Name:

Information Assurance: Homework 2 - Comments

Due September 9, 2009 on compass.

1. Critique the University's Access Control Policy http://www.obfs.uillinois.edu/manual/central_p/sec19-5.html#ff

a) Identify references to other policies.

The campuses and University Administration may implement a more restrictive access control policy if they so desire. (2nd bullet point). In the 4th bullet point refers to the current campus policies on appropriate and acceptable use.

b) Is the policy stating implementation requirements?

Yes, it specifies requirements to guide the implementation but not details of the implementation. For example, in the third bullet it says that access to networks, servers, and systems should be achieved by individual, unique logins. This constrains the authentication implementation. It then goes on to give examples of acceptable login technology.

c) Does the policy explicitly defer implementation details?

In my opinion, this policy does a pretty good job of not sinking in implementation details. It does indicate the use of specific mechanisms such as the use of passwords, encryptions, monitoring, and logging, but it does not identify details, and it specifically defers details on "strong passwords" to another standard that should be generated by the implementing organization.

d) Who are the responsible agents in this policy?

UTMT is identified several times as fleshing out the implementation details of the policy. The enforcement of the overall University Security Policy is the responsibility of the UTMT which is chaired by the Vice President for Administration.

e) Identify one assumption made by the policy.

One obvious assumption is that the encryption algorithms are used that are strong enough to not be broken. There are of course many other assumptions. One of you noted that the policy assumes the applications are well written and only applications that really need administrative access require administrative credentials.

f) Suggest an improvement to one aspect of the policy. Why is this an improvement?

I accepted most things here. Some people suggested being more explicit in implementation requirements which I specifically disagreed with. Others suggested making portions of the policy more explicit. One person noted that the

Name:

last bullet items seems to address two separate issues and should be separated to avoid overlooking the second issue.

2. Policy or mechanism. For each item below, is it a policy or an enforcing mechanism? If it is a policy, identify a mechanism that could enforce it. If it is a mechanism, identify a policy it could be enforcing.

   a) The multimedia equipment in each classroom of the Siebel Center must be only accessible to individuals responsible for teaching in that classroom.

   Policy. Does not indicate how the access will be restricted..

   b) Only registered students of UIUC may use the online services offered by the Engineering Career Services.

   Policy. Again, no specifics on how to implement the limitation to registered students.

   c) A system based on port numbers and traffic analysis should be deployed in the CS department network infrastructure to identify and terminate accesses to online peer-to-peer file-sharing networks.

   Mechanism. Specifies a technique for identifying peer-to-peer file sharing traffic. Specifies that such traffic once it is identified should be terminated.

   d) All individuals attending the UIUC career fairs should be asked to present valid UIUC IDs upon entrance.

   Mechanism. Presumably implementing a policy that restricts access to UIUC career fair attendees to registered UIUC students.

   The VPN service offered by the university can be used by individuals that are (1) university affiliates and (2) in the United States at the time of use.

   Policy. Specifies an access restriction but does not indicate how it will be enforced.

3. You own an online store that sells and ships flowers in the Champaign-Urbana area. Your sales average $600 per day. You are worried about being targeted by a distributed denial of service (DDOS) attacker with the aim of extortion. Such an attack would completely bring down your website, and you do not have any alternative way of doing business. You've heard that the attacker will require on average $1,500 to stop the attack. Once the money is received, the attack will stop within a day. Otherwise, it will continue for 7 days. Based on past data, you expect that the DDOS attackers have a 1% probability of targeting your small site any particular week. The company Akamai offers you a distributed hosting service that reduces the chances of success for such attacks to 20% (otherwise the attackers definitely succeed). Akamai requires an annual premium of $500 for this service.

Name:

a) Compute the annual loss expectancy for the DDOS attack (assuming you do nothing).

*ALE = number of weeks in the year * probability of a successful attack each week * number of days in a week * loss per day = 2184*

This isn't as accurate as it good be. Perhaps you get attacked twice in a week. Perhaps you get attacked will still under the influence of another attack. But with the information given, this is a decent approximation of the expected value of what you would lose in a given year.

b) Suppose you aim to choose one of the following strategies (controls) for year 2010: (1) pay money to the attackers (you don't care about legal consequences), or (2) buy the Akamai service (but in case an attack succeeds, do not pay attackers any money). Provide a risk leverage calculation for each of the above controls.

Case 1)

*New risk exposure = Weeks in a year * probability of successful attack * loss in a day = 52*.01*600 = 312*

*cost of control = weeks in a year * probability of successful attack * payoff fee = 52*.01*1500 = 780*

You will only pay if you get attacked.

Risk leverage = (2184 – 312)/780 = 2.4

Case 2)

*New risk exposure = Weeks in a year * new probability of a successful attack * loss in a week = 52*(.01*.2)*(7*600) = 436*

cost of control = 500

Risk Leverage = (2184 – 436)/500 = 3.496

4. Consider Vigenere cipher:

a) Use the Vigenere tableau at the end to encrypt the phrase "Be secure" with the key "safe".

TEXIUUWI

b) Use the Vigenere tableau to decrypt "TONNFRCFMED" with the key "ball".

Plaintext should be "soccer rules"

c) Determine the key and decode the Vigenere encrypted text posted at http://www.cs.illinois.edu/class/fa09/cs461/assignments/cipher.txt

The key was "gifted". The phrase was from the O'Henry story "The Gift of the Magi"

Name:

d) Describe how you determined the period. You may use automated tools such as the applet discussed in class http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html.

To determine the period, you could have computed the IC over the message and compared that value to the standard IC values.

You could have also looked for repetitions in the cipher text and used the intervals between the repeats to make some guesses on the period.

Name:

```
  | a b c d e f g h i j k l m n o p q r s t u v w x y z
-------------------------------------------------------
A | a b c d e f g h i j k l m n o p q r s t u v w x y z
B | b c d e f g h i j k l m n o p q r s t u v w x y z a
C | c d e f g h i j k l m n o p q r s t u v w x y z a b
D | d e f g h i j k l m n o p q r s t u v w x y z a b c
E | e f g h i j k l m n o p q r s t u v w x y z a b c d
F | f g h i j k l m n o p q r s t u v w x y z a b c d e
G | g h i j k l m n o p q r s t u v w x y z a b c d e f
H | h i j k l m n o p q r s t u v w x y z a b c d e f g
I | i j k l m n o p q r s t u v w x y z a b c d e f g h
J | j k l m n o p q r s t u v w x y z a b c d e f g h i
K | k l m n o p q r s t u v w x y z a b c d e f g h i j
L | l m n o p q r s t u v w x y z a b c d e f g h i j k
M | m n o p q r s t u v w x y z a b c d e f g h i j k l
N | n o p q r s t u v w x y z a b c d e f g h i j k l m
O | o p q r s t u v w x y z a b c d e f g h i j k l m n
P | p q r s t u v w x y z a b c d e f g h i j k l m n o
Q | q r s t u v w x y z a b c d e f g h i j k l m n o p
R | r s t u v w x y z a b c d e f g h i j k l m n o p q
S | s t u v w x y z a b c d e f g h i j k l m n o p q r
T | t u v w x y z a b c d e f g h i j k l m n o p q r s
U | u v w x y z a b c d e f g h i j k l m n o p q r s t
V | v w x y z a b c d e f g h i j k l m n o p q r s t u
W | w x y z a b c d e f g h i j k l m n o p q r s t u v
X | x y z a b c d e f g h i j k l m n o p q r s t u v w
Y | y z a b c d e f g h i j k l m n o p q r s t u v w x
Z | z a b c d e f g h i j k l m n o p q r s t u v w x y
```