

COMPUTER SECURITY

ACCESS CONTROL
(AUTHORIZATION)

Willy Sudiarto Raharjo

Teknik Informatika
Universitas Kristen Duta Wacana

Authorization

Restrict action of authenticated user



- Authentication - Who goes there?
 - Restrictions on who (or what) can access system
- **Authorization** - Are you allowed to do that?
 - Restrictions on actions of authenticated users
- Authorization is a form of **access control**
- Authorization enforced by
 - Access Control Lists
 - Capabilities

Lampson's Access Control Matrix

- **Subjects** (users) index the rows
- **Objects** (resources) index the columns

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rX	rX	r	---	---
Alice	rX	rX	r	rw	rw
Sam	rWX	rWX	r	rw	rw
Accounting program	rX	rX	rw	rw	rw

Access Control List

- **Access control matrix** has all relevant info
- But how to manage a large access control (AC) matrix?
 - Could be 1000's of users, 1000's of resources
 - Then AC matrix with 1,000,000's of entries
 - Need to check this matrix before access to any resource is allowed
 - Hopelessly inefficient

Access Control List

- ACL: store access control matrix by **column**
- Example: ACL for **insurance data** is in **blue**

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwX	rwX	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

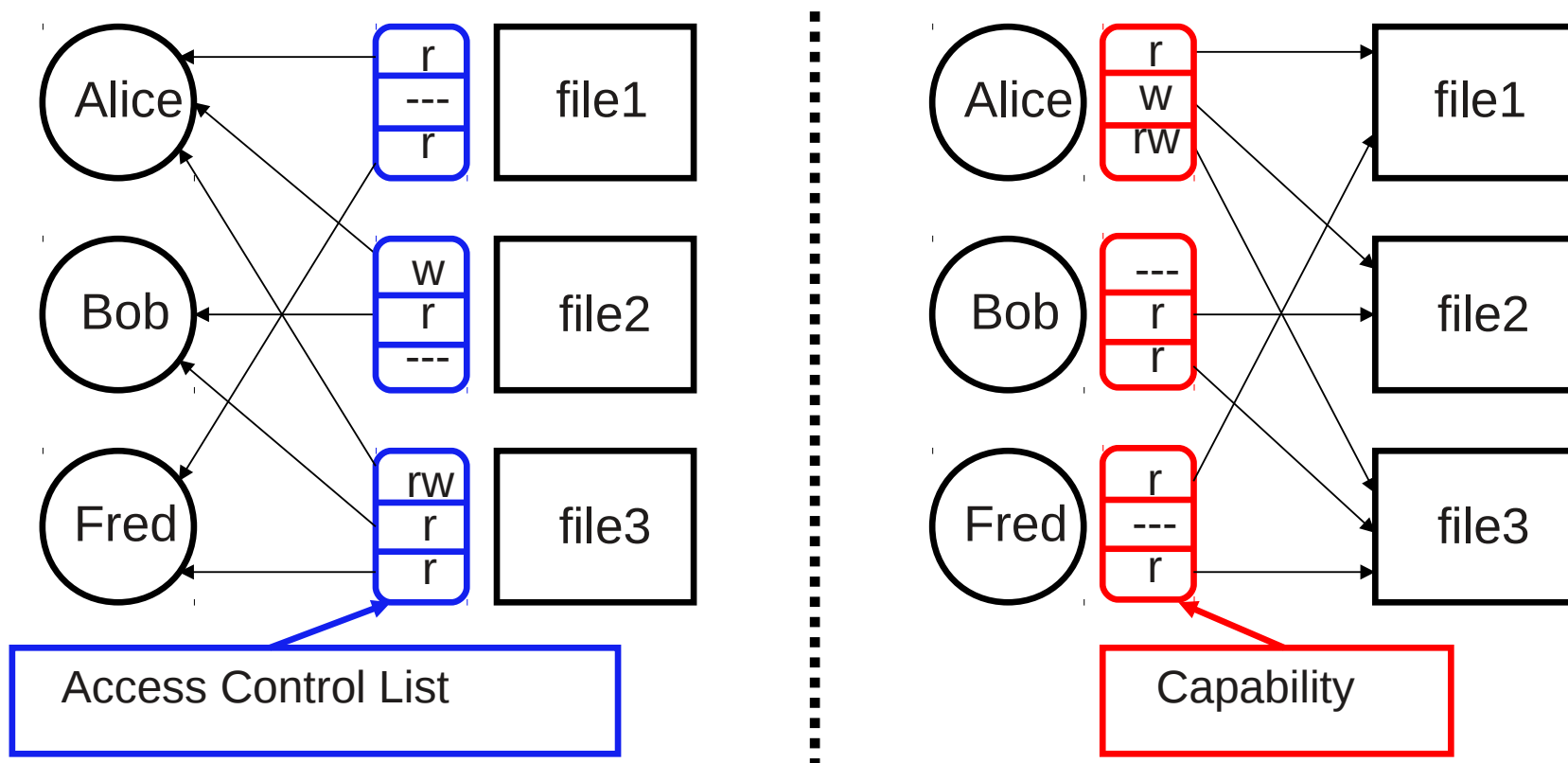
Capabilities (or C-Lists)

- Store access control matrix by **row**
- Example: Capability for **Alice** is in **red**

	OS	Accounting program	Accounting data	Insurance data	Payroll data
Bob	rx	rx	r	---	---
Alice	rx	rx	r	rw	rw
Sam	rwX	rwX	r	rw	rw
Accounting program	rx	rx	rw	rw	rw

ACLs vs Capabilities

- Note that arrows point in opposite directions!
- With ACLs, still need to associate users to files



ACLs vs Capabilities

- ACLs

- Good when users manage their own files
- Protection is data-oriented
- Easy to change rights to a resource

- Capabilities

- Easy to delegate
- Easy to add/delete users
- Easier to avoid the confused deputy
- More difficult to implement
- Capabilities loved by academics

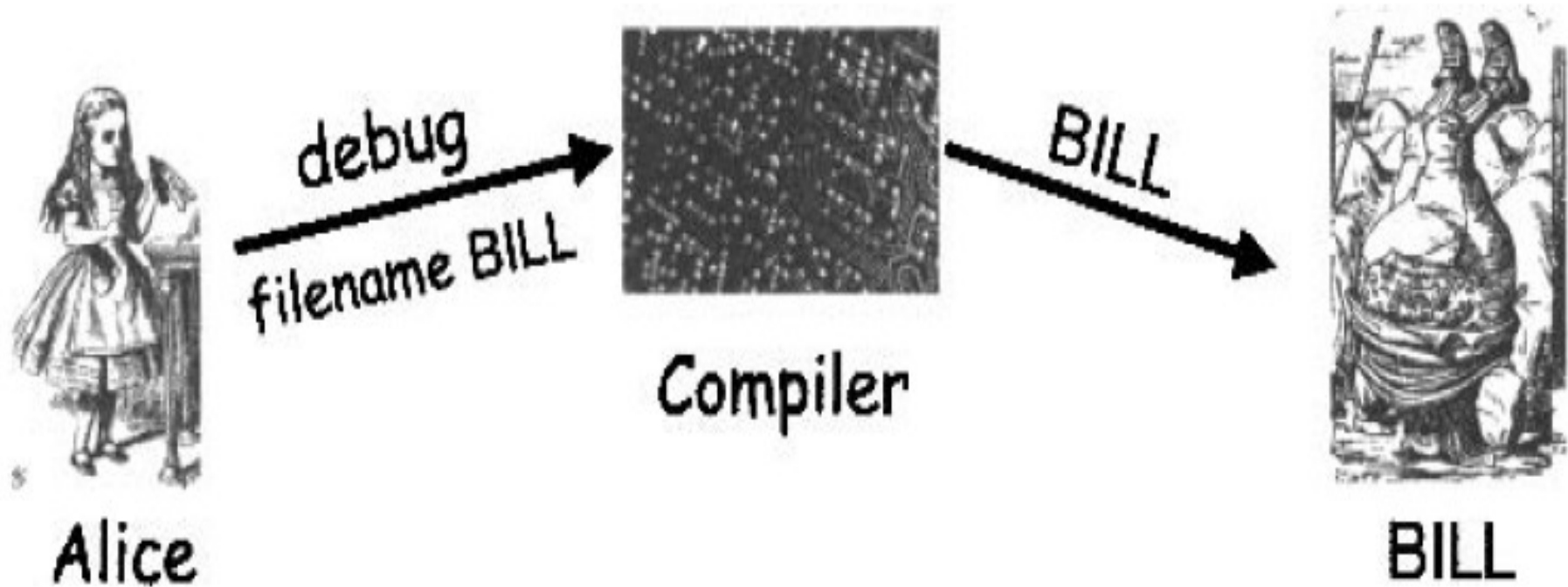
Confused Deputy

	Compiler	BILL
Alice	x	—
Compiler	rx	rw

BILL is a sensitive data

What if Alice tries to invoke the compiler
using BILL as the input?

Confused Deputy



CAPTCHA

- Turing Test

- Proposed by Alan Turing in 1950
- Human asks questions to one other human and one computer (without seeing either)
- If human questioner cannot distinguish the human from the computer responder, the computer passes the test
- The gold standard in artificial intelligence
- No computer can pass this today

CAPTCHA

- CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart
- Automated - test is generated and scored by a computer program
- Public - program and data are public
- Turing test to tell... - humans can pass the test, but machines cannot pass the test
- Like an inverse Turing test (sort of...)

CAPTCHA: Rules of the Game

- Must be easy for most humans to pass
- Must be difficult or impossible for machines to pass
 - **Even with access to CAPTCHA software**
- The only unknown is some random number
- Desirable to have different CAPTCHAs in case some person cannot pass one type
 - Blind person could not pass visual test, etc.

Example

- Test: Find 2 words in the following



- Easy for most humans
- Difficult for computers (OCR problem)

Other Example

Google accounts

Email

willysr@gmail.com

Kata sandi:

Ketik karakter yang Anda lihat pada gambar di bawah ini.

Waxehoni

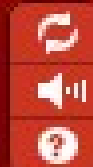
Abjad tidak peka huruf besar-huruf kecil

Buka kunci

overlooks

inquiry

Type the two words:



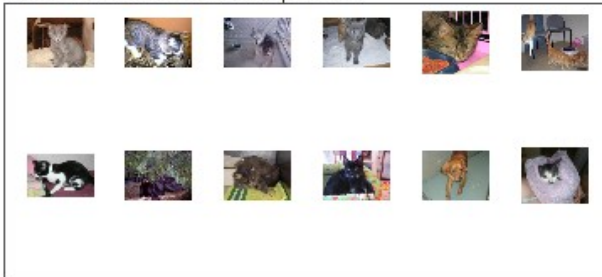
reCAPTCHA™
stop spam.
read books.

ASIRRA



Asirra is a human interactive proof that asks users to identify photos of cats and dogs. It's powered by over three million photos from our unique partnership with Petfinder.com. Protect your web site with Asirra 💎 free!

Please select all the cat photos:



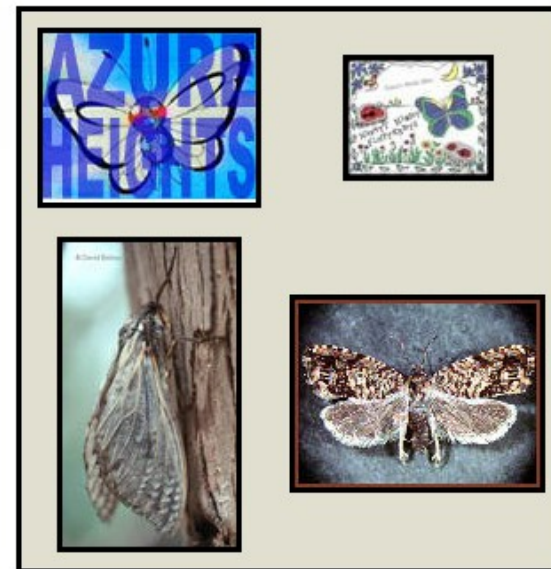
Score Test



Submit

<http://server251.theory.cs.cmu.edu/cgi-bin/sq-pix>

The CAPTCHA project



Choose a word that relates to all the images.



TIP: You can type the first letter of a word and then use the down arrow to find it.

Submit

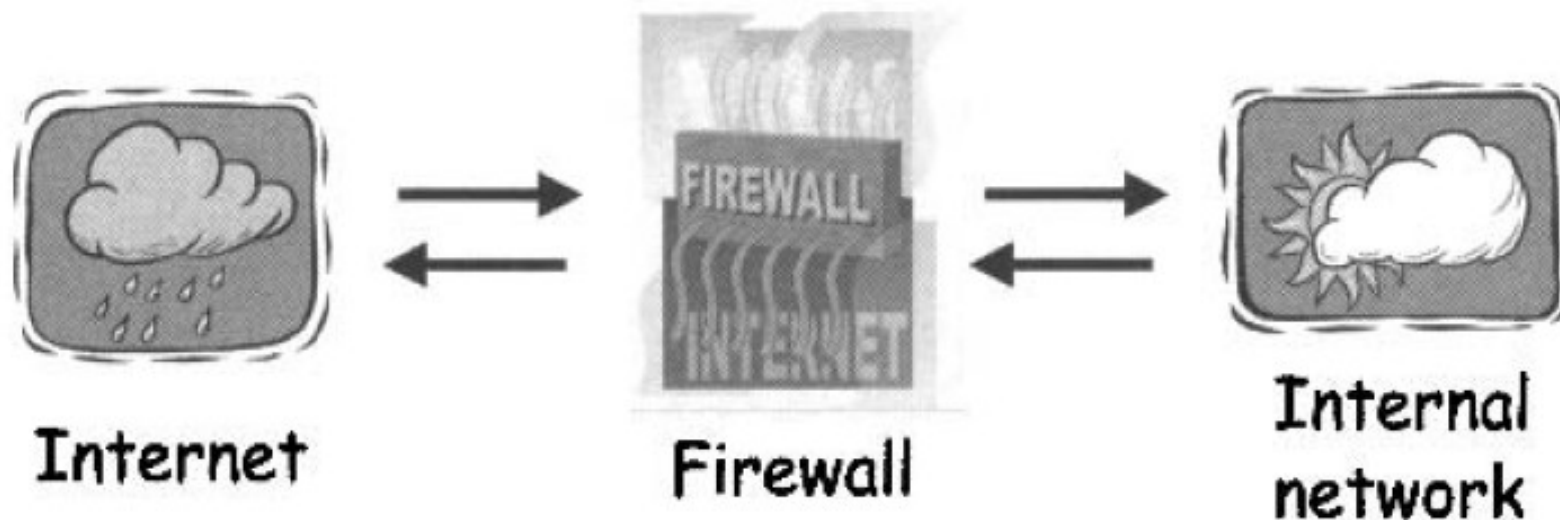
© 2004 Carnegie Mellon University, all rights reserved.

<http://server251.theory.cs.cmu.edu/cgi-bin/esp-pix/esp-pix>

<http://research.microsoft.com/en-us/um/redmond/projects/asirra/>

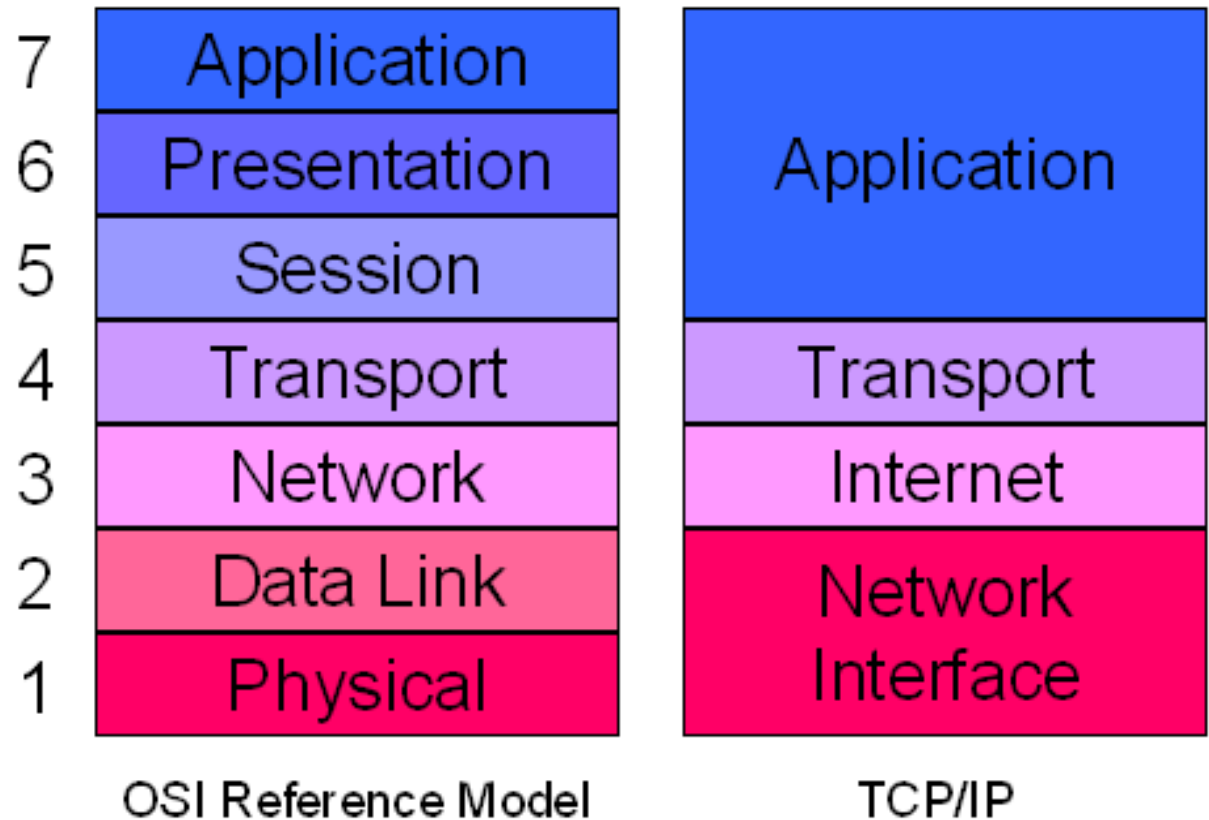
Firewall

- Examine request to access the internal network from public network (Internet)
- Decide to pass or not using rules



Firewall Classifications

- Packet Filters
 - ◆ Network Layer
- Stateful Packet Filter
 - ◆ Transport Layer
- Application Proxy
 - ◆ Application layer

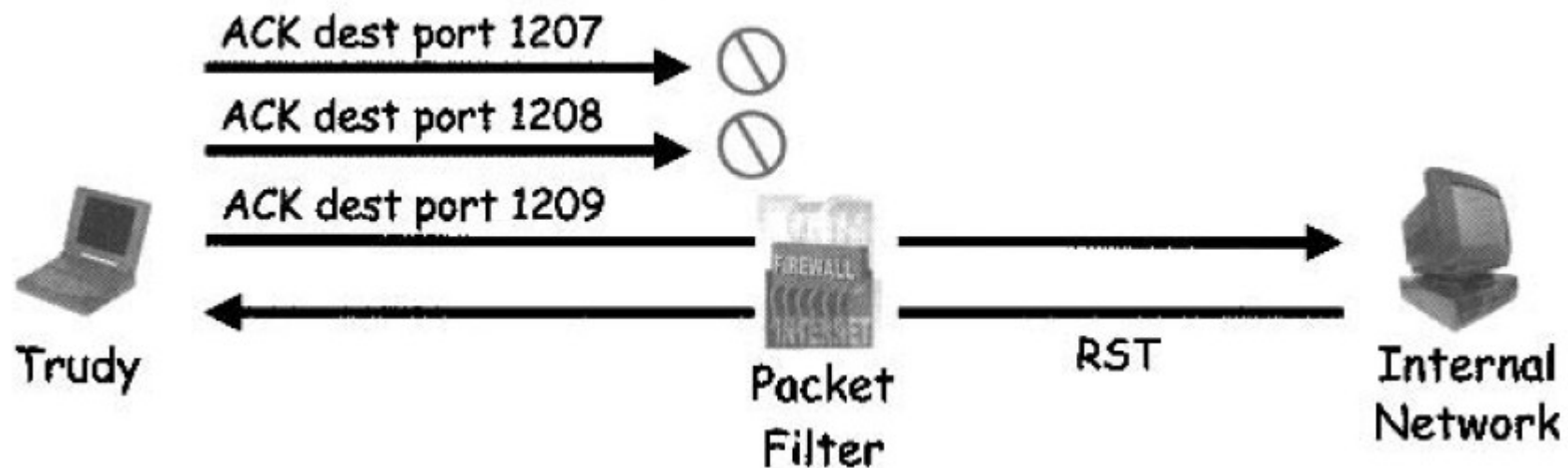


Packet Filter

- Filtering based on information available
 - ◆ Source/Destination IP Address
 - ◆ Source/Destination Port Numbers
 - ◆ TCP Flag Bits
- Efficient in processing
 - ◆ Only processing the headers
- No concept of state
 - ◆ Each packet is treated independently
 - ◆ Can't examine TCP connection

Typical ACL

Action	Source IP	Dest IP	Source Port	Dest Port	Protocol	Flag Bits
Allow	Inside	Outside	Any	80	HTTP	Any
Allow	Outside	Inside	80	> 1023	HTTP	ACK
Deny	All	All	All	All	All	All



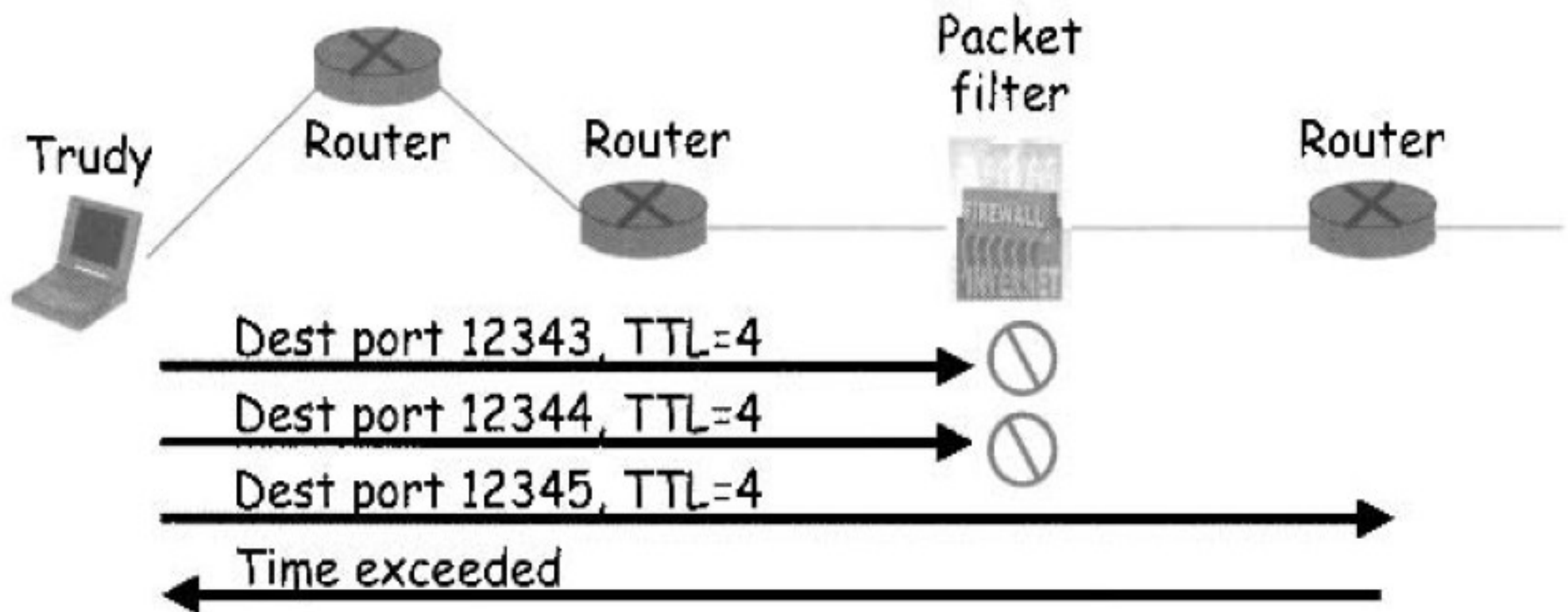
Stateful Packet Filter

- Keeps track of TCP/UDP connection
- Advantages
 - ◆ Keeps track of ongoing connection
 - ◆ Able to prevent many attacks that can't be filtered by normal packet filter
- Disadvantages
 - ◆ Can't examine application data
 - ◆ Much slower as more processing is conducted

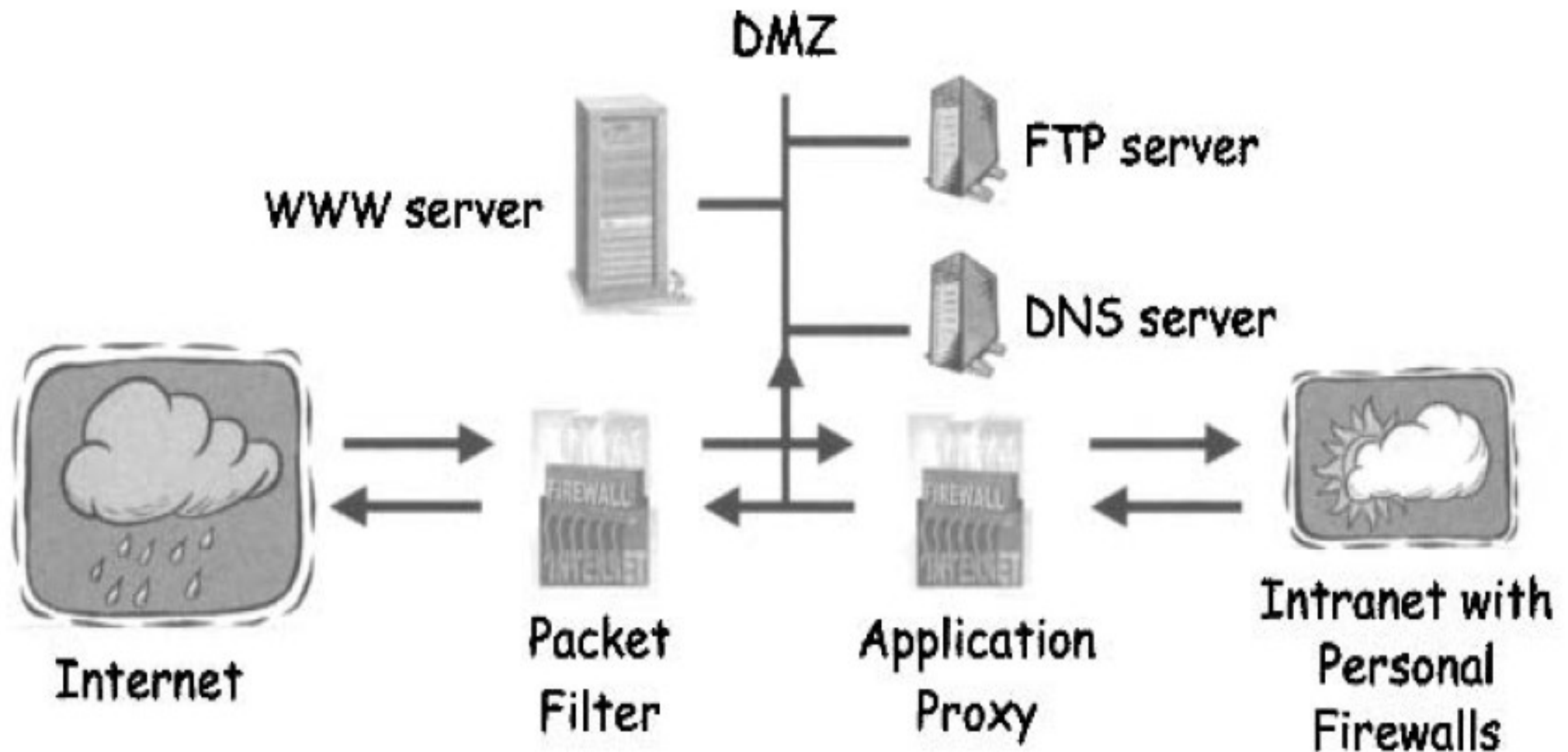
Application Proxy

- Able to verify data inside the packet is safe
- Advantages
 - ◆ Complete view of connection and application data
 - ◆ Able to filter bad data (such as viruses)
- Disadvantages
 - ◆ Slower than previous types
- Packet will be re-created when passing through the firewall
 - ◆ Able to stop firewalk attack

Firewalk



Defence in Depth



Intrusion Detection

- Detect attacks before, during, and after they have occurred
- Two methods of Intrusion Detection
 - ◆ Signature-based
 - Similar to how AV works
 - ◆ Anomaly-based
 - Provide warning if the system behave far from baseline behavior
- Basic Achitecture
 - ◆ Host-based IDS
 - ◆ Network-based IDS

Examples

d85bd44d3eac9aaa8fa4 d85bd44d3eac
6ee04e454278fac09321 6ee04e454278

Spam is grouped by sender and only shows first line

Zosuyrsa | mirazm@yahoo.com | hydroc.awardspac.com/prescription.html | 3 comments

Buy hydrocodone cod overnight Hydromet syrup medication Hydrocodone 5 500 Hydrocodone addiction wit
wellbutrin snorting siteap [URL= http://pastushca.isuisse.com/wellbutrin/siteap.html.com]wellbut
Cool...

Baksaki | mBXMS58@gmail.com | mbyqwo.com/vpg | IP: 207.44.238.95 | 3 comments

Vouloir juste dire bonjour, aujourd'hui un jour frais :) pa7 Cheap Airfare In Europe * Americ
Querer apenas dizer Bello, hoje um dia fresco :) HRT American Airlines Jobs * Airtrea * Blue Jet Air
Nice!

uiofthgkjsh | 4dorsyt52@mail.ru | japansearchf.com.cn | IP: 195.244.128.231 | 3 comments

buy VIAGRA online Buy Viagra Online! Buy Viagra! Generic Viagra! Order Viagra! Cheap Viagra buy V
buy tramadol online Buy Tramadol Online! Buy Tramadol! Generic Tramadol! Order Tramadol! Cheap Tran
buy VIAGRA online Buy Via gra Online! Buy

3 spams from the same IP address

Pzwfuox | qfrmzwco@giddkb.com | 100worldbest.com | 3 comments

viagra alternatives [url=http://www.100worldbest.com/cgi-bin/brick.cgi?user=viagraalternatives]viagr
tramadol hel [url=http://www.qkxyq.com/cgi-bin/ib19/topic.cgi?forum=9&topic=88]tramadol hel[/url
order phentermine [url=http://www.miamisci.org/eff/abb/Forum1/HTML/001038.html]order phentermine[/ur