CS 458 Information Security

Homework 1: Administrivia, Historical Cryptography

**1. Administrivia**

(a) Are following activities encouraged (E) or forbidden (F)?

[Encouraged] Discussing course materials on piazza

[Encouraged] Discussing homework problems

[\*see below] Sharing your homework solution with others

[Forbidden] Sharing quiz answers

[Forbidden] Looking at others’ exam

\* While normally sharing homework solution is a violation of academic integrity,

this course has only ungraded homework, therefore, you’re free to share and discuss your

solutions with your classmates. However, we strongly recommend you to finish each

homework independently before such discussion.

(b) Where can you find a copy of the textbook (and other resources) for free?

IIT Library

(c) [False] Going through slides will be enough review for exams.

(d) What “pain points” do you anticipate for this class? How should you prepare for

them?

This introductory course will touch on a variety of subjects, some of which you

might not have sufficient background in. Solution: Google a lot. Piazza a lot. Read

a lot. Ask a lot. And while you’re at it, help each other!

**2. Key concepts**

(a) The three most important components of computer security, known as the “CIA

triad”, are what?

Confidentiality, Integrity, Availability.

(b) Read the scenario, and identify each item as a threat, an asset, a vulnerability, an

attack, a countermeasure, or an adversary.

**Scenario**: A hypothetical student broke into an office, installed a keylogger,

intercepted login and password, and obtained the hypothetical final exam

ahead of time. Department found out, replaced the hypothetical exam,

and checked all computers for keyloggers.

**Identify**:

o (adversary) the hypothetical student

o (asset) the hypothetical final exam

o (threat) that the student wants (and is able) to obtain the exam ahead of time

o (vulnerability) that the lock on the door can be picked

o (attack) that the exam was stolen

CS 458 Information Security

o (countermeasure) that the department swept for keyloggers

(c) Bonus: identify other threats and vulnerabilities in the above

scenario. Answers may vary.

**3. Intro to Crypto**

(a) Fill in the blanks:

Plain texts are encrypted with a key and an encryption function; the results are

called cipher text, which can be decrypted with a key and a decryption function.

(b) [True] It is common practice to assume the adversary knows the cipher we’re

using.

(c) Is the following attack: cipher text only, **known plain text**, or chosen plain text?

In World War II, Germans used machines called “Enigma”

to encrypt their communications. The code was broken partly

because the allies learned that one message always started

with “nothing to report” and was sent daily using that day’s

rotor configuration.

(d) The mixture of a substitution cipher and a transposition cipher is called a

product cipher.

(e) Encrypt the following text with Caesar cipher and a key of 12 (A -> M, etc.)

TO BE OR NOT TO BE THAT IS THE QUESTION

FA NQ AD ZAF FA NQ FTMF UE FTQ CGQEFUAZ

(Quote by William Shakespeare)

(f) Decrypt the following text; it’s encrypted with Caesar cipher with unknown key

CKSAY ZGIIK VZLOT OZKJO YGVVU OTZSK TZHAZ TKBKX RUYKO TLOTO

ZKNUV K

WEMUS TACCE PTFIN ITEDI SAPPO INTME NTBUT NEVER LOSEI NFINI

TEHOP E

(“*We must accept finite disappointment, but never lose infinite hope*.” -- Martin Luther

King, Jr.)

Hint: There are two ways to solve this problem.

1. Exhaustive search. There are only 26 possible keys; try them all and choose

the one that makes most sense.

2. Statistical analysis. K is the most frequent letter in cipher text, and E is the

most frequently used letter in the English language. Assuming the plain text

is English, guess that E encrypts to K. This approach can be further

elaborated in mathematics and automated.

CS 458 Information Security

(g) How long must the key be to encrypt the following message with one-time pad

(ignore spaces)?

THE DIFFERENCE BETWEEN STUPIDITY AND GENIUS IS THAT GENIUS

HAS ITS LIMITS

62. (Quote by Albert Einstein)

(h) Bonus: decrypt the following text; it’s encrypted with Vigenere cipher with

unknown key

KBPIW LJMUM WLQNM QQWUQ MEEKV PXESJ UBHNX AOMLQ XOCAM PISIM

HNAAU LHUML YILBL WCOXW JXQWE QWZPM LAMLY ILBLW GXHKL GHJXT

MWHQM EEKVP XMTGE PHNMF EZXLY DKBRQ XOCAM PIKGI LWRGH TBOLL

KBPIW LJMLM EKQVH NHSTS GMWKK BPIWL JMLXV APOHN LGRMB BASUB

AMAAP BXZSX FMLXE AT

ITWAS THEBE STOFT IMESI TWAST HEWOR STOFT IMESI TWAST HEAGE

OFWIS DOMIT WASTH EAGEO FFOOL ISHNE SSITW ASTHE EPOCH OFBEL

IEFIT WASTH EEPOC HOFIN CREDU LITYI TWAST HESEA SONOF LIGHT

ITWAS THESE ASONO FDARK NESSI TWAST HESPR INGOF HOPEI TWAST

HEWIN TEROF DESPA IR

(“*It was the best of times, it was the worst of times; it was the age of wisdom, it was the*

*age of foolishness; it was the epoch of belief, it was the epoch of incredulity; it was the*

*season of light, it was the season of darkness; it was the spring of hope, it was the*

*winter of despair.*” - Charles Dickens, *A Tale of Two Cities*)

Hint: look for repeated patterns. For example, KBPIWLJML occurred twice and this

is probably not a coincidence. The two occurrences are 24 positions apart, so the

period is likely a factor of 24. Look for other repeated patterns and determine the

period, and then separate the Vigenere-ciphered text into as many Caesar ciphered

texts.

**4. Super Bonus**

Write an automated Vigenere cipher solver.

Hint: Start by building two programs, one to help you find the period, the other to

decipher the message given a period.

CS458 Information Security

Homework 2: Block Cipher, Symmetric Cryptography

**1. Stream Cipher, Block cipher**

(a) Identify each of the following as: a stream cipher (S), or a block cipher (B).

[stream cipher] One-time pad

[stream cipher] Vigenere cipher

[block cipher] AES

(b) A good block cipher exhibits *avalanche effect*: if we flip one bit in the plain text,

half of the bits are flipped in the cipher text.

Two messages of the same length, *m1* and *m2*, differ by 5 bits. With a good block

cipher, how many bits differ in the two resulting cipher texts? Assume both cipher

texts are *n* bits long.

*n*/2 bits.

(c) Generally, block ciphers are slower than stream ciphers.

(d) What advantages do block ciphers have over stream ciphers?

Block ciphers are the building blocks of many modern cryptographic tools:

• Creating pseudo random number (e.g. one-time pads)

• Constructing hash functions

• Creating MACs

• etc.

**2. DES and AES**

(a) If you are starting a new project that does not depend on other legacy programs,

which cipher would you use, 3DES or AES? Justify your answer.

AES.

• It’s faster.

• It has a larger key space (mitigates exhaustive search).

• It has a larger block size (therefore the same key can encrypt more messages

before it is compromised).

(b) Why is DES broken? Why is 2DES insecure?

The key space of DES is too small (256), and an inexpensive exhaustive search can

be easily done today.

For 2DES, one can launch a meet-in-the-middle attack that reduces the time of an

exhaustive search to around 257 , which is significantly smaller than its key space size

2112 .

(c) **Bonus**: 3DES is often implemented as E(*k3*, D(*k2*, E(*k1*, m))). Why the decryption

in the middle?

1

CS458 Information Security

This is a hack for backwards compatibility -- if we let *k1* = *k2* = *k3* = *k* then 3DES(*k1*,

*k2*, *k3*, *m*) = DES(*k*, *m*).

(d) **Bonus**: both AES and DES use substitution boxes (S-boxes) as part of the

encryption algorithm. For which cipher are the S-boxes invertible? Why could you

decrypt messages using the other cipher when its S-boxes are non-invertible?

AES’s S-boxes are invertible.

DES uses Feistel Network, which doesn’t require the S-boxes to be invertible.

**3. Block cipher modes**

(a) What is the ECB mode? Why should it never ever be used? What modes could

you use instead?

**E**lectronic **C**ode **B**ook mode. It always encrypts the same plain text to the same

cipher text, thereby leaking information about the plain text to the attacker.

You should use, say, CBC (cipher block chaining) or CTR (randomized

counter) modes instead.

*Caveat Lector*! Improperly using CBC or CTR modes could also result in

information leak.

(b) What is a nonce?

It’s a number that’s never used more than once. Often, but not always, the

nonce is randomly generated.

CS 458 Information Security

Homework 3: Cryptographic Hash and MAC, Asymmetric

Cryptography

**1. Crypto Hashes and MACs**

(a) What property must a good cryptographic hash function have?

Collision resistant. There are three levels of collision resistance (see slides); a

good hash function satisfies all of them.

(b) CRC, or cyclic redundancy check, is a message digest that is used to detect

transmission errors. Why shouldn’t we use CRCs as MAC?

CRCs are sent in the clear, and are designed to detect random errors

instead of malicious errors. For a MAC to be useful, it has to be keyed.

(c) Name one situation where integrity is of utmost importance but confidentiality

is not of concern.

Distribution of open source software (e.g. Linux). We want to make sure end

users only download what we want them to, but the content of the files don’t need

to be kept secret.

(d) **Bonus**: *r1*, *r2*, ..., *rn* are independent random variables uniformly distributed

among {1, 2, ..., *B*}. In terms of *B*, what’s the smallest *n* such that ∃*i*≠*j*, *ri* = *rj* with

probability >1/2?

About 1.2 × *B*1/2. Note that as long as {*ri*} are independent and identically

distributed, *n* will be no larger than this number for a collision to be more likely

than not.

(e) **Bonus**: given collision resistant hash function H, how is HMAC

constructed? What are *ipad* and *opad*? What do they stand for?

HMAC(*k*, *m*) = H( *k* ⊕ *opad* || *I* ) where *I* = H(*k* ⊕ *ipad* || *m*)

ipad = 0x36363636... is the inner pad. (0x36 = 001101102)

opad = 0x5c5c5c5c... is the outer pad. (0x5c = 010111002)

**2. Public Key Crypto**

(a) Unlike symmetric ciphers, an asymmetric cipher uses two different keys for

encryption and decryption: a public key and a private key. Which key is used to

encrypt and which to decrypt? (Hint: *hint hint*.)

Both can be used to encrypt or decrypt. Messages encrypted with one key can be

decrypted with the other key.

CS 458 Information Security

(b) A good asymmetric cipher should make the following tasks easy (E) or hard (H)?

[Easy] Generate a key pair

[Easy] Encrypt a message with a public key

[Easy] Decrypt a message with corresponding private key

[Hard] Compute private key given public key

[Hard] A message is encrypted with a public key: decrypt this message given

this public key

(c) Asymmetric cryptography is generally slower than symmetric cryptography

(d) What can we do with asymmetric cryptography that we can’t with symmetric

cryptography?

• Establish session keys

• Authenticate origin of message

• Encrypt message non-interactively (DH)

• etc.

**3. Diffie-Hellman and RSA**

(a) Which protocol would you use to send an encrypted email to your friend, DH

or RSA? Justify your answer.

Diffie-Hellman.

No interaction is required between the two parties to establish a secret key, which

is perfect for emails because they bounce between numerous relay servers before

reaching their destination.

(b) What hard problem does Diffie-Hellman protocol depend on? What

hard problem does RSA depend on?

DH: Discrete Logarithm

RSA: Factorization of big numbers

(c) **Bonus**: φ(*n*) is the number of integers in {1, 2, ..., *n*} relatively prime to *n*. Prove if

*p*, *q* are prime, then φ(*pq*) = (*p*-1)(*q*-1).

In {1, 2, …, *pq*}, *q* numbers are multiples of *p*, and *p* numbers are multiples of *q*,

but we counted *pq* twice. Therefore φ(*pq*) = *pq* – *q* – *p* +1 = (*p*–1)(*q*–1).

CS 458 Information Security

Homework 4: Key Management and Identity

**1. Trusted Third Party**

(a) A trusted third party solves what problem in key management?

Number of keys grows quadratically with the number of parties.

(b) Assuming the third party is indeed trustworthy (i.e. not malicious, e.g. the auth

center in a corporate network), what attacks can compromise the key exchange?

Eavesdropping then replaying

Man-in-the-middle

(c) **Bonus**: In the Needham-Schroeder protocol, what are “*r*1” and “*r*2” called?

What attack do they prevent?

Nonces. Replay attacks.

**2. Digital Signatures**

(a) Bob received a 128-bit AES key and the message “from Alice: use this key to send

me your credit card number”, both encrypted with his public key. Should he do what

the message says? Assume Bob does want to send Alice his credit card number.

No. There’s no way to confirm the message actually came from Alice. Anyone

could have encrypted such a message with Bob’s public key.

\* The wording of this problem is lengthy and awkward to avoid stating “Alice

sent the message”.

(b) We discussed “meet-in-the-middle” attack last week. We’ll talk about “man-inthe-

middle” attack this week. They are completely different concepts, despite

their similar names. Explain what each attack is.

**Meet-in-the-middle**: this was introduced to explain why 2DES was insecure; in

general, a meet-in-the-middle attack occurs when we can split the exhaustive

search for keys into two independent, smaller searches (trading space for time).

**Man-in-the-middle**: this is describing an active attacker that does more than

eavesdropping, and actually tampers with the traffic. A (wo)man-in-the-middle

intercepts messages and replaces them with fraudulent ones of his/her choice.

(c) Digital signatures bind identity to the message.

(d) How are digital signatures different from MACs?

MACs verify the integrity of the message (i.e. it has not been tempered with). When

CS 458 Information Security

used correctly, MACs together with ciphers provide authenticated encryption (both

confidentiality and integrity). Still, you can’t be sure who you’re talking to unless

the message comes with a digital signature (you could be receiving untampered

messages from an attacker).

**3. Web of Trust**

(a) When you visit a website whose URL starts with “https://“, what protocol

are you using?

SSL/TLS. TLS is the new SSL.

(b) When you click on the lock in the address bar on a secure website, it shows

you a certificate. What does a certificate do?

It confirms you’re actually talking to Google and not a malicious site pretending

to be Google.

(c) When you go to your bank’s website and your browser prompts “this

website cannot be trusted”, what just happened?

Your browser is trying to connect with SSL/TLS but the certificate cannot confirm

the site you’re visiting is your bank. Possible causes include (*not* exhaustive):

a. The certificate expired

b. The domain name you’re trying to visit doesn’t match what’s on

the certificate

c. You’re talking to a man in the middle

d. The certificate is self-signed (“Hi, my name is bank; nice to meet you.”)

e. There’s no certificate at all

(d) **Bonus**: in practice, who decides which root certificates are trustworthy?

Your browser. Each browser ships with a list of root certificates they trust, and

the chain of trust starts there.

(e) **Bonus**: can you create a certificate for google.com?

Sadly, yes. Managing the web of trust is a very delicate issue with many

non-technical aspects.

CS 458 Information Security

Homework 5: User Authentication, SSL/TLS

**1. Authentication**

(a) iPhone includes a fingerprint scanner which the user can choose (not) to use.

Do you think activating fingerprint scanning would increase the security of the

cellphone?

Answers may vary. Consider the following points when answering:

• Biometrics has a false positive and false negative rate, especially finger

prints.

• iPhone’s fingerprint scanner is nowhere near industrially secure level.

• iPhone’s fingerprint scanner must be used in conjunction with a

password (each reboot requires the user to enter the password before

they can use fingerprints again.)

(b) Bloom filter is an efficient way to preemptively reject bad passwords with high

efficiency, but it has a false positive rate (incorrectly rejecting good passwords).

What can you do to decrease the chance of a false positive?

Bloom filter’s false positive rate is approximately (1 – e-*kB*/*N*)*k*, so to reduce

false positives, we can increase the number of bits used for the hash functions

(make hash outputs longer).

Note that Bloom filter will never give a false negative (incorrectly accepting a

bad password). Why?

(c) A hotel uses the S/key system to verify if a key card is valid. Alice checks into the

hotel and obtains a key card with password H99(x) where H is a secure hash

function and x is some constant value. She successfully gets into the room. At this

point, Alice’s room lock will accept key card(s) with what password(s)?

H99(x) and H98(x).

(d) **Bonus**: In the historical novel Ivanhoe by Sir Walter Scott, jester Wamba said “If

anyone says anything to you, just say *Pax vobiscum*”. What does *Pax vobiscum* mean?

Peace be with you.

**2. Password Security**

(a) It is common practice not to store user’s password in clear text. However, if an

attacker has seized control of the database, he is likely already capable of

modifying any user data on the site as an administrator. Why bother hashing the

passwords then?

CS 458 Information Security

To prevent attacks on password reuse. Many people use the same username and

password across multiple sites (even their primary email address and bank

account!), so it is important that the compromise of one site does not bring hell

to the user

(b) It is common practice to salt the user’s password in addition to hashing. What

attack does this practice prevent?

To prevent rainbow attack. Without salt, the same password with always be hashed

to the same value (with the same hash function), and attackers have made precalculated

tables for reverse-lookup of common or short passwords. Play with a

rainbow table here: https://crackstation.net/ (you can generate hashes here:

http://www.fileformat.info/tool/hash.htm)

*Caveat Lector*! Do not type your real passwords into these websites (especially the

latter one). Why?

**3. SSL**

(a) What is perfect forward secrecy? What’s one way to achieve it, as websites today

are using?

Perfect forward secrecy means if a session key is compromised, all messages

that are encrypted before that message should still be safe.

Websites today usually generate new public/private key pairs for each new session.

(b) IPSec: Which mode includes the IP header inside the encryption, transport mode

or tunnel mode?

Tunnel mode.

CS 458 Information Security

1

Homework 6: Access Control

**1. Concepts**

(a) The three most important components in access control, all starting with the

letter ‘A’, are what?

Authentication (verifying the user is who he says he is),

Authorization (verifying the user is allowed to execute the command),

Audit (a log of all events for future reference).

(b) Three models of access control we’ll talk about in class are DAC, MAC and RBAC.

What do they stand for?

**D**iscretionary **A**ccess **C**ontrol (owner of object decides who has access at her

*discretion*),

**M**andatory **A**ccess **C**ontrol (user *must* have certain clearance, even if the owner

allows access),

**R**ole-**B**ased **A**ccess **C**ontrol (users are assigned *roles*, and permissions are

given to roles).

(c) In access control, what does an “open policy” mean? What does a “closed policy”

mean?

An open policy allows all access except where noted (uses a blacklist).

A closed policy forbids all access except where noted (uses a whitelist).

(d) What did MAC stand for in cryptography? **Bonus:** what does MAC usually

stand for in networking (as is “MAC address”)?

Message Authentication Code.

Media Access Control. This is not quite the same ‘access control’ as what

we’re talking about right now.

**2. Access Control Matrix**

(a) Three important elements in access control are subjects, objects and access

rights. In an access control matrix, how are the three elements presented?

Each row is a subject. Each column is an object. Each intersection denotes what

access rights that subject has on that object.

CS 458 Information Security

2

(b) [False] “Objects” are another name for the files on a system.

Objects often refer to files, but can be any resource on a computer (such as a

network port or a mutex).

(c) An access control matrix is often sparse, and in implementation people generally

use some other data structures. What are some common ways to implement an

access control matrix?

Access Control Lists (slice by column, used by most modern OS),

Capability Lists (slice by row, sometimes known as *capability tickets* because they

can be passed around to grant other users access),

Authorization Table (list of all triples (subject, object, access right) in the matrix).

**3. Principles**

(a) What does *least privilege* mean? What problems could *least privilege* prevent?

A user executing a command should not have more privilege than needed for that

command.

It prevents user error, as well as malicious activities carried out in the user’s name.

This is why sometimes the OS warns you when you try to sudo (run as admin).

(b) What does *separation of duty* mean? What problems could *separation of duty*

prevent?

A single user should not have enough power to corrupt the entire system (or

any major part of it).

This prevents conflicts of interest, as well as fraud (both by humans and

by malicious programs).

Separation of duty is a more than a computer security principle. The major idea is

that the more people needed to do a certain task, the more difficult it is for them

to collude and do harm.

In security we *always* assume the worst of people.

**4. RBAC**

(a) What advantages does role-based access control have?

RBAC is:

• Flexible (can implement a wide range of access control policies)

• Inexpensive (costs less to administrate)

• Easy to use (less likely for administrators to make mistakes, especially for a

system with 500+ users).

Answers may vary. It’s hard to define what RBAC exactly is because there are many

different interpretations and implementations, but they all share certain properties

like the ones listed above.

CS 458 Information Security

3

(b) Core RBAC specifies users, roles, permissions and sessions. What does RBAC1

add on top of core RBAC? What does RBAC2 add on top of core RBAC?

RBAC1 supports role hierarchy.

RBAC2 supports role constraints, such as *exclusive roles* or *prerequisite roles*.

RBAC3 is a consolidated model that supports everything in RBAC0, 1 and 2.

(c) [True] RBAC supports the principles of *least privilege* and *separation of duty*.

CS 458 Information Security

1

Homework 7: Mandatory Access Control

**1. Mandatory Access Control**

(a) [False] In MAC, resource owners can override system policy and allow other

users access to his resources when the system forbids it.

In MAC, access control is executed at the system level. Users can’t change their own

security clearance or that of any resource they own. If the system denies access, that

decision has to be obeyed.

(b) What is the principle of tranquility? Which principle supports least privilege

better, strong tranquility or weak tranquility?

Principle of tranquility states the security clearances of subjects and objects should

rarely change (never change in strong tranquility).

Weak tranquility supports least privilege better, because all subjects can start with

the lowest clearance and gain access as needs require.

**2. Bell-LaPadula model**

(a) An idiom in the BLP model is “no read up, no write down”. What does

“write” mean here?

It means append, or write extra data into a file without reading or modifying

existing content.

(b) Why don’t we allow subjects with higher clearance to write into files with

lower clearance?

This will provide a path for leaking secrets: Alice can read a secret then write it

to a public file, essentially declassifying the secret.

BLP model supports “trusted subjects”, who are not restrained by the “no write

down” rule (\*-property).

(c) Explain the following concepts in the BLP model:

• ss-property: simple security property. “No read up”.

• \*-property: “no write down”.

• ds-property: discretionary security property. Resource owner can deny

access when the system allows it. Note that if the system denies access,

user can’t allow it!

The textbook provides an interesting anecdote on the name “\*-property”, in a

footnote.

CS 458 Information Security

2

(d) Here are some subjects and objects in a BLP-modeled MAC system. Bigger

number means higher clearance (5 = top secret, 1 = unclassified).

**Task**: fill in the access rights each subject has on each object (read, write,

read+write, or no access). Remember “write” doesn’t imply “read” in BLP

model.

**Task**: fill in the access rights rmeoade+lw. Ermitep, toyr c neoll amcceeasnss) .n Roe amecacecemhs sbs.ue rb j“ewctr ihtea”s doone esanc’th i mobpjelyc t“ r(ereaadd” ,i nw BriLteP,

# 2#

• ss>property:#simple#security#property.#“No#read#up”.#

• \*>property:#“no#write#down”.#

• ds>property:#discretionary#security#property.#Resource#owner#can#deny#

access#when#the#system#allows#it.##

#

Note#that#if#the#system#denies#access,#user#can’t#allow#it!#

The#textbook#provides#an#interesting#anecdote#on#the#name#“\*>property”,#in#a#

footnote.#

#

(d)#Here#are#some#subjects#and#objects#in#a#BLP>modeled#MAC#system.#Bigger#

number#means#higher#clearance#(5#=#top#secret,#1#=#unclassified).#

#

**Object( Clearance(**

**X(** 4#

**Y(** 5#

**Z(** 3#

**W(** 1#

**Task**:#fill#in#the#access#rights#each#subject#has#on#each#object#(read,#write,#

read+write,#or#no#access).#Remember#“write”#doesn’t#imply#“read”#in#BLP#model.#

#

**( X( Y( Z( W(**

**Alice(** w# w# r/w# r#

**Bob(** w# w# w# r#

**Charlie(** r# r/w# r# r#

**Dave(** w# w# w# r/w#

###

**Subject( Clearance(**

**Alice(** 3#

**Bob(** 2#

**Charlie(** 5#

**Dave(** 1#

CS 458 Information Security

3

**4. Other MAC models**

(a) For each of the MAC models below, decide its security focus:

confidentiality, integrity, or conflict of interest?

• (confidentiality) BLP Model

• (integrity) Biba Model

• (conflict of interest) Chinese Wall Model

• (integrity) Clark-Wilson Model

(b) **Chinese Wall Model**: There are two banks (B1, B2), three cable companies (C1,

C2, C3) and four factories (F1, F2, F3, F4) in town, which form 9 datasets and 3 conflict

of interest classes. Here are some facts:

• Alice can read objects in B1 and C2

• Bob can read objects in C1 and F2

• Charlie can read objects in F4

Questions:

• Can Alice be granted read access to objects in C3? No – conflict of interest.

• Can Bob be granted read access to objects in B2? Yes – Bob doesn’t have

access to any Bank databases.

• Can Bob write into any object in C1? No – Bob can read across two CoI classes.

• Can Charlie write into any object in F4? Yes – Charlie only has access to one

database.

CS 458 Information Security

1

Homework 8: Database Security

**Database Access Privileges**

(a) **Granting rights**: Alice grants Bob access with grant option. What does the

command “with grant option” do?

It allows Bob to further grant access rights to others.

(b) **Revoking rights**: read the following scenario, then answer the question.

Alice owns the table T.

In chronological order, these events happened:

(a) **Alice** granted **Bob** full access to table T with grant option.

(b) **Alice** granted **Charlie** full access to table T with grant option.

(c) **Bob** granted **Dave** full access to table T with grant option.

(d) **Dave** granted **Erin** access to table T.

(e) **Charlie** granted **Dave** access to table T.

(f) **Alice** revoked from **Bob** all access privileges to table T.

**Question**: In common practice, at this point in time, who has access to table T?

Who can grant others access to T?

Common practice: a revoke negates the previous grant, as if the grant never

happened. This means the revoke will cascade if other privileges can only happen

because of this grant.

(6) negates (1), so Bob no longer has access to T. Because (1) didn’t happen, (3)

couldn’t have happened, therefore (4) couldn’t have happened. Therefore:

(a) Alice has access to T, and can grant others access to T.

(b) Charlie has access to T, and can grant others access to T.

(c) Dave has access to T, but can’t grant others access to T.

CS 458 Information Security

1

Homework 9: Malware

(a) Starting April 8, 2014, Microsoft will no longer release updates for Windows XP

and has warned that XP users will take the risk of ‘zero day forever’. What is a zeroday

exploit, and why does Microsoft warn so?

A zero-day exploit is a vulnerability in a system that is exploited before a patch

can be released. Microsoft warns XP users of ‘forever zero-day’ because:

(a) security patches are no longer released, and

(b) future updates for newer versions of Windows can be reverse-engineered to

discover vulnerabilities in Windows XP.

(b) What are the defining characteristics of the following kinds of malware?

Virus – Self duplicating

Worm – Self propagating (through network)

Root kit – Hides itself by manipulating system resources

Trojan horses – Hides malicious functionality in seemingly innocent software

(c) Older anti-virus software are mostly signature-based. How have viruses evolved

to avoid signature scanning? What techniques have newer virus scanners adopted?

Newer viruses can be polymorphic or metamorphic (altering binary while

maintaining functionality), intercept system calls to hide itself, or encrypt itself.

Newer virus scanners have shifted from signature scanning to using heuristics and

detecting anomalous behaviors.

(d) In malware, what does *payload* refer to?

Payload is the part of malware that does harm.

CS 458 Information Security

1

Homework 10: Buffer Overflow

(a) Also called stack smashing, stack buffer overflow is dangerous because it can

overwrite \_\_\_\_ pointer.

Return Address

(b) Shell code executed as a result of stack buffer overflow attack is executed

at whose privilege?

The hijacked program’s. This often results in an elevation of privilege for the

attacker, which is bad.

(c) Defenses against buffer overflow can be carried out at compile-time or at runtime.

Name one defense in each category.

Acceptable answers include...

Compile-time:

• Use high-level programming languages that don’t interactive with low-level

details.

• Use updated and safe libraries.

• Enable stack protection (checking for stack corruption, copying return

address pointer, etc.) This is often done by default today.

Run-time:

• Distinguish executable address space from non-executable ones.

• Randomize address (so that the attacker can’t predict what to overwrite the

return address with)

(d) **Bonus:** why can’t shell code have null bytes? How do people obtain a zero

value in shell code?

Because shellcode is often overwriting strings, which ends at a null byte. By xor’ing

a value with itself.

CS 458 Information Security

1

Homework 11: Network Security

(a) You have the IP address 192.168.0.24 under a subnet mask of 255.255.240.0.

At most how many devices can be in the same sub-network as yours?

4096.

(b) In general, how do Denial of Service attacks work?

It takes up the majority of a server’s traffic capacity, thereby preventing other

users from receiving service.

(c) Smurf attack spoofs victim’s address as its source address.

When the message is broadcasted, this causes many computers to simultaneously

send a respond message to the victim, causing denial of service.

(d) SYN flood never completes the TCP three-way handshake by not sending what

signal? How can a dedicated firewall absorb the malicious traffic?

It never sends the final ACK (acknowledge) signal.

A dedicated firewall can check all the client responses and only forward traffic

from clients who properly complete the handshake.

CS458 Information Security

Homework 12: Intrusion Detection

(a) What is the ultimate purpose of an intrusion detection system?

To detect and correct intrusions (unauthorized attempts to gain access to

protected resources).

(b) Expand these acronyms:

• IDS – Intrusion Detection System

• NIDS – Network(-based) IDS

• HIDS – Host(-based) IDS

• IPS – Intrusion Protection System (i.e. an inline NIDS)

(c) What is the difference between an NIDS and an HIDS?

In HIDS, anti -threat applications are installed on every computer, while in NIDS

such applications are only installed at certain points in the network.

(d) [True] Anomaly detection can learn user behavior and gradually change

expectations over time.

(e) [True] Signature detection is a compilation of rules which define “bad” behavior.

(f) What is the most prominent feature of an inline NIDS (aka an IPS)?

An IPS has fast signature detection and can remediate attacks directly in real-time.