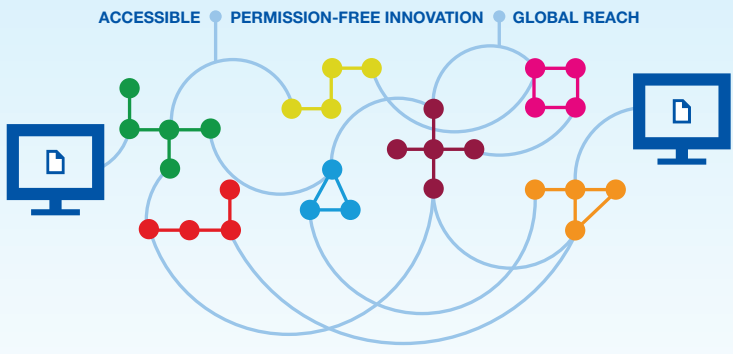
# Collaboration for a **Secure and Resilient** Internet

Internet Society

Learn more at
www.internetsociety.org/security

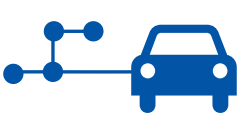
**The Internet is open, interconnected and interdependent**
It's an ecosystem based on collaboration and shared responsibility




Each network is responsible not only for its own security, but also contributes to the overall security of the medium. The challenge is to create a culture of collective responsibility to make the Internet more secure and resilient.

## EXPONENTIAL GROWTH

**The Internet has almost 1 billion hosts**
> 500% growth in ten years



**In 2014, 100 new devices will connect to the Internet each second.** This number is expected to reach 250 devices per second by 2020.

## ATTACKS ON THE RISE

The very same properties of the Internet that underpin its success open up new opportunities for various types of malicious activity.

**Accessible** → open for attacks and intrusion
**Permission-free innovation** → innovative malware
**Global reach** → issues are transborder and spread globally

**300Gbps is the largest attack recorded to date.**
It targeted the anti-spam company spamhaus in 2013.

**55%** increase in average attack sizes in 20 months.

**265%**
Increase in reflection attacks from Q3 '12 to Q3 '13

**28 million**
DNS resolvers pose some kind of security risk

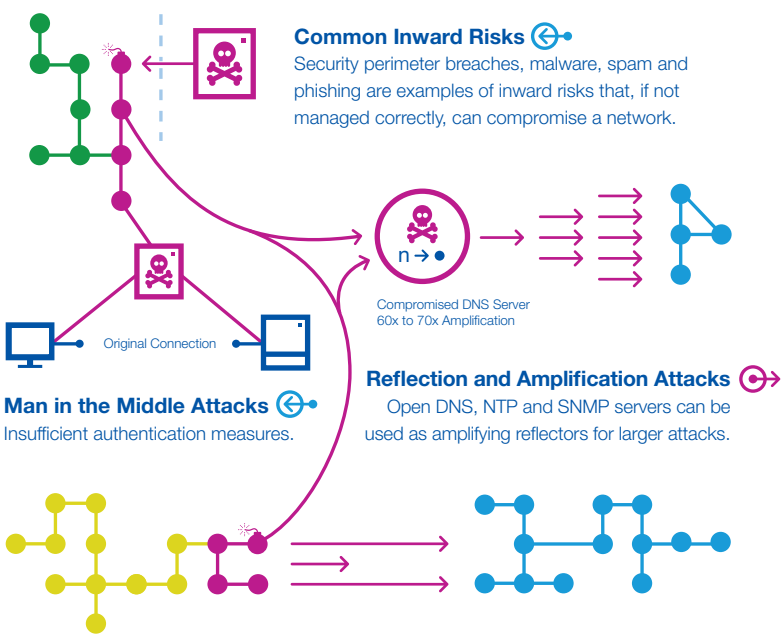
**60 to 70 times**
Potential for amplification attacks

**350% growth**
In large >20Gbps DDoS attacks from 2012 to 2013

**DDoS** An acronym for distributed denial of service attack; the most popular is a reflection-based amplification attack. It leverages unprotected servers on the Internet to launch an attack.

## INWARD AND OUTWARD RISKS

Risks are not only inward. Compromised networks can be used to launch attacks against other networks and across the Internet.




**Common Inward Risks**
Security perimeter breaches, malware, spam and phishing are examples of inward risks that, if not managed correctly, can compromise a network.

**Man in the Middle Attacks**
Insufficient authentication measures.

**Reflection and Amplification Attacks**
Open DNS, NTP and SNMP servers can be used as amplifying reflectors for larger attacks.

**Routing Hygiene**
Networks that handle routing announcements carelessly can be used for hijacking or re-routing other networks' traffic. Networks without anti-spoofing measures can be used as a launchpad for attacks.

## TECHNOLOGY BUILDING BLOCKS

Key measures that administrators can employ to make their networks and the whole Internet more secure and resilient.

**IPsec** • Internet Protocol Security
**TLS** • Transport Layer Security
**Kerberos** • Network Authentication System
**DNSSEC** • Domain Name System Security Extensions
**DANE** • DNS-based Authentication of Named Entities
**RPKI** • Resource Public Key Infrastructure

## TAKE ACTION

Re-evaluate your network risk profile and assessment.
Support actions focusing on global security and resilience.

- Detect, close or protect open resolvers and other potential amplifiers
- Deploy best practices aimed at improving routing hygiene
- Deploy anti-spoofing measures, preventing traffic with spoofed source IP addresses
- Deploy DNSSEC (validation) to secure name resolution for your customers
- Detect and mitigate infected and compromised devices on your network
- Cooperate with other networks in detection, tracing back and mitigation of attacks

Internet Society

Learn more at
www.internetsociety.org/security

**DATA SOURCES:**
Arbor 8th annual Worldwide Infrastructure Security Report, ICT Facts and Figures 2013, Internet Systems Consortium Domain Survey, Prolexic Q3 2013 Global DDoS attack report.