

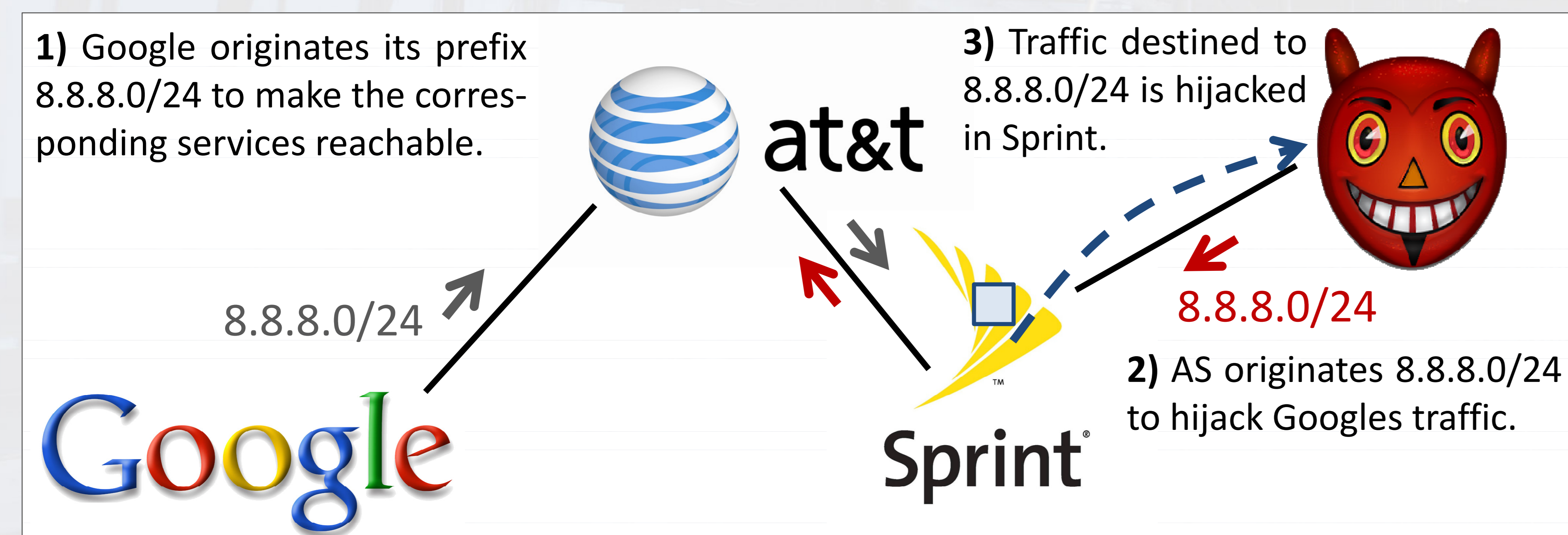
About Prefix Hijacking in the Internet

Prefix Hijacking: Threat and Detection

Border Gateway Protocol – The Problem

Today, global routing is realized by means of the **Border Gateway Protocol (BGP)**. Developed in the early nineties when having mostly scientific networks in mind, the main design goal of BGP was resource frugality. Security issues were largely left out of consideration and standardization: Routing information is **not authenticated**. Thus, ASs may arbitrarily inject, modify, suppress, and fake routing information.

Today, the Internet is a part of the infrastructures being essential for economic applications and public life. Here, BGP's plain trust-model is a serious problem: Mistakes or attacks may cause **instability** and **blackholes**. Traffic may be **redirected**, **eavesdropped**, or **modified**; unacceptable possibilities for fundamental systems and services.



As routing information is not signed, prefixes may be hijacked.

Countermeasures

To prevent intentional and unintentional manipulations, eliminate the known threats, and make Internet routing reliable, protocol extensions to verify the authenticity and authorization of BGP data are needed. However, due to political and technical reasons, **comprehensive solutions** like *Secure BGP* [1] are very **difficult to deploy** in practice. More **light-weight solutions**, as currently standardized and deployed with RPKI-Based Origin Validation by the IETF Secure Inter Domain Routing Working Group [2] **only address** urgent **misconfiguration scenarios** and will certainly need years until they are productively used at large scale.

To bridge the time and protect the global routing efficiently against attacks, **routing information analysis** seems to be an **interesting** tool. Basis for developing detection techniques is an understanding for the threats and their signatures that must be expected.

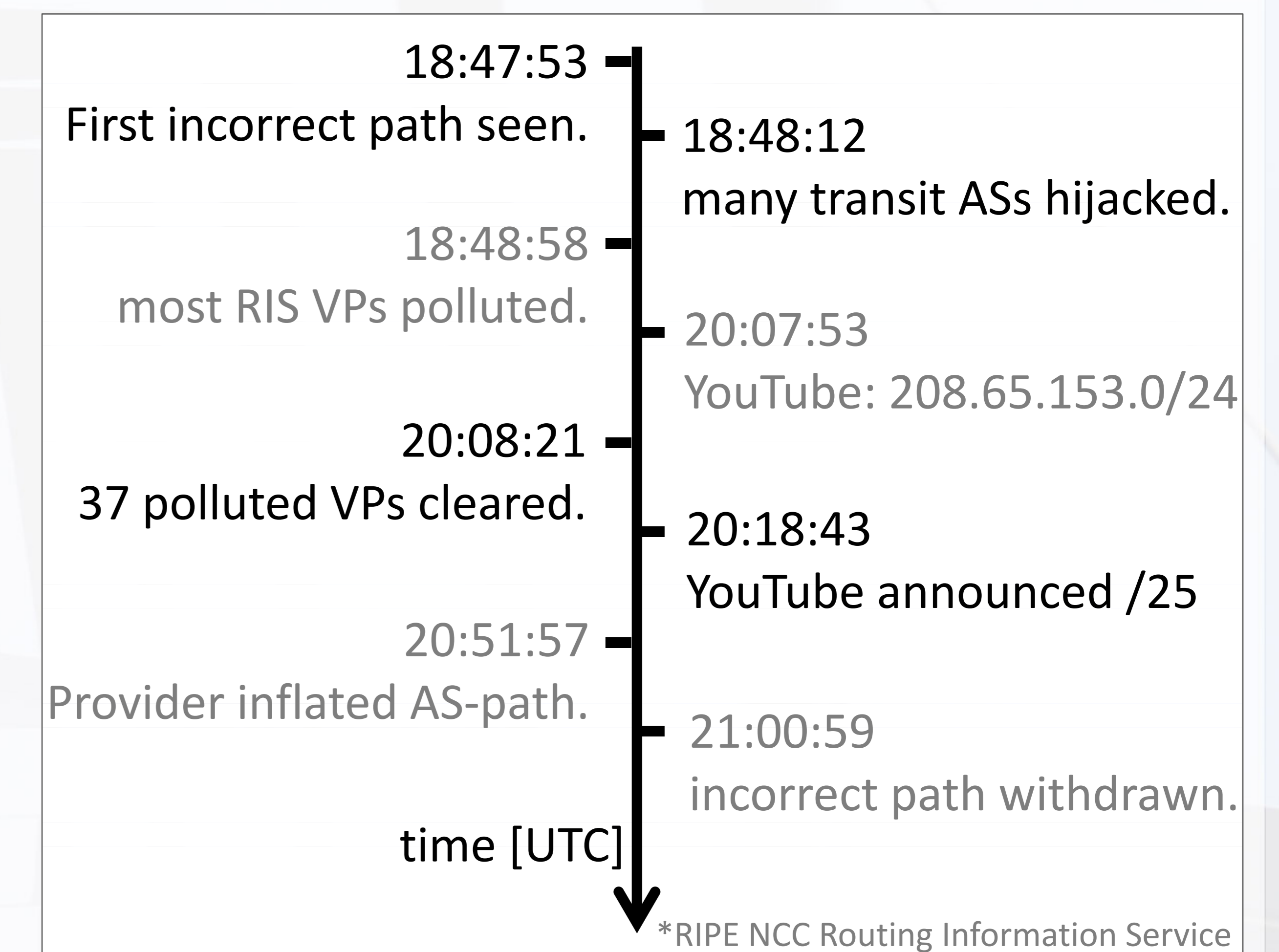
Detection of Prefix Hijacking: The YouTube Event

The YouTube Event

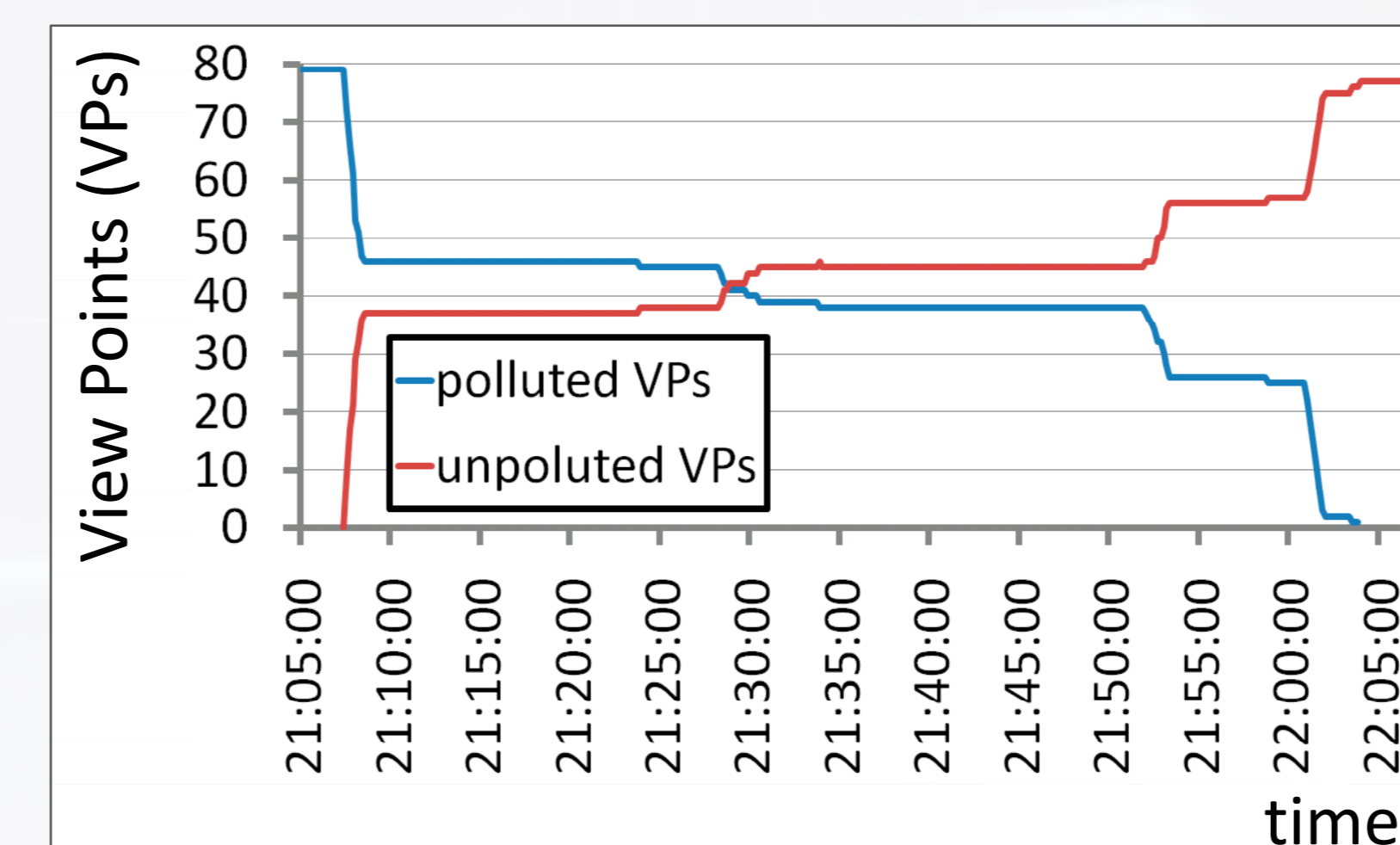
The fact that attacks against the BGP routing is not only of theoretical interest was spectacularly proven in February 2008. On Feb. 24th, Pakistan Telecommunication Company Ltd. (PTCL) started to **originate 208.65.153.0/24**, a sub-prefix of 208.65.152.0/22, **owned**, originated, and used **by YouTube**. The **wrong routing information spread across** large parts of **the Internet** and as more specific paths are preferred, traffic for the hijacked prefix did not reach YouTube anymore. **YouTube became unreachable**.

What happened?

Via the provider (AS3491, BTNA), the advertisement 208.65.153.0/24 made by PTCL spread quickly across the Internet. After less than a minute, most networks monitored by the RIS* project were hijacked. To limit the connectivity problem, YouTube started at 20:07:53 to advertise the same prefix, which limited the scope of the hijack. More specific advertisements and the extension of the AS-path length to the hijacker further reduces the range. At 21:01:00, PTCL identified the misconfiguration and stopped to originate a subspace of YouTube's address space.



Chronological sequence of the YouTube event.



Routing for 208.65.153.0/24 at VPs.

Detection: Concept & Challenges

- Monitor the global routing information in realtime and detect discrepancies and abnormalities.

Challenges and Tasks:

- Specification of signatures that allow for identifying misconfigurations and attacks.
- Development of filters that distinguish illegitimate manipulations from similar but legitimate behavior.
- **It's a search for the Needle in a Haystack.**

[1] Stephen Kent, Charles Lynn, and Karen Seo: Secure Border Gateway Protocol (S-BGP), in IEEE Journal on Selected Areas in Communications, Vol. 18, No. 4, April 2000
[2] P. Mohapatra, J. Scudder, D. Ward, R. Bush, R. Austein: BGP Prefix Origin Validation, IETF SIDR Internet-Draft, July 2011