Cybersecurity for Future Presidents 2016:

Final Exam

Part A **(3 points per question)**

1. When you speak, the signal your voice provides is a

***a. Analog***

b. Digital

signal.

2. Consider that your voice signal has been captured by a cell phone. The packets transiting the switches in the telephone network represent your voice as

a. Analog

***b. Digital***

data.

3. In general, it’s easier to compress data represented in

a. Analog

***b. Digital***

format.

4. Suppose you want to protect your phone conversation against eavesdropping by encrypting the voice signal, but you want to make the most efficient use of the available telephone lines (minimize the bandwith consumed by the traffic). Would you:

a. Encrypt first, then compress

b. Compress first, then encrypt

Explain your answer:

5. Suppose your speech is digitized by sampling it 8,000 times per second, and *each sample* represents one of 256 levels.

a. How many bits are needed to represent a single sample?

**<8>**

b. If no compression is applied, how many bits per second must be transmitted to capture the signal? (Use *x* as your answer for (a) if you didn’t obtain one.)

**<64,000>**

6. The collection of software and hardware on which system security depends (i.e., that part of the system which, if compromised, can violate system security) is referred to as:

**<The Trusted Computing Base or TCB>**

7. List two key differences between circuit-switched and packet-switched networks?

1. Difference #1:

**<Circuit switched: has a setup and data transfer phase, all data transits same path through the network, circuits not shared during a call, headers not required on data?**

1. Difference #2:

**<Packet switched: no connection setup required, packets from the same call may transit different paths, data divided up into packets, packets require headers readable by switches (routers)>**

8. What signaling property of the circuit switched telephone network was exploited by “phone phreaks” in the 1960s to manipulate the telephone network for their own purposes?

**<in band signaling>**

9. What bitwise logical operation is applied to encrypt a stream of data bits using a string of key bits:

**<XOR>**

10&11 Apply the operation named in the previous question to combine the following data bits with the key bits. Then fill in the appropriate decryption key bits and decrypt the encrypted bits (assume symmetric key cryptography):

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Data bits | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| Key bits | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| Encrypted bits | **1** | **0** | **1** | **1** | **0** | **1** | **0** | **0** |
| Decryption key bits | **0** | **1** | **0** | **1** | **0** | **1** | **0** | **1** |
| Decrypted data bits | **1** | **1** | **1** | **0** | **0** | **0** | **0** | **1** |

12. What property desired of the keystream (i.e., key bits) seems to be lacking in the previous question?

**<the key stream doesn’t seem to be random at all>**

13. Recalling the video using mixing of paint colors to illustrate Diffie-Hellman key exchange. What was the crucial property of mixing paint colors that enabled the two parties to agree on a shared secret color of paint without an eavesdropper being able to deduce it?

**< mixing of paint is easy, but unmixing is hard – it’s a one-way function>**

14. A SQL-injection attack depends on what type of software error?

**<failure to validate input, input validation error>**

15. What important piece of data is typically overwritten in a buffer overflow attack?

**<return address on the stack>**

16. What is the hard problem on which Rivest, Shamir, and Adleman based their public key cryptographic algorithm?

**<factorization of large numbers>**

17. Explain the difference between identification and authentication.

**<< identification is the assertion of a claimed identity. Authentication is the presentation of proof that the claimed identity is valid. >>**

18. When biometrics are used for authentication, it is crucial that an attacker not be able to inject data into the path between the biometric device and the system software that performs the authentication checking. What is the mechanism that provides confidence that this communication is not interfered called?

**<Trusted Path> <might also accept VPN, but it’s not quite right>**

19. A fundamental component of the bitcoin system is the blockchain, which provides a record for all bitcoin transactions. The transactions are grouped into blocks. It’s important that the blocks all be linked together. What cryptographic operation provides the basis for linking all the past transaction blocks to a new block?

**<cryptographic hash, secure hash>**

20. The Stuxnet attack incorporated exploits based on as many as four “zero-day” vulnerabilities. What is a zero day vulnerability?

**<it’s an exploitable vulnerability that is unknown to the software vendor and the world in general, hence there are generally no protections against it or monitoring for its exploitation>**

Part B **(6 points per question)**

1. In broad terms, how do the U.S. and E.U. approaches to privacy regulation differ?

**<US is sectoral, addressing different areas with different laws, regulations.>**

**<EU is broad, with a common data privacy directive across all sectors>**

2. In the U.S., which Federal agency is responsible for assuring that companies abide by their published privacy policies?

**<Federal Trade Commission, FTC>**

3. List three characteristics of genomic data that distinguish it from other kinds of health-related data

**<long lived/static>**

**< unique/distinguishes individuals>**

**< kinship/exposes parentage>**

**< value persists over time>**

**< reveals health/behavior information (potential for disease)>**

**< mystique: may reveal more in the future>**

4. Under what conditions do HIPAA protections apply to genomic data?

**<the data must be held by a “covered entity” ie a healthcare provider, insurer, health plan, etc.>**

5. List three requirements that a system for public elections should satisfy

**<assure only eligible voters cast ballots>**

**<assure ballot is cast as voter intends>**

**<assure anonymity of the vote (can’t trace vote back to voter)>**

**<assure the votes are counted correctly>**

**<prevent vote buying, vote fraud>**

**<provide audit trail to support investigation in case of trouble>**

6. How did the Estonian remote voting system deal with the prevention of possible coercion of votes cast remotely?

**<the system permits multiple ballots to be cast remotely; only the last one counts. Further, voter can go to the polls in person and vote there, in which case only that vote is counted.>**

7. Following problems with punch card voting systems in Florida in the 2000 Presidential election, The Help America Vote Act provided a one-shot appropriation for U.S. jurisdictions to purchase new voting equipment. List a positive and negative effect of this legislation.

a. Positive effect:

**<positive: encouraged the replacement of outdated voting systems>**

b. Negative effect:

**<negative: the one-shot infusion meant that companies were incentivized to get into the market quickly but not to make products that would stand the test of time.>**

8. The E.U. has instituted a form of a “right to be forgotten” which is implemented through restrictions on search engine behavior. Explain the following:

1. how does a user make a request (for restricting information)?

**<request to search company (eg Google) that specified information that is “no longer relevant” to oneself not be returned by searches>**

1. if the request is allowed, how does the search engine implement the restriction.

**<search company implements by filtering out links in question when the search originates in E.U. country and mentions the individual name>**

9. Name a U.S. law that makes eavesdropping of the content of electronic communications illegal for ordinary citizens, but authorizes it under specific conditions for law enforcement purposes.

**<The Electronic Communications Protection Act (or just ECPA) >**

10. What distinguishes surveillance for foreign intelligence purposes from surveillance for law enforcement purposes? Discuss.

**<law enforcement surveillance is generally for collecting evidence that can be used in court to prosecute crimes. Foreign intelligence surveillance is concerned with collecting information for national security purposes – criminal intent is not at issue. However there is some overlap between the spaces as information collected for foreign intelligence may sometimes reveal criminal activity and be passed to law enforcement under legal constraints. >**

Part C **(10 points each question)**

Read the supplied article and, bringing to bear what you have learned in the course, write:

1. A short summary of the main points made in the article

2. A critique of the positions taken by the article: what points are weak, what is left out?

3. What are the strongest points in favor of the article’s position?

4. What are the strongest points against the article’s position?

5 & 6.Write two questions you would pose to the author, one in favor and one against the article’s position, if this were a debate paper on the topic

Greg Austin, “Time to Strengthen Cyber Security,” East West Institute, February 3, 2014.

1. Summary

2. Critique: what points are weak, what is left out?

3. Strongest points in favor of article’s position

4. Strongest points against the article’s position

5. Question 1 for the authors:

6. Question 2 for the authors