Computer Security 10. Exam 2 Review Paul Krzyzanowski Rutgers University Spring 2017 Merch 4, 2017 CS 419 © 2017 Paul Krzyzanowski

Question 1(a)

Suppose you come across some old text in the form

GEPPQ IMWLQ EIPWS QICIE VWEKS RIZIV QMRHL SAPSR KTVIG MWIPC LEZMR ...

Also suppose you know it is English text and it is encrypted. How would you determine if the text was enciphered with a transposition or a substitution cipher?

- Perform a frequency analysis
- If the frequencies match those of English text then it is a transposition cipher

CS 419 © 2017 Paul Krzyzano

Question 1(b)

Suppose you come across some old text in the form

GEPPQ IMWLQ EIPWS QICIE VWEKS RIZIV QMRHL SAPSR KTVIG MWIPC LEZMR ...

Suppose you decide you are looking at a substitution cipher. How would you determine if the text was encrypted is a monoalphabetic or polyalphabetic substitution cipher?

- · Look at the frequency analysis
- If the frequencies match those of English text but for the wrong letters, then you have a monoalphabetic substitution cipher
- If the frequencies are close to uniform then you have a polyalphabetic substitution cipher

March 4, 2017

CS 419 © 2017 Paul Krzyzanowski

Question 2

What does it mean for a cryptographic hash to be collision-free?

- When people refer to a collision-free cryptographic hash, they mean it is collision resistant
- It is hard to find two messages M₁ & M₂ such that H(M₁) = H(M₂)

Pigeonhole Principle

If n items are put into m containers, with n > m, then at least one container must contain more than one item

- A hash is a fixed number of bits, which can hold a finite set of values
- You can have a larger, potentially infinite, set of inputs

March 4, 201

CS 419 © 2017 Paul Krzyzanowski

Question 3

Why is the one-time pad not widely used even if it offers perfect secrecy?

- The key must be as long as the message and never reused
- The problem of secure communication has been replaced with the problem of secure key transmission

March 4, 2017

CS 419 © 2017 Paul Krzyzanowski

Question 4

If Alice has Bob's certificate (assume she has validated it already), how can she convince herself that she is talking to Bob?

Have Bob prove that he has the corresponding private key

Option 1

- Alice generates a random string (nonce)
- She asks Bob to encrypt it with his private key & send the results
- She decrypts the result using the public key in Bob's certificate

Option 2

- Alice generates a random string (nonce)
- She encrypts it with the public key in Bob's certificate
- She sends it to Bob & asks him to decrypt the message with his private key and send her the results

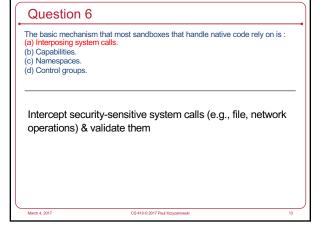
If the resulting message = original nonce, it's Bob

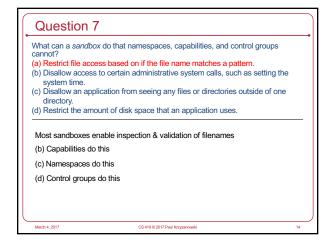
March 4, 2017

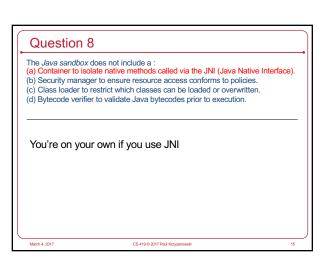
119 © 2017 Paul Krzyzanowski

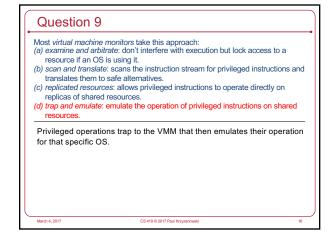
A security advantage of using containers over using a combination of cgroups, namespaces, and capabilities is: (a) Simpler configuration avoids comprehension errors. (b) Containers provide better isolation. (c) Containers are a form of sandboxing. (d) Containers do not require administrative privileges. Many containers are built on top of control groups, namespaces, and capabilities (b) Namespaces provide great isolation (c) Containers aren't any more a form of sandboxing than capabilities and namespaces (d) They don't to run apps but neither to namespaces & cgroups. They require root privileges to install

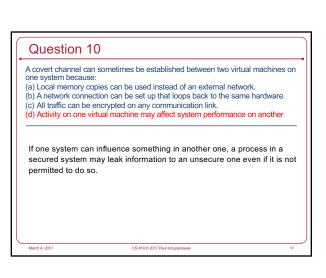
CS 419 © 2017 Paul Krzyzanowski

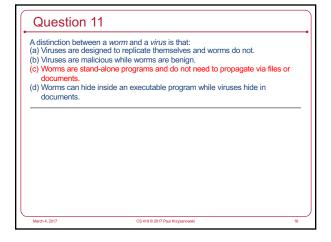


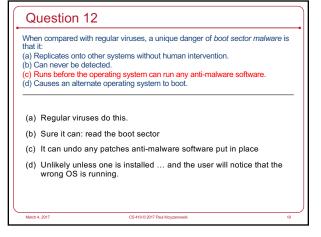




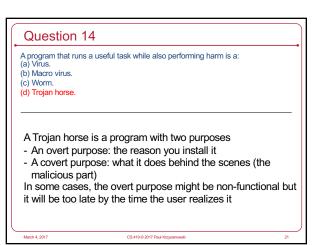


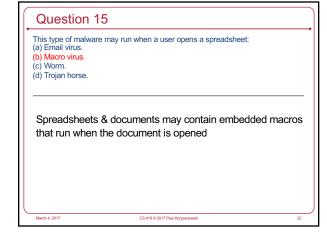


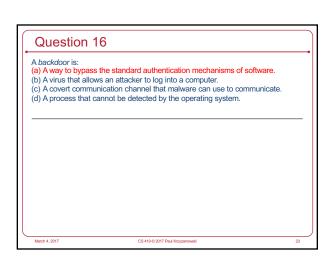




A program that allows an attacker to access a computer while hiding its presence is called a: (a) Rootkit. (b) Backdoor. (c) Trojan horse. (d) Masqueraded authenticator. The key point is hiding its presence. Rootkits are programs that hide their presence – and often provide hackers with privileged access to a system

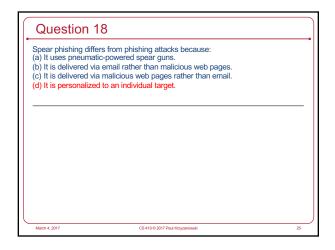




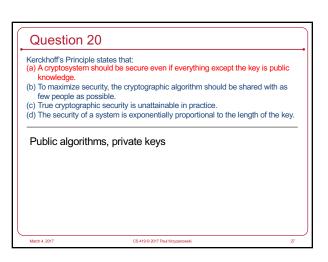


A hypervisor rootkit will: (a) Embed itself within the operating system and bypass authentication requests. (b) Install programs that enable an adversary to log in with administrative privileges. (c) Run underneath the operating system to detect and log events of interest. (d) Force the system to boot an alternate hacked version of the operating system. A hypervisor is the lowest-level software, operating between the hardware and the operating system - The OS does not know of its existence - The hypervisor can intercept privileged instructions and all system interrupts

CS 419 © 2017 Paul Krzyzanowski



A virus signature is: (a) A hash of the code that makes up the virus. (b) A portion of the code that makes up the virus. (c) An encrypted hash of the virus code. (d) Data that identifies the author of the virus. Virus signatures have nothing to do with digital signatures. They're just a subset of code used for signature scanning by anti-malware software



```
Question 21

Suppose that you can crack a 56-bit key in one day. How long would it take to crack a 112-bit key?

(a) Two days.
(b) 56 days.
(c) 3,136 days.
(d) 197 trillion years.

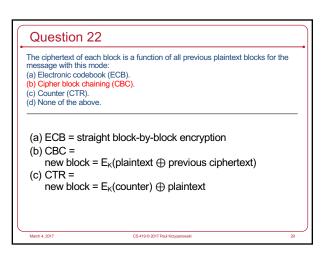
You don't need to do exact math here — you have 56 more bits Each bit doubles the search time.

56-bit key = 1 day ⇒ 57-bit key = 2 days

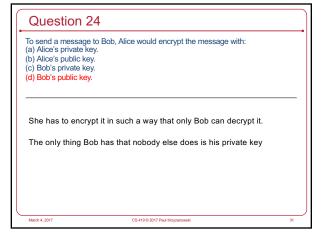
1 extra bit ⇒ ×2; 2 extra bits ⇒ ×4; 3 extra bits ⇒ ×8

10 extra bits ⇒ × 2<sup>10</sup> = × 1024 days
20 extra bits ⇒ × 2<sup>20</sup> = × ~1 million days ⇒ this is way more than 3,136
30 extra bits ⇒ × 2<sup>30</sup> = × ~1 billion days

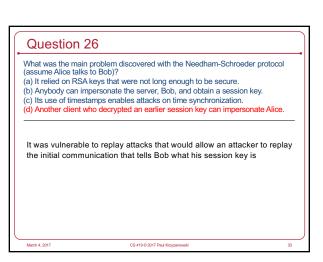
56 extra bits ⇒ × 2<sup>56</sup> = 7.2 × 10<sup>16</sup> days = 7.2 × 10<sup>16</sup> days = 197 × 10<sup>12</sup> years
```



Which algorithm does not rely on one-way functions? (a) RSA. (b) AES. (c) Diffie-Hellman. (d) SHA-2. (a) RSA is based on the difficulty of factoring large products of primes. The modulus, n = pq(b) AES is just a set of substitutions & permutations (c) Diffie-Hellman is based on the discrete log problem (d) Hash functions are irreversible and hence one-way

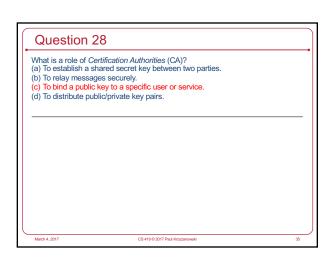


A hybrid cryptosystem uses: (a) Different algorithms for each direction of data transmission. (b) A public key algorithm to transmit a key and a symmetric algorithm for the data. (c) Two levels of encryption for increased security: data encrypted with a symmetric algorithm is then encrypted with a public key algorithm. (d) A symmetric algorithm to transmit the data and a public key algorithm to transmit a hash of the data. Hybrid cryptosystem: Public key cryptography for transmitting a key Symmetric cryptography for communication



When Alice receives a Kerberos ticket to talk to Bob, it can be decrypted:
(a) Only by Alice & Kerberos.
(b) Only by Bob & Kerberos.
(c) Only by Alice, Bob, & Kerberos.
(d) Only by Alice and Bob.

Kerberos has all the keys
The ticket is the sealed envelope that Alice cannot decode



CS 419 3/22/19

