下世代Network Slicing模組設計

課程單元：網路切片之安全性導論

國立中山大學 資訊工程系
授課教師：李宗南教授
教材編撰：林芸琦

目錄
CONTENTS

01 課程目標

課程目標

- SDN 安全性
- NFV 安全性
- Network Slicing 安全性

02 SDN 安全性

SDN 安全性 - 邏輯集中式控制中心 2/1

- 邏輯集中式控制中心(logically centralized controllers)因為其實體的實作方式(將各軟硬體功能集中於單一某硬體上)，可能導致重要權限被集中攻擊
- 雖然SDN集中控制可以實作成類似於分散式系統的方式，但實作過程中可能產生漏洞
- 因為SDN的集中式控管為一個單一個體，從控制中心到資料或應用面只有一個安全對話機制，但實際上不同設備間的連接需要不同強度的安全管理

SDN 安全性 - 邏輯集中式控制中心 2/2

- 預期透過將SDN集中控制中心建構在安全的計算環境中來維持安全性

SDN 安全性編程式訪問

- 由於SDN提供客戶端或應用端編程式訪問(programmatic access)因而產生一些風險
- 新的商業模式中的客戶發送的訊息處於開放式的管理環境中
  - 保護資料完整性以及第三方數據
  - 業務管理上實時控制訊息
  - 不同業務間的控制訊息的隔離

03 NFV 安全性

NFV 安全性

- 網路功能虛擬化(NFV):網路節點可由軟體創造虛擬節點，不需設置實體節點，虛擬化節點無法由物理進行保護，如何維護其安全性也成為5G解決目標
- 內文文字
  - 內文文字縮排
  - 內文文字縮排
  - 內文文字縮排
- 內文文字
  - 內文文字縮排
  - 內文文字縮排
- 內文文字

04 Network Slicing 安全性

Network Slicing 安全性

- 網路切片: 為了三種應用場景提供差異化安全服務，實現客戶安全分級服務
- 針對低延遲的應用場景，5G網路控制功能需要部屬在網路邊緣或與基站融合部屬，5G核心網路下沉到接入網，5G提供的安全保障也隨之下沉

基礎設施的安全性

- 因為多個網路切片實例可能架設在同一台基礎設備上，所以應該網路切片實例間的交叉影響以及資料的洩漏，確保獨立性
  - 例如不同的網路功能應該使用不同的虛擬機或容器(container)；網路切片實例中專用的網路虛擬功能(Virtual Network Function/VNF)應在邏輯上獨立

網路管理的安全性

- 網路切片管理生命週期中，每一階段皆有可能受到攻擊
  - 惡意軟體可能直接攻擊網路切片模板，進而影響後續所有網路切片實例
  - 若網路切片實例處理不當，網路切片實例運行時，攻擊可能會通過配置的接口，在實例運行結束得到機密資料
- 營運商會授權給承租人一些網路功能以及接口使用權利
  - 換句話說，承租人必須通過認證才能夠使用網路功能以及接口

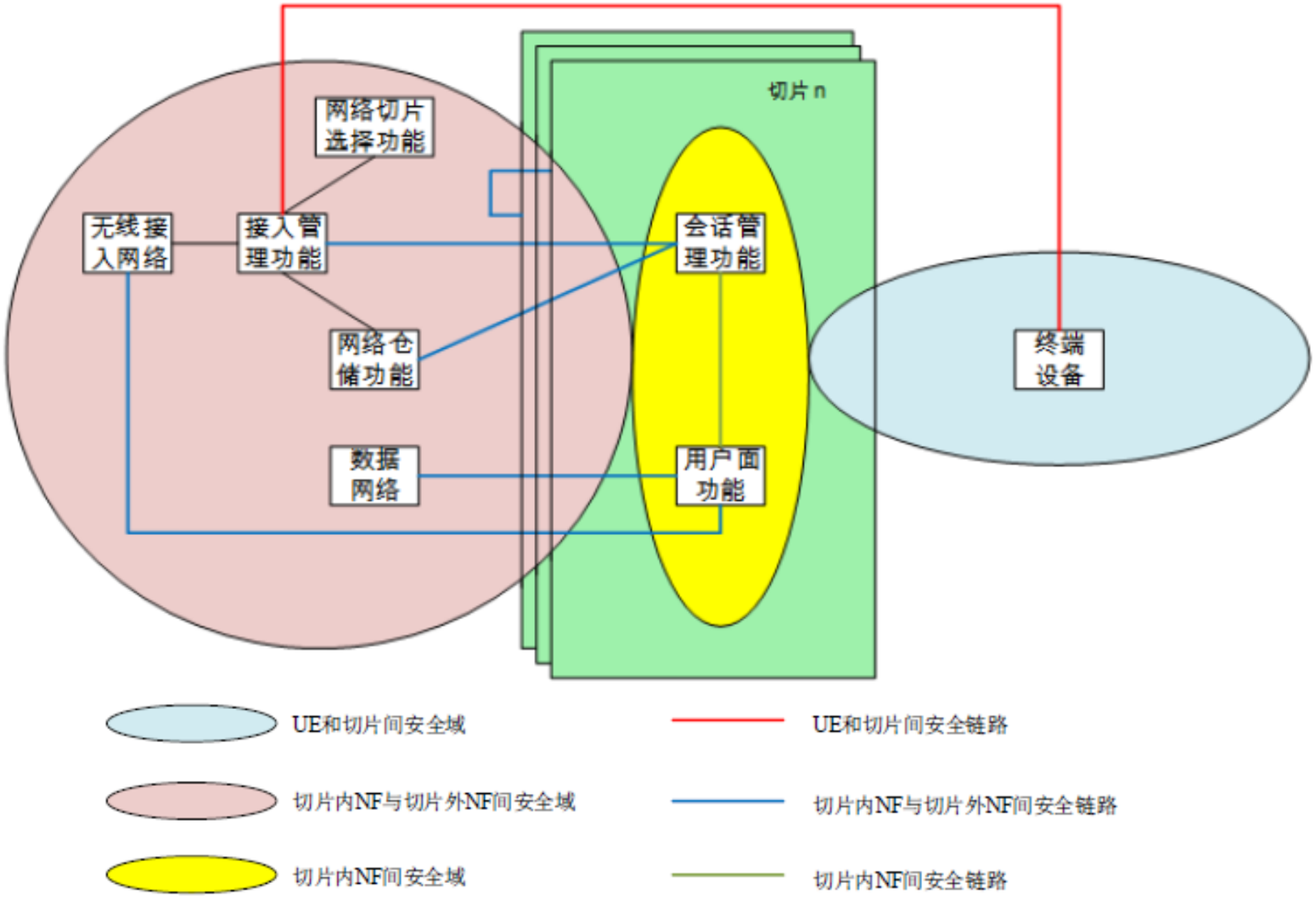
網路切片實例安全性

- To guarantee security for the network services provided by an NSI, it requires embedding the security mechanism and security provisioning entity
  - Security isolation
  - Slice access control
  - Customized security mechanisms

多層次切片安全 1/2

- 切片安全機制主要包含三個方面
  - UE與切片間的安全
  - 切片內NF(網絡能力)與切片外NF間的安全
  - 切片內NF間安全

Network Slicing 安全性 - 多層次切片安全 2/2



UE與切片間的安全 1/2

- 由AMF對UE進行鑒權，從而保障接入網路的UE是合法的
- PDU會話機制來防止UE的未授權訪問
  - AMF通過UE的NSSAI為UE選擇正確的切片
  - 當 UE 訪問不同切片內的業務時，會建立不同的PDU 會话，不同的網絡切片不能共享PDU 會話
  - 建立PDU 會話的信令流程可以增加鑒權和加密過程

UE與切片間的安全 2/2

- PDU會話機制來防止UE的未授權訪問
  - UE 的每一个切片的PDU 會話都可以根據切片策略採用不同的安全機制
  - 當外部數據網絡需要對UE 进行第三方認證时，可以由切片内的會話管理功能（SMF）作为EAP 認證器，為UE 進行第三方認證

切片內NF(網絡能力)與切片外NF間的安全

- 由於安全風險等级不同，切片內NF 與切片外NF 間通信安全可以分為三種情況
  - 切片內NF 與切片公用NF 間的安全
  - 切片內NF 與外網設備間安全
  - 不同切片間NF 的隔離

切片内NF與切片公用NF間的安全 1/2

- 公用NF可以訪問多个切片内的NF
  - 切片内的NF需要安全的機制控制来自公用NF 的訪問，防止公用NF 非法訪問某个切片内的NF
- 網管平台通過白名單機制對各个NF進行授權
- 切片内的SMF 需要向網絡倉儲功能（NRF）註冊，當AMF 為UE 選擇切片時，詢問NRF，發現各個切片的SMF
  - AMF 和SMF 通信前，可以先進行相互認證，實現切片内NF（如SMF）與切片外公共NF（如AMF）之間的相互可信

切片内NF與切片公用NF間的安全 2/2

- 可以在AMF 或NRF 做頻率監控或者部署防火墙
  - 防止Dos/DDos 攻擊
  - 防止惡意用户將切片公有NF 的资源耗盡

切片内NF与外網設備間安全

- 在切片内部署防火牆則可以使用虚擬防火牆，不同的切片按需編排
  - 切片外部署防火牆則可以使用物理防火牆，一个防火牆可以保障多个切片的安全

切片内NF与外網設備間安全

- 比如，部署时可以通過VLAN（虚拟局域网）/VxLAN（虛擬擴展局域網）劃分切片，基於NFV的隔離来實現切片的物理隔離和控制，保證每个切片都能獲得相對獨立的物理资源，保證一个切片異常後不影響到其他切片

切片内NF間安全

- 切片内的NF 之間通信前，可以先進行認證，保證對方NF 是可信NF，然后可以通过建立安全隧道保證通訊安全，如IPSec

異構網路下安全保證 1/2

- 提供統一認證架構
  - 5G網路需支持多種接入技術(例:WLAN、LTE、固定網路等)，5G需要一個統一的認證框架融合不同的接入認證方式，支持多種接入方式和接入憑證，從而保證所有終端設備安全地接入網絡
- 按照需求提供安全保護
  - 滿足多種應用場景中終端設備的生命週期要求、業務的時延要求

異構網路下安全保證 2/2

- 提供隱私保護
  - 滿足用戶隱私保護以及相關法規要求
- 針對異構網路性質對安全做加強以及改善4G原有安全問題(例:IMSI(國際移動用戶標示)暴露問題)
  - 用戶身分標示的保護須兼容LTE認證信令

NFV/SDN、切片及能力開放下安全保證 1/2

- NFV/SDN引入網路的安全，包括虛擬基相關的安全、軟件安全、數據安全、SDN控制器安全等

- 切片的安全，包括切片安全隔離、切片安全管理、UE接入切片的安全、切片之間通信的安全等

NFV/SDN、切片及能力開放下安全保證 2/2

- 能力開放的安全，既能保證開放的網路能力安全的提供給第三方，也能保證網絡的安全能力(如:加密、認證等)能夠開放給第三方使用

- 用戶隱私訊息從封閉平台轉移到開放平台上，隱私暴露風險提高，需要更高的隱私保護
  - 例:智能交通中，車輛位置行駛軌跡

參考資料

[1] 5G網路安全需求與架構白皮書 IMT-2020(5G)推進組

[2] https://www.sdnlab.com/19818.html

[3] <An Introduction to Network Slicing>

[4] < China Mobile_5g Service Guaranteed Network Slicing >