Internet Security
An “Edgy” Business

Jaap Akkerhuis, NLnetLabs

Daniel Karrenberg, RIPE NCC

Overview

- Internet Architecture
- Challenges
- Security Tactics
- Security Policies !!!??!!

Internet Architecture

- Internet: network of networks
  - – Little intelligence inside the networks
    - DNS (naming) is just an application !
  - – Application live at the edges
  - – Intelligence at the edges
  - – See also: RFC1958

Network Edges

- Towards the End-Systems
  - Applications live here
  - Services live here

- Between Networks
  - Routing lives here

Challenges

- Network Infrastructure
  - Little intelligence
    - Little potential for exploitation and abuse
  - Key business assets
    - Lots of motivation for security
  - Clear Responsibility
  - Thus: Not a major problem

Challenges

- End-Systems (“Hosts”, PCs, Servers)
  - Intelligence here: Versatile tools for abuse
  - Poorly defended: Many not designed for net
  - Increasing bandwidth: Effective weapon
  - Attacking others: Little incentive for security
  - Responsibility widely distributed
  - Botnets: Many end-systems make awesome weapons

Securing the Internet

- Cannot be done centrally
- Attention to the edges
- Applications need to be fixed
  - Servers (mail, web etc).
  - End user machines (can be turned into servers)

Secure Application edges

- Servers need to be fixed:
  - Separation of functions
    - front and back offices
  - KISS: Keep it simple
  - Switch off unnecessary services
  - etc, ...

Secure Network Edges

- Two way packet filtering (BCP 38)
  - No incentive nor costs recovery
- Guidelines development
- User quarantine at startup
  - Defense against application edges
    - Done at US university semester start

Secure Application edges

- End user machines:
  - Not designed with networks in mind
  - Can be turned into servers: Bot Nets
    - DDOS sources
    - Spam sources
  - Hold owners responsible?
  - Hold suppliers responsible?

Security Policy

- There is no silver bullet
  - Not just a technical measure
- Follow the money
  - Some spam reduction seen after court cases
    - (anecdotal evidence)
  - Perpetrators hide in non-prosecuting jurisdictions

International Distributed Nets

- The internet
  - The separate nets which makes it
- National policies won’t work well
  - Classical national telecom networks

    are disappearing

    ITU model as well?

Policy Challenge

Define effective security policies

- distributed
- “edgy”
- including end-systems

Do not limit development of the Internet by centralistic and constraining policies.