Qualifier Exam in Information Security

Spring 2010

You have to answer at least one question in each section and get at least 60 points to pass the exam.

1 Network Security

Problem 1, 10 points.
After many years of experimental research, Iron Screen Labs releases a state of the art intrusion detection system targeting core ISP providers. This new IDS is 99.99% accurate, far outpacing the competition. Given the volume of traffic seen by providers, approximately one out of every 10,000,000 packets represents an attack.

(a) Given the above information, what is the detection accuracy of this IDS?
(b) Assume that the links within core ISP routers operate at a constant rate of 1 Giga-Packets (GPps) per second. How many false positives will be observed per second?
(c) In order to reduce the number of false positives, Iron Screen Labs decides to improve the accuracy of their detector. How accurate does the detector need to be to reduce false positives to one per second?

Problem 2, 10 points.
Neuman and Ts’o compare Kerberos to “authentication by assertion”. Explain why Kerberos provides a more secure authentication solution.

Name two protocols that rely on authentication by assertion. For each, explain an attack against the protocol and explain how the protocol could be or has been strengthened.

Problem 3, 10 points.
What is the end-to-end argument? What is its implication to network security?

How do IPsec-based VPNs violate the end-to-end argument? Give one argument for and against the use of this security mechanism.

2 System and Software Security

Problem 4, 10 points.
A reference monitor interposes on operations or object accesses, and it can enforce an access control policy constraining such access. Typical reference monitors are implemented in-kernel or as separate processes sandboxing the execution of a monitored process. An alternative design, called an inlined reference monitor (IRM), inserts the monitoring logic into the original code of the monitored process.

(a) What advantages might an IRM provide when compared to a more traditional sandbox?
(b) List and justify a set of assumptions that must hold true over the monitored process for an IRM within the process to be secure. Justify the completeness of your list.

**Problem 5, 10 points.**
The Federal Financial Institution Examination Council (FFIEC) mandated in 2005 that financial institutions such as banks must use a stronger authentication method than the password based single factor authentication that was commonly used at the time. However, FFIEC did not suggest what banks needed to do to meet the stronger authentication requirement. Several companies have offered solutions that utilize passwords and additional features to meet this mandate. For example, IP geolocation techniques can be used to estimate the location of a user who is logging in based on the IP address of his or her machine. The reputation associated with an IP address could be another feature, and operating system running on the client machine and the user’s ISP are additional features that could also be used. A request from a user must not only provide the correct password but its features must match those associated with the user.

To enhance security, it is desirable that we do not store values of these additional features directly with other user account information on the server machine where authentication is performed. Discuss how such a scheme can be implemented when the server is able to verify their values without storing them directly. To reduce false negatives, you should allow a login with correct password when the user is no more than distance d from the normal location. Similarly, other factors could allow limited deviation from the correct value.

Since the values of these features can vary over time (e.g., user may do online banking while on travel), to reduce false negatives, we may allow access when only a subset of the feature values match. Can the implementation above be adapted so a correct password with a subset of matching features is sufficient to access online services?

Does a scheme based on the features listed about really provide much stronger authentication than passwords as was required by FFIEC? Explain your answer.

**Problem 6, 10 points.**
Memory protection and logical isolation across processes/address spaces is an important building block for trustworthy computing systems. In modern processors, the memory management unit (MMU) of the processor implements several memory protection related functions in hardware. In addition, the operating system maintains segment/page tables which are used to ensure that a process is only able to access main memory that has been allocated to it.

We discussed protection of resources either using access control lists (ACLs) or capabilities (C-lists). How would you characterize memory protection in processors like the x86. Would you classify it as an ACL based system or a capability based system? Explain your answer.

In a virtualization based system like Xen, memory protection relies on the hardware as well as the hypervisor and the guest operating system running in each VM. Since OS typically maintains page tables and we want minimal changes to it when it runs on a hypervisor, the OS and Xen must share responsibility for managing page tables to ensure that memory protection works correctly. Discuss what page table related operations can be performed by the OS and what must be handled by the hypervisor.
3 Cryptography

Problem 7, 10 points.
Alice has set up an online database that answers queries about stocks and other financial products. Users’ queries are of the form “tell me the value of stock \langle \text{STCK} \rangle between dates \langle \text{START} \rangle and \langle \text{END} \rangle.” To protect her users’ privacy, Alice requires that queries be encrypted as they travel over the network. What abstract security properties should the encryption scheme provide, and what might it reasonably leave out? Justify your answers.

Problem 8, 10 points.
Alice is trying to decide between two different block ciphers, FOO and BAR, for her application. Both FOO and BAR have the same block size and key length. She’s confident that at least one of them is secure, but isn’t sure which. As a hedge, she decides to combine them into a single new block cipher BAZ, defined as:

\[
\begin{align*}
BAZ_k(x) &= FOO_k(BAR_k(x)) \\
BAZ_k^{-1}(y) &= BAR_k^{-1}(FOO_k^{-1}(y)).
\end{align*}
\]

Alice finds its performance to be acceptable, but is BAZ a sound design from a security point of view? If so, argue/prove it (you may assume that at least one of FOO and BAR is a secure block cipher). If not, explain why, and if possible, salvage it by suggesting a secure construction in the same spirit.

Problem 9, 10 points.
Show that for any IND-CPA secure public-key encryption scheme, the size of the ciphertext after encrypting a single bit is superlogarithmic in the security parameter \(k\). That is, \(|Enc_{pk}(b)| = \omega(\log k)\) for any bit \(b\) and legitimately generated \(pk\).