2014-09-30

Threat Model Analysis of Router Backdoor

draft-song-router-backdoor-00

Haibin Song

Ning Zong

Motivation

- Routers might be doubted having backdoors, but vendors will claim they have no backdoors
  - *Vendors would like to verify its innocence*
  - *Operators/regulators would like to make sure the equipment is secure*
- Assume that we could find some approach that can verify whether back door exist in a router
  - No backdoor. Then it can verify the innocence of vendors.
  - Yes, there is backdoor. Then in the opposite aspect, it helps the administrators to detect it.
  - Still not clear. But it can mitigate the distrust between each other.
- *This draft will mainly talk about the threat models but leave the solutions for future study*

Scope

- In scope
  - Threat models of *inherent* router backdoors
- Out of scope
  - Anything related to third party implanted backdoors or system vulnerabilities
  - Anything related to security attacks to the routers

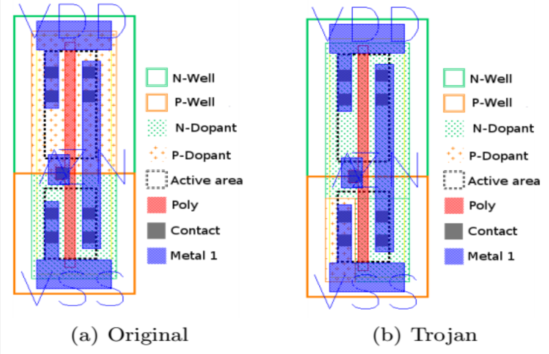
Before Moving Ahead…

- Analyze threat models MERELY from technical / research perspective

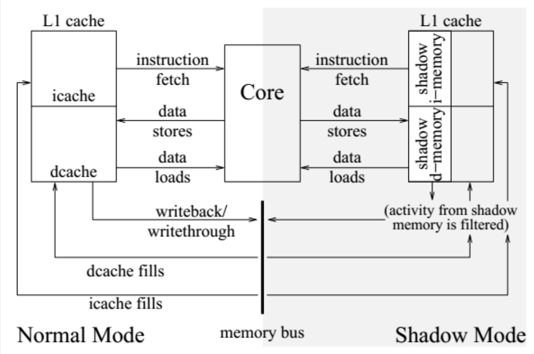
- All the information about threat models are from various PUBLIC sources, like Internet articles/release, academic papers, etc.
  - NOT based on ANY real world products
  - Vendor NEUTRAL analysis only

Backdoor Classification

- Implementation Classification
  - Hardware backdoors
    - E.g. specific designed transistor, shadow circuit



(a) Original (b) Trojan

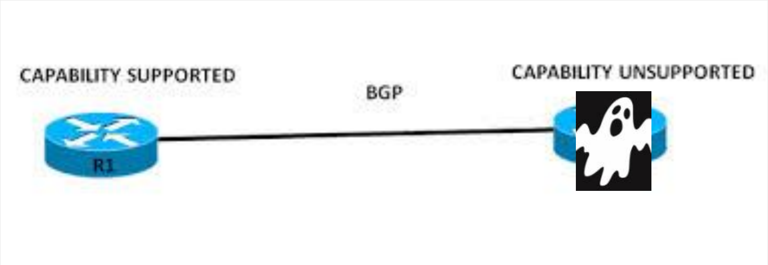


  - Software backdoors
    - Hidden functions triggered by specific designed packets
    - Illegally get the root control, e.g. *TCP 32764 backdoor*
    - Etc.

Backdoor Purpose

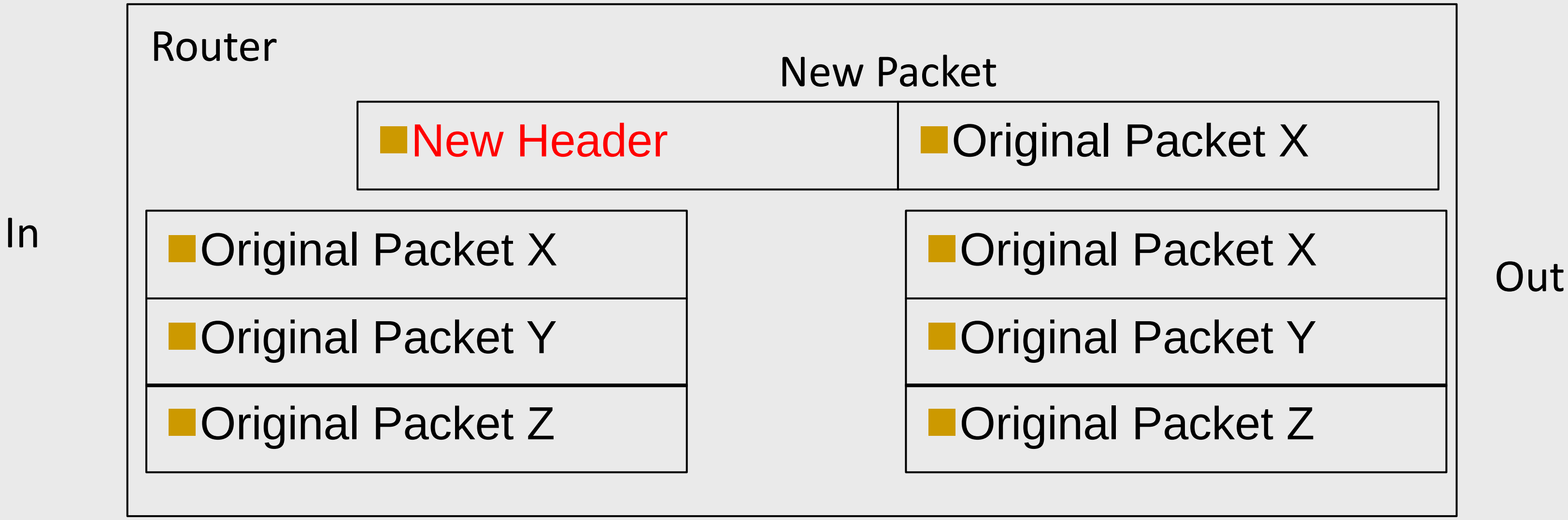
- Traffic eavesdropping (mainly suspected)
  - Targeted or pervasive

- Equipment malfunction
  - Control over time, location, component and in which behavior to make the router malfunction



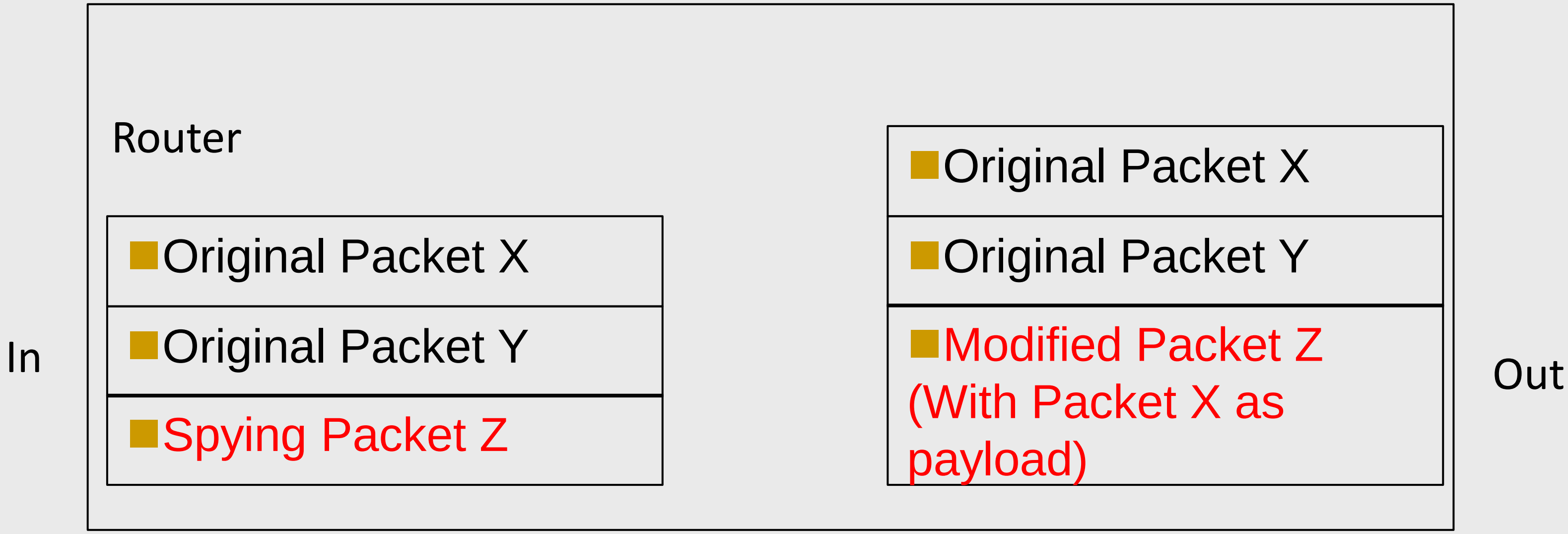
Traffic Eavesdropping

- A spying router can encapsulate the original user packet and send to another destination for information collection
  - New packet is generated!
    - Source address: itself or others
    - Destination address: NMS or other controlled destination



Traffic Eavesdropping (Cont.)

- A spying router monitors user packets information, and then encapsulates that information to an existing e2e session that was designed for eavesdropping
  - There is No new packet
  - The spying session can be encrypted



In

Router

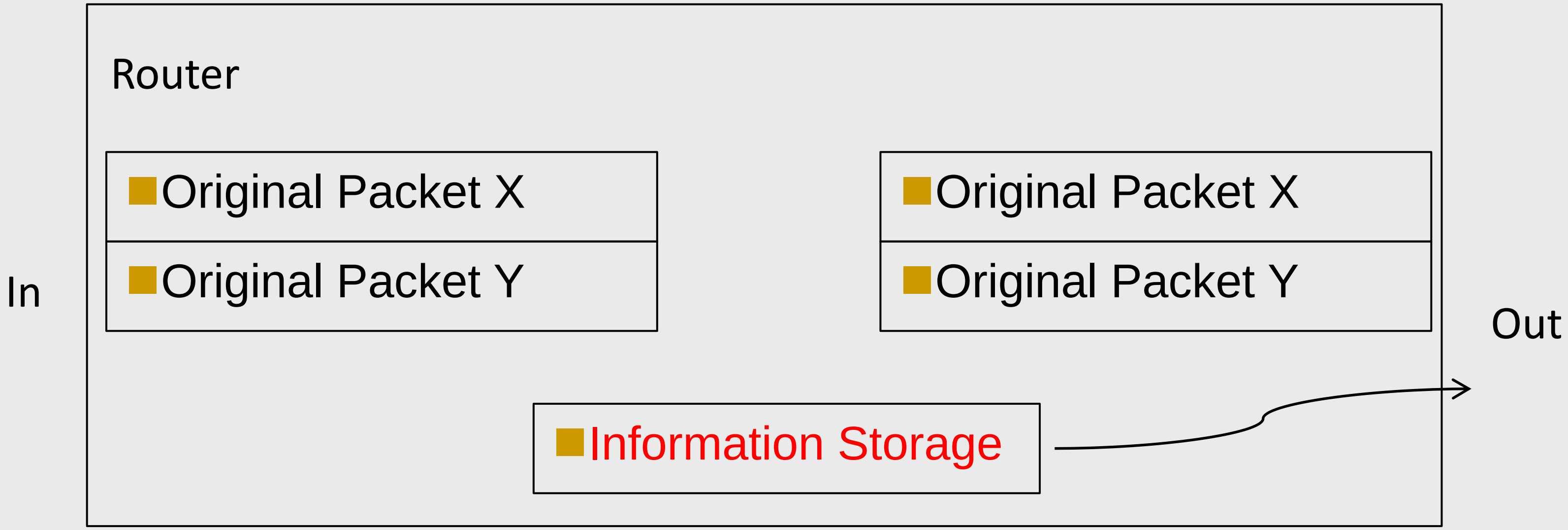
- Original Packet X
- Original Packet Y
- Spying Packet Z

- Original Packet X
- Original Packet Y
- Modified Packet Z (With Packet X as payload)

Out

Traffic Eavesdropping (Cont.)

- A spying router can also have a backdoor of storage, and provide access to it through unknown ways
  - A spying router can leave illegal root control to its control body, and the information is only accessed when needed



Equipment Malfunction

- A back door can make the router malfunction
    - With enabling the backdoor in the key routes, it can destroy the functioning of a whole network

- Usually, the control body gets root control over the router , the malfunctioning behaviors include but not limited to:
    - packet dropping
    - illegal routing table modification
    - illegal packet modification
    - Stop working

Next step

- Call for interest and more contributors to this draft, to develop a more comprehensive threat model for inherent backdoor.

Xie Xie!

(i.e. Thank you in English)