Security in Future Internet

2012. 5. 21

CS Hong

KHU

Outline

- Introduction to Security
- Security Issues in Current Internet
- Trustworthy Internet and Source Address Validation
- Traceback
- Security in Future Internet

Introduction to Security

Terminology

- Computer Security
  - automated tools and mechanisms to protect data in a computer, even if the computers are connected to a network
    - against hackers (intrusion)
    - against viruses
    - against Denial of Service attacks
- Internet (network) Security
  - measures to prevent, detect, and correct security violations that involve the transmission of information in a network or interconnected network

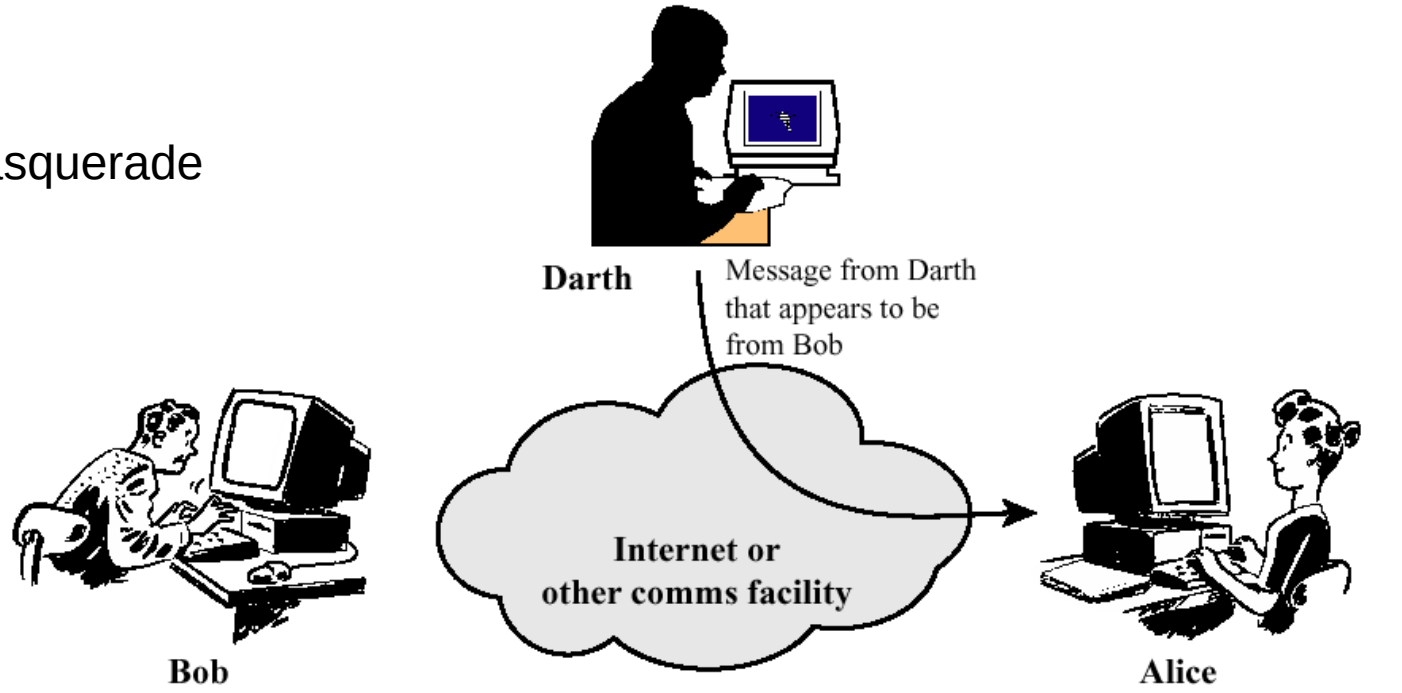
Attacks

- Passive attacks
  - interception of the messages
    - Eavesdropping
  - What can the attacker do?
    - use information internally
    - release the content
    - traffic analysis
  - Hard to detect, try to prevent

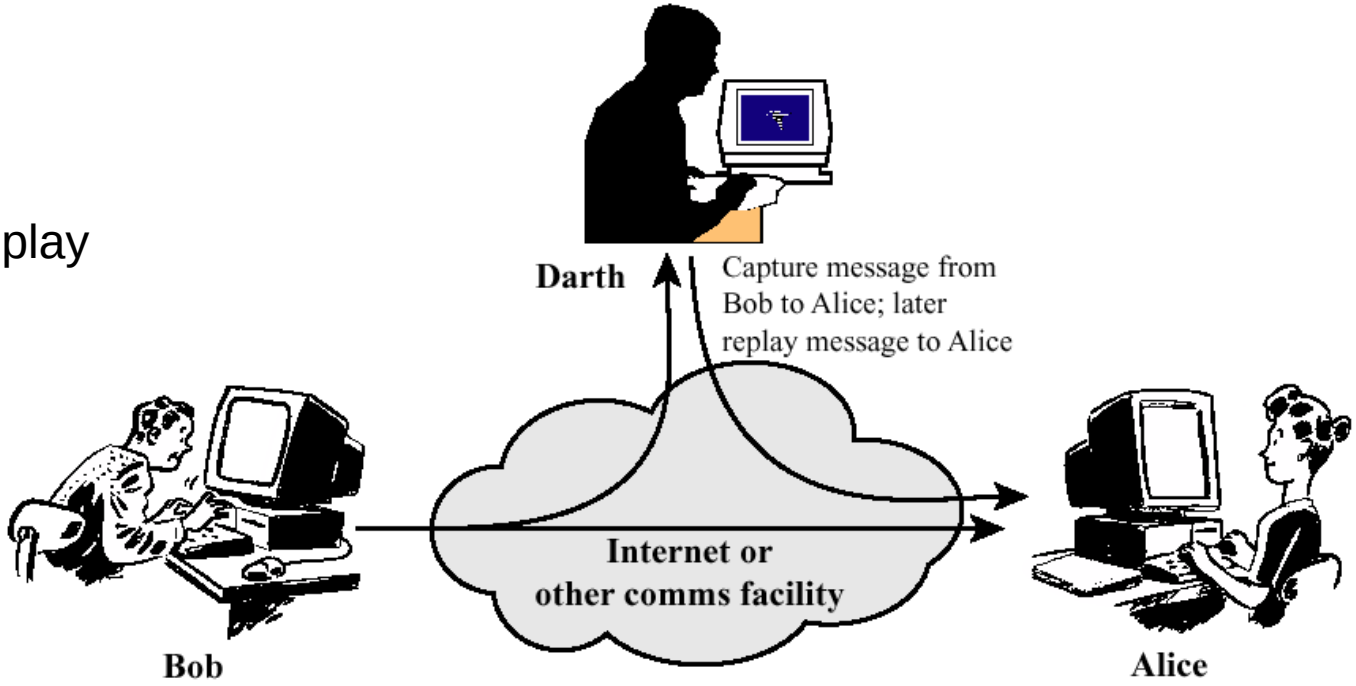
Attacks

- Active attacks
  - Involves interruption, modification and fabrication, etc.
  - Masquerade, impersonating
    - pretend as someone else
    - possible to get more privileges
  - fabrication
    - create a bogus message
  - Replay
    - passively capture data and send later
  - Denial-of-service
    - prevention the normal use of servers, end users, or network itself

Masquerade

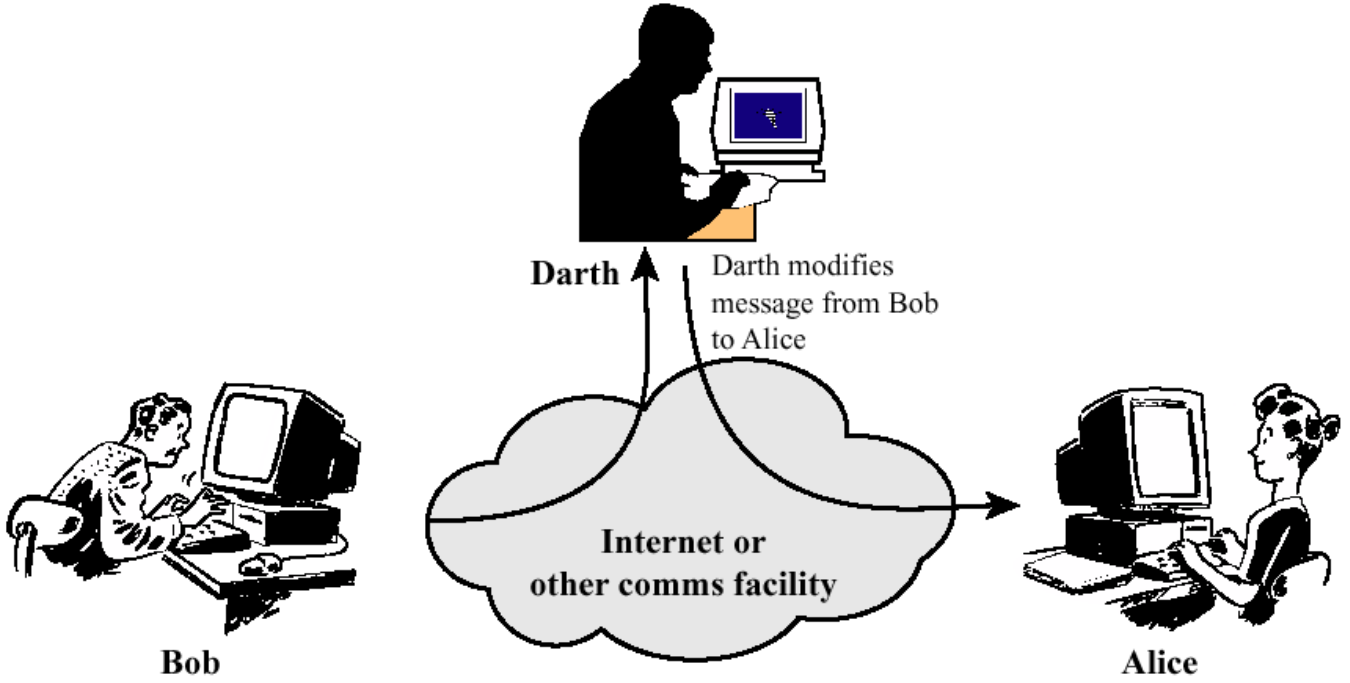


Replay



Attacks

- Active attacks (cont'd)
  - deny
    - repudiate sending/receiving a message later
  - Modification (tampering) <-> intact
    - change the content of a message



Basic Security Services

- Authentication <-> impersonation
  - assurance that the communicating entity is the one it claims to be
  - peer entity authentication
    - mutual confidence in the identities of the parties involved in a connection
  - Data-origin authentication
    - assurance about the source of the received data
- Access Control
  - prevention of the unauthorized use of a resource
- Data Confidentiality
  - protection of data from unauthorized disclosure
  - traffic flow confidentiality is one step ahead

Basic Security Services

- Data Integrity <-> tampering
  - assurance that data received are exactly as sent by an authorized sender
  - I.e. no modification, insertion, deletion, or replay
- Non-Repudiation
  - protection against denial by one of the parties in a communication
  - Origin non-repudiation
    - proof that the message was sent by the specified party
  - Destination non-repudiation
    - proof that the message was received by the specified party

Security Mechanisms

- Basically cryptographic techniques/technologies
  - that serve to security services
  - to prevent/detect/recover attacks
- Encipherment
  - use of mathematical algorithms to transform data into a form that is not readily intelligible
    - keys are involved

Security Mechanisms

- Message Digest
  - similar to encipherment, but one-way (recovery not possible)
  - generally no keys are used
- Digital Signatures and Message Authentication Codes
  - Data appended to, or a cryptographic transformation of, a data unit to prove the source and the integrity of the data
- Authentication Exchange
  - ensure the identity of an entity by exchanging some information

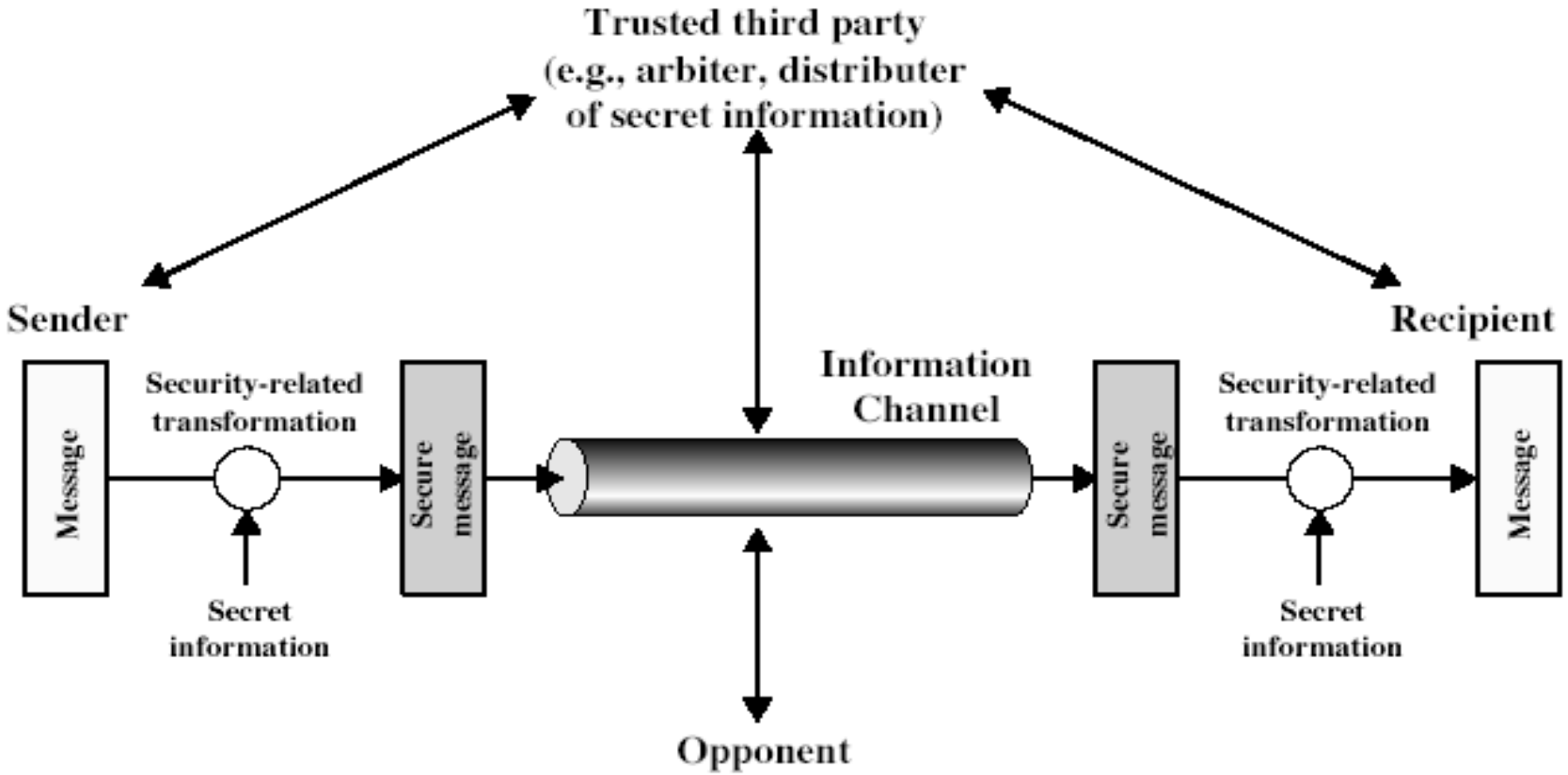
Security Mechanisms

- Notarization
  - use of a trusted third party to assure certain properties of a data exchange
- Timestamping
  - inclusion of correct date and time within messages
- Non-cryptographic mechanisms
  - traffic padding (for traffic analysis)
  - intrusion detection
    - monitor, detect, and respond
  - firewalls

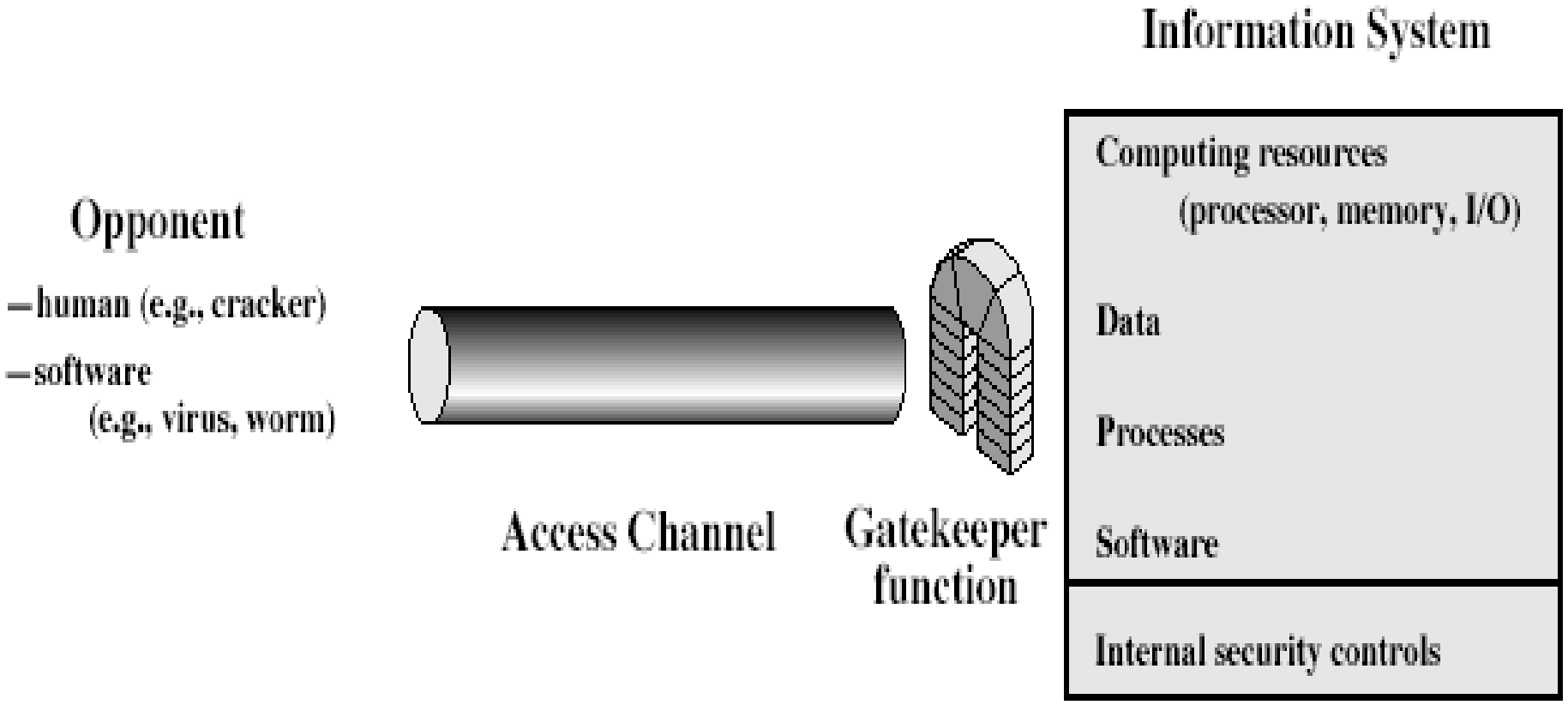
And the Oscar goes to …

- On top of everything, the most fundamental problem in security is
  - SECURE KEY EXCHANGE
    - mostly over an insecure channel
  - Let's brainstorm on this issue!

Model for Network Security



Model for Network Access Security



Aspects of Computer Security

- Mostly related to Operating Systems
- Similar to those discussed for Network Security
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability
  - Dependability

Security Issues in Current Internet

Background

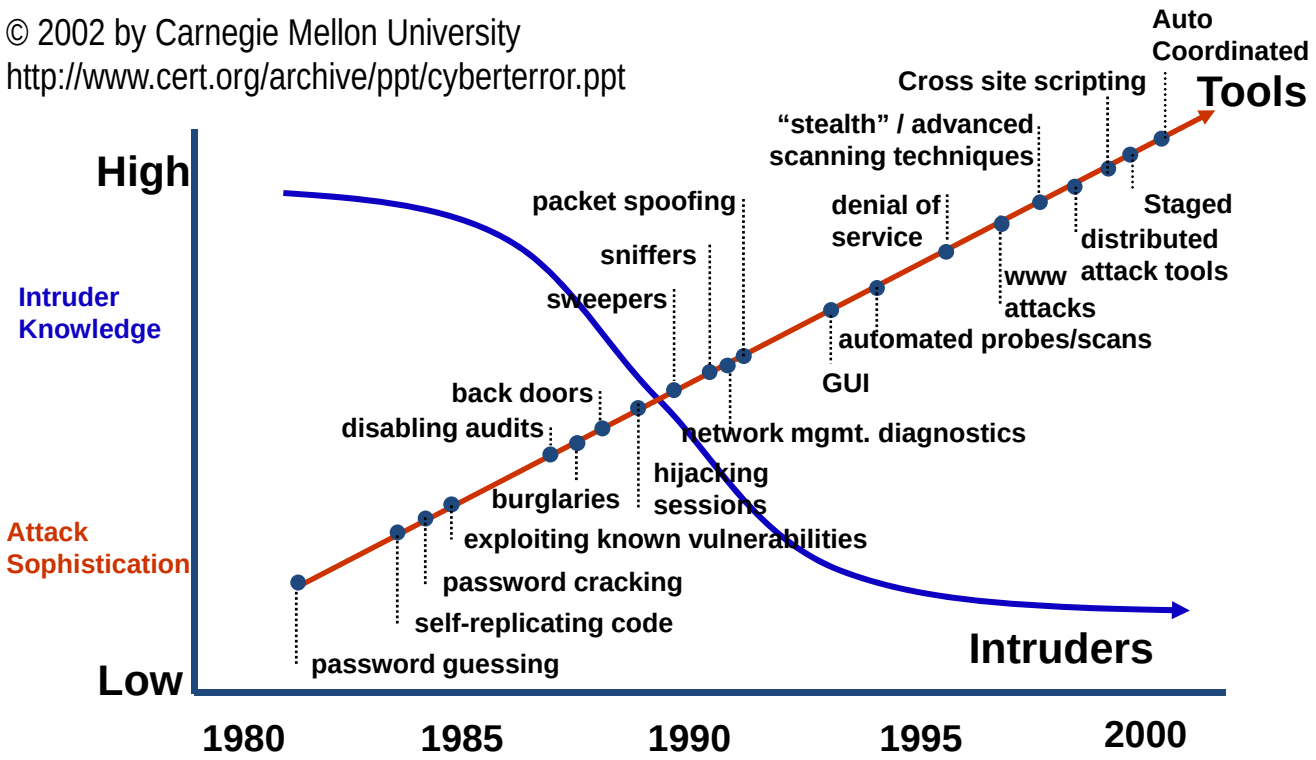
The Internet

- The best thing of the Internet is everyone connects to each other
- The worst thing of the Internet is everyone connects to each other
- When Internet was designed, it was just for a research community, therefore the trust and security was not considered

Internet Security Issues

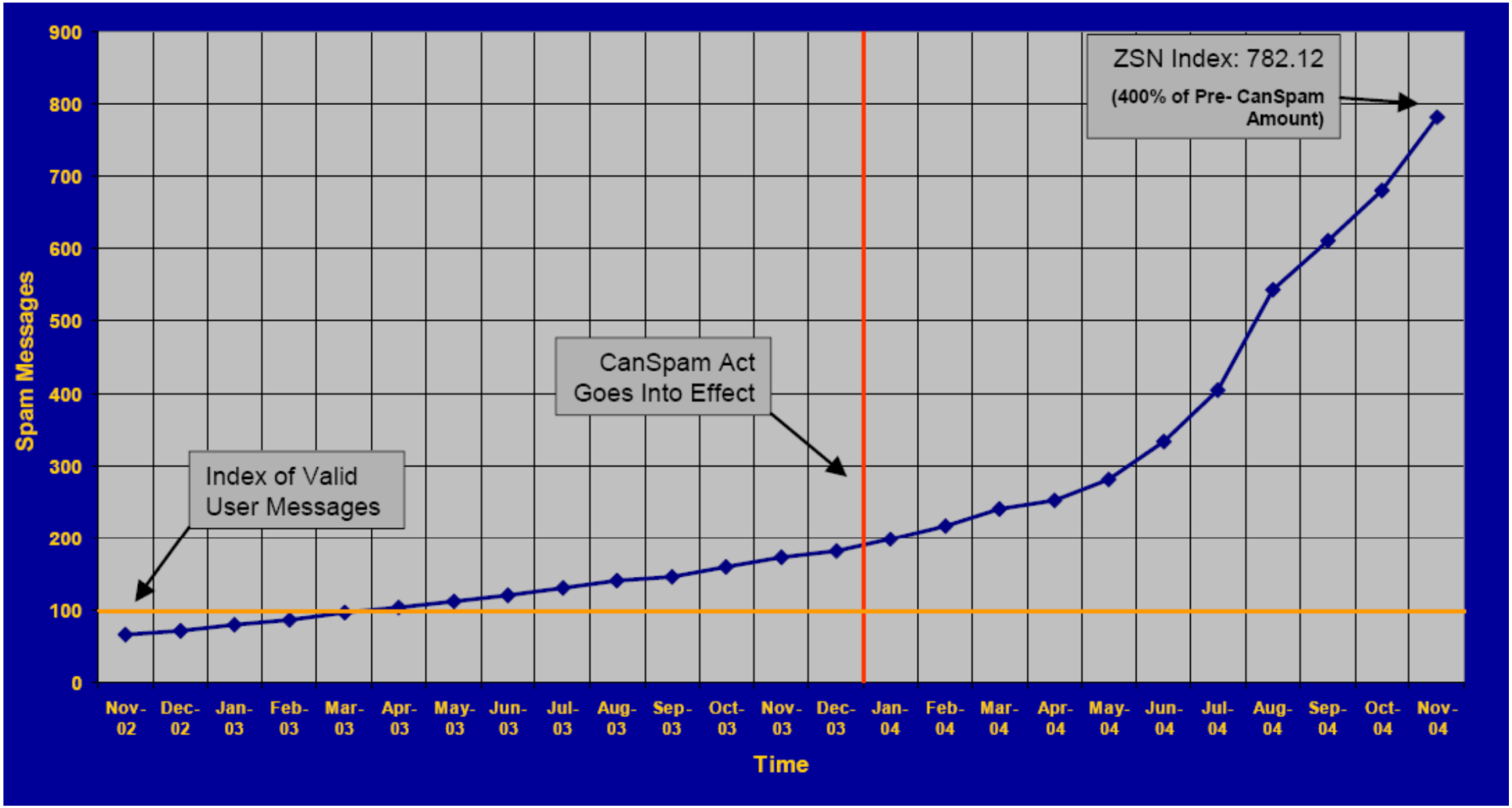
- Internet Worm (1988)
- Sniffing Attack (1994)
- Sequence Number Attack (1995)
- Denial-of-Service Attack (DoS)
- Distributed DoS Attack (DDoS)
- Distributed Reflected DoS attack (DrDoS)
- ……

Trend

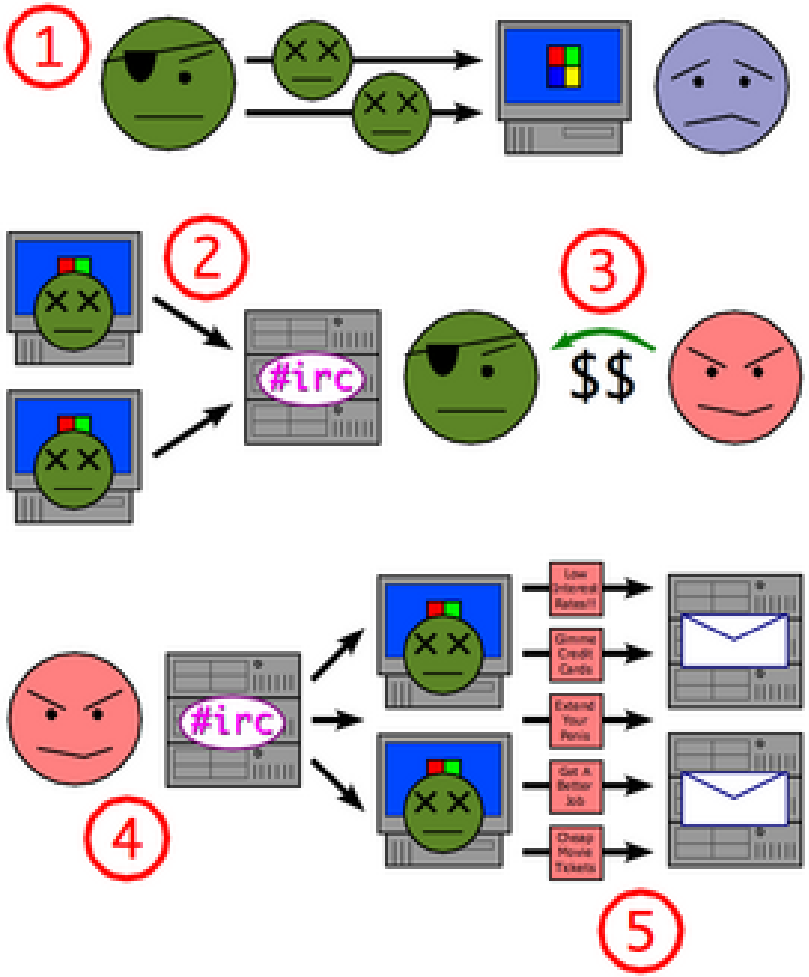


- there are many more vulnerabilities and attacks
- some of these cannot be prevented by technical means, but only with careful procedures and education of people

Spam

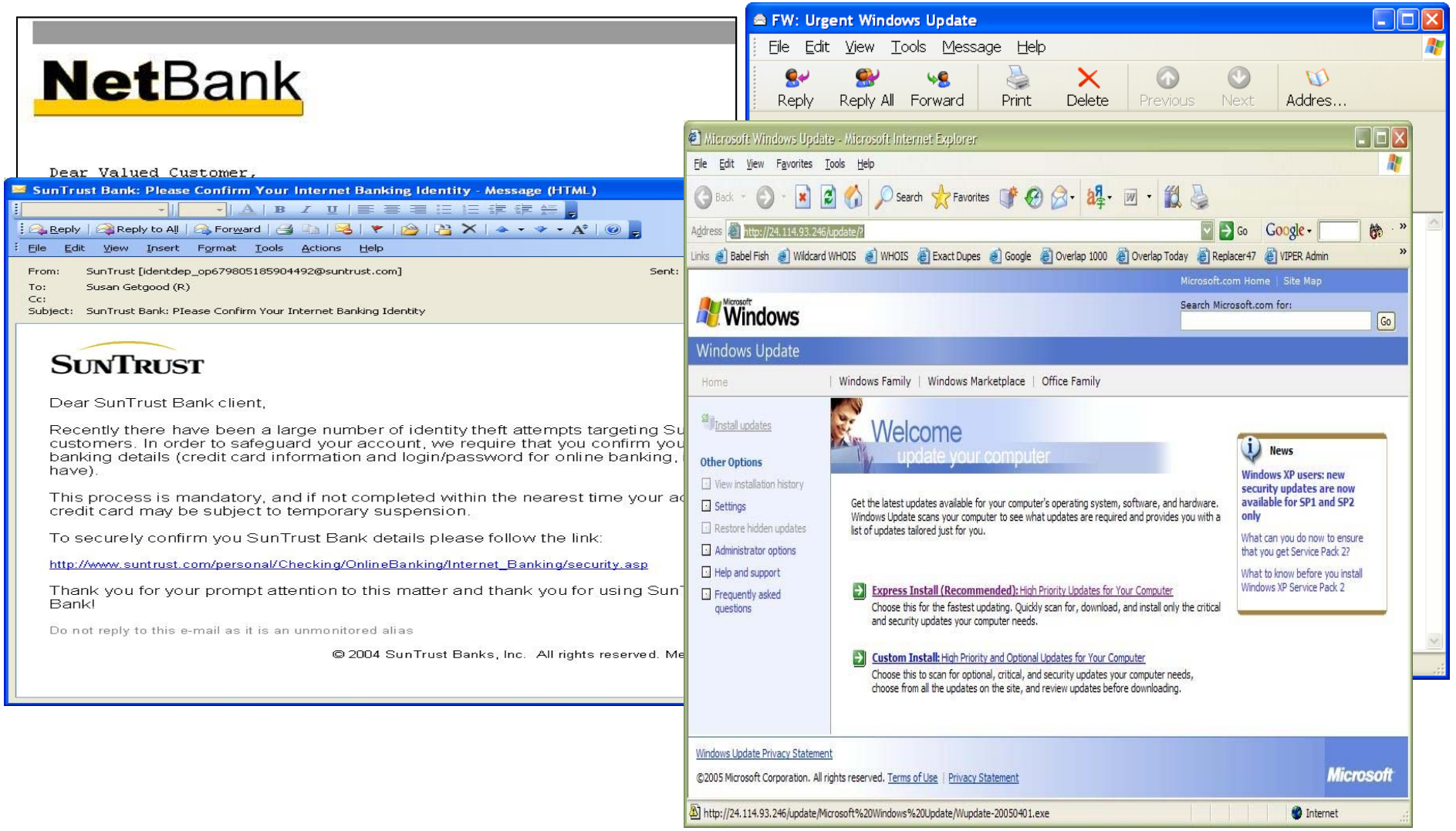

ZSN Index: 782.12
(400% of Pre- CanSpam Amount)
CanSpam Act Goes Into Effect
Index of Valid User Messages
Spam Messages
Time
0
100
200
300
400
500
600
700
800
900
Nov-02
Dec-02
Jan-03
Feb-03
Mar-03
Apr-03
May-03
Jun-03
Jul-03
Aug-03
Sep-03
Oct-03
Nov-03
Dec-03
Jan-04
Feb-04
Mar-04
Apr-04
May-04
Jun-04
Jul-04
Aug-04
Sep-04
Oct-04
Nov-04

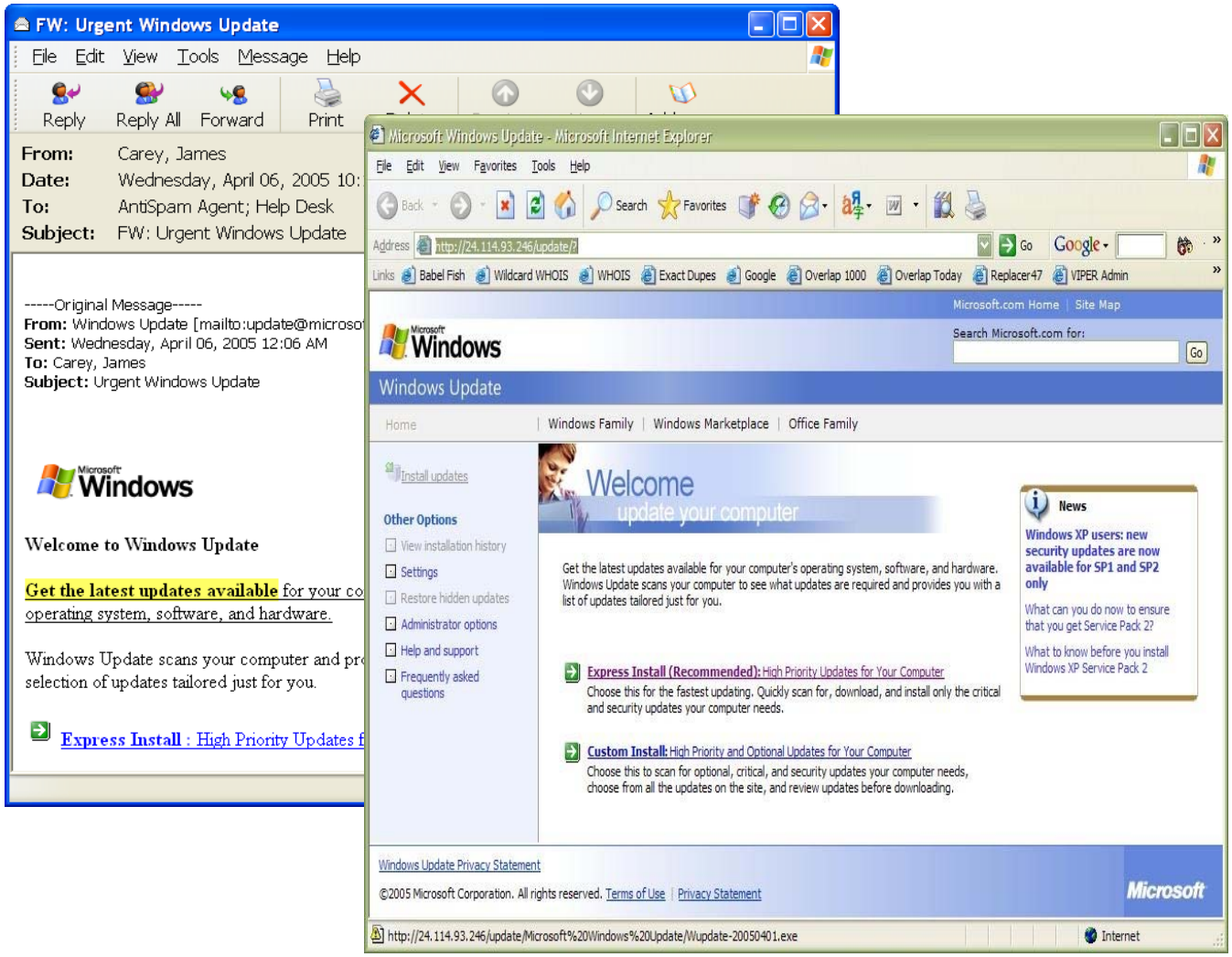
Ways of SPAMs



1. Hacker attacks directly or by controlling botnet
2. Criminals hire a hacker to attack
3. Organized Criminals hire botnet to launch attacks

Phishing


NetBank
Dear Valued Customer,
SunTrust Bank: Please Confirm Your Internet Banking Identity - Message (HTML)
From: SunTrust [identdep_op67980518590449 2@suntrust.com]
To: Susan Getgood (R)
Subject: SunTrust Bank: PIease Confirm Your Internet Banking Identity
SUNTRUST
Dear SunTrust Bank client,
Recently there have been a large number of identity theft attempts targeting Su
customers. In order to safeguard your account, we require that you confirm you
banking details (credit card information and login/password for online banking,
have).
This process is mandatory, and if not completed within the nearest time your ac
credit card may be subject to temporary suspension.
To securely confirm you SunTrust Bank details please follow the link:
http://www.suntrust.com/personal/Checking/OnlineBanking/Internet_Banking/security.asp
Thank you for your prompt attention to this matter and thank you for using Sun
Bank!
Do not reply to this e-mail as it is an unmonitored alias
© 2004 SunTrust Banks, Inc. All rights reserved. Me
FW: Urgent Windows Update
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addres...
Microsoft Windows Update - Microsoft Internet Explorer
Windows Update
Home
Windows Family
Windows Marketplace
Office Family
Other Options
Welcome
update your computer
Get the latest updates available for your computer's operating system, software, and hardware. Windows Update scans your computer to see what updates are required and provides you with a list of updates tailored just for you.
Express Install (Recommended): High Priority Updates for Your Computer
Choose this for the fastest updating. Quickly scan for, download, and install only the critical and security updates your computer needs.
Custom Install: High Priority and Optional Updates for Your Computer
Choose this to scan for optional, critical, and security updates your computer needs, choose from all the updates on the site, and review updates before downloading.
News
Windows XP users: new security updates are now available for SP1 and SP2 only
What can you do now to ensure that you get Service Pack 2?
What to know before you install Windows XP Service Pack 2
Windows Update Privacy Statement
©2005 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement
Microsoft


FW: Urgent Windows Update
File Edit View Tools Message Help
Reply Reply All Forward Print
From: Carey, James
Date: Wednesday, April 06, 2005 10:
To: AntiSpam Agent; Help Desk
Subject: FW: Urgent Windows Update
-----Original Message-----
From: Windows Update [mailto:update@microsof
Sent: Wednesday, April 06, 2005 12:06 AM
To: Carey, James
Subject: Urgent Windows Update
Windows
Welcome to Windows Update
Get the latest updates available for your co
operating system, software, and hardware.
Windows Update scans your computer and pr
selection of updates tailored just for you.
Express Install : High Priority Updates f
Microsoft Windows Update - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://24.114.93.246/update/?
Go Google
Links Babel Fish Wildcard WHOIS WHOIS Exact Dupes Google Overlap 1000 Overlap Today Replacer47 VIPER Admin
Microsoft.com Home | Site Map
Microsoft Windows
Search Microsoft.com for:
Go
Windows Update
Home | Windows Family | Windows Marketplace | Office Family
Install updates
Other Options
View installation history
Settings
Restore hidden updates
Administrator options
Help and support
Frequently asked questions
Welcome
update your computer
Get the latest updates available for your computer's operating system, software, and hardware. Windows Update scans your computer to see what updates are required and provides you with a list of updates tailored just for you.
Express Install (Recommended): High Priority Updates for Your Computer
Choose this for the fastest updating. Quickly scan for, download, and install only the critical and security updates your computer needs.
Custom Install: High Priority and Optional Updates for Your Computer
Choose this to scan for optional, critical, and security updates your computer needs, choose from all the updates on the site, and review updates before downloading.
News
Windows XP users: new security updates are now available for SP1 and SP2 only
What can you do now to ensure that you get Service Pack 2?
What to know before you install Windows XP Service Pack 2
Windows Update Privacy Statement
©2005 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement
Microsoft
http://24.114.93.246/update/Microsoft%20Windows%20Update/Wupdate-20050401.exe
Internet

Accelerator: Underground Economy

Floor 4:
Attacks to business , government

Floor 3:
Personal IDs
Bank IDs

Floor 2:
Botnets

Floor 1:
Hacking software

Example:

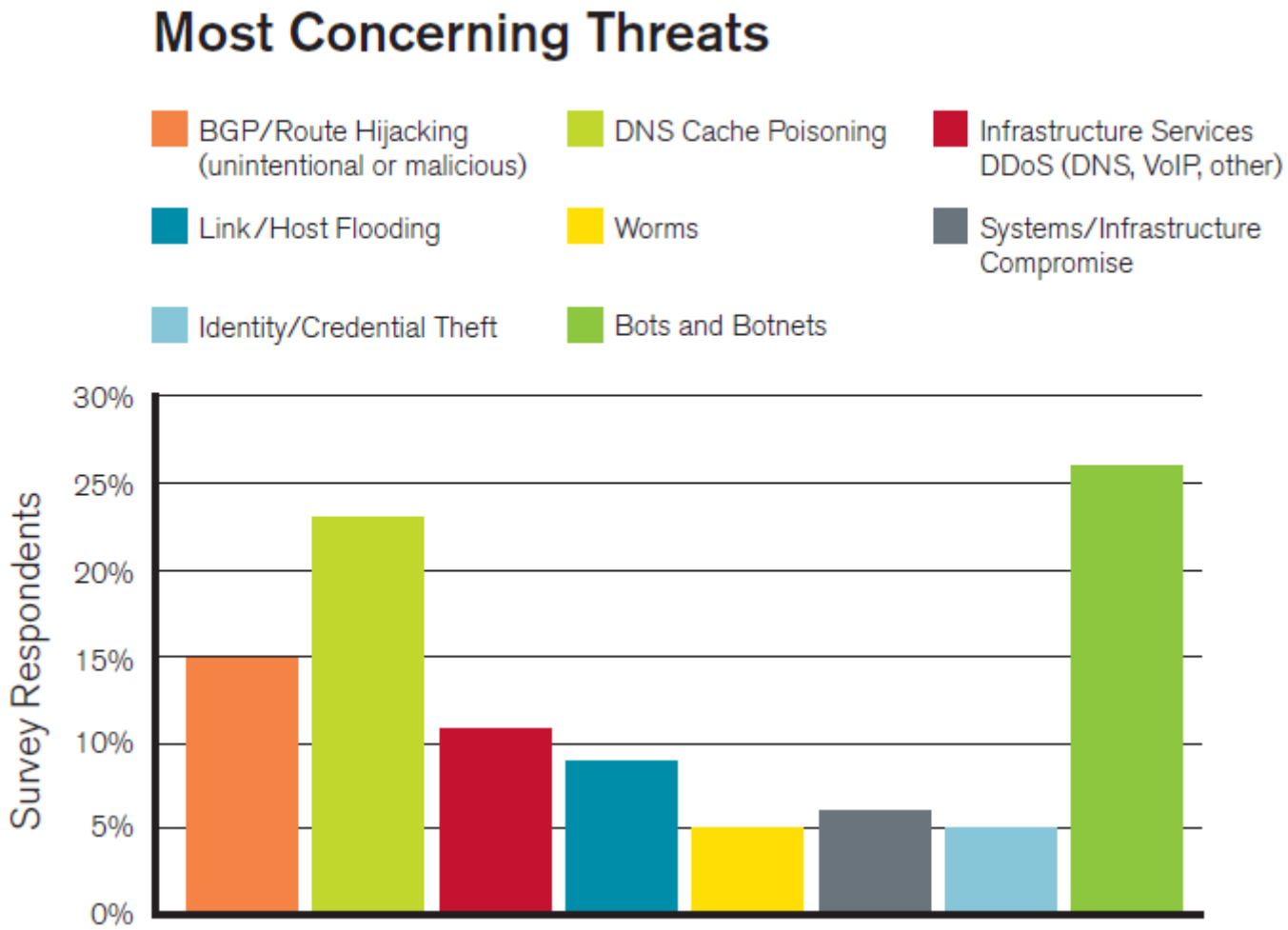
Subject: **I offer the DDoS attack service !**
From: ddos@safe-mail.net <DDOS Service>
Date: 3/3/05 10:54
Newsgroups: alt.2600.cardz

HI,

I offer the DDOS attack service, I offer estimate of expense on hour base. Free demonstration (10 minutes).
The price is based on the difficulty to pull down the target website, for the free demonstration or information please contact :

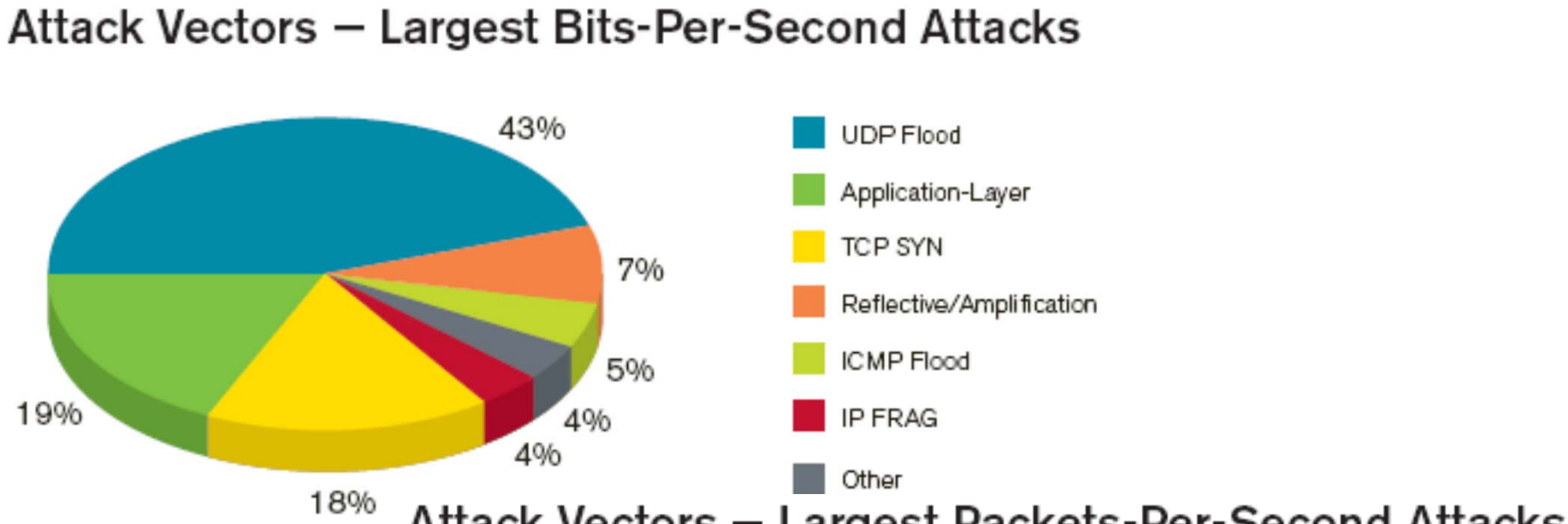
DDOS Service at : ddos@safe-mail.ne

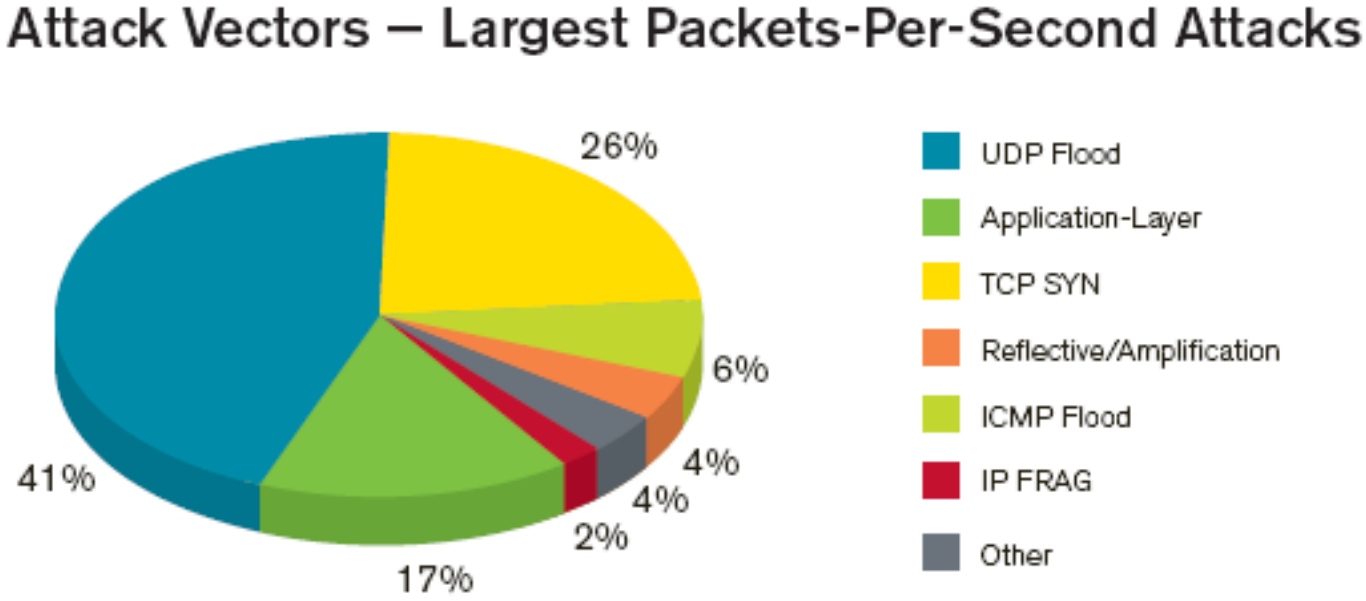
Most Concerning Threats



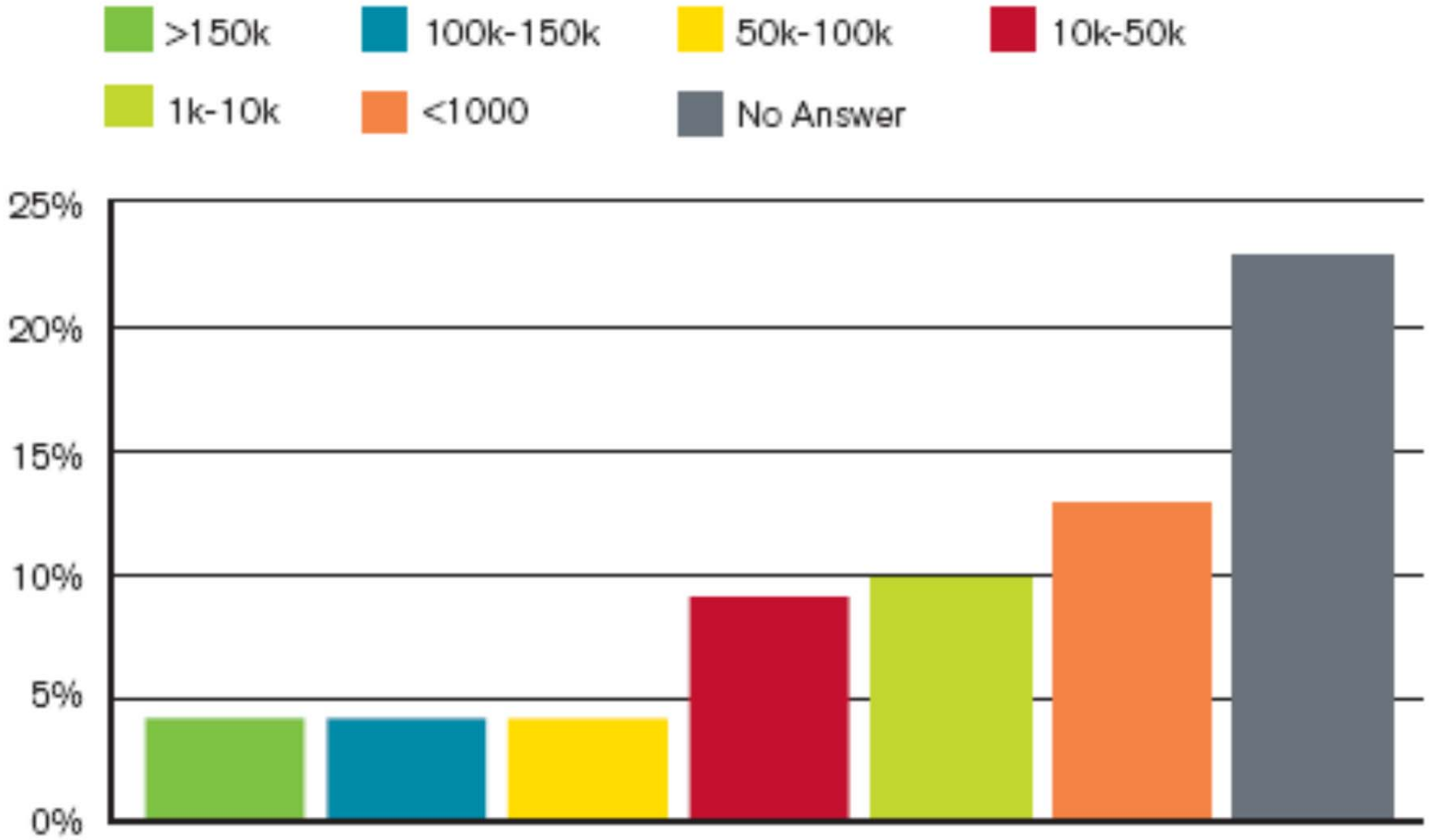
WORLDWIDE INFRASTRUCTURE SECURITY REPORT ARBOR Networks, Oct 2008

Attack Vectors



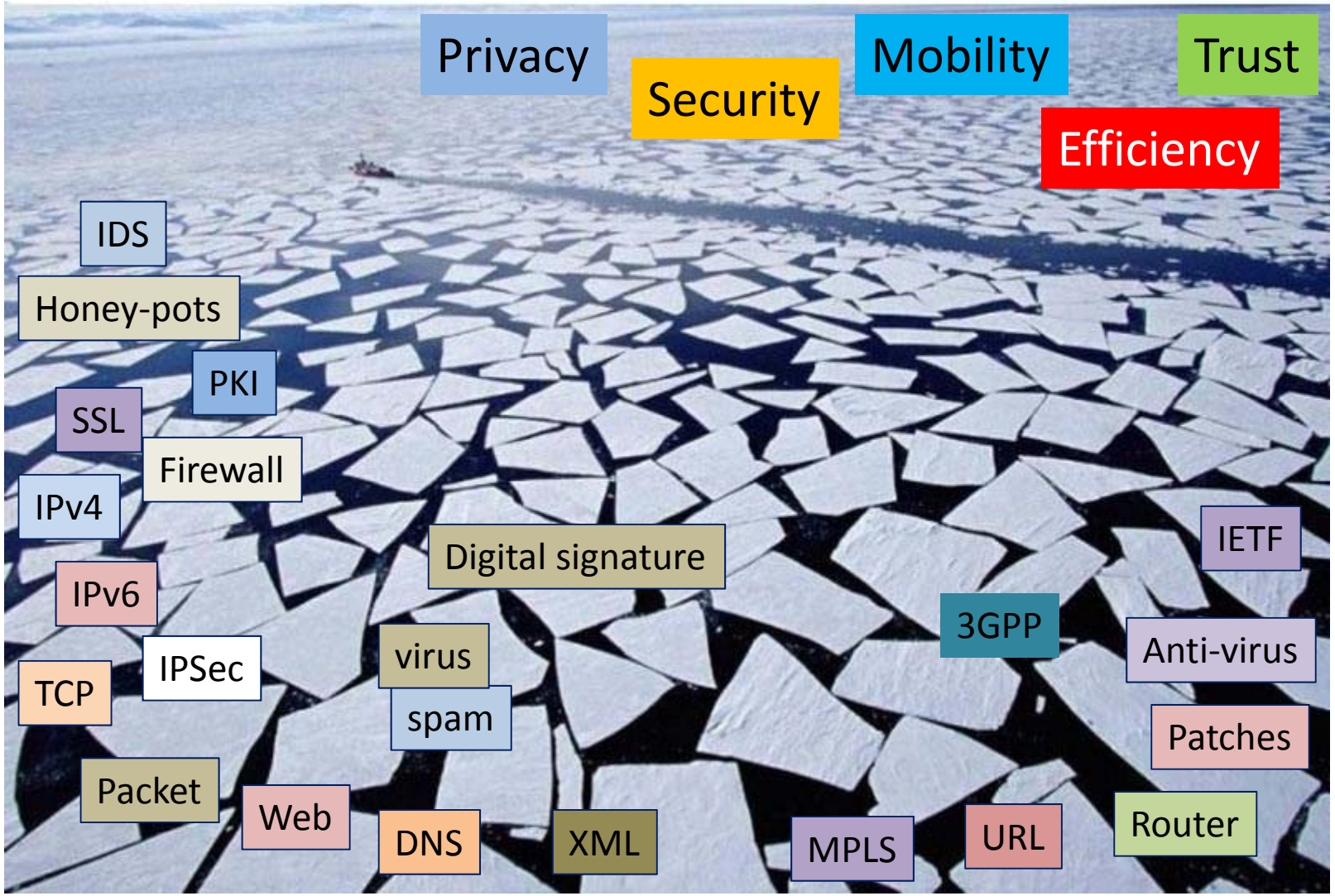


Botnet


>150k
100k-150k
50k-100k
10k-50k
1k-10k
<1000
No Answer
25%
20%
15%
10%
5%
0%

The Internet is Broken

--David Clark [22]

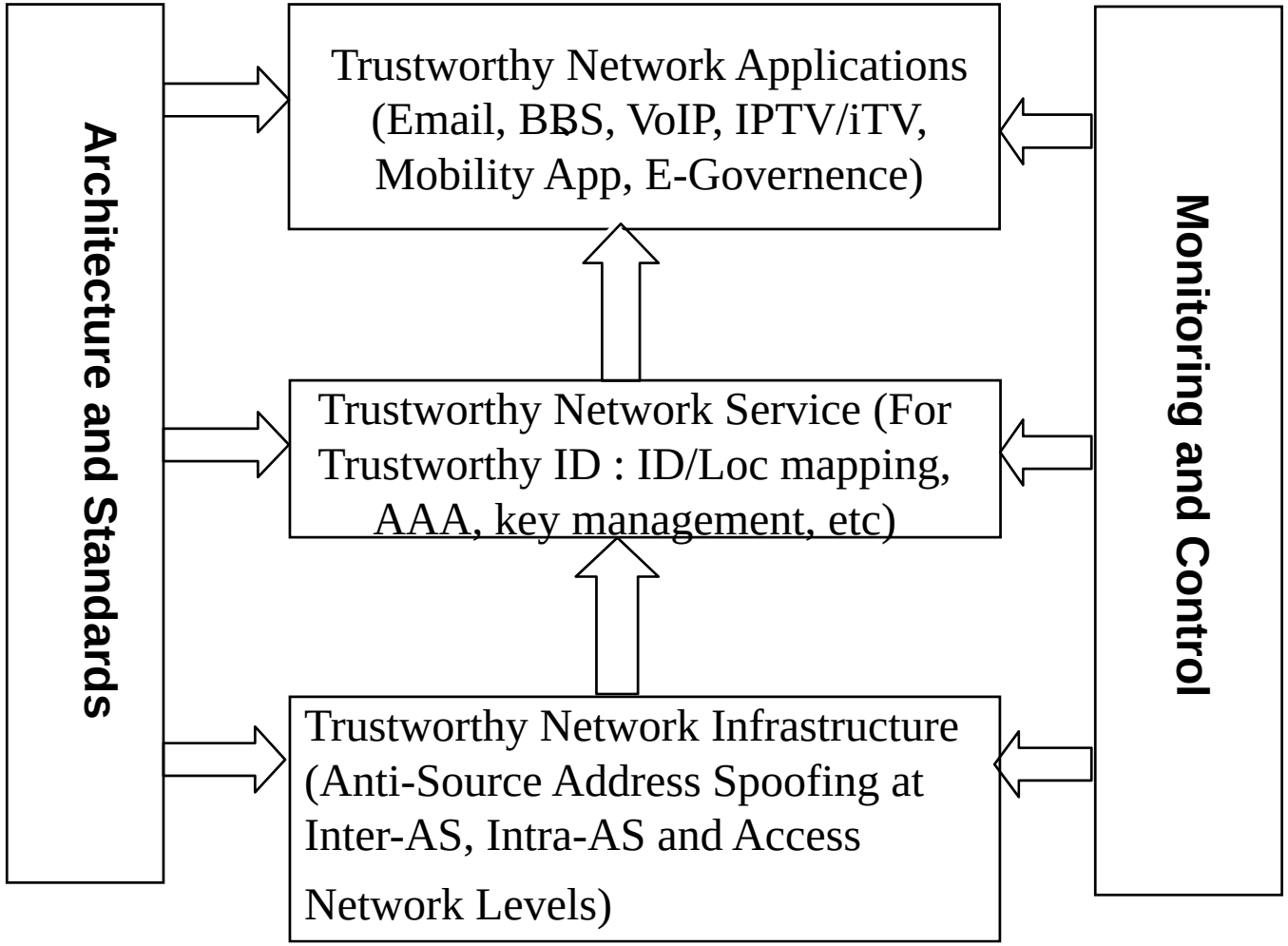


Trustworthy Internet and Source Address Validation

The Prosperities of Trustworthy Internet

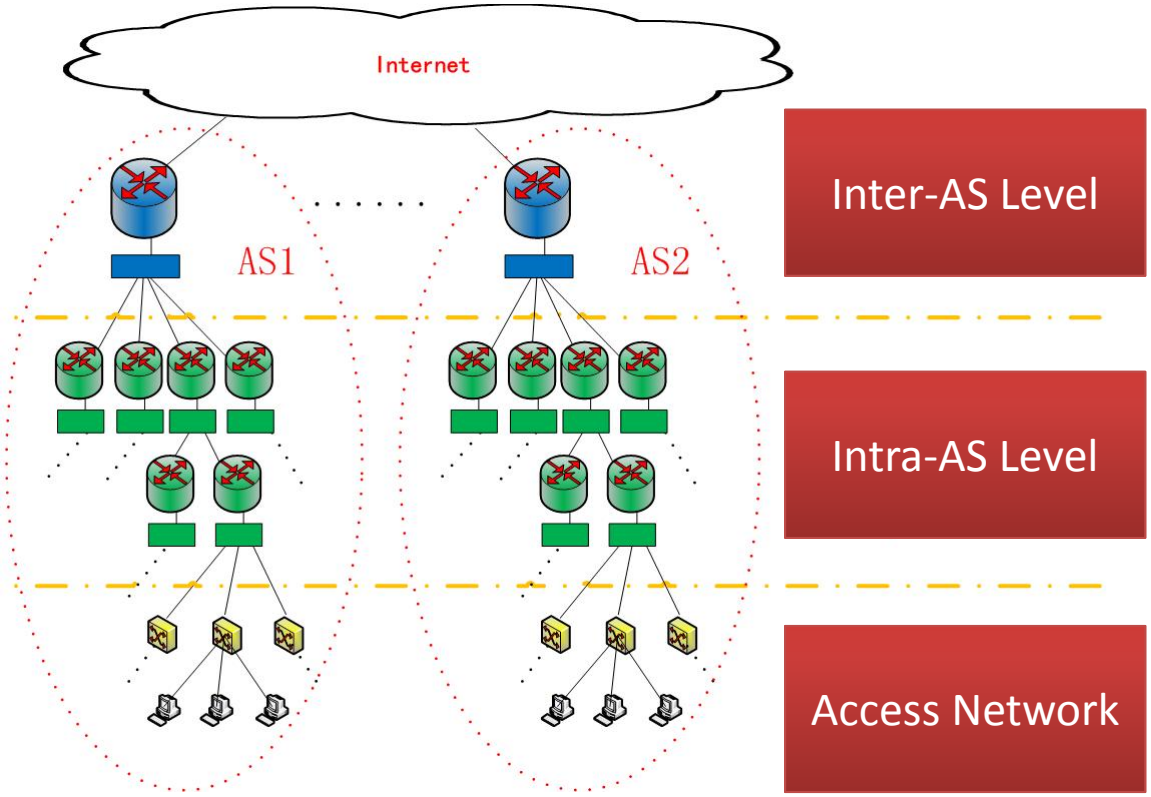
- Trust is the expectation that a device will behave in a particular manner for a specific purpose.
- Properties of Trustworthy Internet
  - Security, and Authenticity, Accountability, Privacy
  - Availability: Reliability, Resilience Service
  - Controllability: Monitoring and Control (Cross-layer)

Trustworthy Internet: MOST Science &Technology Support Project



Source Address Validation Architecture

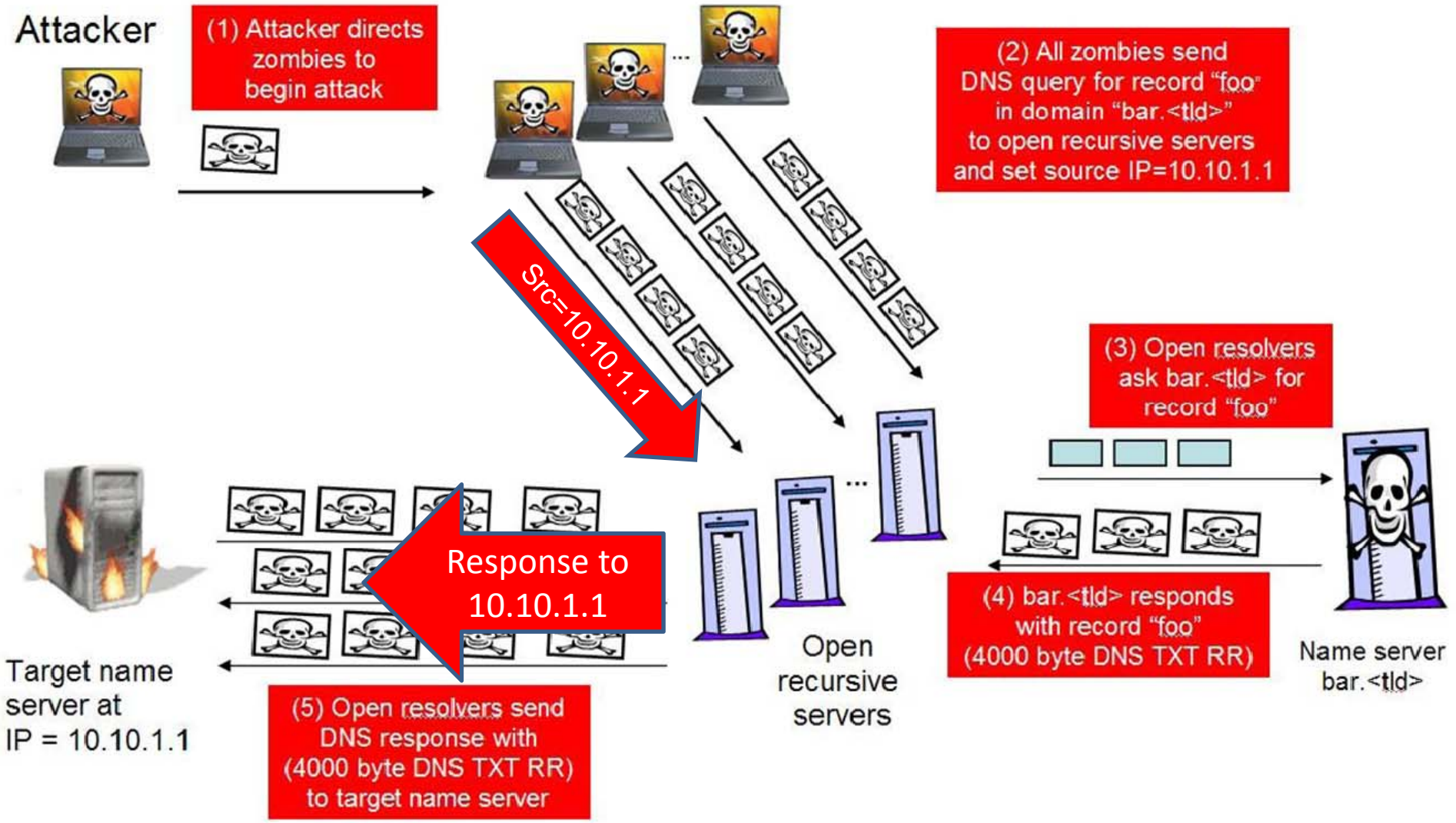
- RFC5210, J. Wu, J. Bi, X. Li, G. Ren, K. Xu, (SAVA)[9]



IP Spoofing

- Computers can send packets with forged IP source addresses.
- Frequently used in attacks
  - DrDoS [1]
  - SYN Flood [2]
  - TCP Hijack [3][4]
  - DNS Cache Poisoning [5]
- Can also ..
  - Hide real attacker
  - Amplify the power of attack
  - Weaken the power of defense system
  - Defeat IP address based authentication

DrDoS Example



Korean sites targeted in ongoing DDOS

- July 2009, many Korean sites were under DDoS Attacks:
  - the Ministry of National Defense
  - Foreign Affairs and Trade
  - Republic of Korea National Assembly
  - the Grand National Party
  - Naver blog, Naver mail,
  - Shinhan Bank, Korea Exchange Bank…
- The attacks took advantages of IP spoofing, making it harder to defense

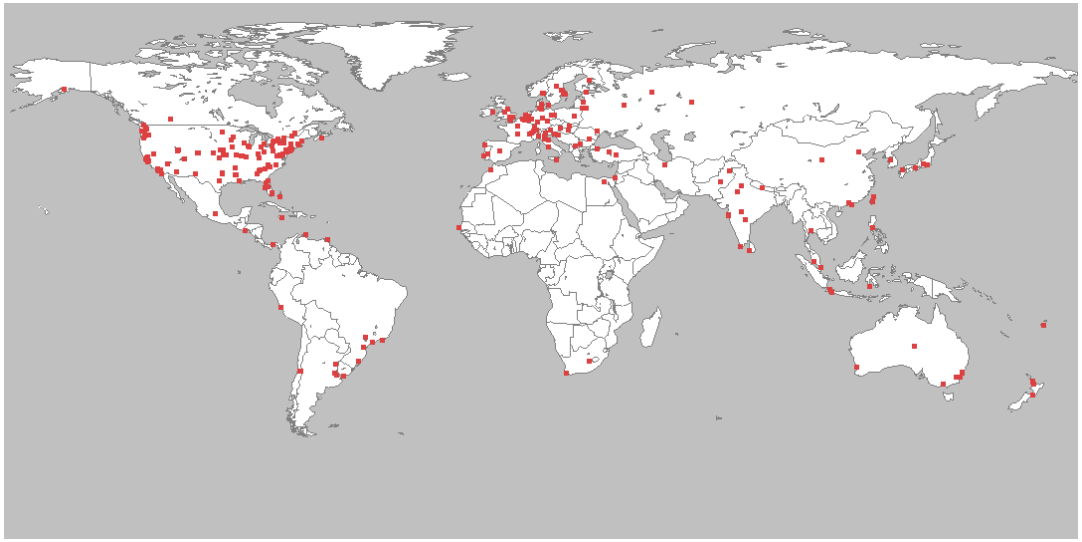
Statistics

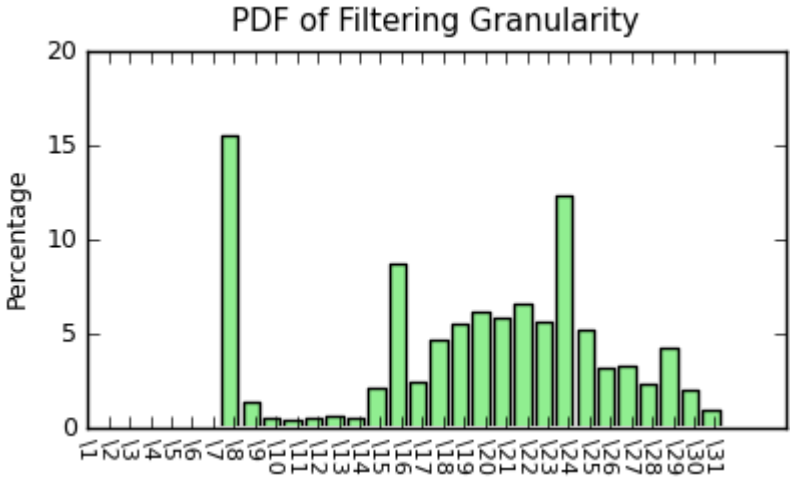
- There are about 4000 IP spoofing attacks every weak [6]
- At least 24% autonomous systems are spoofable [8, MIT spoofer project]
- US and China are top 2 target counties of the spoofing packets [7, CAIDA telescope]

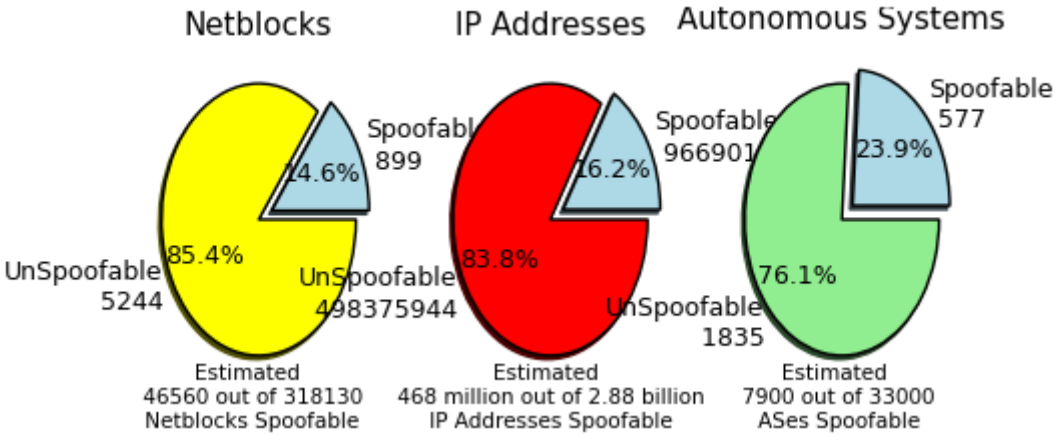
MIT ANA Spoofer [8]

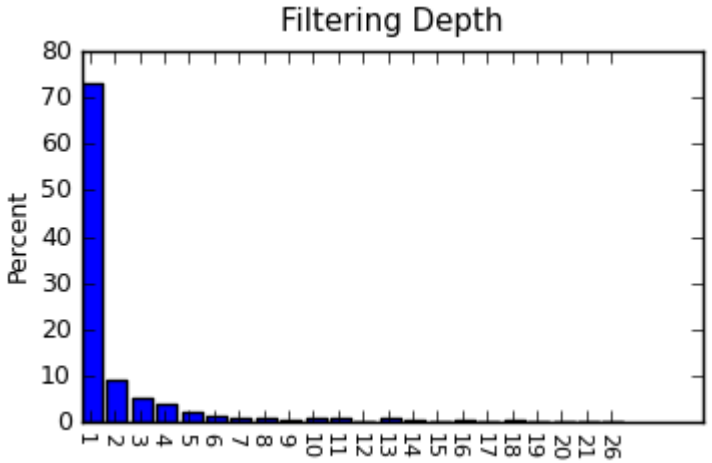
- The MIT ANA Spoofer project measures the Internet's susceptibility to spoofed source address IP packets.
- It measure various source address types (invalid, valid, private), granularity (can you spoof your neighbor's IP address?), and location (which providers are employing source address validation?)
- The research is particularly relevant given the regular appearance of new spoofed-source-based exploits, despite decades of filtering effort.

Spoofer Statistics





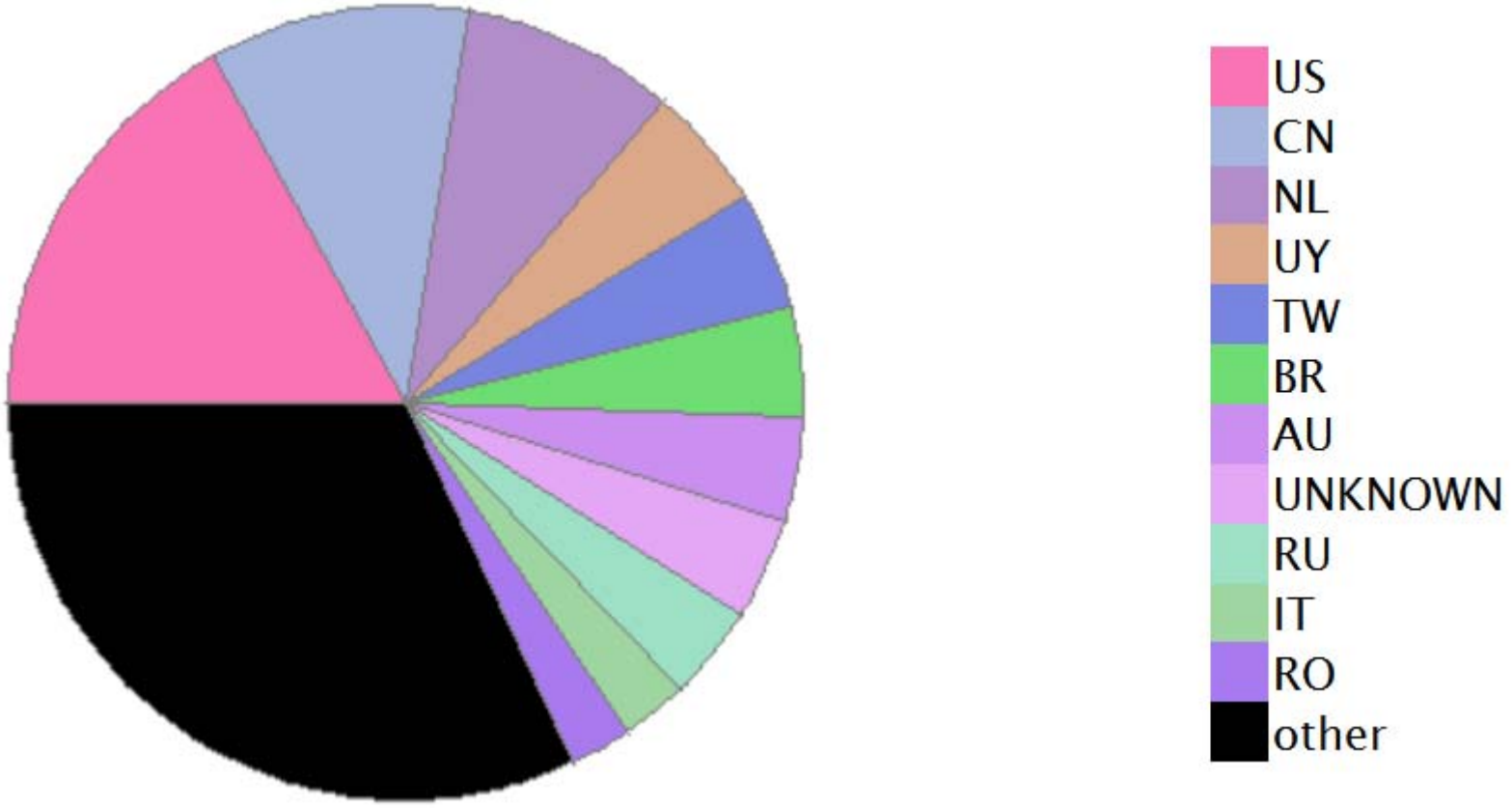




CAIDA Telescope [7]

- A network telescope is a portion of routed IP address space on which little or no legitimate traffic exists.
- Monitoring unexpected traffic arriving at a network telescope yields a view of certain remote network events. Among the visible events are various forms of flooding DoS attacks, infection of hosts by Internet worms, and network scanning.

Telescope Statistics – CAIDA 2010.11.14



RESEARCHES ON METHOD DESIGN

History

- 2001: DPF, SIGCOMM [11]
- 2001: Hash-Based IP Traceback, SIGCOMM[12]
- 2002: SAVE, INFOCOM [13]
- 2003: HCF, CCS [14]
- 2005: SPM, INFOCOM [15]
- 2006: IDPF, INFOCOM [16]
- 2006: StackPi, JSAC [17]
- 2006: Passport, USENIX SRUTI [18]
- 2007: BASE, Asia CCS [19]
- 2008: AIP, SIGCOMM [20]

Taxonomy

- Proactive
  - Route based filtering
  - End-to-end filtering
  - Approaches in access network
- Reactive
  - Traceback

Proactive: Route based filtering

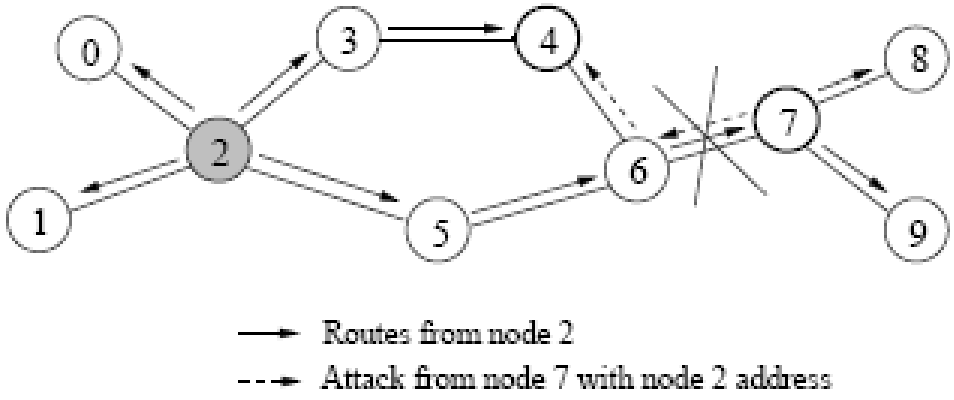
- Ingress Filitering
- Distributed Packet Filtering
  - SAVE
  - IDPF
- Passports

Ingress Filtering

- Ingress Filtering for Multihomed Networks
  Best Current Practice (RFC 3704)
  - Ingress Access Lists
  - Strict Reverse Path Forwarding
  - Feasible Path Reverse Path Forwarding
  - Loose Reverse Path Forwarding
  - Loose Reverse Path Forwarding Ignoring Default Routes

Distributed Packet Filtering (DPF)

- A framework of distributed packet filtering
  - SAVE, IDPF, BASE are under this framework
- Methodology
  - Assume that nodes has the knowledge of which direction a source address will arrive in.

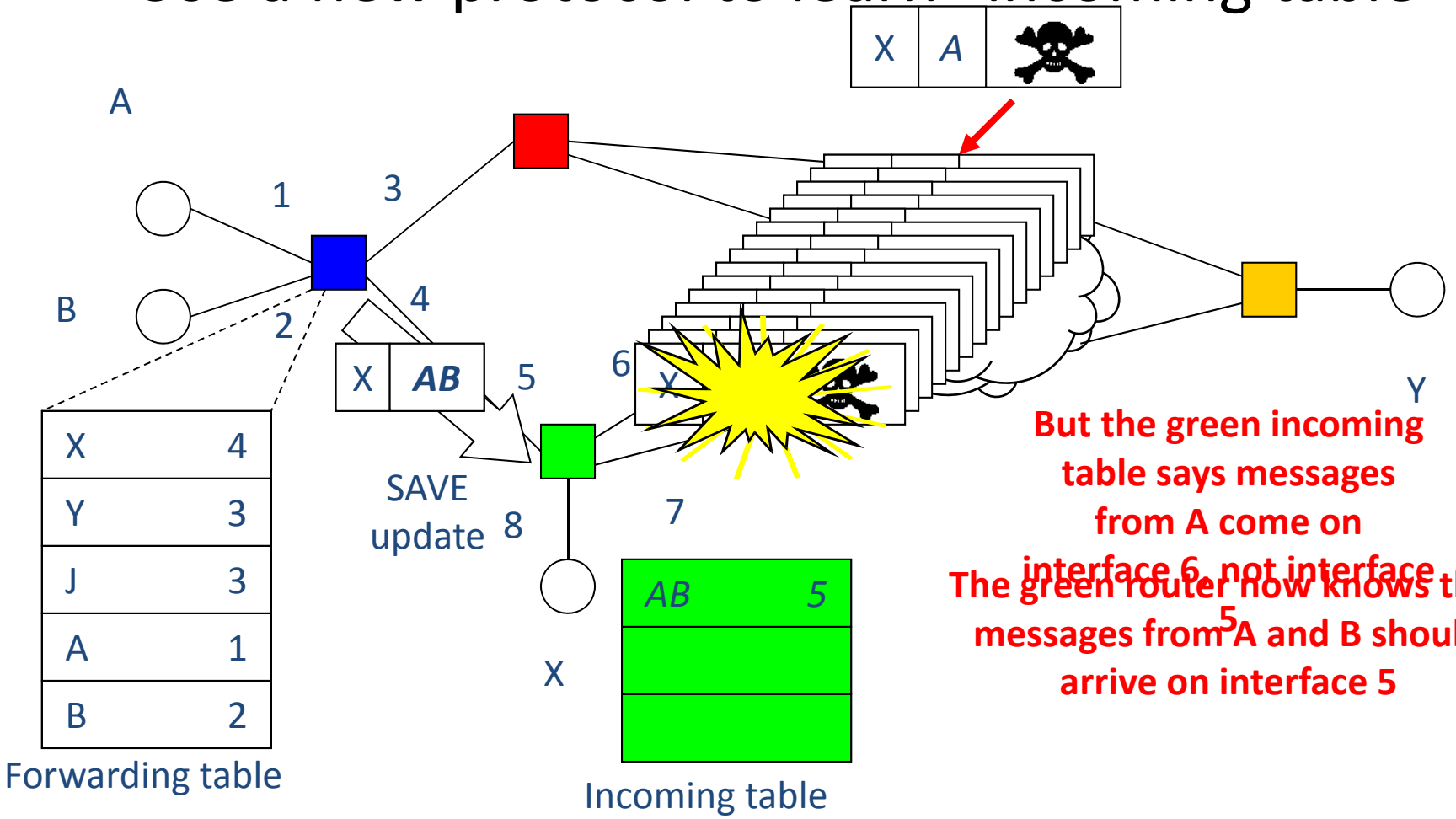


Distributed Packet Filtering (DPF)

- DPF is a milestone
  - DPF gives an analysis framework for route-based filtering methods. And it inspires a lot of new works under the framework.
- DPF raises a key problem
  - How to learn the direction of a source address?
  - The follow-ups of DPF mainly focus on resolving this problem.
    - SAVE: Use separate protocol
    - IDPF: Use inter-AS “valley-free” principal
    - BASE: Use BGP extension

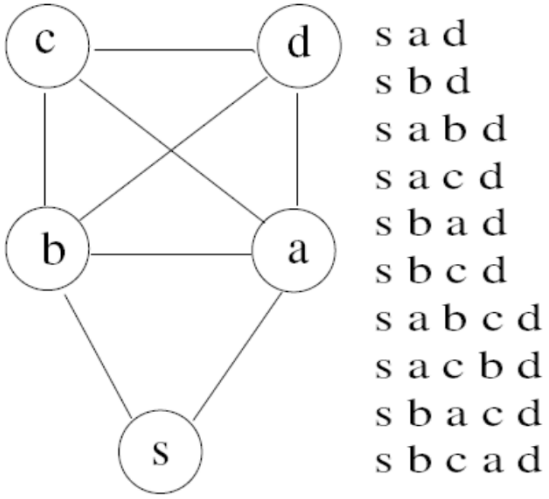
SAVE:
Source Address Validity Enforcement

- Use a new protocol to learn "incoming table"



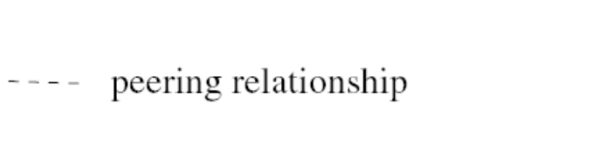
IDPF： Inter Domain Packet Filters

- IDPF establishes “address-direction” table based on inter-AS routing policy. (valley-free)
  - Use the policy to compute “Feasible Routes”
  - Packets from infeasible routes are dropped.

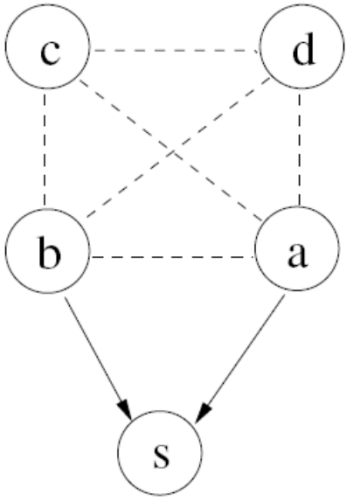


s a d
s b d
s a b d
s a c d
s b a d
s b c d
s a b c d
s a c b d
s b a c d
s b c a d

All possible routes



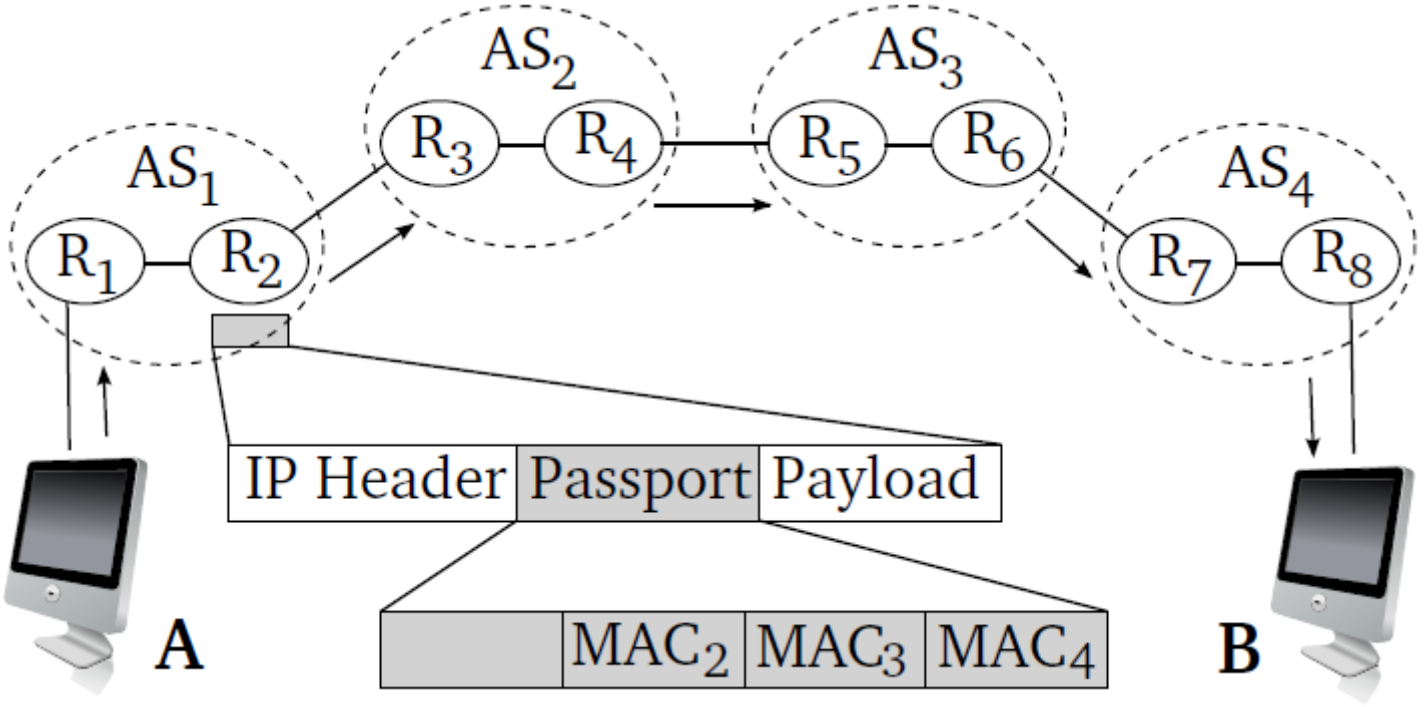
s a d
s b d



Feasible routes constrained by routing policy

Packet Passport

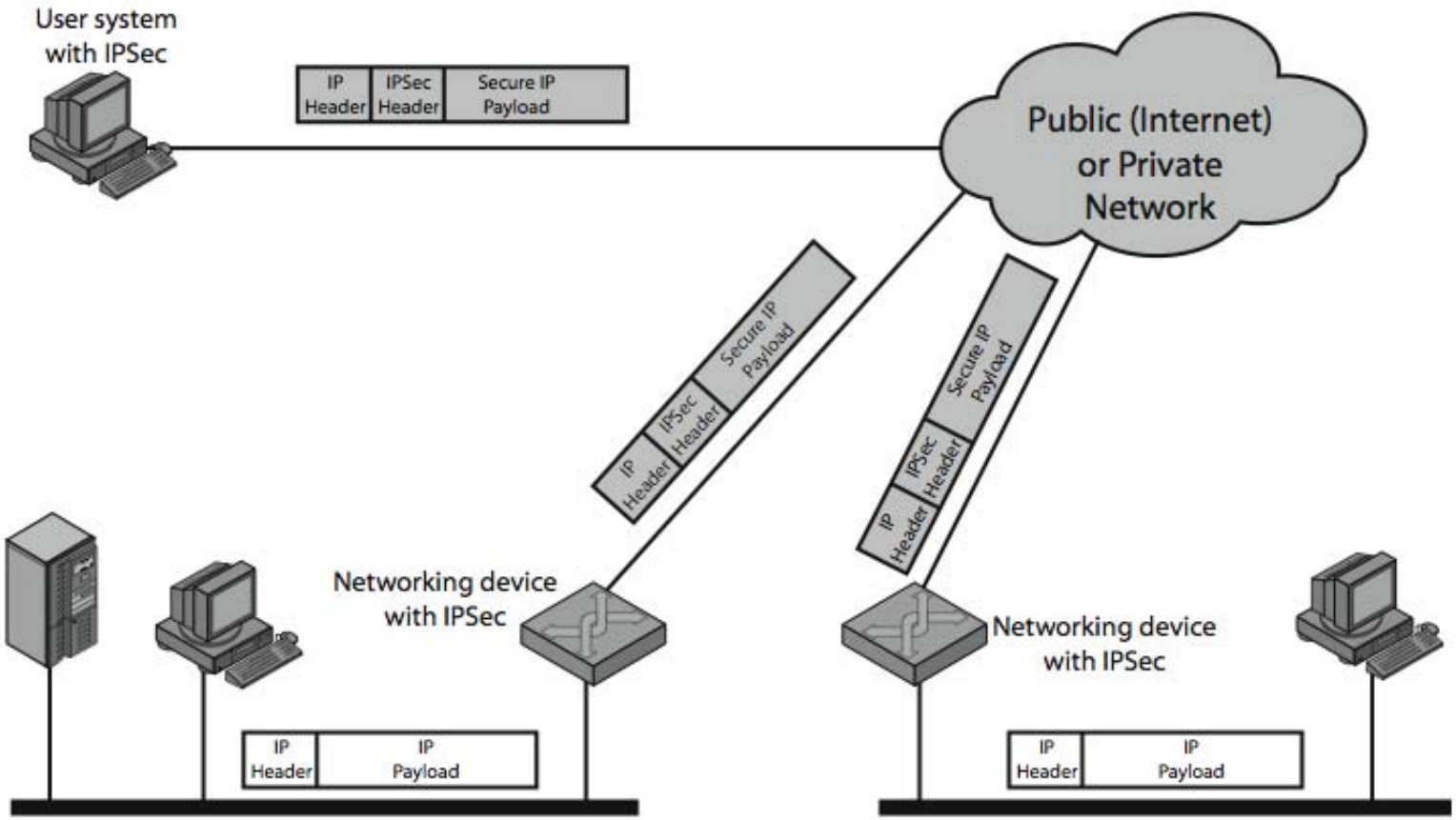
- Each check point on the path expects an MAC of the packet. And these MACs are inserted into the packet at the origin AS.



Proactive: End-to-end filtering

- IPSec
- HCF
- SPM

IPSec


User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Networking device with IPSec
Networking device with IPSec
IP Header
IP Payload
IP Header
IP Payload

IPSec

- IPSec requires high computation. So itself is vulnerable to DoS.
- Should be supported by PKI, which is problematic in large scale

HCF: Hop Count Filtering

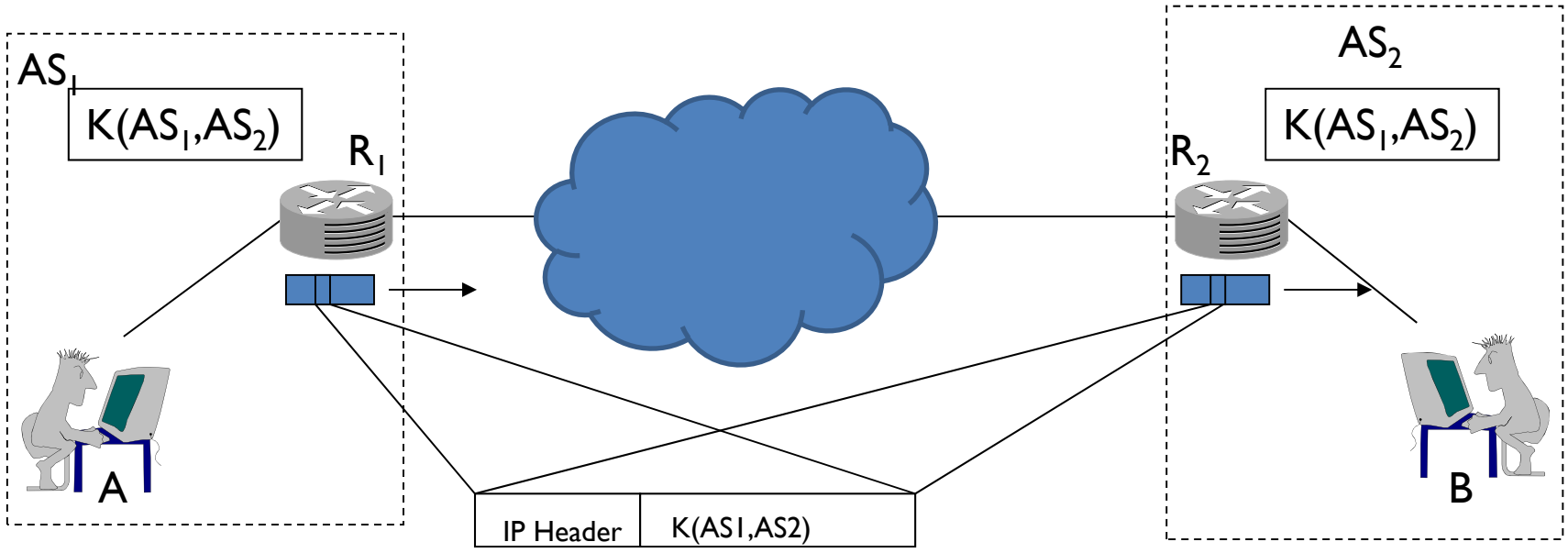
- HCF filters packets with invalid TTL.
  - Learn the number of hops from src to dst.
  - Calculate valid TTLs
    - Initial TTL value is always set to 30,32,60,64,128,255
- Features
  - Light-weighted
  - Benefits the deployer
  - Do not need cooperation.

HCF: Hop Count Filtering

- Weakness
  - Valid TTL can be cracked by attackers.
  - Drop valid packets if route changes
    - Then number of hops changes

SPM: Spoofing Prevention Method

- Each pair of src/dst ASes negotiate a key.
- The key is tagged into the packet by the border router of the src AS, and checked by the border route of dst AS.



IETF SAVI WG

- Both IPv4/IPv6 are covered
- Trust network device, do not change host
- Support all kinds of address allocation method
- Support multiple addresses/topology changing/mobility under the same subnet
- Attack-free
  - Prevent forged DHCP server, RA, NA…
  - Set max bounding entries

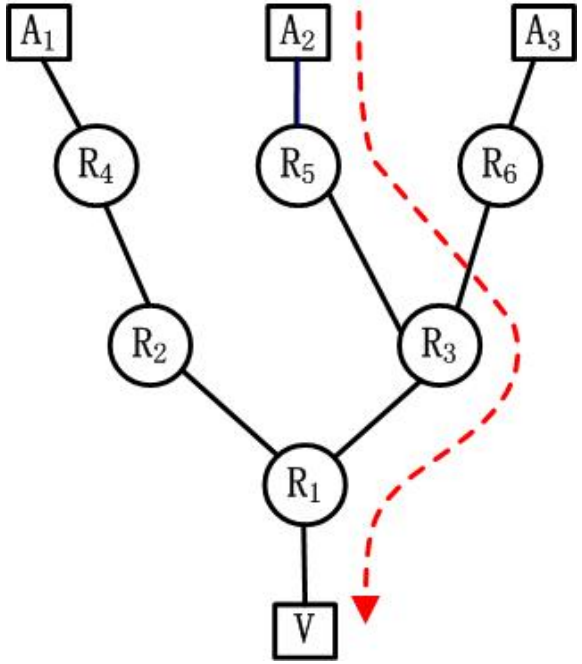
Source Address Validation Improvements

- Focus on the “Access Network” level of SAVA
- Drafts
  - draft-ietf-savi-threat-scope
  - draft-ietf-savi-framework
  - draft-ietf-savi-dhcp
  - draft-ietf-savi-fcfs
  - draft-ietf-savi-send

Traceback

Reactive: Traceback

- **Traceback Problem** [23]: to identify the machines that directly generate attack traffic and the network path this traffic subsequently follows.



（1）Locate attack sources

（2）trace attack paths

Difficulty and Current Situation

- Difficulty in Traceback
  - Internet is stateless in itself
  - Packet is forwarded only on its destination address
  - Packet lacks of valuable information for traceback
  - NAT and Firewall are widely used in Internet
  - overhead and precision of existing traceback schemes
- Current Situation
  - In 1999, Researchers began to study traceback. But every traceback scheme solves some problems and simultaneously incurs other problems.
  - So far, none of traceback schemes has been deployed in the Internet.

Classification

- Link Testing
  - test upstream routers hop by hop
  - Input Debugging and Controlled Flooding [24]
- Packet Marking
  - mark path information in packet header
  - PPM [1], StackPi [25], Randomize & Link [26], An AS-Level Overlay Network for IP Traceback [27]
- logging
  - path information is stored in routers or server
  - Hash-based IP Traceback [28], One-bit Random Marking and Sampling (ORMS) [29]
- Traceback based on ICMP
  - routers send new ICMP packets to the receiver
  - iTrace [30]

Link Testing

- **Main idea:** network manager begins to check router closest to the victim, and subsequently traces the router closest to the attacker. Network software and hardware are not modified in Link Testing, but it can only trace ongoing attack. Link Testing consists of two types of schemes: **Input Debugging** and **Controlled Flooding**

Input Debugging

- **Main idea:** Firstly, Network manager extracts attack signatures from attack packets, and then checks the router closest to the victim where the input debugging is applied, and confirm the input port of attack packets, This process is repeated recursively on the upstream routers.
- **Shortcomings:** considerable management overhead; traceback process is slow

Controlled Flooding

- **Main idea:** to flood links with large bursts of traffic and observes how this perturbs traffic from the attacker. By observing changes in the rate of attack packets, the victim can therefore deduce which link the packets are coming from. This process is repeated recursively on the upstream routers.
- **Shortcomings:** it is a DoS by itself; it requires any victim to have a good map of the Internet.

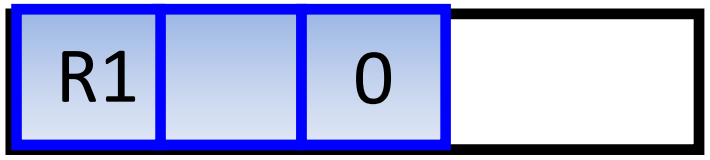
Packet Marking

- **Main idea**: routers mark packets that pass through them with path information. Packets for marking are selected at random with some fixed probability. As the victim gets the marked packets, it can reconstruct the full path.

- **Shortcomings:** backward compatibility; high compute overhead in the victim; high false positives

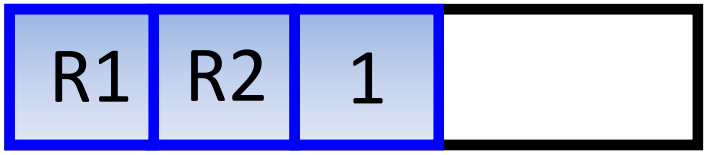
Probabilistic Packet Marking (PPM)

- **Main idea：** routers mark packets with a fixed probability, marking information is a triple <start address, end address, distance counter>, start address and end address are IP addresses of two end routers belonging to a link, distance counter logs the distance between marking routers and the victim。



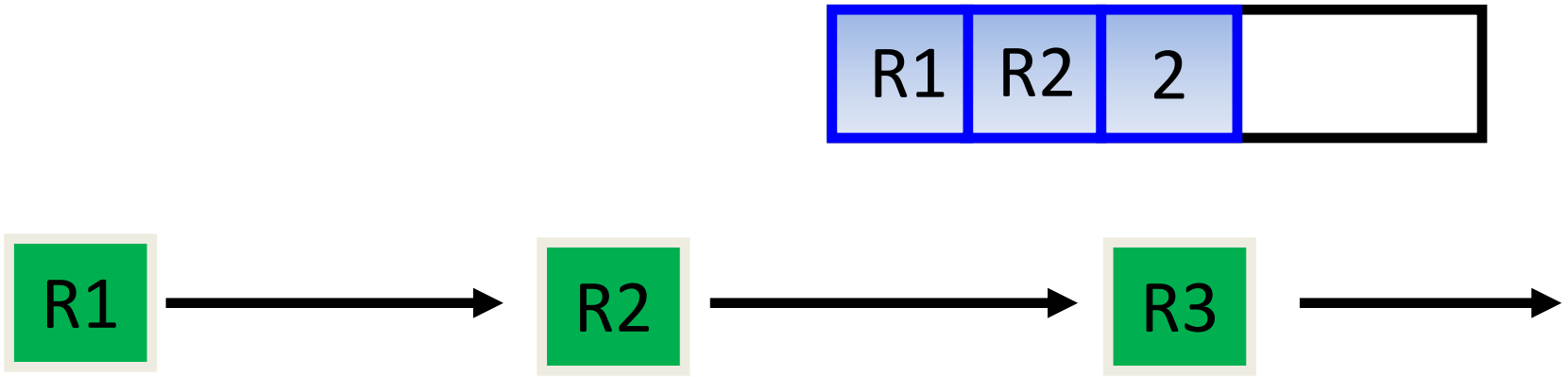
Probabilistic Packet Marking (PPM)

- **Main idea：** routers mark packets with a fixed probability, marking information is a triple <start address, end address, distance counter>, start address and end address are IP addresses of two end routers belonging to a link, distance counter logs the distance between marking routers and the victim



Probabilistic Packet Marking (PPM)

- **Main idea**： routers mark packets with a fixed probability, marking information is a triple <start address, end address, distance counter>, start address and end address are IP addresses of two end routers belonging to a link, distance counter logs the distance between marking routers and the victim。

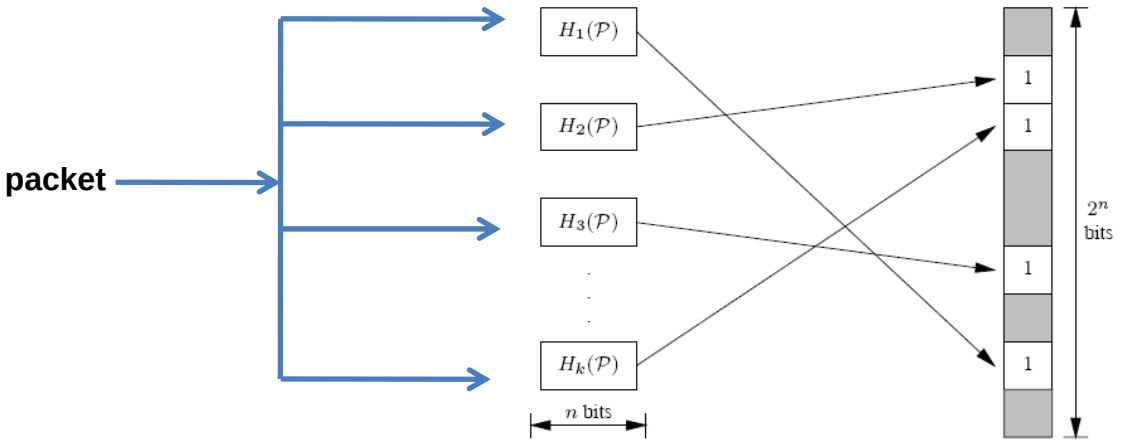


Logging

- **Main idea:** every router stores information of every packet that passes through the router. When the router is queried later, it can determine if a certain packet passed through it.

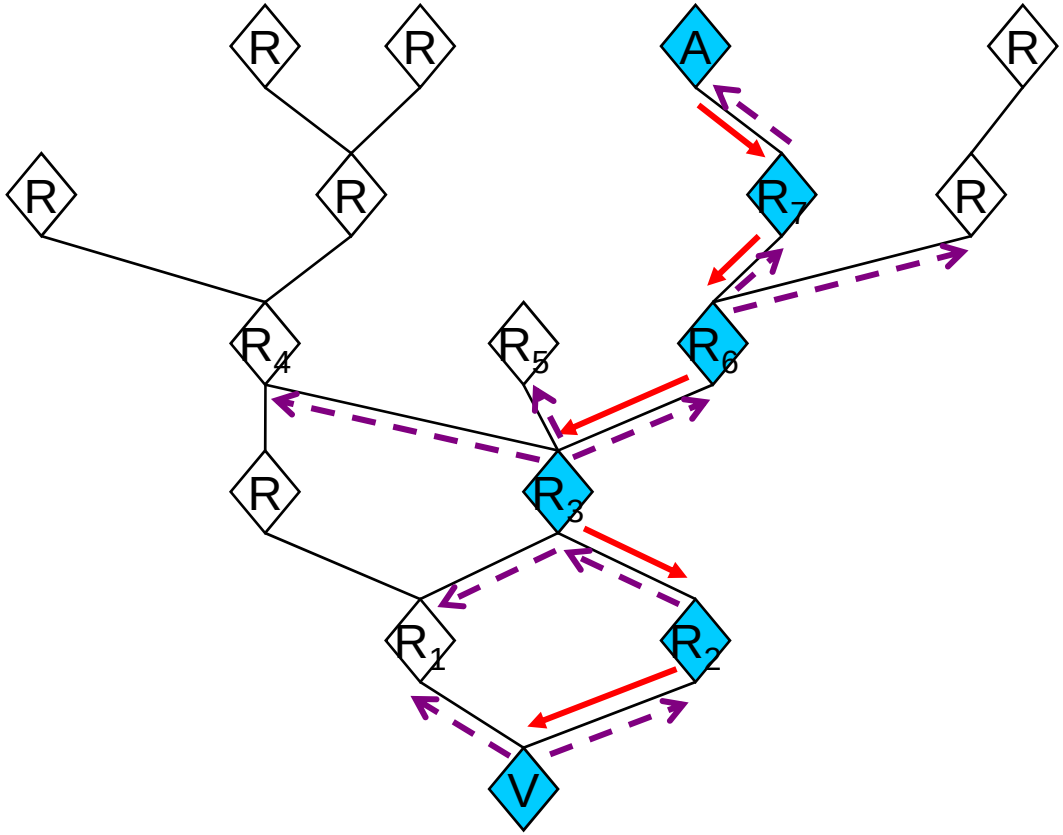
Hash-based IP Traceback (SPIE)

- **Main idea：** every router maintains BF (Bloom Filter) and writes signature of every packet passing through the router into BF.
- **Shortcoming：** the compute and storage overhead of router is large



Hash-based IP Traceback (SPIE)

- Traceback process



note： red solid line is attack path
purple dashed line is traceback process

Traceback based on ICMP

- **Main idea:** when router forwards packets, it sends new ICMP messages to destination host. New ICMP message includes: IP address of the router, IP address of downstream (or upstream) router. The victim will receive enough ICMP messages and reconstruct attack path

- **Shortcomings:** require a large number of ICMP messages, false positives and false negatives are high

Compare

metrics \ method	Controlled Flooding	PPM	SPIE	iTrace
ISP cooperation	need	no	no	no
Packet number	more	more	one	middle
overhead	Additional traffic	Computer Overhead of victim is high	Computer and storage overhead is high	Additional traffic
precision	Not precise when facing DDoS	False positive is high	False negative is 0	False positive is high
Easiness to escape	easy	middle	hard	easy
Traceback DDoS	no	yes	yes	yes
Incremental deployment	yes	yes	no	yes

Security in Future Internet

New Threats

- New Usages => New threats
  - New landscape
    - Massive multi-parties applications programs (Alice & Bob relationship is over …)
    - 500 Mega-machines, 3 Giga-people, 1 tera-objects (Security is not scalable …)
    - Huge flows of multimedia content and virtual distributed services (traceability will be difficult, indeed impossible)
    - Interconnection with the physical world : sensors and actuators (end of an intangible world)
  - Digital world : **a vast ecosystem of critical infrastructures** (how to control and master ?)
    - Mobility of devices, persons, groups, swarms of things
    - Privacy issues : European Identity cards, Anonymization, fragmented identity
    - **Addiction of users, Inescapable Infrastructures** (individual, enterprise, society)
- Major threats => illegal computer programs
  - Emergence of combined opportunities for attackers : **coïncidence of**
    - **Massive Power for everyone** : an end-user will have at his disposal Billions of Mips over the networks (new equilibrium of computing power)
    - **Pervasive connections to physical reality** : possibility to join and disturb the distributed physical world (physical presence will be too dangerous for terrorists, because of CCTV networks of surveillance)
  - **New generation of attackers, failures**
    - Organized cybercrime: criminal organization, but also untrusted service operators (telecom, network service, security brokers…)

Future Internet Attacks

- Attacks through user cooperation
  - Users are increasingly lost in the dynamic, recursively overlaid structures and distributed applications
  - Attract, threaten, fool users to cooperation
- Attacks through travels from Virtual to Real, back and forth
  - Attacks through dependencies: attack infrastructure A to provoke failures in infrastructure B
- Botnet attacks
  - Focus botnet power on targets, today mostly click fraud and DDoS
  - In future massive computations & data mining: inference, predictions
- Illegal content distribution attacks
  - Today mostly copyrighted material
  - Tomorrow: massive distribution of classified and illegal material through steganography and P2P networks

Future Internet Attacks

- Cyberwars
  - Secret and special services disrupting the IT infrastructures of enemy states
  - State sovereignty: massive disinformation and opinion manipulation, influence on elections in third states
- Internet assassinations
  - Remark: already implicitly possible today through connected object tracking
  - In future through direct object control and disruptive actions on objects resulting in “incidents”
- Cyberterrorism
  - disrupt services, provoke accidents in certain regions, kill certain citizens, disinformation, propaganda
- Personal attacks leading to virtual solitude and depression
  - Identity theft, identity usurpation, targeted ads, illicit banking operations
  - Killing digital reputation, provoking digital isolation

Trust, Security, Dependability & Privacy in FI

Issues to be validated

- **Identity of physical persons**
  - Identity management, accountability, responsibility: end-user, software editor, Service Provider, etc
  - Catalog of authentications (Accountability & non repudiation)
  - Privacy
- **Identity of virtual entities and physical artifacts**
  - Internet of Things (Massive and extremelqy tiny objects) : Statistical security (traceability)
- **Infrastructures**
  - Necessity to create a new trusted infrastructures
- **Distributed Learning Machines in Security**
  - Traffic analysis & monitoring : early detection
  - Distributed security detection
  - Seamless (through heterogeneity), mobility and massivity (extreme data rate & volume)
- **Digital governance**
  - Protection of the user (ethical behavior) from the rest of the world
  - Protection of the society from the user (hacker, cyber crime, cyber terrorism)

New security paradigms for Internet resilience

- The new art of sharing secrets
  - How to split between address – location & identity ?
  - Design new mechanisms for authenticity
    - Protocols to ensure trust properties for routing
    - No lies, no spoofing
- The new art to be accountable and liable
  - Sharing trust in the end to end actor's chain within the collaborative environment
- The new art of remaining free and private
- Top down approach : different granularities
  - Need to secure systems of systems
  - Need to secure any participating system
  - Need to secure every entity

Acknowledgement

- Some slides are borrowed from:
  - Artur Hecker, Security, Dependability and Trust in the Future Internet
  - Goce Armenski, Internet Security
  - Jun Bi, Security in Future Internet

Reference

1. V. Paxson, .An analysis of using reectors for distributed denialof-service attacks,. *ACM Computer Communications Review (CCR),* vol. 31, no. 3, Jul. 2001.
2. CERT, .Cert advisory ca-1996-21 TCP SYN ooding and IP spoong attacks,. 1996, http://www.cert.org/advisories/CA-1996-21.tml.
3. P. Watson, .Slipping in the window: TCP reset attacks,. In Cansecwest/core04 Conference, 2004.
4. M. Dalal. Improving TCP's robustness to blind in-window attacks. Internet Draft, May 2005.
5. J. Stewart, .DNS cache poisoning - the next generation,. LURHQ,Technical Report, Jan. 2003.
6. D. Moore, C. Shannon, D. Brown, G. Voelker, and S. Savage, .Inferring internet Denial-of-Service activity,. ACM Transactions on Computer Systems, vol. 24, no. 2, May 2006.
7. CAIDA, http://www.caida.org/data/realtime/telescope/.
8. The MIT ANA Spoofer Project, http://spoofer.csail.mit.edu/
9. J. Wu, J. Bi, X. Li, G. Ren, K. Xu, RFC 5210

Reference

10. Bellovin, S., "Security Problems in the TCP/IP Protocol Suite," Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989.
11. K. Park and H. Lee. On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets. ACM SIGCOMM 2001, August 2001.
12. Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, W. Timothy Strayer, Hash-Based IP Traceback, ACM SIGCOMM 2001, August 2001.
13. J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang. SAVE: Source Address Validity Enforcement Protocol. INFOCOM 2002, June 2002.
14. Jin, G., Wang, H., and Shin, K. G. “Hop-count filtering: an effective defense against spoofed DDoS traffic”. In Proceedings of the 10th ACM conference on Computer and communication security. Washington D.C., USA, 2003.
15. A. Bremler-Barr and H. Levy. Spoofing prevention method. In Proceedings of IEEE INFOCOM, Miami, July 2005.
16. Z. Duan, X. Yuan, J. Chandrashekar, Constructing inter-domain packet filters to control IP spoofing based on BGP updates. In Proceedings of IEEE Infocom, 2006.

Reference

17. A. Yaar, A. Perrig, D. Song, StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense, in IEEE JSAC 2006.
18. Xin Liu and Xiaowei Yang, David Wetherall and Thomas Anderson, “Efficient and Secure Source Authentication with Packet Passports”, SRUTI ’06.
19. Heejo Lee, Minjin Kwon, Geoffrey Hasker and Adrian Perrig,”BASE: An Incrementally Deployable Mechanism for Viable IP Spoofing Prevention,” ASIACCS’07, 2007, Singapore.
20. David G. Andersen, Hari Balakrishnan, Nick Feamster, Teemu Koponen, Daekyeong Moon and Scott Shenker. Accountable Internet Protocol (AIP). In Proc. SIGCOMM, Aug 2008, Seattle, WA.
21. R. Beverly, A. Berger, Y. Hyun, and k claffy, “Understanding the efficacy of deployed internet source address validation filtering”, Proc. 9th ACM SIGCOMM conference on Internet measurement conference, pp. 356–369, 2009.
22. David Talbot, “The Internet Is Broken”, Technology Review, December 2005/January 2006, MIT Press.
23. S. Savage et al., “Network Support for IP Traceback,” IEEE/ACM Trans. Net., vol. 9, no. 3, June 2001, pp. 226–37.

Reference

24. H. Burch and B. Cheswick, “Tracing Anonymous Packets to Their Approximate Source,” Proc. USENIX LISA, 2000, pp. 319–27.
25. Yaar, A; Perrig, A; Song, D, “StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense” IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 2006, 24(10):1853-1863
26. Goodrich, MT, “Probabilistic packet marking for large-scale IP traceback,” IEEE-ACM TRANSACTIONS ON NETWORKING, 2008, 16 (1): 15-24.
27. Castelucio, A; Ziviani, A; Salles, RM, “An AS-Level Overlay Network for IP Traceback,” IEEE NETWORK, 2009, 23(1): 36-41.
28. A. C. Snoeren et al., “Hash-based IP Traceback,” SIGCOMM 2001.
29. Minho Sung; Jun Xu; Jun Li, et al., “Large-scale IP traceback in high-speed Internet: practical techniques and information-theoretic foundation,” IEEE/ACM Transactions on Networking, 2008, 16(6): 1253-66.
30. S. M. Bellovin, “ICMP Traceback Messages,” IETF draft, 2003, http://tools.ietf.org/html/draft-ietf-itrace-04.