Internet Routing Security

Henk Uijterwaal
Manager New Projects Group
RIPE NCC

Roundtable meeting, 7 February 2006

Outline

- Introduction
- DISI
- DNSSEC
- Certification of Internet Resources
- Conclusions

Introduction

- I'm going to show security problems with the Internet
- Do not panic, it is not as bad as it seems
- Disclaimer:
  - Technology has been simplified
  - Explain the main ideas, not the implementation

Outline

- Introduction
- DISI
- DNSSEC
- Certification of Internet Resources
- Conclusions

Deployment of Internet Security Infrastructure DISI

- Umbrella for the NCC to do security related work with its customers
- Motivation (spring 2000)
  - The Internet had become a standard tool for doing business
  - Where people do business, people exchange euro's. Where money is exchanged, bad guys show up
  - All kinds of technologies popping up to secure data
  - Many of them require coordination between providers or at a central point
  - RIPE NCC

DISI

- Goals:
  - Investigate security related development, select what is relevant for our membership
  - Assist in deployment: Coordination, tool development, training and documentation
- Activity since late 2000
  - Project manager with a changing team
- Community feedback through the RIPE tech-sec WG (and others)
- Liaise with the IETF, RIRs, operator forums, …

DISI Focus

- 2001-2006: DNSSEC
- 2005+: Certification of Internet resources

Outline

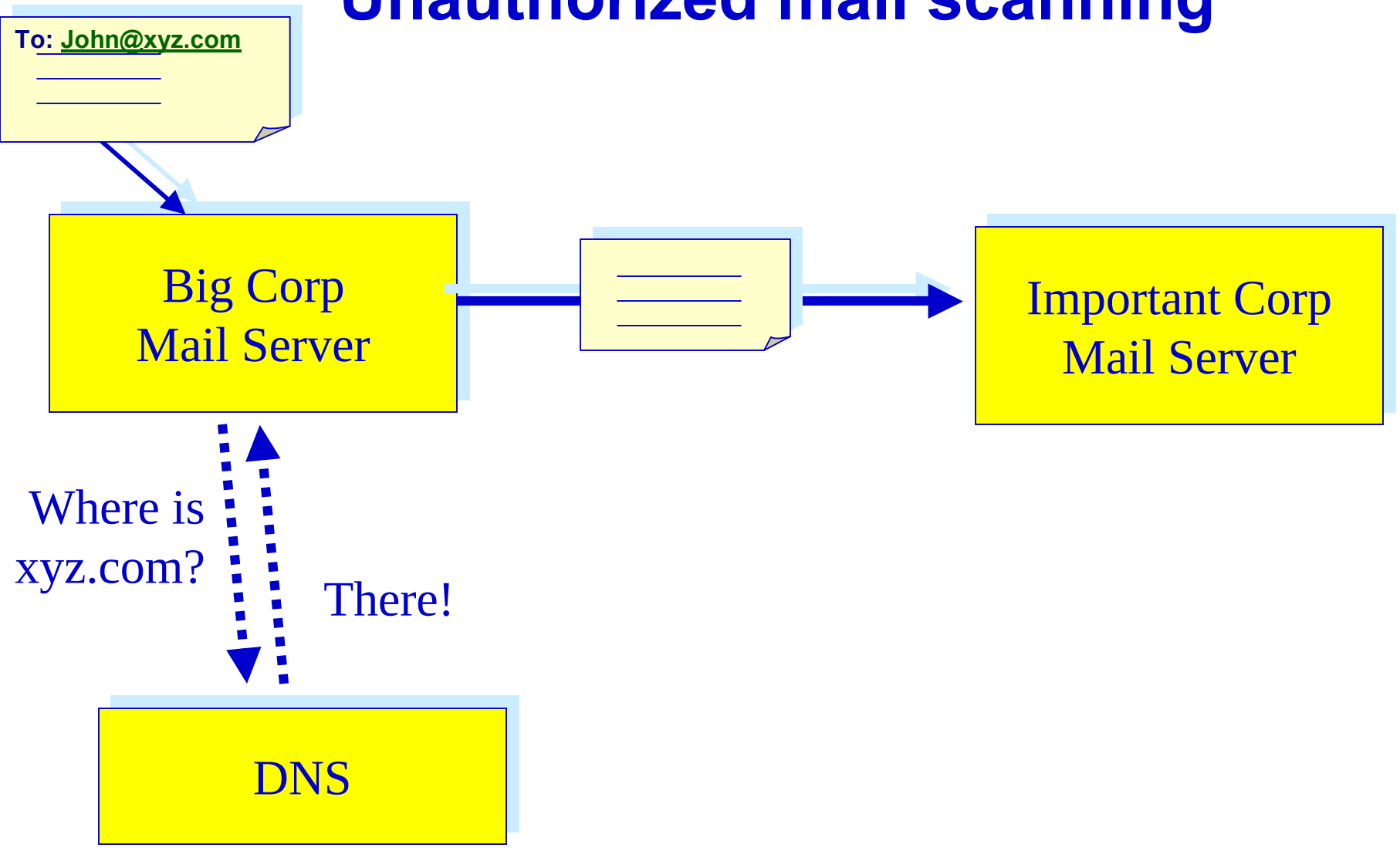
- Introduction
- DISI
- DNSSEC
- Certification of Internet Resources
- Conclusions

Background

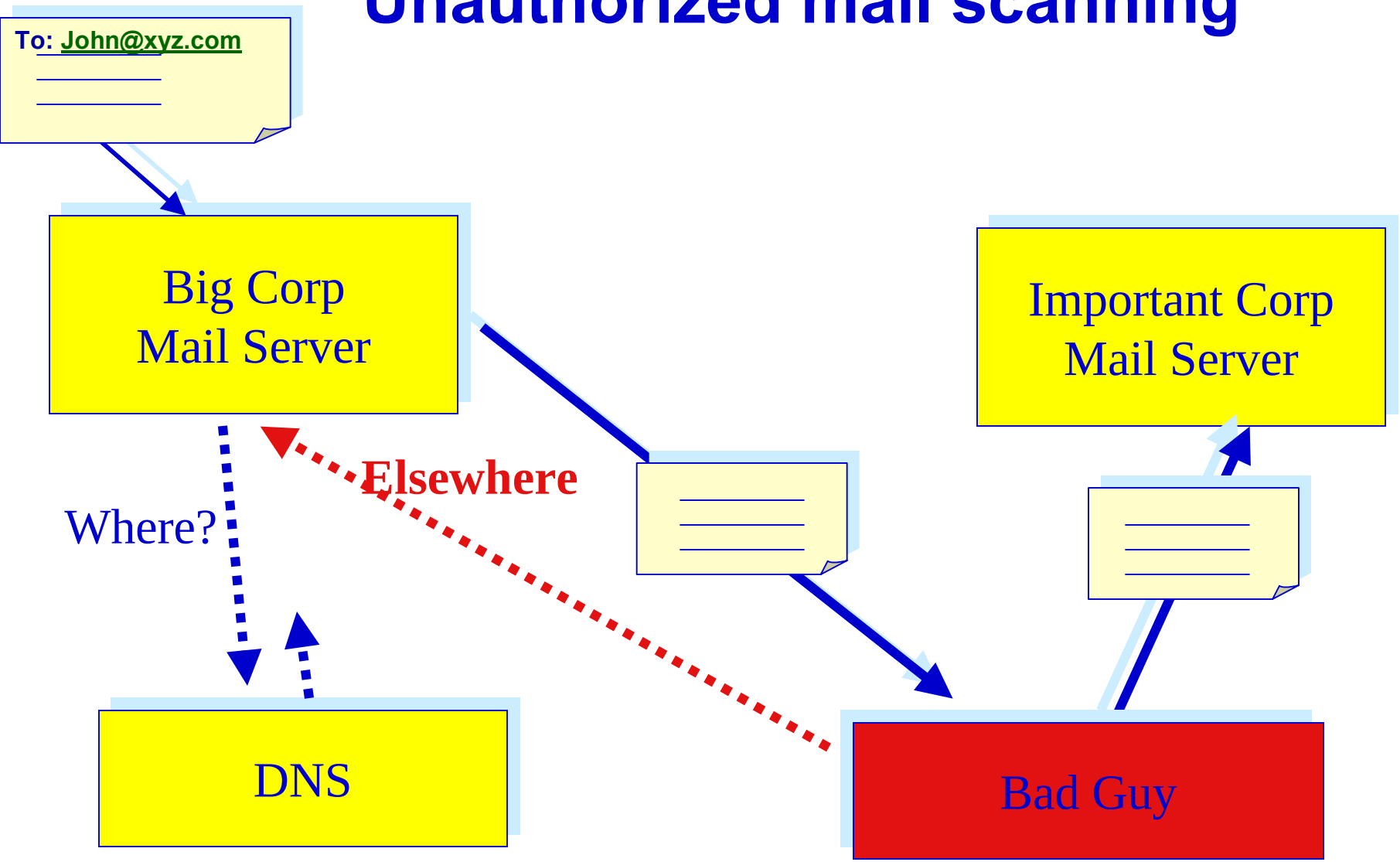
- Computers are good with numbers, people are good with names
  - 4132@194.109.6.51 or henk@uijterwaal.nl ?
- DNS provides a mapping from names to addresses
- Reverse DNS for the other way around
- Distributed database maintained by registries
- People rely on this data

- What if DNS data is modified by an unauthorized party between registry and user?

Example: Unauthorized mail scanning



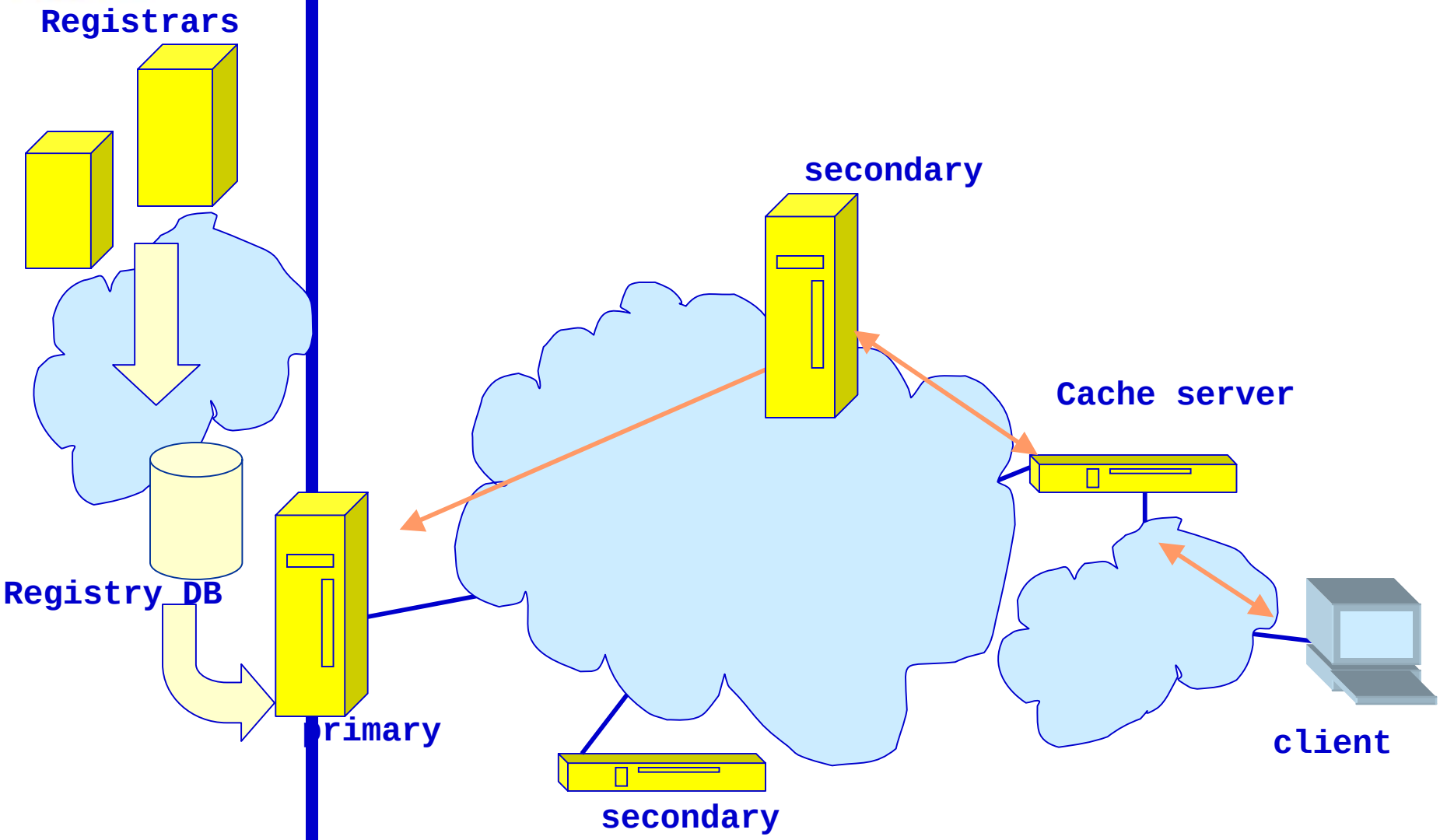
Example: Unauthorized mail scanning



Why is this an issue

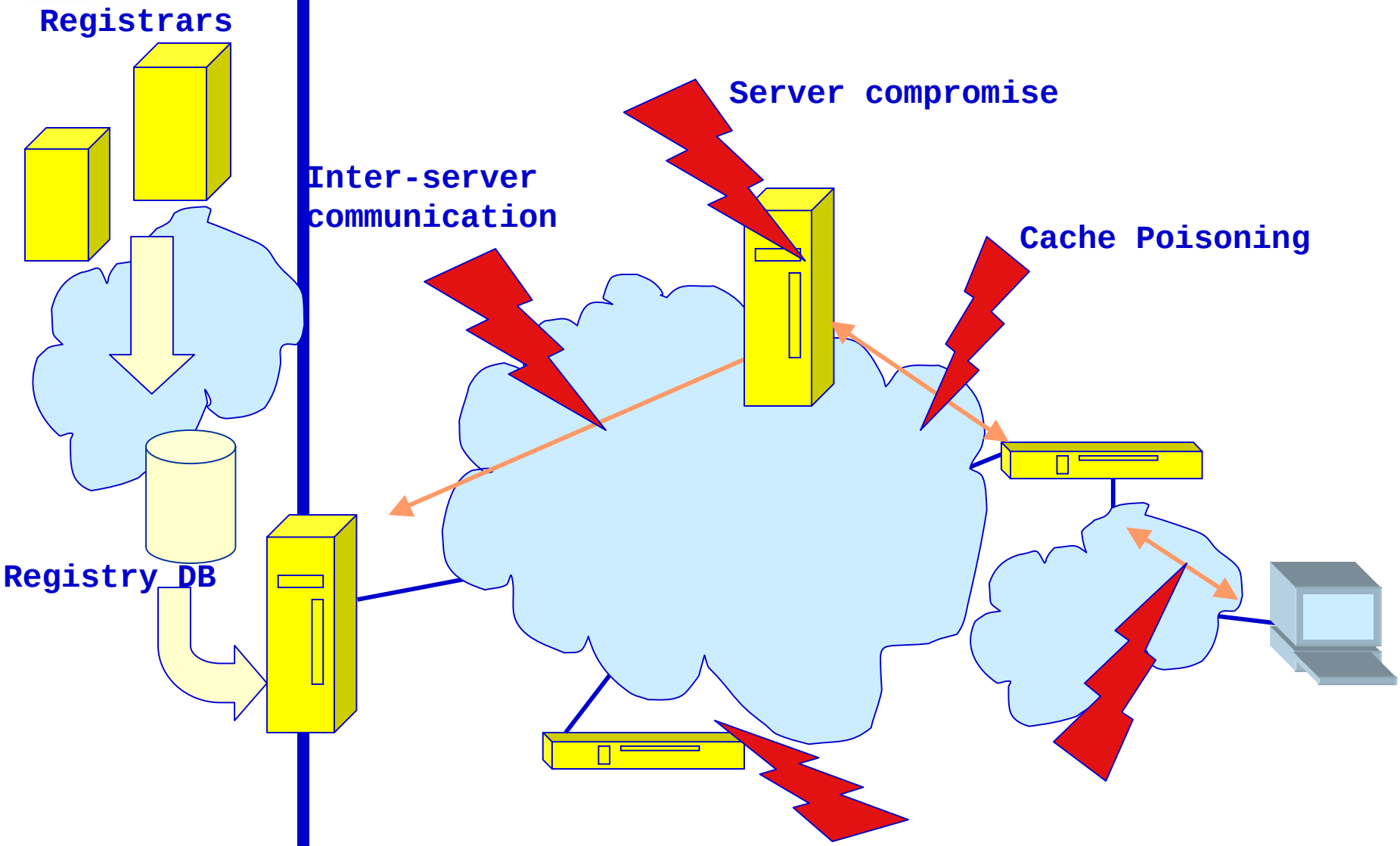
- Snooping on email or other data
- Phishing
- Fake data sources (stock tickers)
- Enum: redirect a call to your competitor to you
- …

DNS Architecture



Provisioning DNS Protocol

Possible Attacks.



Provisioning

DNS Protocol

The solution: DNSSEC

- DNSSEC authenticates data exchanged in the DNS system
  - Source of the data is who you think it is
- DNSSEC provides integrity verification
  - Data has not been modified since it was released
- Uses cryptographic signatures
- Hierarchical (. → .nl → uijterwaal.nl)

- It does not provide authorization
- It does not provide confidentiality

Metaphor

- Compare DNSSEC to a sealed transparent envelope.
- The seal is applied by whoever closes the envelope
- Anybody can read the message
- The seal is applied to the envelope, not to the message

Development and deployment

- 2000: “Let’s deploy this”
  - Reverse DNS tree maintained by the RIPE NCC
  - Our zones (ripe.net, ripencc.net, …)
  - Collaborate with ccTLDs for forward zones
- … well, the technology is not yet ready…
- RIPE NCC participated in the development of the technology and standards
- Roll-out started in 2005
  - All zones signed by 31/1/2006
  - You can use it

Outline

- Introduction
- DISI
- DNSSEC
- Certification of Internet Resources
- Conclusions

Certification

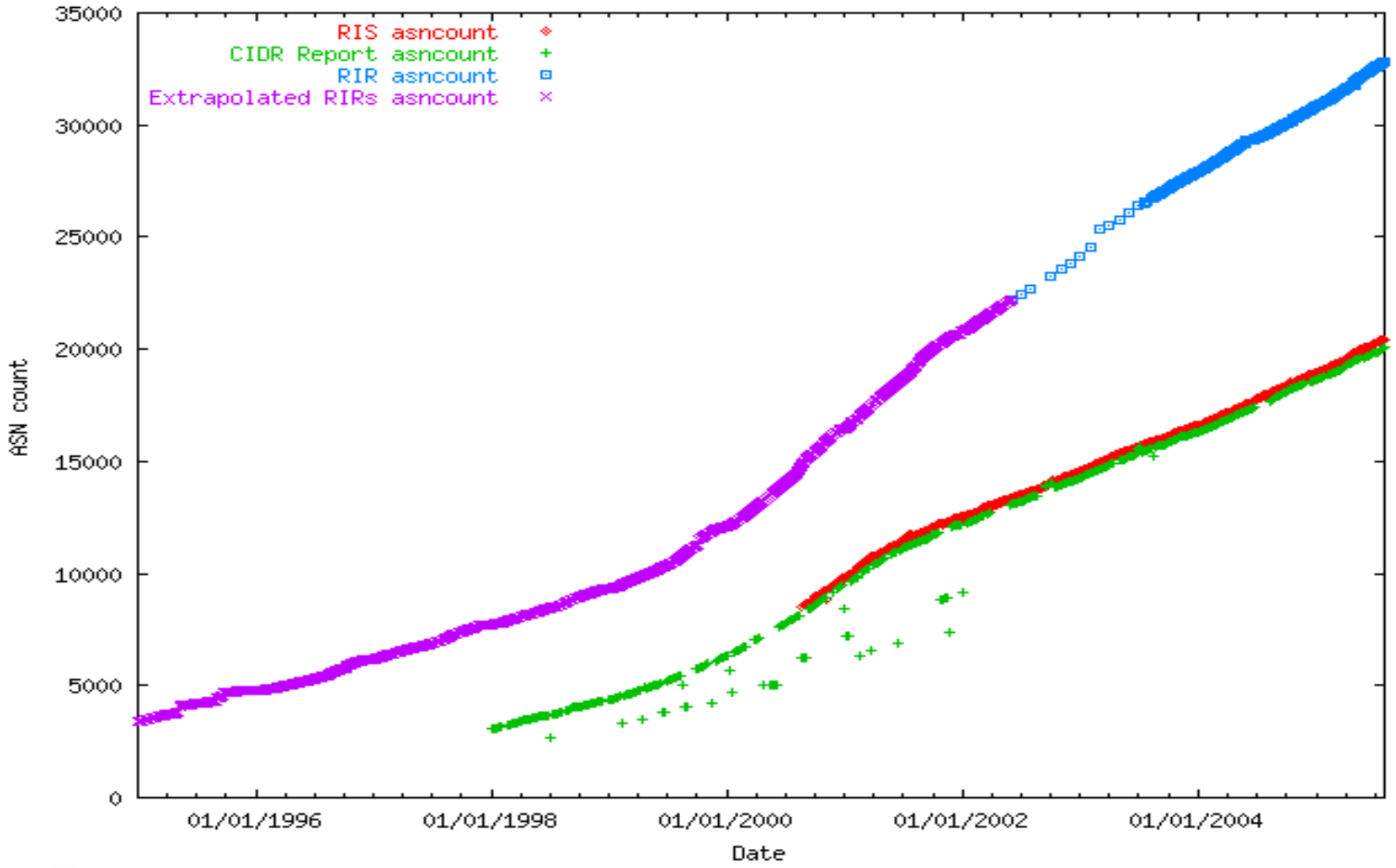
- Why is this an issue?
- Two problems
  - Resources handed out
  - Address and Routing security
- Certification can solve both

Resources handed out

- Internet resources (IP, AS) are limited resources
- Allocation is based on “demonstrated need”
- RIR policies all say that a resource must be returned if it is no longer needed
- This does not happen in practice

Total Number of ASN seen

Assigned (■,■) Actual (■,■)

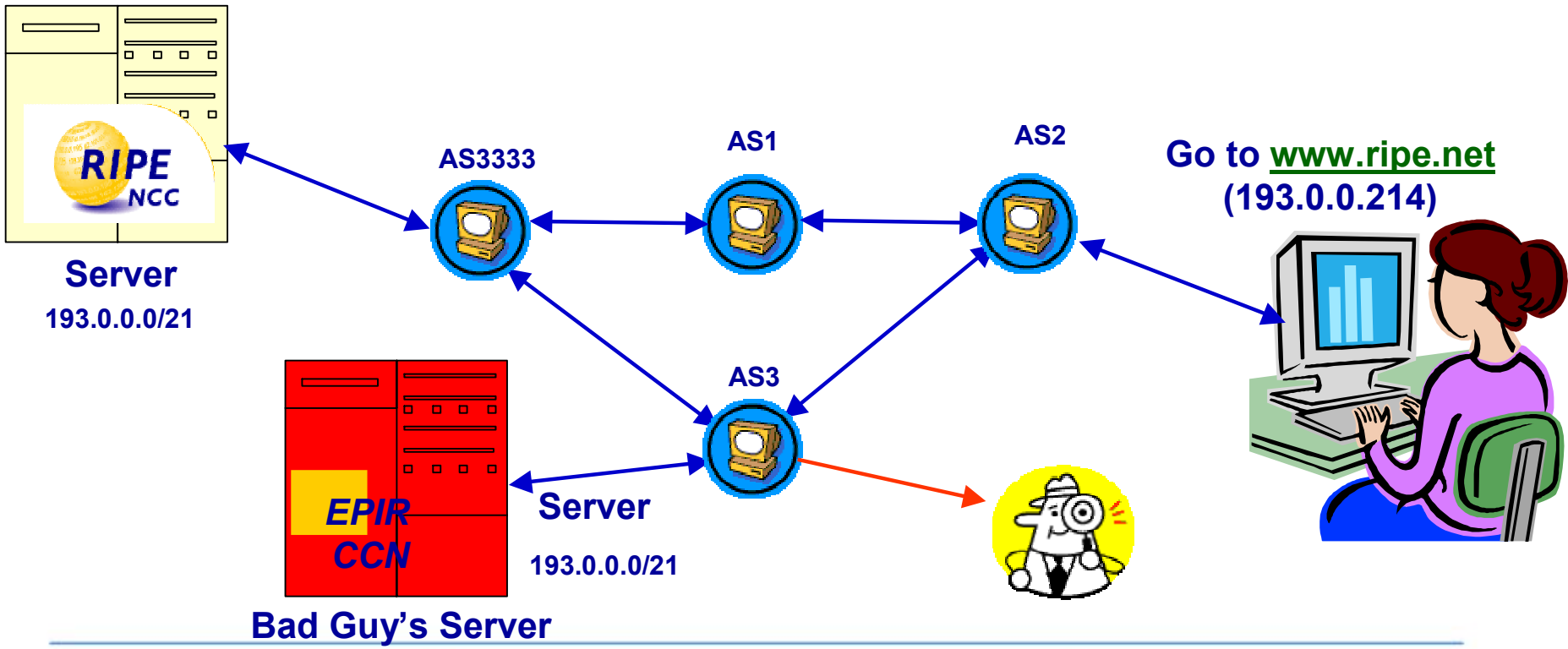


Resources handed out

- Little or no incentives to return resources
  - More and more unused resources over time
  - Recycling would reduce consumption
- Uniqueness extremely important
  - One never knows if a site will reuse an address
  - This makes it hard to recycle blocks
- Certificates are the solution

Address and Routing Security

- Is this a valid address?
- Who injected this into the network?
- Is the forwarding path acceptable?



Certificates

- An document issued by a well-known authority that says that the holder is allowed to use a resource
- In this case:
  - Computer file (X.509)
  - Contains data about the addresses
    - Range (IP, AS)
    - To whom they have been issued
    - Validity dates (“good through …”)
    - …
  - Digitally signed and protected based on a PKI
    - Public Key Infrastructure

Public Key Technology

- A technique to sign and encrypt messages
- Uses some really weird mathematics
- Two keys:
  - One to encrypt messages (“Secret” or “Private”)
  - One to decrypt messages (“Public”)
  - Cannot guess one from the other

Public Key Technology

- "Hello, I am Henk"
- 25b2d2325bab59804fb8083e
- "Hello, I am Henk"

- Original message
- Encrypted with private key
- Decrypted with public key

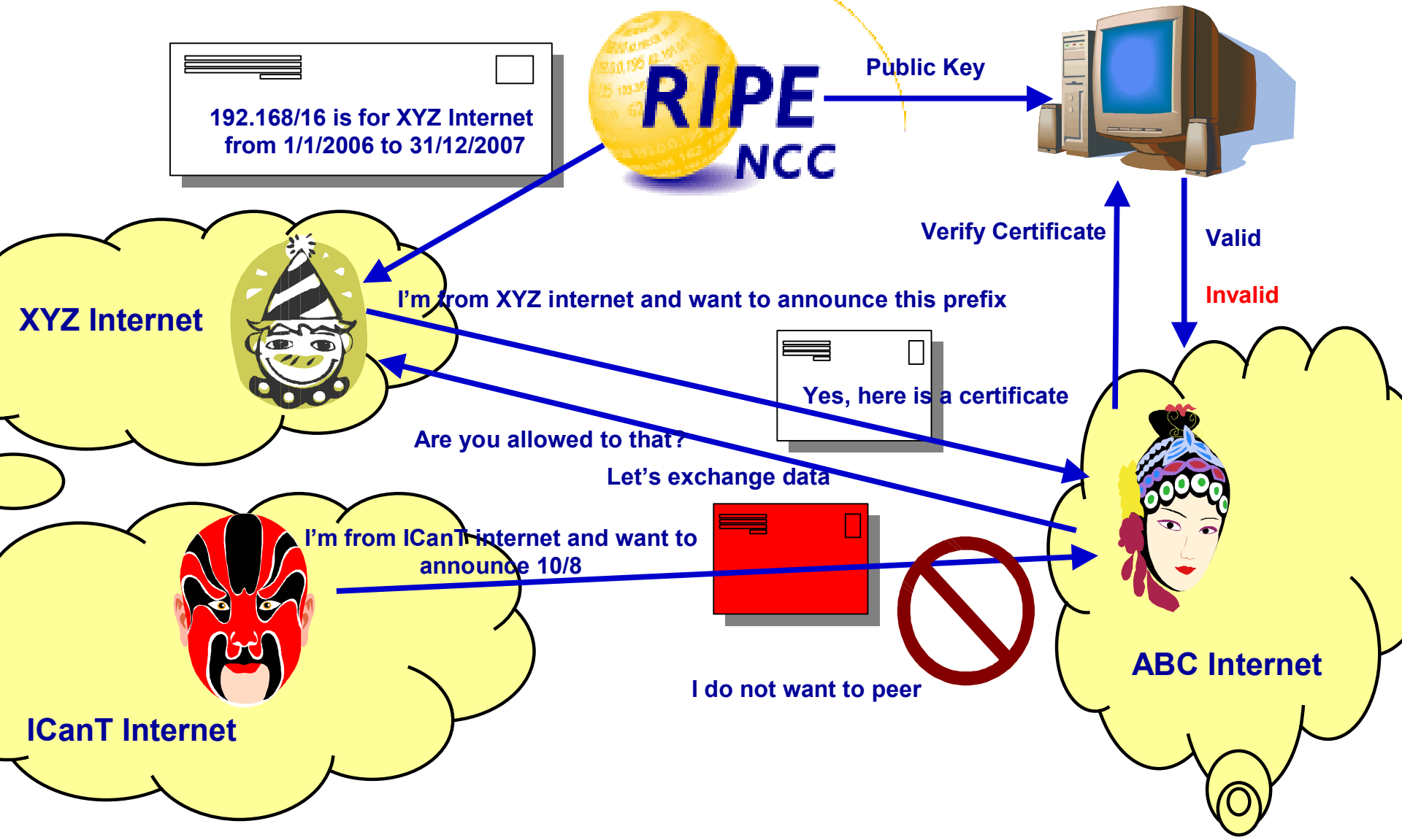
- 25b2d2325bab59804fb8083f
- Invalid message

- Modify the message…
- Can't decrypt

- "Hello, I am Hank"
- 2347dc609af964c9e28086ce

- Guess message
- You can't

Putting it all together



State of the technology

- Certification is mature and standard technology
- Combining this with routing is **not**
  - Needs protocol changes
- Various proposals under discussion in the IETF:
  - sBGP, soBGP, psBGP, …
  - It will be a while before one is selected
  - Then has to be implemented
- Discussion going on elsewhere as well
  - RIPE42 (2002)
  - US DHS workshops (2005)

State of the technology

- However: all technologies require certification
- Set this up now
- Activities:
  - APNIC trial (2005)
  - Preliminary study @ RIPE NCC
- Requires inter-RIR coordination
  - Cross certification
  - Consistent user interface
  - Workshop March 2006
- RIPE NCC proposal expected April 2006

Outline

- Introduction
- DISI
- DNSSEC
- Certification of Internet Resources
- Conclusions

Conclusions

- DISI: Umbrella for the RIPE NCC to work on security related items
- DNSSEC: Secures the DNS, can be used today
- Certification of Internet Resources: the next big step

Questions?