Rischi per l'utente nell'uso delle wi-fi non cifrate

ANDREA LORA
CNR – ISTITUTO CRISTALLOGRAFIA – ADRRM1 MONTELIBRETTI
ANDREA.LORA@CNR.IT

#garrws14

Funzionamento Reti basate su Captive Portal

- L'AP annuncia l'SSID
- L'utente si connette alla rete
- L'AP mette l'utente in client isolation
- Assegnazione IP da parte del DHCP.
  Traffico internet bloccato.
- Traffico HTTP/S reindirizzato a captive per login (o registrazione)
- Login Ok? Traffico internet sbloccato

802.11 & Captive Portal

Vantaggi

- Soluzione ben collaudata
- Facile utilizzo
- Registrazione dell'utenza on premise
- Non necessita di software aggiuntivo

Svantaggi

- Traffico in chiaro
- SSID non garantisce identità

Denial of service

- Layer 1: Wi-Fi Jamming
- Layer 2: Deauthentication / Disassociation Attack
- Layer 3+ Tipici dello stack IP

- Questi attacchi generano disservizio, ma diventano un mezzo per poter sfruttare altri attacchi

DoS Layer 1 – RF Jamming

- I pacchetti vengono inviati attraverso una canale che occupa una certa frequenza.
- La banda del canale è una risorsa condivisa e limitata
- E' possibile per un attaccante occupare il canale
- Causa elevata latenza, riduzione velocità trasmissione.

DoS Layer 2 – DeAuth Attack

- 802.11 prevede una serie di frame atti al suo funzionamento
- Uno è il frame DeAuthentication: viene inviato dall'AP alla Station e forza la Station a rieseguire l'autenticazione
- Il Frame è spoofabile. Un attaccante può generare DeAuth frames fingendosi l'AP e causando la perdita delle funzionalità di rete
- NB: Il frame nello standard attuale non viene crittografato (ne soffrono anche le reti basate su WEP/WPA/WPA2). 802.11w introduce la crittografia di questo (ed altri) frame di gestione

DoS Layer >2 – DHCP Starvation

- Per permettere l'accesso al captive portal il client deve essere in grado di stabilre connessioni TCP/IP
- Un DHCP deve quindi essere presente per fornire l'indirizzo IP
- Un attaccante può inviare numerose richieste di collegamento all'AP, spoofando il MAC address
- Il pool è limitato

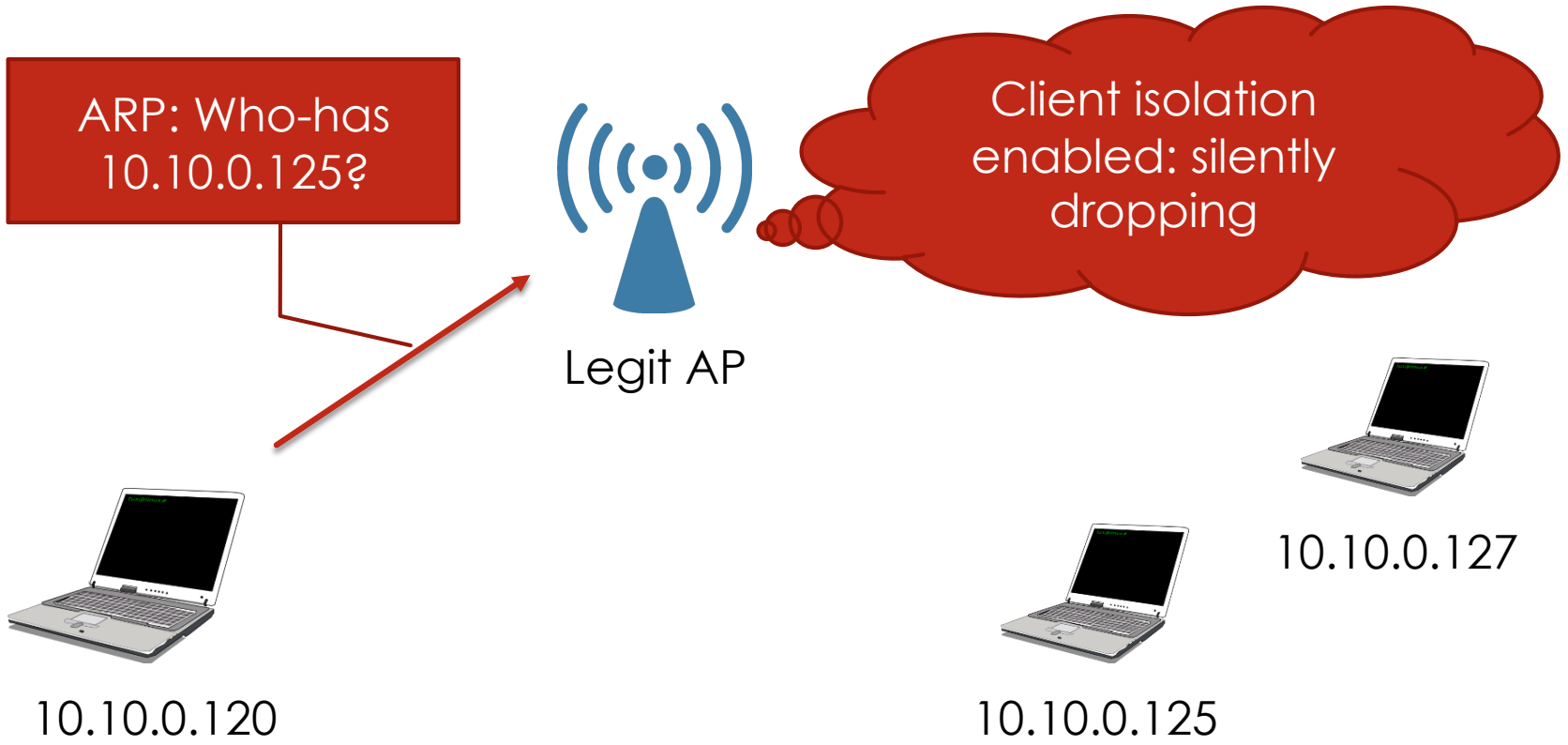
MITM / Hijacking

- Attacchi che mirano alla sottrazione di informazioni sensibili
- L'attaccante si finge il gateway e può leggere il traffico di un client ignaro
- Su rete ethernet l'attacco si porta avanti con ARP Spoofing
- Su wifi
  - Arp Spoofing (se non c'è Client Isolation)
  - Direct Connection (bypassando l'AP)
  - Rogue Access Point (the evil twin attack)

Client Isolation

- Inibisce la comunicazione tra dispositivi collegati alla stesso AP
- Aumenta la sicurezza dei client impedendo che utilizzino traffico broadcast per trovare risorse presenti sulla rete locale (Condivisioni SMB p.e.)
- Evita l'ARP poisoning
- Purtroppo il canale di comunicazione non è sicuro

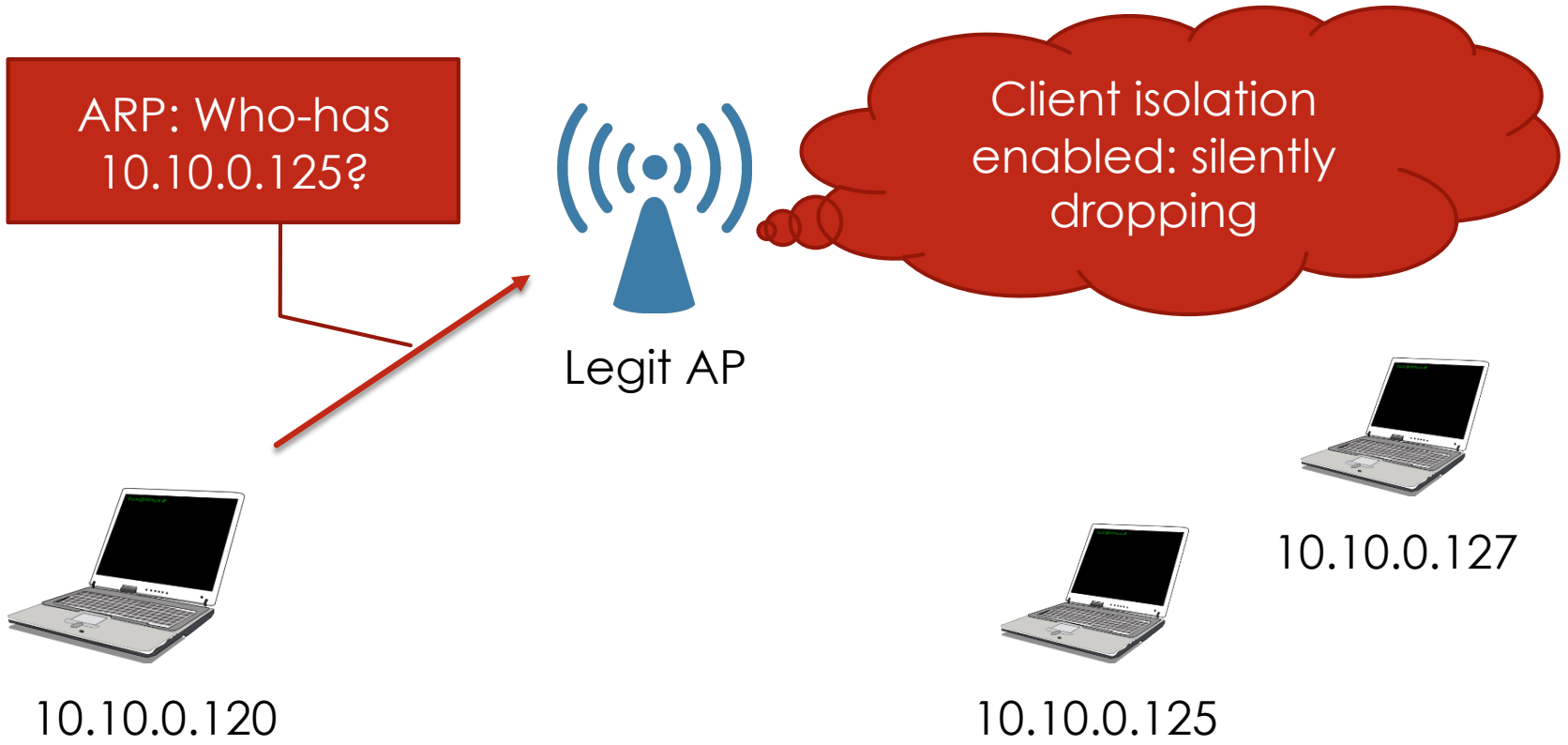
Client Isolation



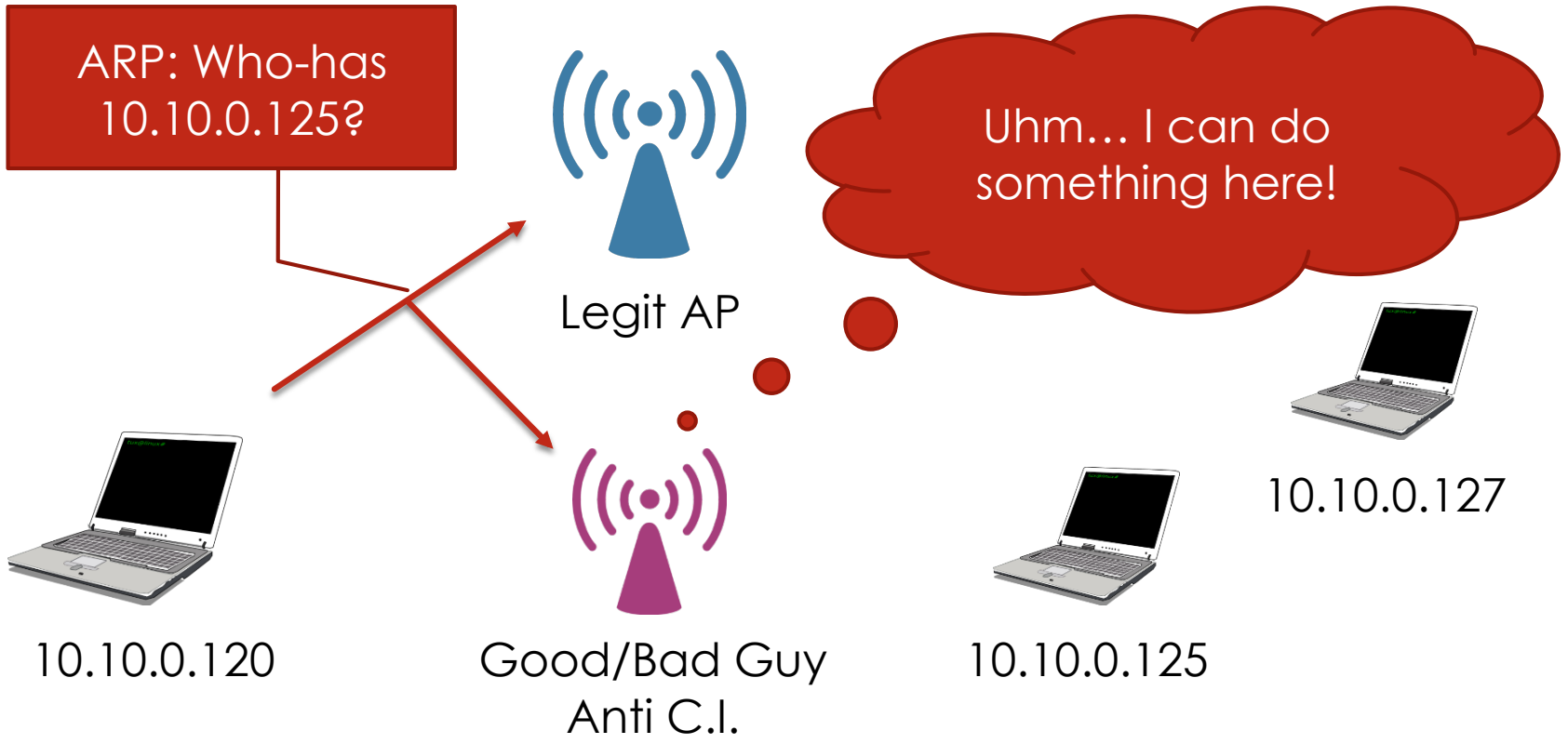
Direct Connection

- Utilizzando pacchetti di tipo RAW un dispositivo è in grado di immettere frames sul canale radio forgiando pacchetti arbitrari (Packet Injection)
- Su reti non protette un apparato terzo è in grado di inviare pacchetti fingendosi l'AP
- Questi pacchetti non possono essere bloccati dall'AP. Il traffico raggiunge direttamente le Station che non è in grado di capire se è in presenza di traffico legittimo o spoofato

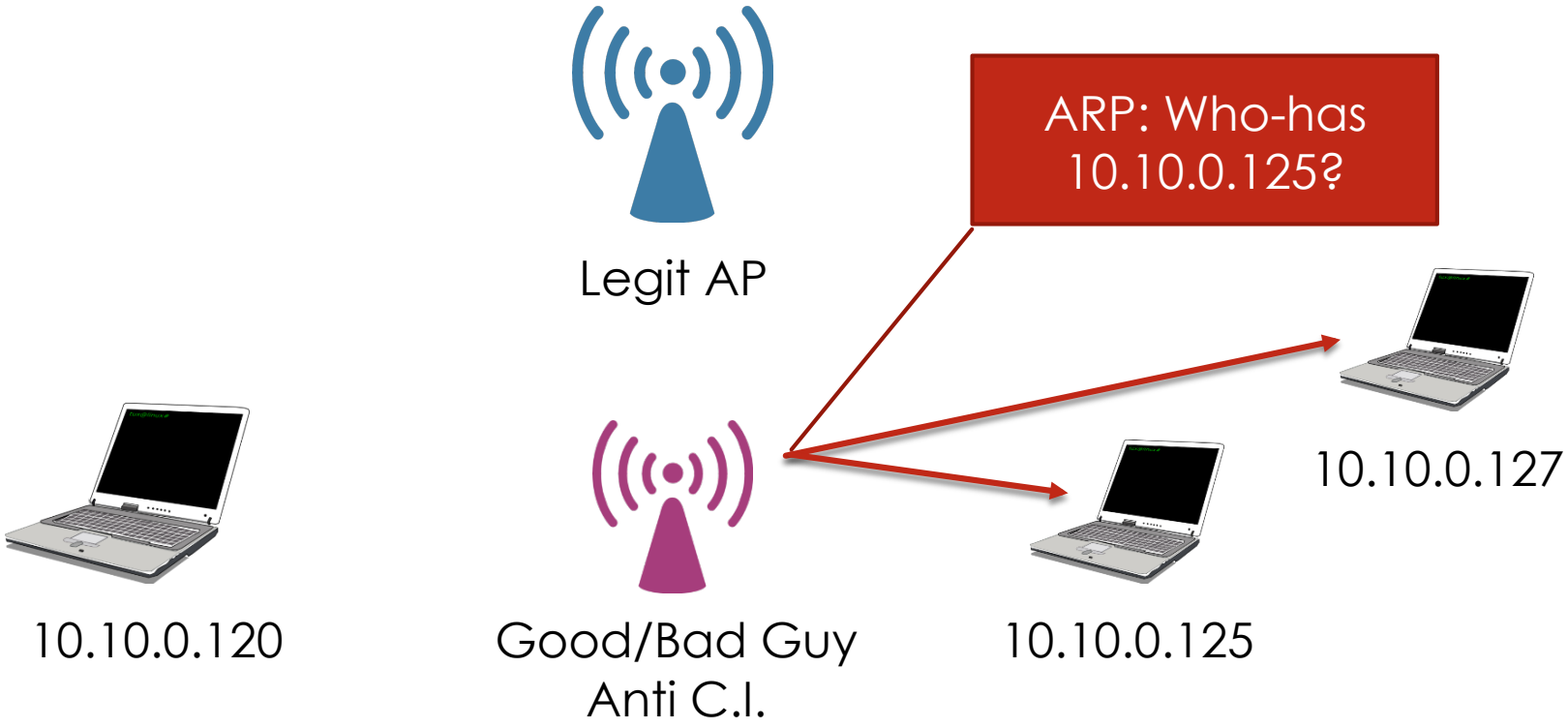
Client Isolation



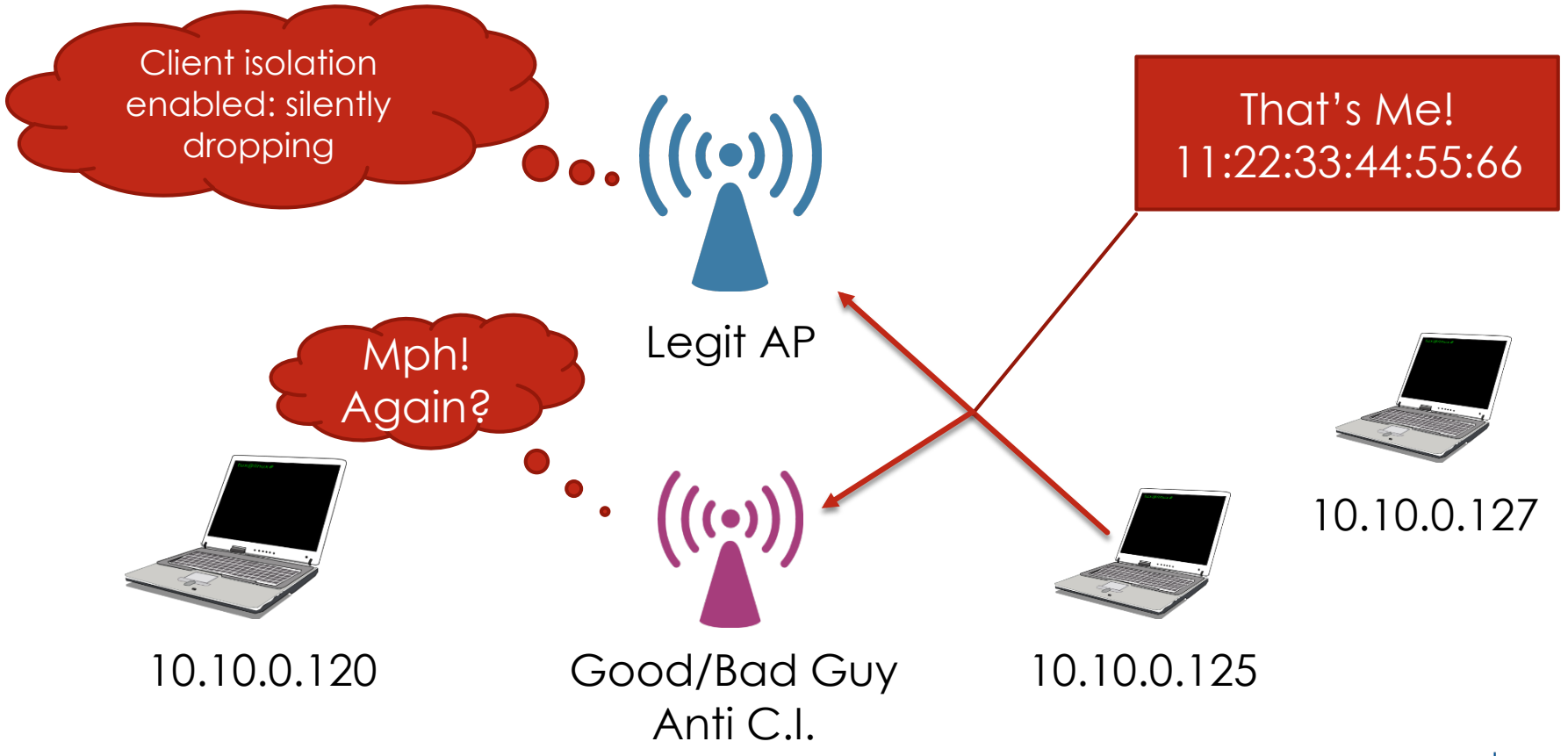
Client Isolation - Defeated



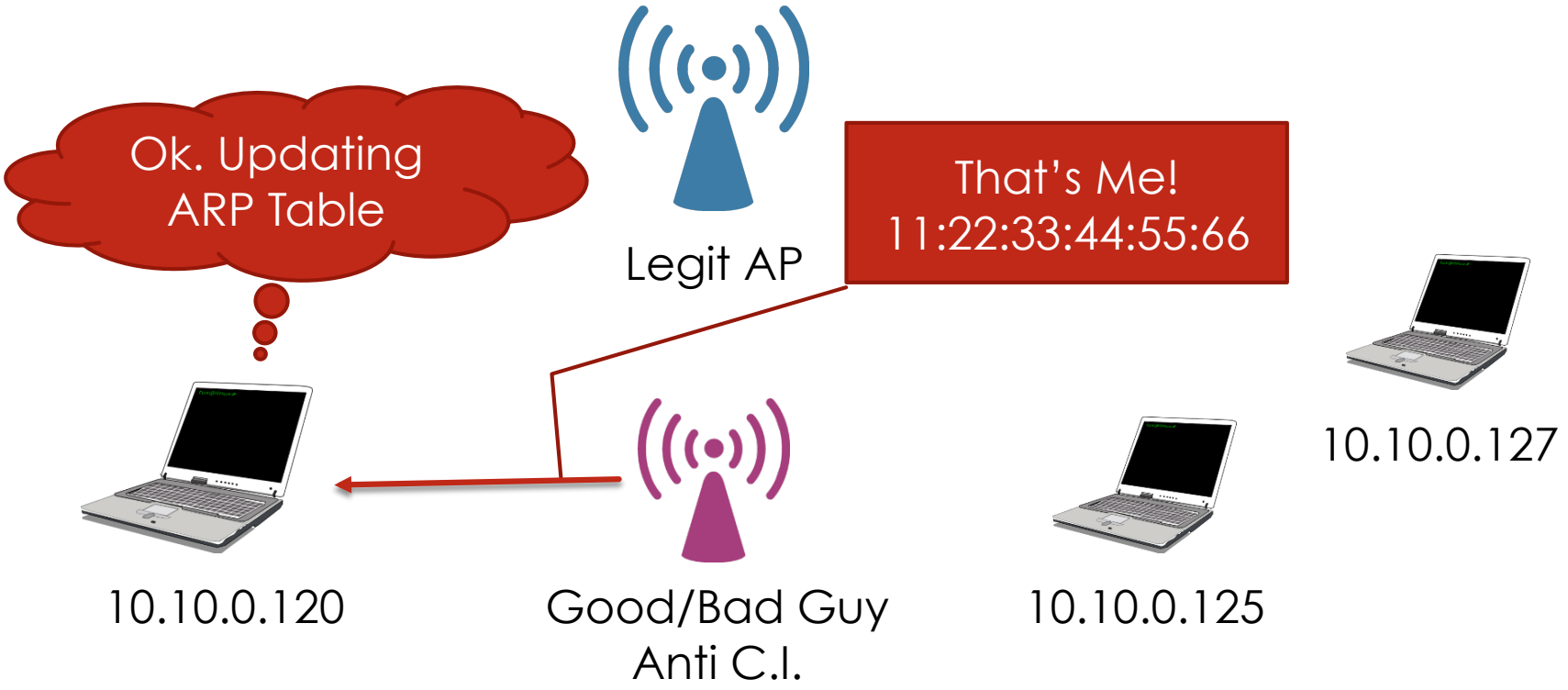
Client Isolation



Client Isolation – Defeated



Client Isolation – Defeated



Client Isolation – Defeated

- L'AP ignora il traffico dei client destinato alla rete locale
- Un secondo dispositivo può quindi farsi carico di distribuire questo tipo di traffico spacciandosi per l'AP. Non ci saranno collisioni di pacchetti.
- E' evidente come sia possibile eseguire attacchi di ARP poisoning anche in situazioni di client isolation
- L'attacco potrebbe non essere rilevato dai consueti IDS
- L'attaccante non è collegato all'AP

Rogue Access Point

- Un Rogue Access Point è un AP sotto il controllo di un attaccante
- Un client non può capire la differenza tra un AP legale e uno di tipo rogue
- Il RAP diventa il gateway dei client, con tutto ciò che comporta
  - Eavesdropping
  - Hijacking
  - Il limite è la creatività

Rogue Access Point – Evil Twin

- Per Evil Twin si intende un RAP che annuncia un SSID conosciuto al client
- Come sceglie l'SSID da clonare?
  - Controllando le connessioni AP-Station attive
  - Osservando le probe che il client sta inviando alla ricerca di AP conosciuti
- L'attacco utilizza tecniche DoS nel caso il client sia già collegato, tentando di forzarne la disconnessione

TLS/SSL

- Transport Layer Security garantisce una cominicazione sicura end-to-end rendendo impossibile l'eavesdropping
- Rende sicura una comunicazione su canale insicuro
- Protegge i siti che visitiamo (https)
- Protegge anche altri servizi (smtp/pop/imap)
- Il problema?
  - L'utilizzo viene spesso dato per scontato.
  - Nel caso di https quello che in larga parte lo abilita è un codice 30x su richiesta http

TLS/SSL – HTTP codes

Client: request http://www.google.it

↓

Server: 302 Found. New location https://www.google.it

↓

Client: request https://www.google.it

↓

Server: 200 Ok. Here's the content

TLS/SSL – Defeating it

- Una volta che il gateway è compromesso le comunicazioni in chiaro possono essere manipolate
- Cosa succede se il codice 300 non dovesse mai arrivare, ma al suo posto venisse inserito direttamente il contenuto della pagina richiesta?
- Se non si va esplicitamente a cercare nella barra degli indirizzi il valore https la pagina richiesta viene visualizzata correttamente
- SSLSTRIP è un tool scritto da Moxie Marlinspike che esegue questa operazione

TLS/SSL – Defeating it with SSLSTRIP

- Agisce come un proxy trasparente tra il client e il server
- Quando riceve dal server un link di tipo https riscrive la pagina al volo, e la serve al client
- <a href=https://….it> diventa <a href=http://…it>
- Tutti i link della pagina visualizzata dal client vengono strippati della componente sicura
- In memoria tiene una mappa delle richieste. I server vengono effettivamente interrogati via https ma ai client vengono passate informazioni in chiaro
- NB: Non agisce su chiamate dirette https:// dal browser

TLS/SSL – Defeating it with SSLSTRIP

Client (intercepted by SSLSTRIP): request http://www.google.it

↓

SSLSTRIP to server: request http://www.google.it

↓

Server: 302 Found. New location https://www.google.it

↓

SSLSTRIP to server: request https://www.google.it

↓

Server: 200 Ok. Here's the content

↓

SSLSTRIP to client (in http): Ok client. Here's the content

TLS/SSL + HSTS

- HTTP Strict Transport Security è un meccanismo in cui un server dichiara che le connessioni ad un certo host DEVONO essere effettuate tramite HTTPS
- Una volta che il browser ha visitato una pagina così configurata trasformerà internamente tutte le richieste http in https.
  - Codice HTTP 307, Internal redirect.
- Si dichiara nell'header di una connessione HTTPS
  - Strict-Transport-Security: max-age=expireTime [; includeSubdomains]
  - Alcuni browser hanno una lista di siti preconfigurati con HSTS

TLS/SSL + HSTS – HTTP codes

Client: indirizzo digitato http://www.gmail.com

↓

Client: 307 Internal redirect https://www.gmail.com

↓

Client: request https://www.gmail.com

↓

Server: 200 Ok. Here's the content

SSLSTRIP e HSTS

- SSLSTRIP non è in grado di intercettare le richieste inviate a siti per cui è presente un record HSTS
  - www.gmail.com è un sito sicuro da visitare
  - www.miosito.it è un sito sicuro da visitare SE già visitato in precedenza (l'header HSTS è stato memorizzato)
- Può ancora essere efficace in determinate condizioni
  - www.ilmionuovosito.it non è sicuro da visitare SE non è mai stato visitato prima
  - www.gmail.com non è sicuro da visitare SE ci si arriva tramite un link

SSLSTRIP+ e HSTS

- SSLSTRIP+ è una nuova versione che consente l'attacco anche su siti teoricamente protetti da HSTS
- Presentata al Blackhat Asia 2014 da Leonardo Nve
- Quando il client richiede una pagina http il contenuto viene modificato in due modi:
  - Viene modificato https in http (come l'originale)
  - Viene modificato il record dns in maniera da sembrare simile, ma non uguale
- Un server DNS sincronizzato con SSLSTRIP+ si occupa di fornire risposte coerenti al client

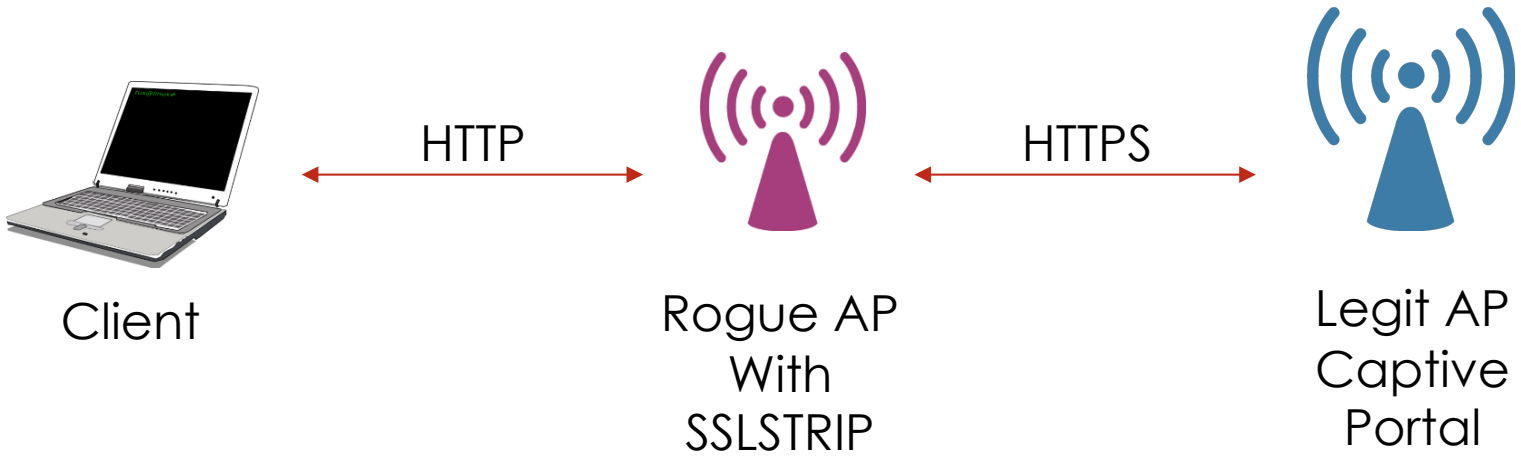
SSLSTRIP+ e HSTS

- L'utente chiede la pagina www.google.it
- SSLSTRIP fornisce la versione http non protetta del contenuto
- SSLSTRIP sostituisce i link presenti nella pagina
  - https://mail.google.com
  - http://mail.gooogle.com (Una o in più, deceptive)
- Se si clicka sul link gmail il client tenterà di collegarsi ad un dominio diverso che viene risolto dall'attaccante
- Il browser controlla il record HSTS di gooogle.com, non risultando presente accetterà di visualizzarlo

HSTS e Captive Portals

- I Captive Portals sono un caso molto svantaggiato in questo contesto
- Non possono essere protetti da HSTS in maniera preventiva (l'attaccante può modificare il nome a domino)
- Un attacco di tipo Rogue Access Point – Evil Twin non cambia l'esperienza utente (tranne per la connessione non https)

Captive Portals vs SSLSTRIP + RAP



Social Engineering – Root CA

- Altri attacchi sono possibili, alcuni coinvolgono l'ingegneria sociale
- L'utente può essere convinto dal captive che per rendere più sicura la connessione abbia bisogno di installare un certificato
- Se un attaccante riesce ad installare un certificato Root all'interno di un client può intercettare e proxare le richieste pur mostrando nel browser che la connessione è https
- SSLSNIFF consente questo tipo di attacco

802.1x – Securing the channel

- Tutti gli attacchi illustrati sono possibili …
  - perché il traffico passa in chiaro
  - perché l'SSID non dà la certezza dell'identità dell'AP
- 802.1x risponde a queste due esigenze
  - Il traffico è crittografato per utente, generando una coppia di chiavi utilizzabile solo per un singolo client.
    - **No eavesdropping, il traffico di un utente è cifrato singolarmente**
    - **No direct transmission, impossibile eludere la client isolation**
  - Usa i certificati per garantire l'identità del server
    - **No Rogue AP**

802.1x – Hole 196

- 802.1x non è immune da problemi
- AirTight ha scoperto che una certa feature di WPA2 poteva essere utilizzata come vulnerabilità
- L'ha chiamata Hole196 perché derivava dalla pagina 196 del documento IEEE che illustra lo standard 802.11
- Il documento descrive l'esistenza di due tipi di chiavi:
  - Una coppia di chiavi per proteggere il traffico **unicast**
  - Una chiave GTK per proteggere il traffico **multicast**
- Visto che una ARP reply può essere broadcast sarebbe possibile generare una ARP poisoning anche su una rete 802.1x …
- se è **disattivata** la Client Isolation

802.1x – Eduroam

- Uno degli esempi di WiFi federato
- Presente in più di 60 paesi
- Utilizza un tool chiamato CAT (Configuration Assistant Tool) per permettere una configurazione semplice dei client

Grazie per l'attenzione!

andrea.lora@cnr.it
http://calliope.mlib.cnr.it/
AdRRM1 – Montelibretti
CNR – Istituto Cristallografia
06/90672622

DoS Layer 1 – RF Jamming

- Semplice implementazione attraverso suite aircrack-ng
- Si inviano pacchetti UDP (anche a indirizzo non esistente) floodando il canale
- # airmon-zc start wlan0 #channel
- # airtun-ng -a hwaddress1 mon0
- # ifconfig at0 10.1.0.1
- # arp -a 10.1.0.2 hwaddress2
- # udpflood.pl 10.1.0.2 0 0 0