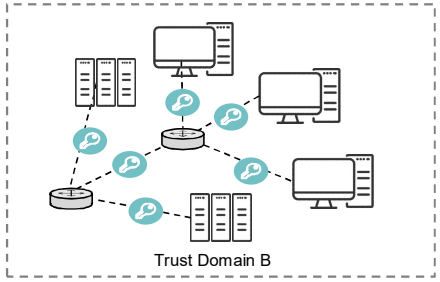
Trust domains members trustworthiness is continuously measured and distributed within the domain.

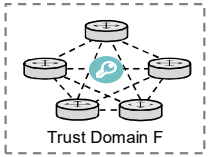
Trust Domain members jointly enforce an organizational security policy.

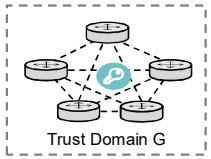
Trust Domains

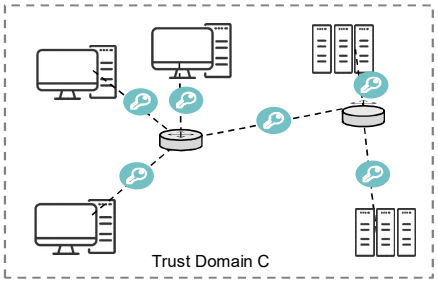


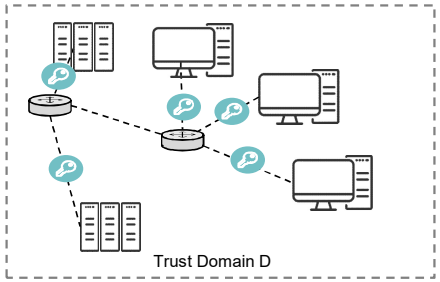








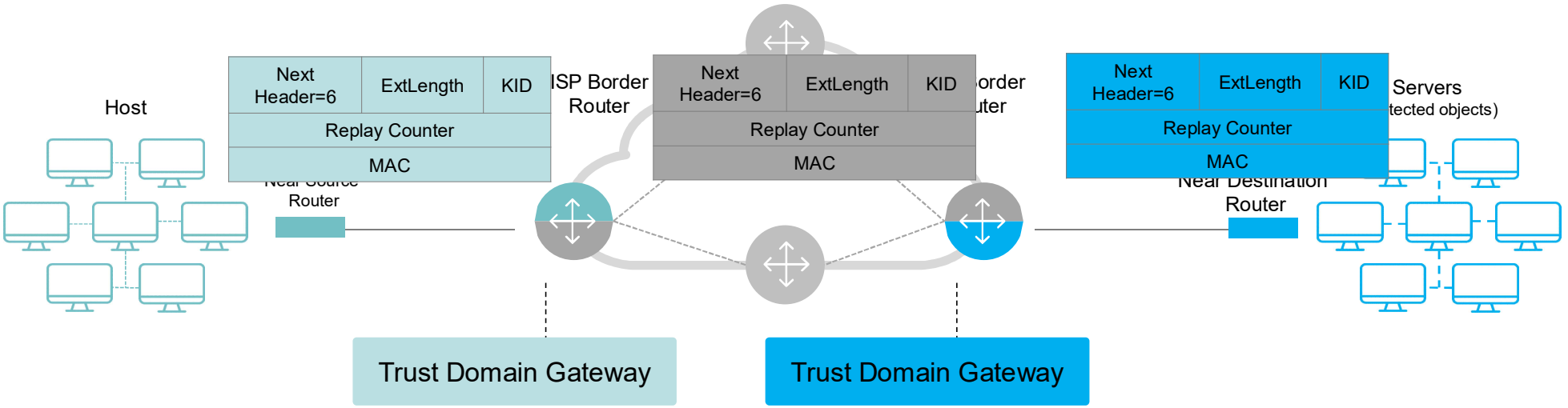




HUAWEI TEL-AVIV RESEARCH CENTER

Network5.0 ALL CONNECTED WORLD

What Is Transitive Trust?

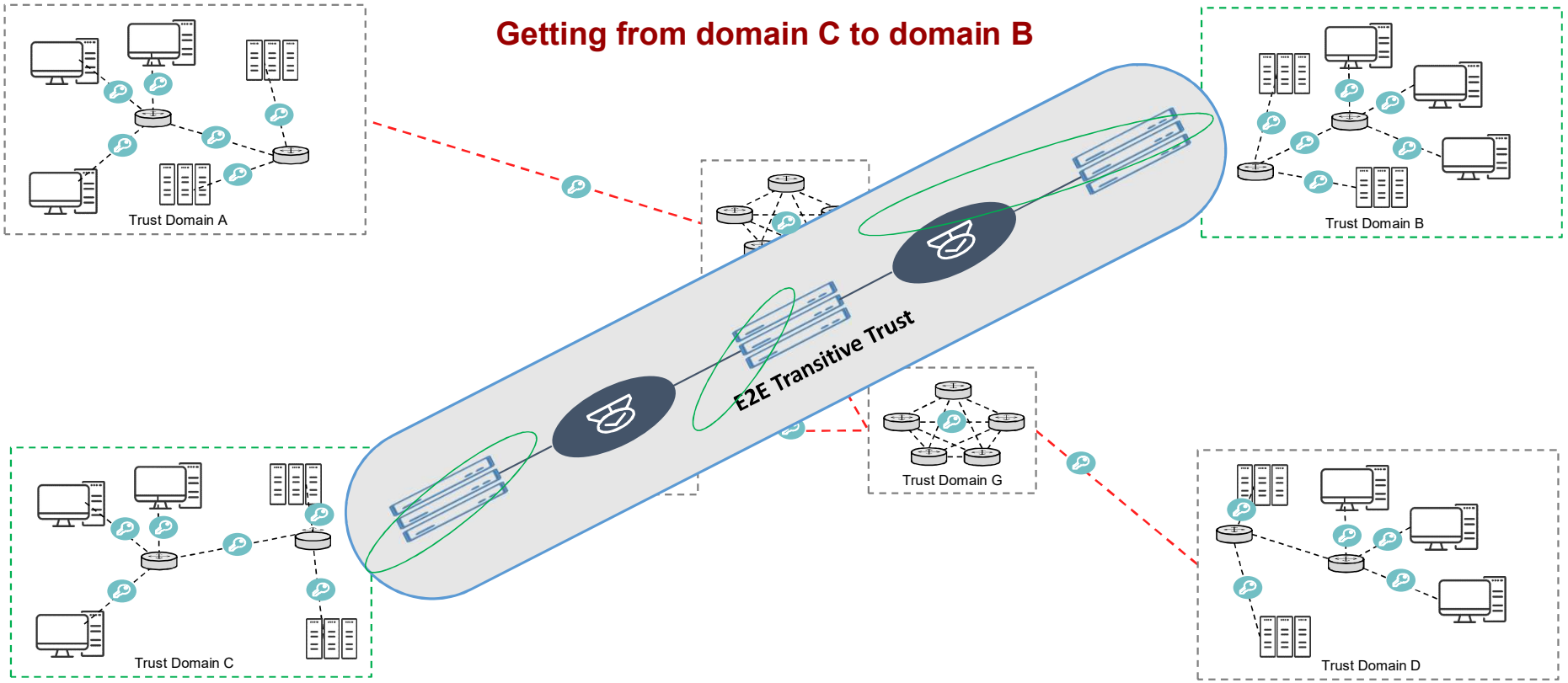


Transitive trust allows to expand trust scope between different trust domains delivering end to end trust without key management scale issues.

Transitive trust is achieved by trust domain gateway entities which are members of at least two trust domains.

During trust domain transitions, trust attributes can be modified or dropped.

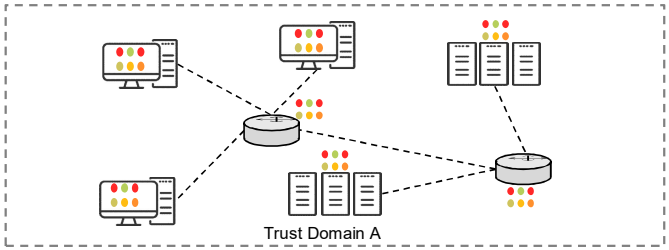
Transitive Trust



STIP - Scalable Trusted IP networks

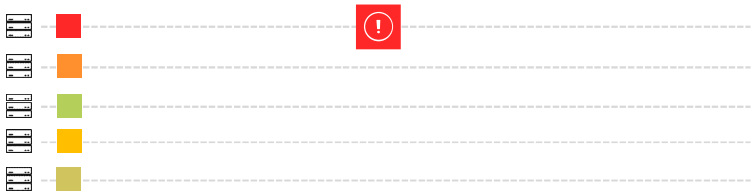
Trustworthiness

Trust Domain

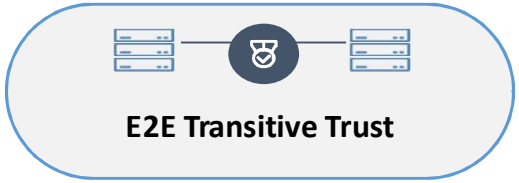


Control plane

Data plane



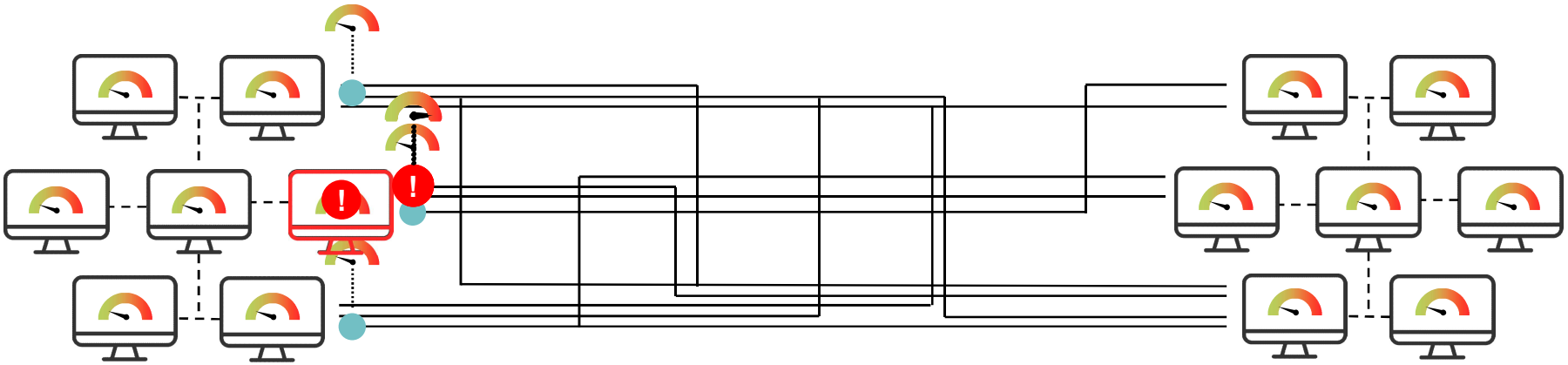
Trust Extension



Transitive Trust

‹
#

STIP's Effect On The Network



- Client connects to the server, creates a connection carrying the application payload.
- The network elements can inspect the TE in the packets.
- Forwarding decision is based on the TE's content, and on the issuer's trustworthiness.

Use Case: Campus Network Authorization

Next Header=6	ExtLength	KID
Replay Counter		
MAC		

Mandatory basic TE that protects the IP header.

Next Header=6	ExtLength	KID
Replay Counter		
Type=TW	Length=x	Val=K
Type= Capabilities	Length=x	Val=K
MAC		

Add trustworthiness and user capabilities TLs.

Next Header=6	ExtLength	KID
Replay Counter		
MAC		

Verify required permissions against capabilities and drop the TLs.

Summary - Trustworthiness in the IP Layer

Network is currently not part of the security scene and industry must find ways to include and involve the network.

STIP is a step towards leveraging security in the IP layer.

Network security matters and brings value to multiple use cases.

Why Now ?

- ETSI's IPE
- Berkley's extensible Internet

Contact us

This is an on-going research and we would appreciate feedbacks and comments

Please contact:

Sara.Bitan@Huawei.com

Adi.Molkho@Huawei.com

HUAWEI TEL - AVIV RESEARCH CENTER

Network5.0 ALL CONNECTED WORLD

Thank you

www.huawei.com

HUAWEI