Qualifier Exam in Information Security

Spring 2011

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. Describe techniques that malicious web sites use to evade the detection by search engines (such as Google) and security scanners. Design a system to defeat such evasion.

Problem 2, 10 points. Neuman and Tso compare Kerberos to authentication by assertion. Which is better for security and why? Give an example of a protocol that uses authentication by assertion to prove your point.

Problem 3 , 10 points. The state of Georgia decides to open new HOT Lanes, which allow drivers willing to pay money to have access to HOV tra?c lanes. Citizens wishing to be able to bypass heavy tra?c can simply purchase a Peach Pass, which is a simple transponder that communicates with overhead readers every quarter mile. These readers will detect the presence of a transponder and, if authentic charge the corresponding account or, if not authentic (or absent) must take a picture of the o?ending cars license plate. In order to encourage drivers to join the program, the State makes such transpon- ders very cheap, which means that they have extremely limited memory and are not powerful enough to perform encryption and decryption operations. The protocol by which the reader veries the authenticity of the transponder must satisfy the following properties:

- A valid transponder can repeatedly authenticate a car.
- Once a transponder communicates with a reader, the value can not be replayed successfully by an eavesdropping adversary.
- All readers are networked, so accepted values are instantaneously known by all readers.
- The transponder only has enough memory to store a User ID and an additional 20 byte value.
- Transponders must be able to authenticate for at least ve years, which is approximately twice its expected battery lifetime.

Design a transponder authentication protocol satisfying the requirements above. What 20 bytes of data do you initially program into the reader? Why does your protocol prevent reuse of replayed transponder values?

2 System and Software Security

Problem 4, 10 points. You work in a large company and its chief security officer (CSO) just announced that all enterprise computers and devices are going to only run software that has been

evaluated and marked as "trusted". In other words, such code (applications, services, OS subsystems etc.) must either directly come from a trusted source or from a source trusted by another trustworthy source. Several techniques, such as tamper-resistant hardware (e.g., TPM), secure boot and attestation could be useful for one to build a system like this.

First, present an architecture and provide high level descriptions of protocols that you think such a system should utilize to achieve the goal that it only runs trusted code. State any assumptions you make and describe the correctness requirement and why your system meets it.

Would such a system provide better security? What are some of the threats that could undermine its security guarantees?

Are there practical challenges associated with such a scheme? Are those likely to be overcome in the near future?

If the company allows employees to access sensitive information on mobile devices, would that introduce new problems?

Problem 5, 10 points. Cloud computing and cloud security are constantly in the news. From a technical perspective, what are the security challenges that are unique to the cloud computing environment? If there are some, how can they be addressed? If not, justify your answer.

Problem 6, 10 points. Kernel extensions can utilize segment and page protection bits (SPL and PPL bits) provided by the x86 architecture to ensure that an extension does not have uncontrolled access to kernel data and code. Why does the x86 provide both SPL and PPL bits? How do they relate to various rings in which code could be executed to restrict its privileges? Explain your answer.

3 Cryptography

Problem 7, 10 points. Does collision-resistance of a function family imply one-wayness? Does one-wayness of a function family imply collision-resistance? Do the answers change for a case of a hash (length-compressing) function family? Justify your answers. No security proofs are needed for implications, but please provide the references if you use known results. Provide counter-examples for non-implications.

Problem 8, 10 points. Consider a variant of RSA encryption scheme, where the key generation is the usual algorithm for RSA-based schemes, encryption of a message $m \in \{0,1\}^k$ is done as $c \leftarrow m_{pad}^e \bmod N$, where e, N are from the public key and $m_{pad} = 0^k \| r \| 0^k \| m$ for random $r \in \{0,1\}^k$ and is viewed as a member of Z_N^*. The decryption algorithm performs the usual RSA decryption and checks if m_{pad} is formed correctly before outputting the message (otherwise $\perp$ is returned).

Show a chosen-ciphertext attack on this scheme. Use the fact that multiplication by 2 is just a leftward bit-shift.

Problem 9, 10 points. The goal of coversystem is to hide the mere existence of any secret communication between parties. A coversystem uses a "channel," which produces an unbounded stream of "documents" to generate its "covertexts." Possible real-world channels include news feeds, images

downloaded from photo-sharing sites, etc. For our purposes, we model a channel as an oracle C. Every time it is invoked, C returns an element from some fixed document space D, drawn uniformly at random. The adversary may depend upon the channel, but the coversystem itself does not depend on the particulars of the channel or its distribution – it should be efficient and remain secure for any valid channel. We model a shared-key coversystem for message space $\{0,1\}$ using three ppt algorithms as follows.

- The key-generation algorithm $\mathcal{K}(1^k)$ takes the security parameter and outputs a shared secret key K.
- The encoding algorithm $\mathcal{E}^C(K,b)$ takes a secret key K, a message bit $b \in \{0,1\}$, and oracle access to a channel C, and outputs a covertext $c \in D^\ell$ for some ℓ that is a parameter of the scheme.
- The decoding algorithm $\mathcal{D}(K,c)$ takes a secret key K and a covertext c, and outputs a bit.

Note that only the encoding algorithm uses access to the channel.

(a) (5 points) Using the algorithms and syntax described above, give a formal, concise definition of correctnessness for a coversystem. Your definition may allow for a small probability of incorrect decoding. (Make sure that your definition allows for any valid channel.)

(b) (5 points) Give a formal, concise definition of covertness under chosen-plaintext attack for a coverystem. Your definition should capture the property that a covertext "looks like" ℓ documents drawn independently at random from the channel. Again, make sure that your definition applies to any valid channel.