Säkerhet i gränsrouting

-relaterade hot och skydd
- test av sårbarheter

Anders Rafting, Post och telestyrelsen

Michael Liljenstam, Omicron Ceti AB

Agenda

- PTS säkerhetsarbete inom publik elektronisk kommunikation
- BGP: Sårbarheter, hot och konsekvenser av attacker
- Test av sårbarheter
- Sammanfattning & slutsatser

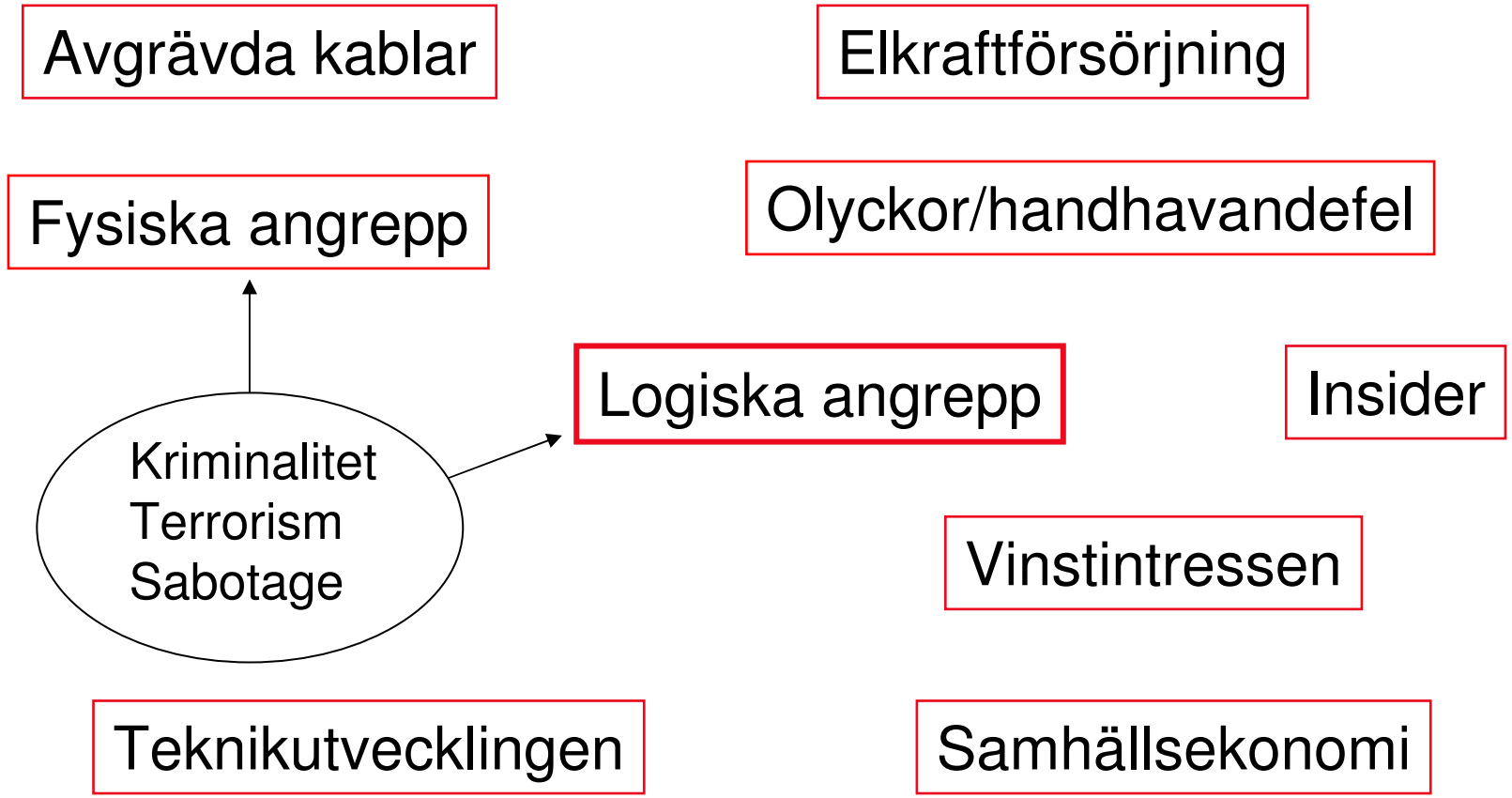
PTS säkerhetsarbete inom publik elektronisk kommunikation

PTS roll är att se till att allmänt tillgänglig elektronisk kommunikation fungerar tillfredsställande och säkert för alla i sund konkurrens

PTS agerar utifrån en säkerhetsnivå som bestämts av marknaden:

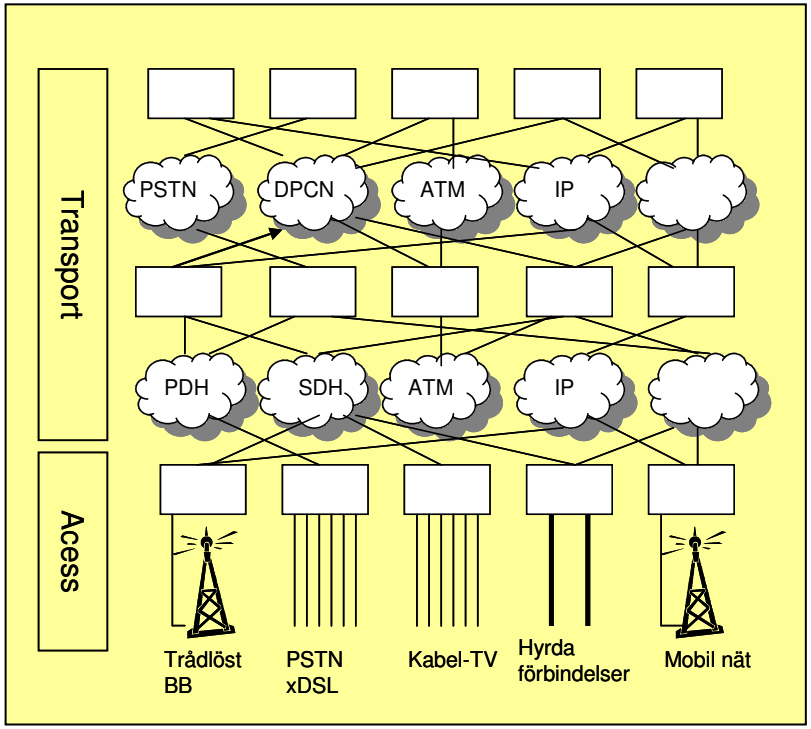
- Upphandling av robusthets- och säkerhetshöjande åtgärder
- Samarbete med näringslivet
- Reglering av säkerheten enligt lag (Ekomlagen + Toppdomänlagen)

Hotbild

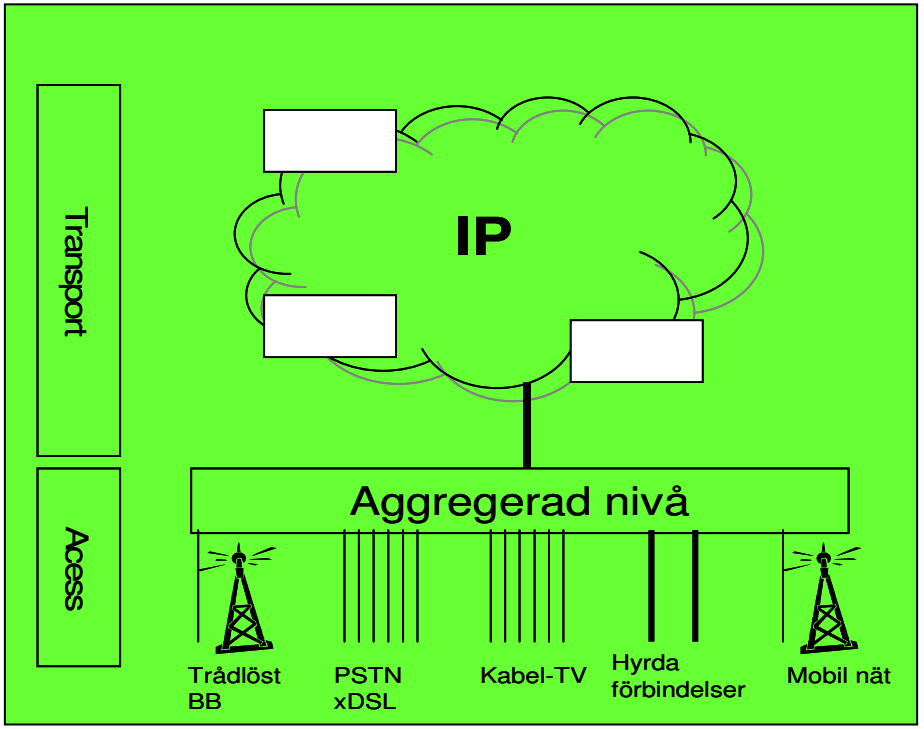

Avgrävda kablar
Elkraftförsörjning
Fysiska angrepp
Olyckor/handhavandefel
Logiska angrepp
Insider
Kriminalitet
Terrorism
Sabotage
Vinstintressen
Teknikutvecklingen
Samhällsekonomi

Näten konvergerar mot IP

Idag



I framtiden



→ mer tryck på BGP

BGP: Sårbarheter, hot och konsekvenser av attacker

- Ingen möjlighet att verifiera uppdateringar
- Exponerat för tillgänglighetsattacker

- Intrång i router (router hijacking)
- Bedräglig modifiering av routing information

- ISP–nät isoleras från omvärlden
- Trafik försvinner – blackholing
- Trafik dirigeras till felaktig eller falsk destination….

- Omdirigering och avlyssning av abonnenttrafik gör det möjligt för angripare att:

  - Undersöka och avtappa abonnenttrafik och skicka den vidare till avsedd destination
  - Modifiera abonnenttrafik och skicka den vidare till avsedd destination
  - Ta bort valda delar av abonnenttrafik
  - Ge sig ut för att vara abonnenter genom att ta emot trafik riktad avsedd för dem och svara å deras vägnar

Initiativ till säkerhetsförbättringar

Skydd av routinginformationen

- Förbättringar av BGP med kryptografiska skydd
  - Secure BGP (S-BGP) [BBN]
  - Secure Origin BGP (SoBGP) [Cisco]

- IETF har en arbetsgrupp för routing-protokollsäkerhet (rpsec)

Tills sådan lösning kan rullas ut

- Realtidskontroller av data (mindre stringent kontroll)
  - Listen & Whisper [Berkeley, m.fl.]
  - Kontroll av ursprung mot IRR [UC Riverside]
  - Kommersiell övervakningstjänst [t.ex. Renesys]

Test av sårbarheter

Syfte och mål:

- Förbättrad förståelse för befintliga och potentiella sårbarheter
- Genom fysiska experiment och simuleringar ta fram förbättrad BCP
- Gemensamma ansträngningar för att uppdaterad BCP förankras och tillämpas på en global nivå

Attack-experiment och simuleringar

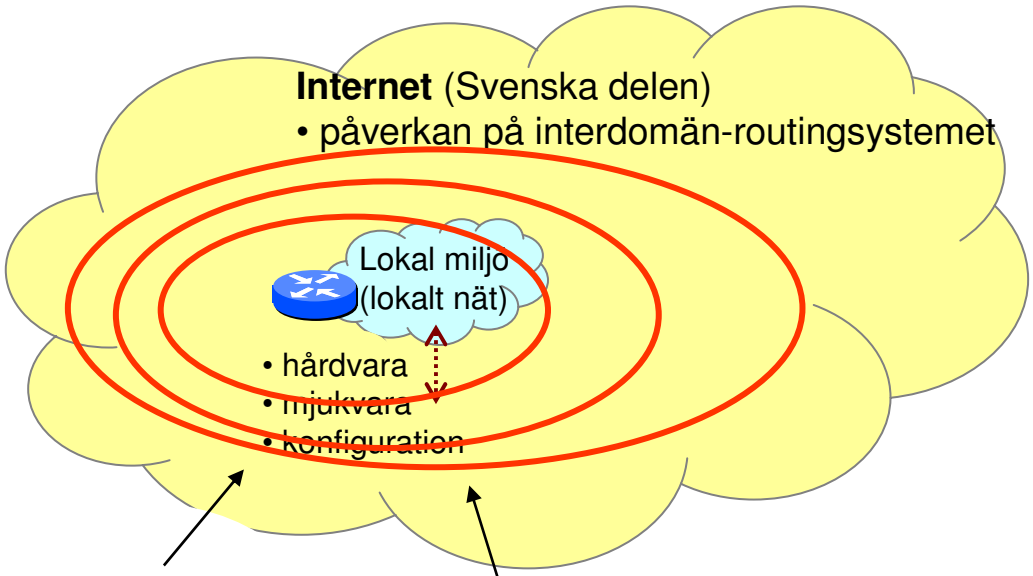
Inriktning

- Studera ett urval kända sårbarheter

Mål för experiment

1. Bättre förståelse för svagheterna
2. Kontrollera om de åtgärdats / kvarstår
3. Grund för simuleringar, med avsikten att försöka uppskatta konsekvenserna av attacker

Metodik



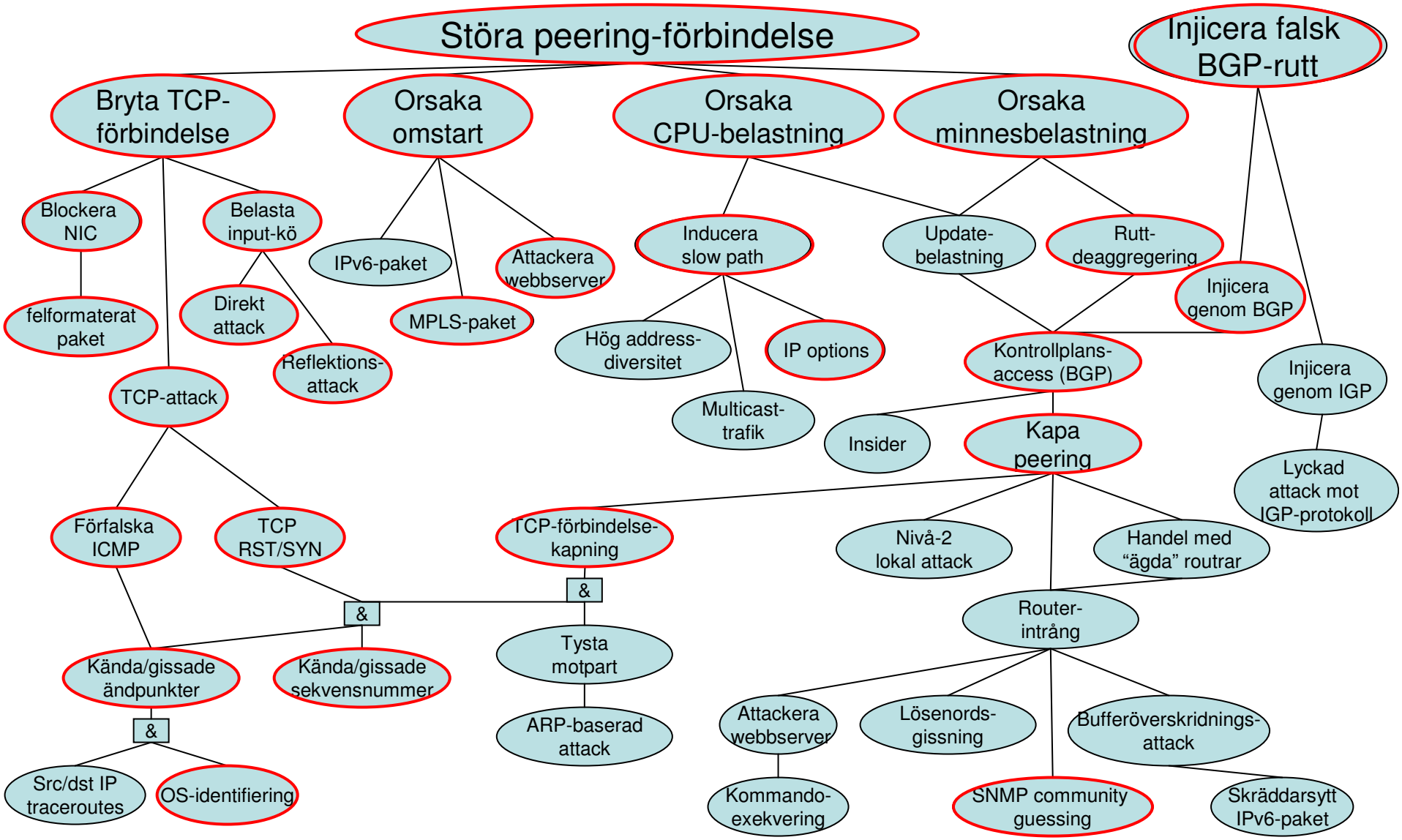
Experiment

”primära effekter”
- intrång
- omstart
- överbelastning (CPU,minne)

Simuleringar

”sekundära effekter” / konsekvenser
- spridning av falsk rutt-information
- effekter av router-krasch
- rutt-dämpning

Attack-träd


Störa peering-förbindelse
Injicera falsk BGP-rutt
Bryta TCP-förbindelse
Orsaka omstart
Orsaka CPU-belastning
Orsaka minnesbelastning
Blockera NIC
Belasta input-kö
IPv6-paket
Attackera webbserver
Inducera slow path
Update-belastning
Rutt-deaggregering
Injicera genom BGP
felformaterat paket
Direkt attack
MPLS-paket
Reflektions-attack
Hög address-diversitet
IP options
Kontrollplans-access (BGP)
Injicera genom IGP
TCP-attack
Multicast-trafik
Insider
Kapa peering
Lyckad attack mot IGP-protokoll
Förfalska ICMP
TCP RST/SYN
TCP-förbindelse-kapning
Nivå-2 lokal attack
Handel med "ägda" routrar
&
&
Router-intrång
Kända/gissade ändpunkter
Kända/gissade sekvensnummer
Tysta motpart
&
Attackera webbserver
Lösenords-gissning
Bufferöverskridnings-attack
ARP-baserad attack
Src/dst IP traceroutes
OS-identifiering
Kommando-exekvering
SNMP community guessing
Skräddarsytt IPv6-paket

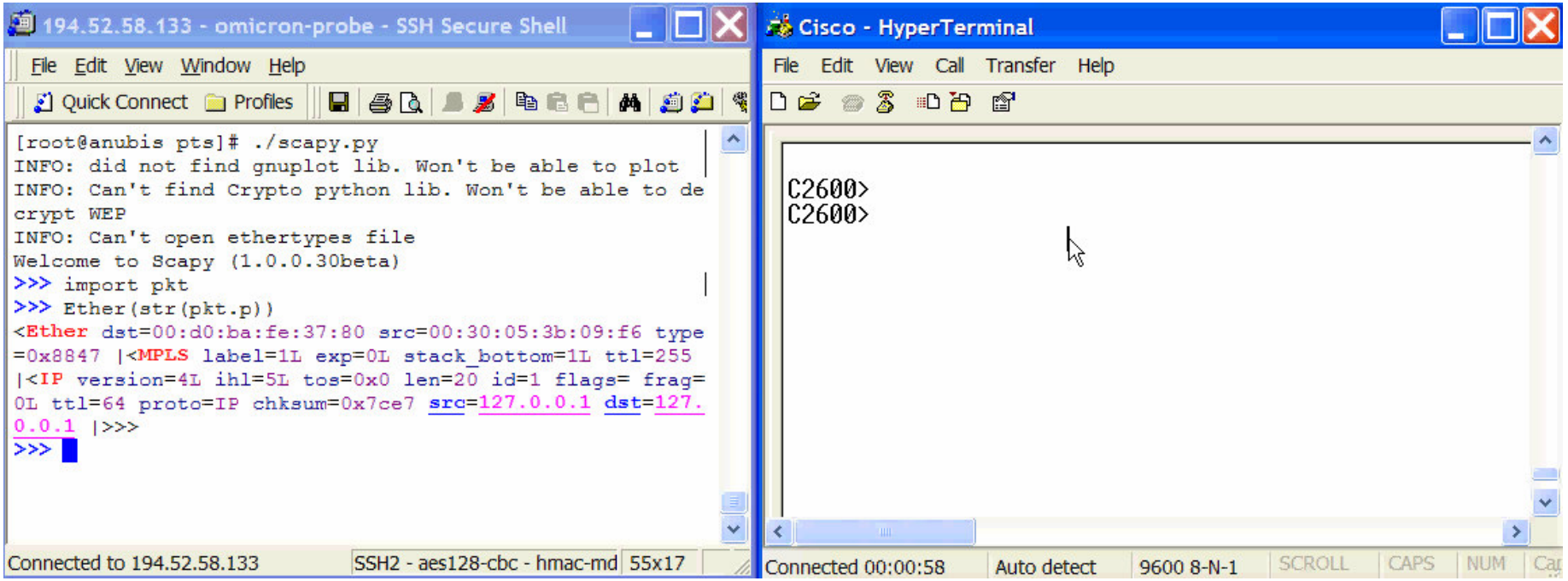
Exempel på ett praktiskt experiment

Återskapa attack mot en känd MPLS-relaterad sårbarhet

- Mindre routrar, IOS versioner som stöder MPLS
- Åtgärdat i nyare OS-versioner

Angripare

Router-konsol



Några observationer

- TCP-sårbarheter
  - Störningsattack för att bryta förbindelse

    ⇒
    - Svårare att genomföra i praktiken än först förespeglats
    - Svårare med moderna OS-versioner, även utan extra MD5-skydd
  - Injicering av BGP-update

    ⇒
    - Endast praktiskt om förbindelsen kan avlyssnas
- Belastningsattacker
  - Mer reellt hot mot peering-förbindelser

    ⇒
    - Behov av skyddsåtgärder

Simuleringsmodell

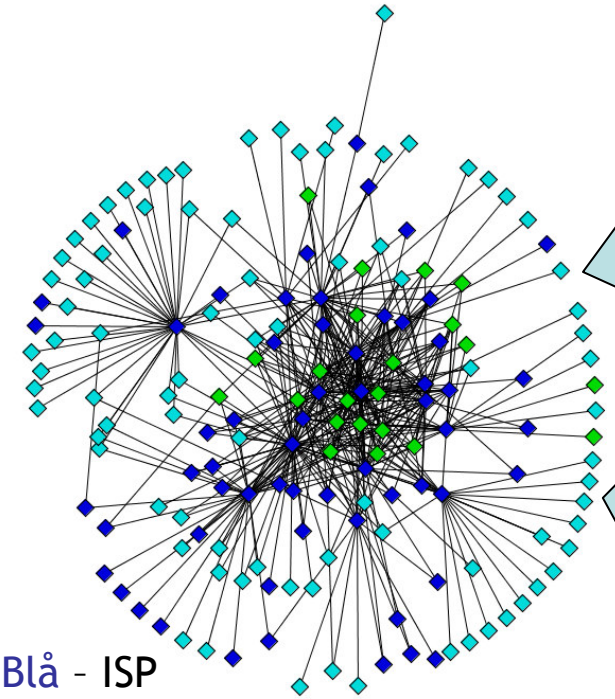
Svenska delen av interdomän-routingsystemet

Paket-nivå simulator (SSFNet)

- Detaljerade protokoll-modeller
  - BGP
- Använts tidigare för att studera BGP
  - Routing-konvergens
    [Griffin & Premore, ICMP'01]
  - Route-flap-dämpning
    [Mao et al., SIGCOMM'02]

Validering

- Jämförelse med BGP-mätdata:
  - Routingtabeller



Blå - ISP
Cyan - kund
Grön - granne

- AS-topologi
  - BGP-data
  - routingregistret
  - lista över svenska ISPer
- AS-egenskaper
  - Marknadsandel
- Routing-policy
  - routingregistret

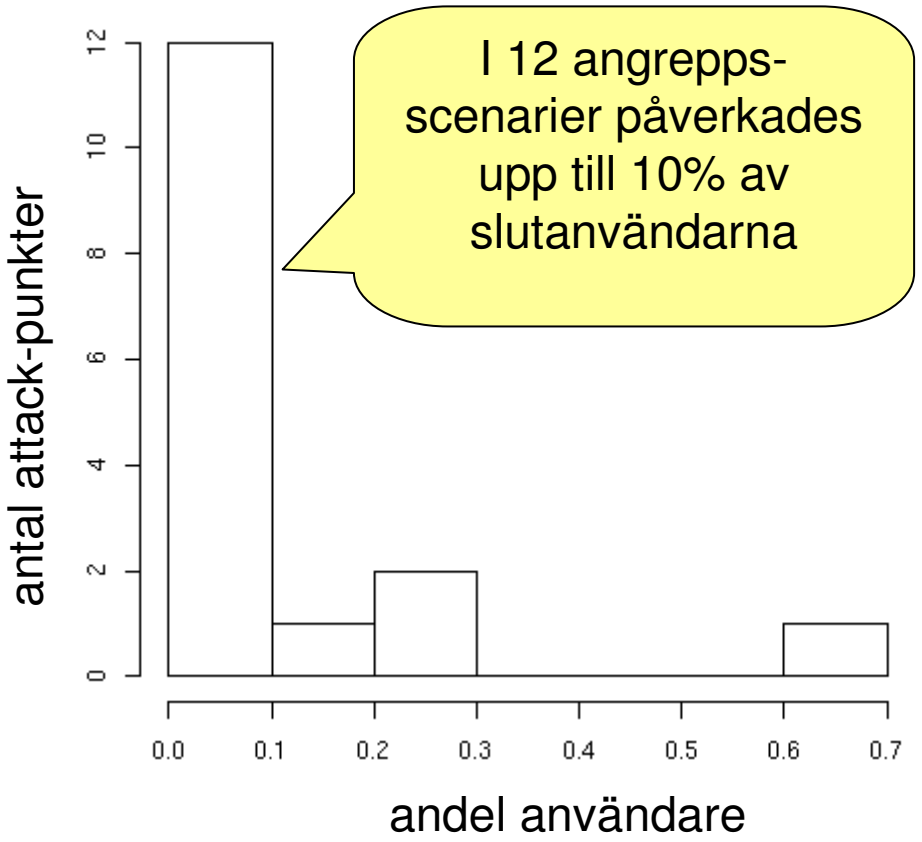
Simulerad attack: exempel-scenario

Annonsering/injicering av falsk routing-information

- Deaggregering av prefix
- Olika angreppsobjekt
- Befintligt skydd: defensiv filtrering
- Försiktiga antaganden
  - Defensiva filter från all tillgänglig information

⇒ undre gräns för konsekvenser

- Exempel-mål: bank



Slutsatser & sammanfattning

Resultat och rekommendationer

- Viktigt med skyddsåtgärder mot belastningsangrepp
  - Enkla belastningsattacker större hot än TCP-attacker
- Viktigt att uppdatera mjukvaran även i routrar
- Använd tillgängliga BCP:er, t.ex. Cymru, Cisco
  - Studerat skyddseffekt av dessa
- Detaljerad rapport kommer att publiceras inom kort

Simulerad spridning av falsk information in systemet

- Bra skydd mot vissa scenarier – liten slutanvändarpåverkan
- Enstaka fall med stort genomslag $\Rightarrow$ marknadskoncentration
- Dagens metoder ger inte ett heltäckande skydd

Berörda parter bör överväga möjligheten att införa någon form av förstärkt skydd i väntan på en standardiserad lösning…

Tack!