Use Case Consolidation

Peter Chunchi Liu
Huawei
Use Case Consolidation

1. Data leakage prevention during wide area transmission
   - While uploading data from Campus to DC
   - While communicating from Campus to Campus
   - While training remotely from DC to AI-DC
   - For data residency considerations (within country border)

2. Orchestrate paths that meets client-customized trustworthy property requirements
   - Reliability/resilience/robustness properties

3. Routing auditing
   - Prove traffic went through *specific elements*
   - Prove traffic went through *elements with certain properties*

Business Use Case

Operator high-security connectivity for businesses
- No-leakage guarantee
- Data residency guarantee
- Trust/Security Level Assurance

Service Function Chaining (SFC) orchestration
Problem Statement

Peter Chunchi Liu
Huawei
Why VPN/TLS/... is NOT enough?

No perception to the trustworthiness of bearing network element, so traffic can be accessed and processed by insecure devices, permitting further attacks.

- Crypto-exploit
  - Store-Now, Decrypt Later attacks (Quantum computer attack)
  - Crypto that was secure at the time of deployment but not secure anymore (MD5)
  - Poor crypto engineering/implementation
  - Other unknown crypto vulnerabilities that permits cryptanalysis, obtaining more than negligible information $\epsilon$ about plaintext message $m$
- Plaintext exposure
  - Star-topology for VPNs implies a privileged middlebox (encryption is not end-to-end but segment-to-segment)
- Traffic analysis
  - Traffic analysis for pattern recognition
  - The attack is not about adversary getting all plaintext decrypted, but obtaining any additional information more than it should
- No routing audit statement
Problem Statement

**Goal:** Achieve dependable hop-by-hop forwarding on top of trusted devices and links only, so to **minimize data leakage/exposure to insecure/untrusted devices**.

**Why?:** The data, plain or encrypted, if accessed by insecure/untrusted devices, could be copied, cryptanalyzed for decryption or forgery; or dropped.

“**Trusted**” device: Integrity-checked device that executes forwarding dependably.
A long standing problem
Correctly propagated routing information does NOT guarantee correct forwarding

Steps to dependable hop-by-hop forwarding

1. • Routing information propagation
   BGPSEC

2. • Router make forwarding decisions
   NO guarantee for correct forwarding decisions because we have little to no control of the device execution integrity.

• We (used to) assume router is stateless hop-by-hop, not trusted, provides no security guarantee, doing the best it can.
• Under this assumption, routing security have been forced to narrow its focus on assuring the correctness of routing information during propagation.
• Does that really suffice? No! But it was the best we could do.
Why NASR now?
RATS foundationally changed assumptions to routing security
RATS: Establish a level of confidence in the trustworthiness of remote peers

<table>
<thead>
<tr>
<th>Without RATS</th>
<th>With RATS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Assumption of Devices</strong></td>
<td><strong>Security Assumption of Devices</strong></td>
</tr>
<tr>
<td>Not trusted/no trustworthiness</td>
<td>Device has different trustworthiness properties</td>
</tr>
<tr>
<td></td>
<td>• Finer-granularity of discretion is now possible</td>
</tr>
<tr>
<td></td>
<td>Correctly propagated routing information does NOT guarantee correct forwarding</td>
</tr>
<tr>
<td></td>
<td>Is your device <em>really</em> unconditionally trustworthy?</td>
</tr>
<tr>
<td></td>
<td>• Security by obscurity is bad</td>
</tr>
<tr>
<td></td>
<td>Is your device <em>really</em> unconditionally trustworthy?</td>
</tr>
<tr>
<td></td>
<td>• Security by obscurity is bad</td>
</tr>
<tr>
<td>Completely trusted</td>
<td>Internet</td>
</tr>
<tr>
<td></td>
<td>Limited Domains</td>
</tr>
<tr>
<td></td>
<td>Internet</td>
</tr>
<tr>
<td></td>
<td>Limited Domains</td>
</tr>
</tbody>
</table>

Important flow
One more step... how to say a device is “trusted”?

- Integrity-checked device from hardware to configuration so as to deliver dependable or deterministic forwarding.

- Device with certain security/trustworthiness properties that meet client requirement.
- We focus on defining objective options for clients to choose from.

Trusted? Yes!

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Trusted? Also yes!
If this is what client wants && is attested.

1 YANG w/ provenance
2 BGPSEC
3 BGP Flowspec
4 Flap Damping
5 Anti-DDoS
6 uRPF
7 xx ciphersuite/PQ-keys
8 MACSEC
9 Root of Trust
NASR Goal

1. Allow clients to choose desired security/trust properties of his received network service

2. Achieve dependable forwarding by routing on top of only devices that satisfies certain trust requirements

3. Provide **auditable** evidence that certain packets or flows traversed a network path that has certain trust or security properties.