Securing the Internet
Threats, Trends and Tussles

Dr. Roger P. Karrer

Senior Research Scientist

Deutsche Telekom Laboratories

TU Berlin

Berlin, Germany

Security threats

- Bots by numbers
  - … the botnet owners in the Netherlands operated a network of over 1.5 million computers. In California, a 20-year-old botnet owner was arrested who controlled a network with approximately 400,000 computers.
- Fighting is far from easy
  - An Israeli antispam company said Thursday that a junk e-mailer's vendetta is behind attacks this week that took down its site, five hosting providers and one of the internet's largest blog networks.
- Economic threat
  - The costs for the online transaction service Protx (UK), for instance, which had to fight off several DDoS attacks, amounted to about US$ 500,000.
  - A study shows that the economic losses of a one-week Internet blackout in Switzerland, with a Gross Domestic Product of 482 billion Swiss francs, would amount to 5.83 billion francs = 1.2%
- Law changes
  - A new law has been introduced in the UK which will put you in jail for a maximum of 10 years if you launch a DDoS attack. UK's Britain's Computer Misuse Act which was written well before the days of the WWW contained flaws that could possibly let DDoS attackers fall through holes in the law.

☞ Exploiting security vulnerability is a business today

☞ Challenge: how to secure the Internet?

Security: whys

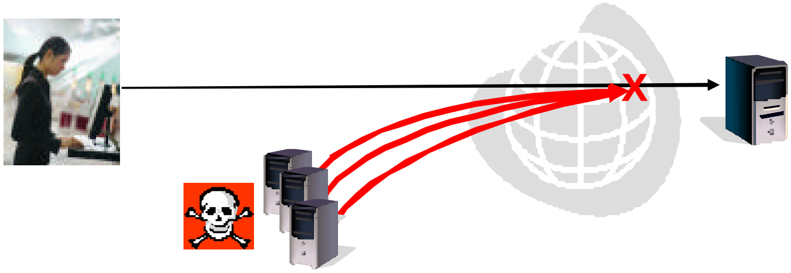
- Why is security a problem?
  - Anybody can inject any traffic at any rate at any time from any source to any destination
  - Internet principle: freedom
  - Responsible for the success of today’s Internet
- Why is it difficult to solve?
  - Remove some “anys” – but which ones, and how?
    - “Anybody” via authentication
      - Threat to privacy
      - Annoying
    - “Any destination” via ingress filtering or authentication
      - Deployability
      - User annoyance?
    - “Any rate” with cost (pay-per-mail)
      - Unpopular
      - Unfair to low income

Outline

- Motivation
- Edge-based capabilities
  - Authentication-based solution against DDoS flooding attacks
  - Concept
  - Incentives
- Trends in DDoS attacks
  - Towards a perfect DDoS attack
  - Implications
- Architectural considerations
  - Design for Tussles
  - Virtualization

Flooding Attacks in the Network

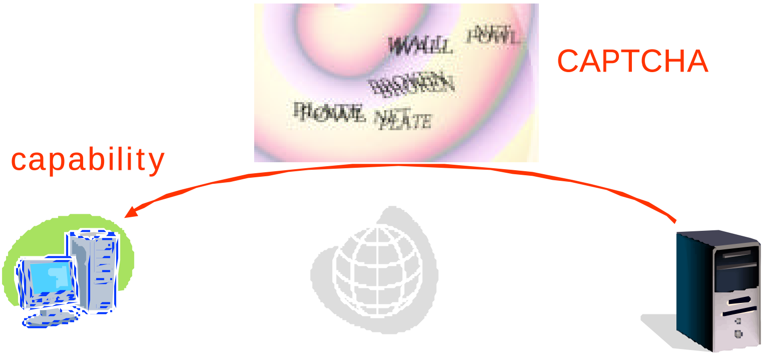
- Anybody can send data … in the Internet
  - Assumption: end systems can be trusted
  - Assumption: the “network” is dumb
  - Philosophy: the Internet shall be open
  - Wrong today!
- Implication: flooding attacks on the network



Challenges

- Defense against flooding attacks is difficult:
  - What is unsolicited traffic?
  - Who and how can identify unsolicited traffic?
  - How can it be addressed?
- Paradox situation
  - End system
    - Can define, maybe indentify it
    - But not defend
  - Network
    - Can defend
    - But can not define and identify
- Solution: Edge-based capabilities (EC)
  - Joint work with Dr. Ulrich Kühn, now Sirrix AG Security Technologies

EC Concept (1/2): Capabilities

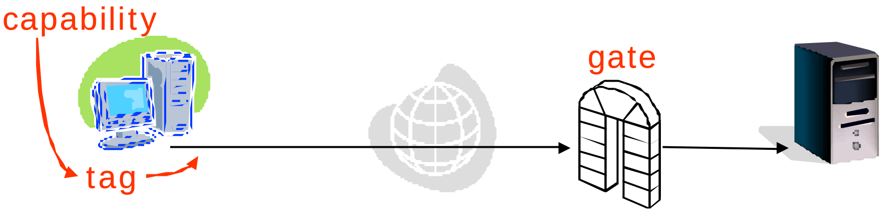


- Capability := permission to send
  - Granted by the receiver or an “authentication authority”
  - Examples:
    - CAPTCHA: to distinguish bots from human users
    - RFID if the server is known to a server
    - VoIP: registered phone number at the receiver

Question

- What does a sender do with a capability?
  - Not sufficient that the sender and the receiver know
  - We need to protect the network …
- Who ensures that only legitimate packets are in the Internet?
  - And how?
  - Protection must be before the end system

EC Concept (2/2): Edge-based



capability

tag

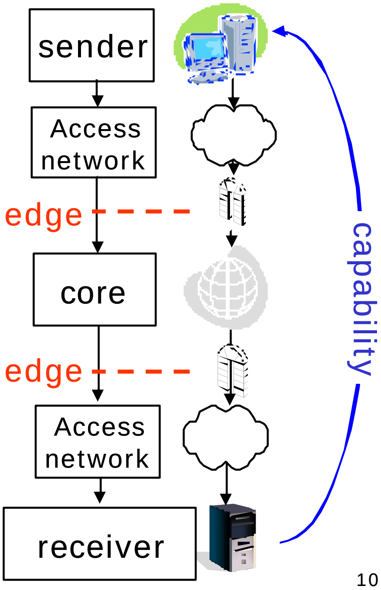
gate

- Capability allows the sender to calculate cryptographic tags
    - Included in every IP packet
- Gate controls traffic based on tags
    - Packets with tags: high priority
    - Packets without tags / wrong tags: low priority
- Gate at the edge: for performance reason

Edge + capabilities = EC

Sender-side edge: protection against malware spread

Receiver-side edge: protection against flooding



sender

Access network

edge

core

edge

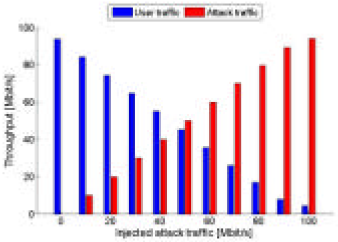
Access network

receiver

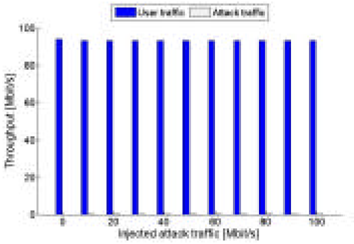
capability

Testbed results

- Local testbed
  - 4 PCs: gate, server, zombie, legitimate
  - 100 Mbps link
  - Inject traffic at predefined rate
  - Measure traffic at the server
- Results
  - Without EC
    - User traffic degrades as a function of injected attack traffic
  - With EC
    - Only legitimate traffic passes
    - Attack traffic is filtered out



Without EC



With EC

Summary of EC

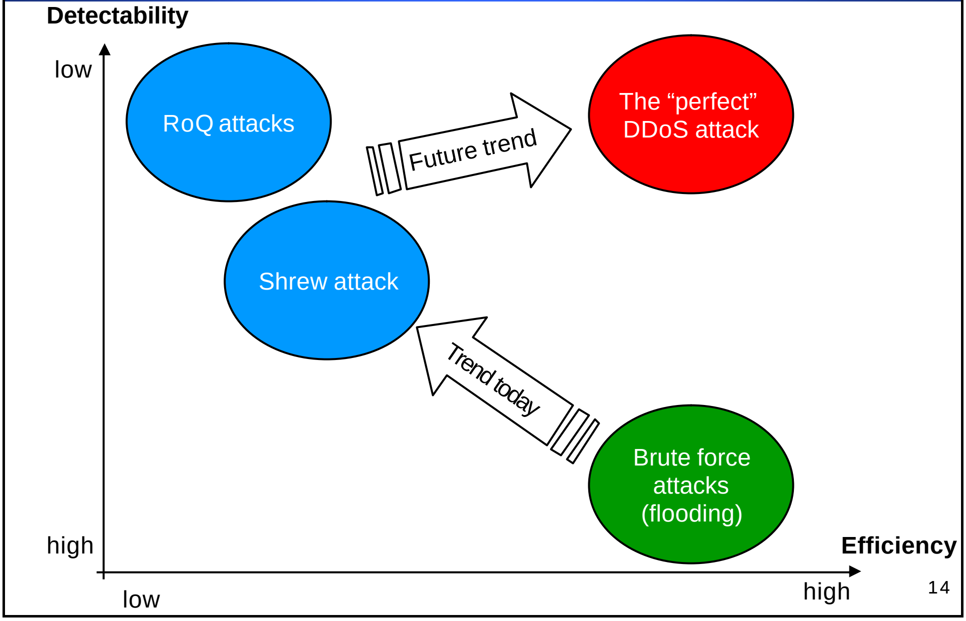
- Solution to identify and mitigate DDoS attacks
  - Combines end systems and the network
  - Presented: one solution, but in fact a framework
    - CAPTCHAs are just *one* example
  - Easily deployable
- Incentives to deploy and use EC
  - ISP
    - Provide protection service to a server
    - Protect its access network
  - Servers
    - Get protection against flooding attacks
  - Client
    - Challenge provides higher priority at the gate

☞ Deployability and incentives are key advantages

Outline

- Motivation
- Edge-based capabilities
  - Authentication-based solution
  - Concept
  - Incentives
- Trends in DDoS attacks
  - Towards a perfect DDoS attack
  - Implications
- Architectural considerations
  - Design for Tussles
  - Virtualization

Trends in DDoS attacks



Current sophisticated attacks

- Shrew attack: a low-rate DDoS attack
  - Send high-rate UDP bursts
  - Long breaks with no attack
  - Exploits features of TCP
- RoQ attack: Reduction of Quality
  - Trades off attack rate and impact
    - Only RoQ, not full DoS
    - Low detection probability
- Current sophisticated attacks are
  - Still detectable: high bursts, periodic bursts
  - Not 100% effective

☞ Can we do any better?

Towards the “perfect” attack

- Perfect attack:
  - 100% impact on legitimate traffic
  - 0% detectability
  - ☞ Understand the limitations of detection systems and botnets
- Concepts
  - Coordination
    - Create unsuspicious pattern: various bots, all low rate
    - Achieve attack traffic at the target
    - Botnets allow distributed attack at low rate
  - Use network feedback
    - For coordination
    - Shooting ourselves in the foot…
  - Use primarily TCP traffic
    - UDP only to fill gaps

☞ Any detection mechanism based on flow observation is useless

Outline

- Motivation
- Edge-based capabilities
  - Authentication-based solution
  - Concept
  - Incentives
- Trends in DDoS attacks
  - Towards a perfect DDoS attack
  - Implications
- Architectural considerations
  - Design for Tussles
  - Virtualization

Architectural considerations

- Security issues must be addressed
  - Internet is vital for everyday life, business
  - But: no free lunch!
- Options
  - Find the right solution
    - Preserve freedom and Internet architecture
    - Wishful thinking
  - Compromise freedom
    - Authentication, capabilities, payments
    - People are not ready
  - Find an alternative way to build architectures (clean slate)
    - Build for tussle
  - Virtualization (clean slate)
    - Multiple Internets

Design for tussle

- Internet architecture is ossified
  - Unflexible
  - Need a flexible architecture
- Flexibility
  - Modularization and customization
  - Security “plugins”
  - Defined by
    - End systems and networks
    - Users and the providers
- Tussles contain different aspects
  - Technical
  - Business
  - Social

Virtualization

- Virtualization of networks
  - Virtualization of end systems known
    - One PC
    - Multiple OSes run on top, in parallel
  - Extend to networks
    - One physical infrastructure
    - Multiple Internet architectures
    - ☞ Away from the one-size-fits-all
  - Example
    - One Internet that is very secure, but tedious to use
    - One “best-effort” Internet like today
    - etc
  - Implications
    - Users: how to handle multiple architectures?
    - Business: inter-operability?
    - Legal issues: who is allowed to have architectures?

Conclusions

- Researchers are aware of the security problems
  - Solutions are being investigated
    - In the current Internet: capabilities
    - For a future Internet: clean slate design
- Society is not aware of the dimensions
  - Who is willing to pay for security?
  - Who is able to protect his devices?
  - ☞ Awareness is needed!
- Security is a business aspect
  - Affects ISPs: problems and opportunities
  - Users: mostly problems
  - "The dark side": pushes sophistication and threats!