Giuseppe Augiero

Augiero.it

festival ICT

11 NOVEMBRE 2015
FIERA MILANO CONGRESSI

BGP HIJACKING

ovvero Alice e Bob non sono al sicuro

GIUSEPPEAUGIERO

WHOAMI?

Festival ICT 2015 - Milano - BGP Hijacking-ovvero Alice e Bob non sono al sicuro.

BGP HIJACKING

CONTENUTI

Introduzione

Introduzione al Bgp

Incidents

Casi reali di bgp hijacking

Hijacking e tipologie di attacco

Che cosa è questa tipologia di attacco?

DISCLAIMER

SCOPO DIDATTICO

Il seguente materiale ha scopo unicamente didattico.

REATO PENALE

Qualsiasi attività di hijacking, intercettazione sono reati punitili penalmente

SCOPI DIVERSI

Qualsiasi altro utilizzo delle informazioni riportate in queste slide è vietato.

USI IMPROPRI

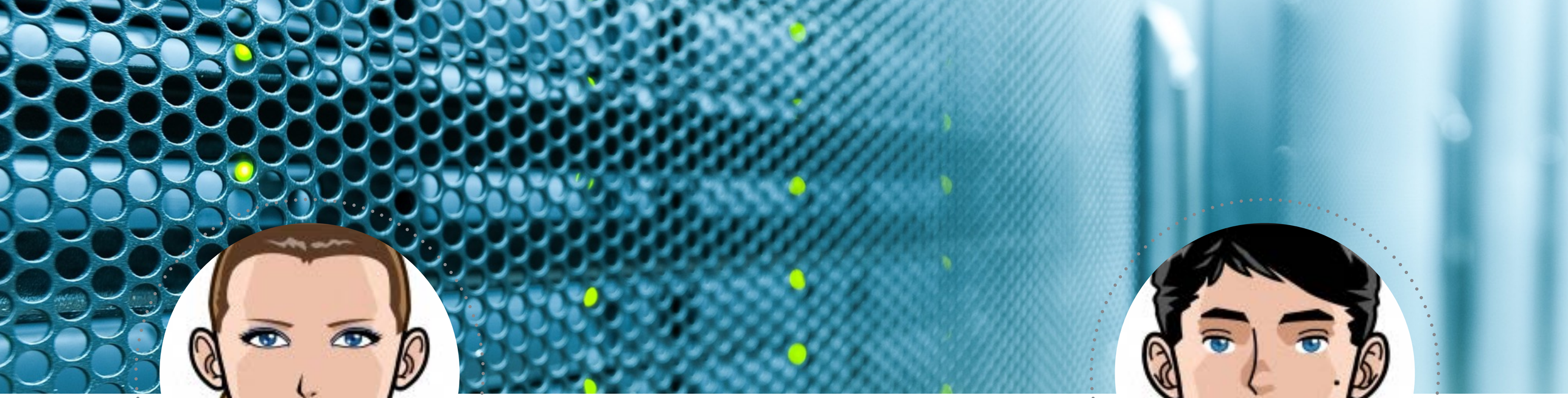
L' autore non si assume alcuna responsabilità per usi impropri.

FOCUS

Attacco

Riconoscimento

Soluzioni



ALICE
Utente

★★★★☆

Bob
Utente

★★★★☆

ALICE E BOB ...

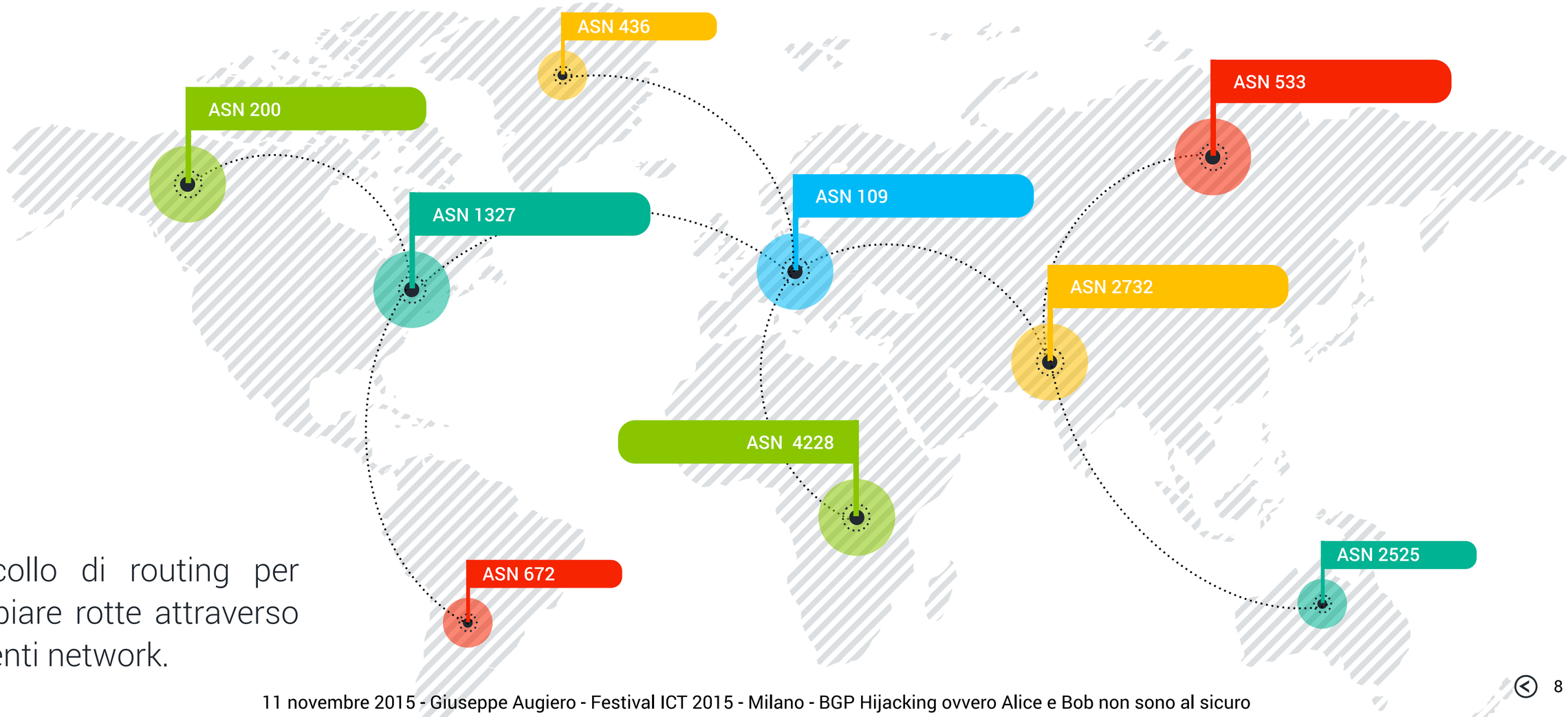
“4°Episodio”

INTRODUZIONE

Festival ICT 2015 - Milano - BGP Hijacking ovvero Alice e Bob non sono al sicuro.

BGP

BORDER ROUTER PROTOCOL



Bgp

Protocollo di routing per scambiare rotte attraverso differenti network.

BGP FEATURES

- Path Vector Protocol
- Incremental Updates
- Traffic Engineering
- Autonomous System

AUTONOMOUS SYSTEM

BGP HIJACKING

- Insieme di reti gestite con la stessa policy di routing (e di solito della stessa proprietà).
- Il concetto di AS è una pietra miliare per BGP.
- Ogni AS deve essere registrato presso il rispettivo RIR.
- Ogni AS è identificato con un numero univoco a 32 bit.

BGP OPERATIONS

BGP HIJACKING

- Impara più percorsi attraverso i router Bgp interni ed esterni.
- Seleziona il percorso migliore e lo scrive nella tabella di routing (RIB).
- Il percorso migliore viene inviato agli altri speakers.
- Sono adottate policy per la scelta del path.

UPDATE MESSAGE

Sicurezza?

Update
Usati per inviare ai router con cui esiste una relazione le informazioni di raggiungibili relative ad un singolo cammino.

Open
Messaggi usati per la procedura di Neighbor Acquisition.

Notification
E' usato per inviare una notificazione di errore ai router vicini.

Keepalive
Messaggi usati per manifestare l'attività del router ed evitare che scada l'Hold Timer.

1%

- Bgp rappresenta una infrastruttura critica per internet.
- Errori di configurazione colpiscono circa l'1% delle entry delle routing table.
- Il sistema attuale è vulnerabile ad errori umani e ad attacchi.

INCIDENTS

Festival ICT 2015 - Milano - BGP Hijacking-ovvero Alice e Bob non sono al sicuro.

INCIDENT
BITCOIN
HIJACKING

- Attacchi tra ottobre 2013 e maggio 2014.
- Annuncio dei prefissi dei più grandi provider mondiali (Amazon, Ovh, Digital Ocean…).
- Attaccante: provider Canadese.
- L'obiettivo dell'operazione era quello di intercettare i dati fra i miners e i mining pools. Si stima che nei primi 4 mesi sono stati "guadagnati" 83.000 $.

INCIDENT
CENSORSHIP
HIJACKING

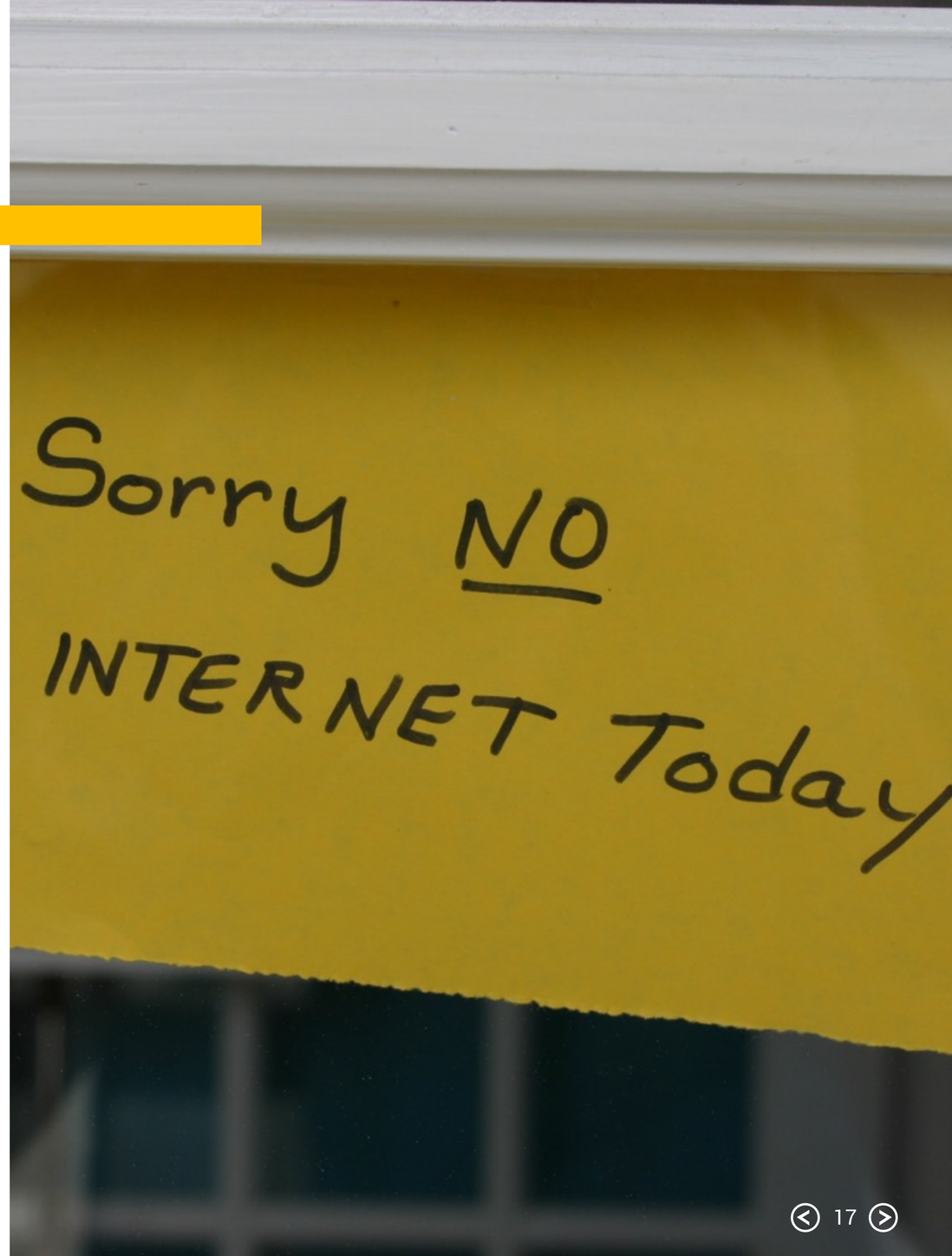
- 28 - 30 marzo 2014
- Il presidente turco richiede il blocco di twitter.
- Primo step: Blocco dei dns di Turk Telekom.
- Secondo step: annuncio degli ip dei più famosi dns (Google, OpenDns, Level3).
  Annuncio di /32.
  Blocco di altri servizi tra cui Youtube.

INCIDENT
SPAMMING
HIJACKING

- Viene usato l’ip squatting per bypassare le reputation list.
- Due casi interessanti.
- Caso Russo.
- IRR e Radb. Annunci a breve durata.

INCIDENT
SIRIA
HIJACKING

- Non nuova a queste attività.
- Annunci di breve durata.
- Tre main stream provider.
- Qualunque sia la causa principale o l'intento, il risultato è stato che gli utenti hanno sofferto di una breve interruzione parziale o degrado delle prestazioni, mentre il traffico di alcuni di utenti mondiali veniva indirizzato alla Siria.

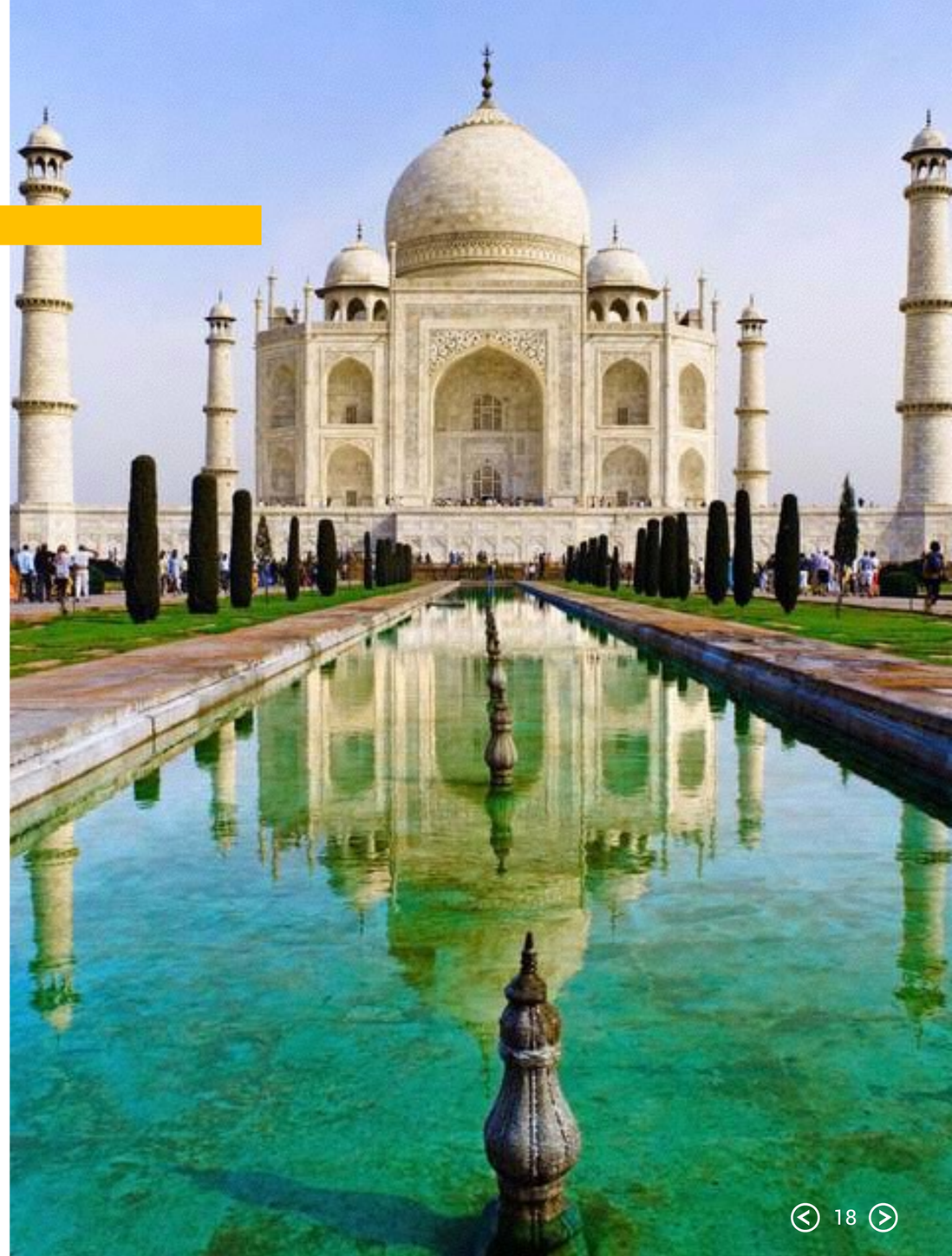


INCIDENT

PUÒ AVVENIRE SEMPRE...

HIJACKING

- 6 novembre 2015
- Provider Indiano: Airtel
- Annunciati migliaia di prefissi.
- La portata dell'hijacking è stata notevole in quanto due grandi AS hanno accettato e propagato gli annunci fatti da Airtel



PRENDIAMO IN PRESTITO

Festival ICT 2015 - Milano - BGP Hijacking ovvero Alice e Bob non sono al sicuro.

TRAFFICO NEW YORK-LOS ANGELES DIROTTATO

IL NOCCIOLO DELLA QUESTIONE

Perché qualcuno dovrebbe attaccare il protocollo BGP?

Perché il traffico in ingresso può essere intercettato in maniera passiva?

Perché il traffico in uscita verso specifiche destinazioni può essere intercettato?

Perché è difficile notare che sia in atto un hijacking?

BGP PROTOCOL

BGP HIJACKING

- Il protocollo Bgp è un protocollo semplice ed è uno dei più anziani.

BGP FAIL?

BGP HIJACKING

- Implementazione su diverse tipologie di router.
- Le rotte sono costruite hop-by-hop.
- Fiducia nei vicini.

BGP POLICY

BGP HIJACKING

- Le policy Bgp possono essere complesse nella loro gestione.
- Sono tutte locali e non esiste una coordinamento globale.
- Le policy locali permettono di accettare, propagare o rigettare le rotte.
- Presentano varie vulnerabilità.

BGP SECURITY

BGP HIJACKING

- Tra AS gli annunci di routing sono accettati senza (quasi) nessuna convalida.
- Per un operatore di rete **è possibile annunciare prefissi di rete di qualcun altro senza permesso**.
- Il prefisso può essere leaked.

BGP HIJACKING

- Malicious or not?

BGP HIJACKING (II)

BGP HIJACKING

- Un operatore malintenzionato può rubare prefissi o può intercettare, mettere in blackhole o modificare il traffico in transito.

- Un buon operatore può, di tanto in tanto, anche fare (involontariamente) hijacking di una rete di qualcun altro a causa di un errore.

BGP HIJACKING (III)

BGP HIJACKING

- Un dipendente malizioso di un buon operatore è quindi in grado di leggere e modificare il traffico.

- L'accesso non autorizzato alle risorse di un operatore può essere utilizzato anche per effettuare hijacking.

BGP HIJACKING (IV)

BGP HIJACKING

- E’ difficile capire se un annuncio di rotte errate sia causato da un attacco oppure da un errore di configurazione (es. As 7007).

BGP - LOCAL HIJACKING

BGP HIJACKING

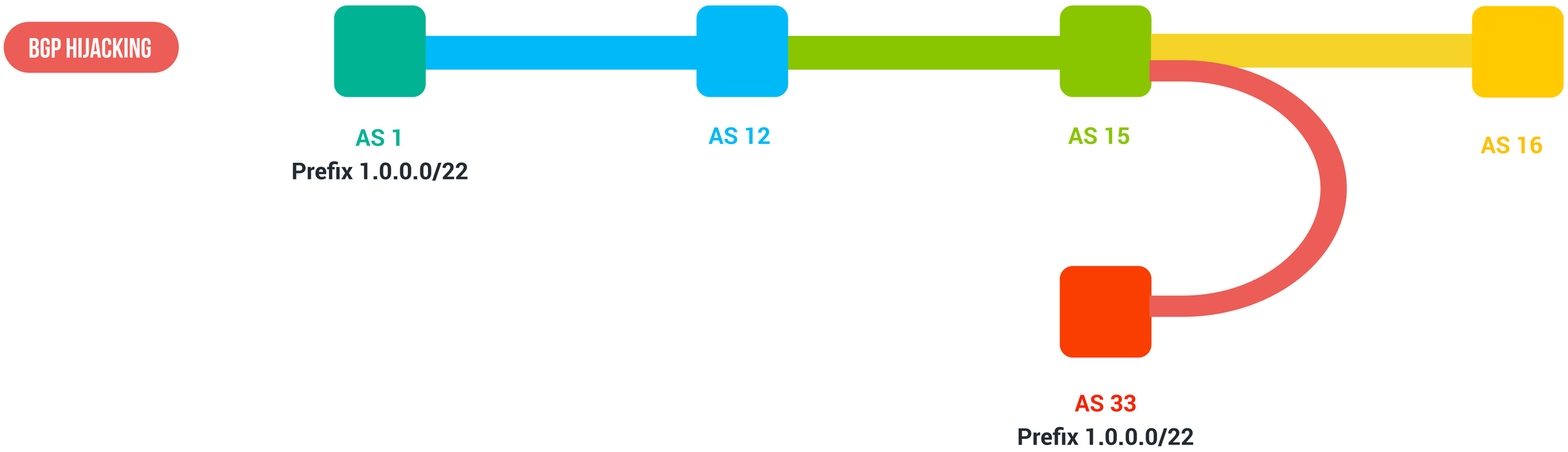
- E’ possibile effettuare anche Hijacking locali (all’AS).
- Dipende dalla posizione dell’attaccante e del suo AS.

TIPOLOGIE DI ATTACCO

Festival ICT 2015 - Milano - BGP Hijacking ovvero Alice e Bob non sono al sicuro.

BGP ATTACK (I)

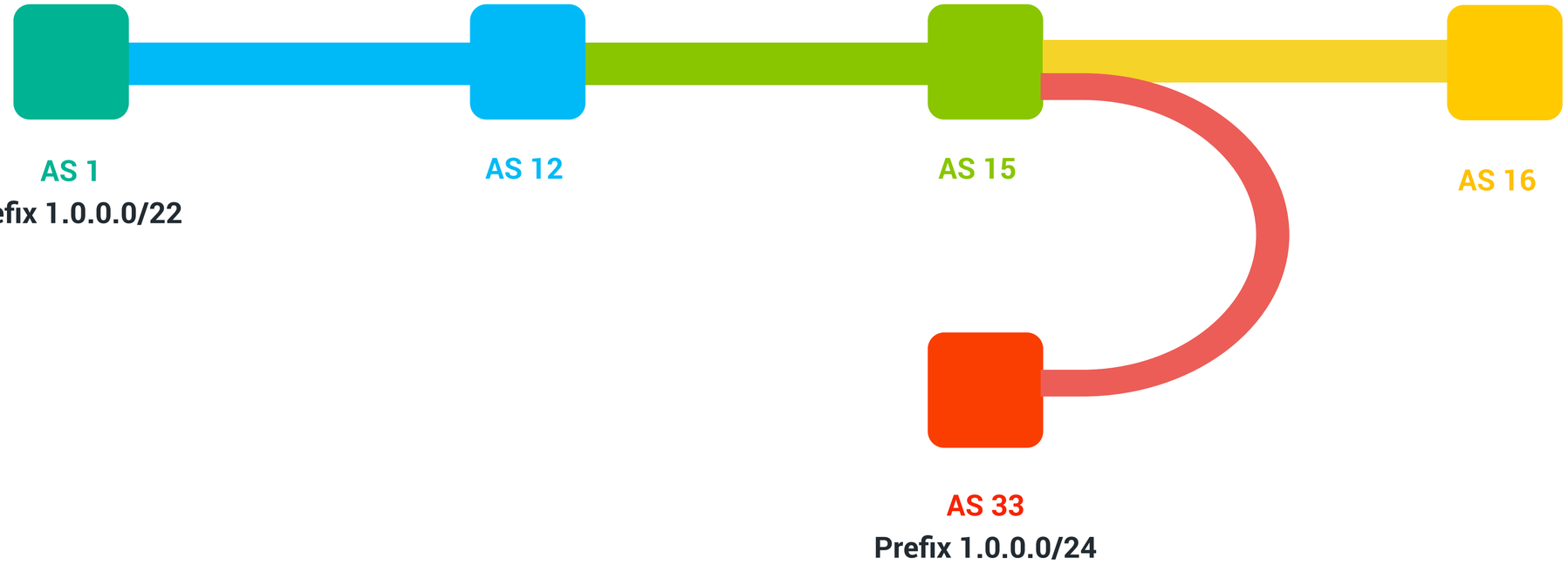
Prefix-Hijacking (MOAS)



BGP
ATTACK (II)

De Aggregation

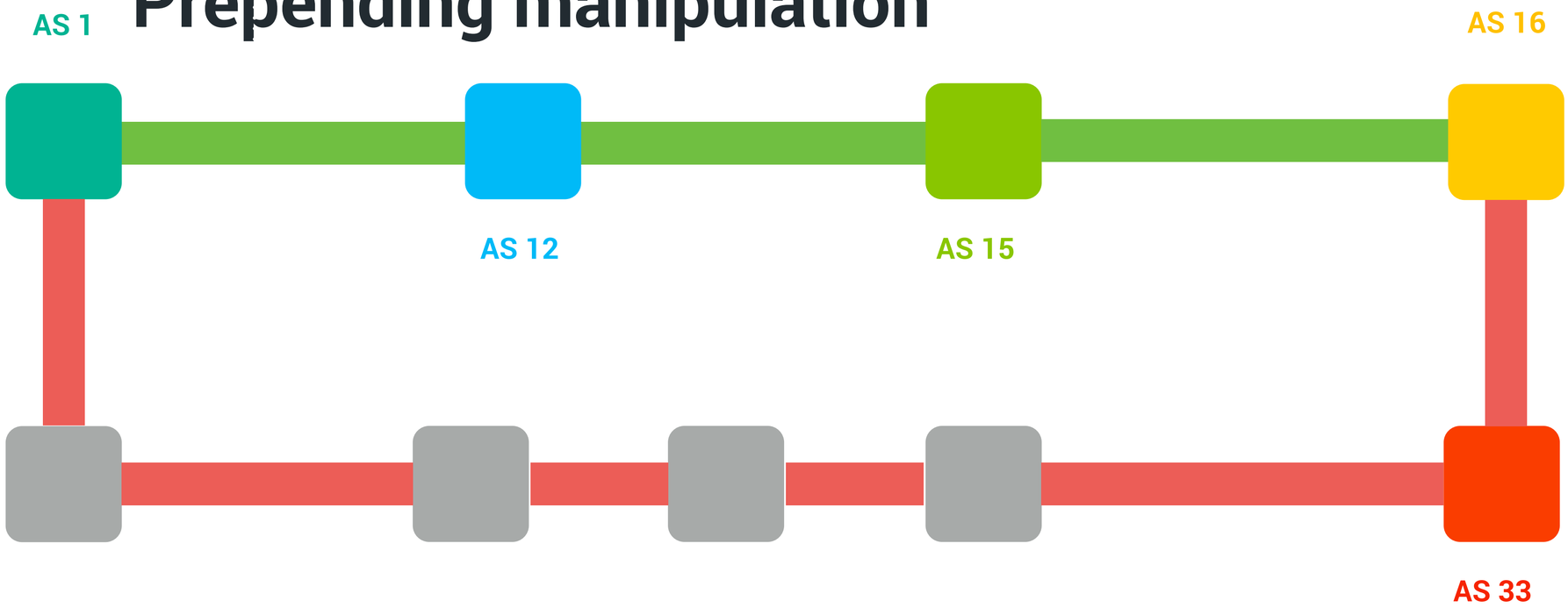
BGP HIJACKING



BGP ATTACK (III)

Prepending manipulation

BGP HIJACKING



BGP
ATTACK (IV)

SOLUZIONI?

Festival ICT 2015 - Milano - BGP Hijacking ovvero Alice e Bob non sono al sicuro.

ROUTING SECURITY

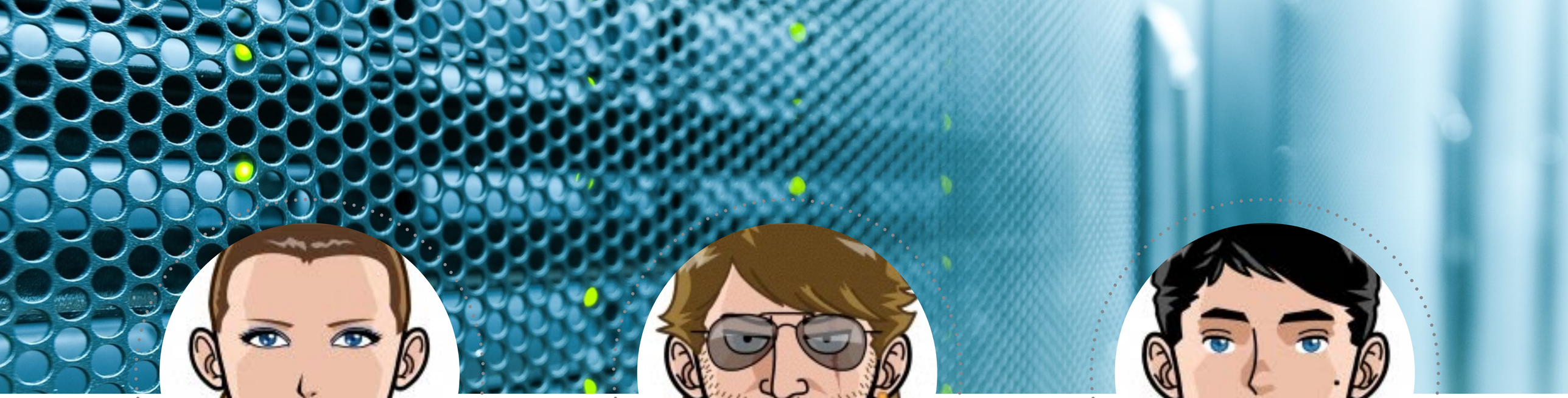
La sicurezza del routing è una cosa complicata.

ROUTING SECURITY

- Esistono interessanti soluzioni per “contenere” il problema.
- Sono molte le soluzione di sicurezza proposte ma nessuna risolve tutti le problematiche.
- Primo obiettivo è la prevenzione.
- Consapevolezza che l’incident può accadere sempre.

ROUTING SECURITY

- L’impatto di una attacco BGP potrebbe essere molto elevato.



ALICE
Utente

★★★★☆

Mallory
MITM

★★★★★

Bob
Utente

★★★★☆

ALICE E BOB NON SONO AL SICURO!!!

Domande?

Giuseppe Augiero

www.augiero.it

talk@augiero.it

@GiuseppeAugiero

festival ICT

11 NOVEMBRE 2015
FIERA MILANO CONGRESSI

BGP HIJACKING

ovvero Alice e Bob non sono al sicuro