Technische Universität München
Chair for Network Architectures and Services
Prof. Dr. Georg Carle

27.02.2013

BA / MA / DA thesis
SEP / Guided research
Student assistant job

AN EARLY WARNING SYSTEM
FOR BGP HIJACKING

Motivation

The world wide network is designed to be a fault-tolerant system. Failure of nodes or links is unproblematic for the network as a whole: routing protocols will adjust the traffic flow to take a different path through the network.

Internet-scale routing is based on the exchange of route knowledge between its participants, and implicitly assumes global trust. This allows misconfigured routers and attackers to inject illicit routes into the routing system, and thus to redirect traffic of other networks into their own. Up to this day, it is a difficult task to detect such attacks, and prevention is even harder.

In this thesis, you will learn a great deal about the sophisticated AS hijacking attack. You will study real-world incidents and design an early warning system to disclose and even prevent future attacks.

Your Tasks

Getting in touch with data sources
First, you have to make yourself familiar with available data sources. These include the RIPE whois database, DNS(SEC) registration data and BGP routing tables.

Analysis of real-world incidents
It is essential for the design of an early warning system to have a deep understanding of the attacker's motivation. Based on the paper *"A Forensic Case Study on AS Hijacking: The Attacker's Perspective"* (ACM SIGCOMM CCR 04/2013), you will infer necessary preconditions and tangible goals from a real attack.

The early warning system
With combined analyses of the given data sources, you will find ASes that are most suitable for an attack. Your results will be published on a light-weight website and made accessible via a simple API. In addition, endangered ASes will be consequently monitored for hijacking attempts.

Evaluation
Beside the chance of detecting ongoing hijacking attempts, you will analyze the global AS hijacking threat in general. This includes statistics on the number of endangered ASes and their characteristics like geographic peculiarities etc.

Requirements

- Explorative nature
- Knowledge on inter-domain routing
- Programming skills (Python, some PHP, Bash is nice-to-have)

Keywords

Internet routing, border gateway protocol, autonomous systems, prefix hijacking

Further information:
http://www.net.in.tum.de/en/theses

Contact:
schlamp@in.tum.de