Cyber Outlook

A Different View of Info Security

January 2017 - Vol. 3 No. 1

Dear Cyber Outlook Reader,

The gym is crowded with people trying to keep resolutions, so it must be a new year, and time for a new series in Cyber Outlook.

You're probably aware of claims made in both popular and cyber security media that Al Qaeda and ISIS make significant use of steganography. You may also have read that steganography is an effective approach for concealing data being exfiltrated by an advanced persistent threat.

So, we are beginning a series which will cover all branches of steganography. As always, we will do our best to make the material practical and interesting, without requiring lots of prior background. And, of course, we continue our popular "Ask the Expert" column, and our cyber-security word puzzle.

We always welcome comments. You can contact us through the links at the end of the newsletter.

Regards,
Adam Enosh
VP, Marketing

Uncovering Steganography, Part 1

Do you remember the scene in the movie *The Lost World: Jurassic Park*, where Jeff Goldblum and Julianne Moore were being chased down a creek bed by a dinosaur, which had a double row of bony plates covering its back? This was a stegosaurus, whose name comes from the Greek word **stegos**, which means “covered”, and the Latin word **saurus,** which means “lizard”. The term **steganograph**y comes from the same root, plus the Greek word **graphe,** which means “writing.” So steganography is “covered writing”, and there are three families of methods for doing the covering.

This series of articles will explain how various forms of steganography work, how you can detect whether someone is using steganography to conceal information, and how you can reveal the concealed information.

Steganography is the process of hiding information in a carrier. A carrier can be an image or stream of images (visual), a stream of sound (audio), or a text document. The most common approaches to steganography are image-based or audio-based, if the volume of published papers on the subject is a valid indicator. Text or linguistic steganography, which modifies a text document to conceal a message, includes a variety of approaches. They cover the entire spectrum of linguistic sub-fields:

- orthography – how to write and spell words
- morphology – how to form individual words
- lexicography – determining the meaning of individual words
- syntax – how to structure words into groups
- semantics – determining the meaning of word groups
- discourse – how to structure groups of words into larger units

In this article, we begin by explaining a general approach to detecting the use of steganography.

1. **Catalog the applications on the target system.**

If we find a tool that is commonly used for one of the steganography methods, then we have good reason to suspect that someone is hiding something on this system. We will include a list of steganography tools at the end of the last article in this series, which covers each of the three steganography families of methods (visual, audio, linguistic).

2. **Catalog the data files on the target system.**

People sometimes change the extensions of files they are trying to hide. A PDF file might have an extension of “.xls”, or a Word document might have an extension of “.wav”. The only way to check for this subterfuge is to load every data file with a program that should be able to process it. If the application is unable to load the data file, then we use a special tool to inspect the header, change the extension to the real type, and re-load it. If someone takes the trouble to misname a file, they are almost certainly trying to hide something.

3. **Sort the cataloged data files by type and by size.**

We are hoping that our suspect kept the original carrier file, in addition to the one which has been changed to include the secret message. The whole point of steganography is to introduce changes which are not perceptible to the human senses. So, if we suspect steganography, we seek out files that can be looked at (visual), listened to (audio), or read (linguistic). If we found steganography tools, we will know which of the three families to concentrate on. If we found misnamed files, we also know which of the families are relevant. Creating these two catalogs can take a lot of labor. Forensic work only happens in 60 minutes on television shows.

4. **Process all files of the same size and type.**

Compare each pair of files which have the same type, and use the same amount of storage on disk.

a. If the type is graphic (PNG etc), view each pair of files of same size and type. Do they look the same?
b. If the type is audio (WAV etc), listen to each pair of files of same size and type. Do they sound the same?
c. If the type is text (PDF etc), read each pair of files of same size and type. Do they say the same thing?

5. **Run a hashing algorithm on pairs of files that seem to be the same content.**

If the hash values differ, you should suspect steganography. One file may simply be a copy of the other, which we can check by using a tool that does a byte-for-byte comparison. Even if they aren't absolutely identical, they may not be the result of using steganography. How can we tell?

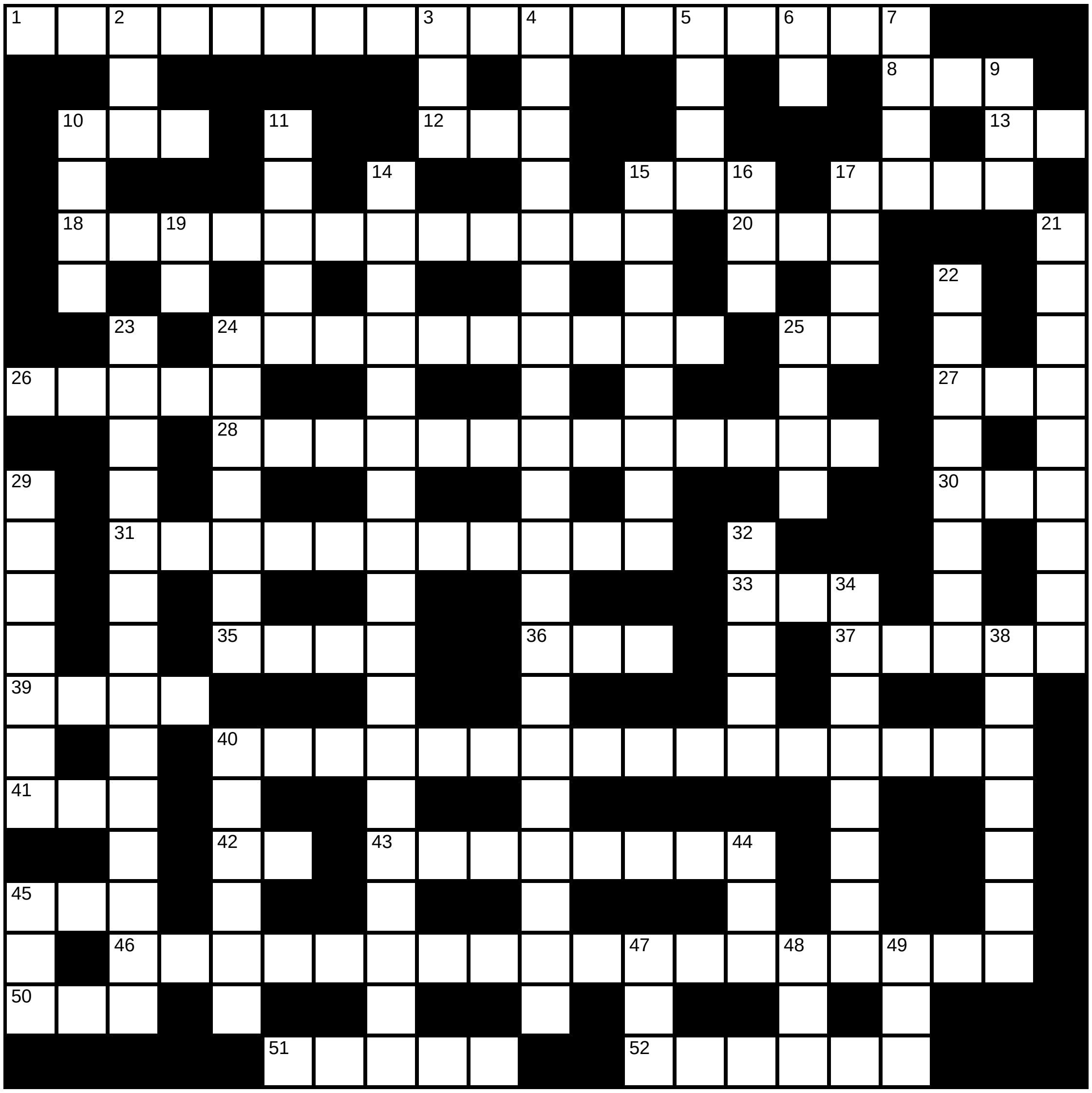
In Our Next Issue

Uncovering Steganography, Part 2: Linguistic Steganography – Orthographic Approaches
CISSP Crossword Puzzle

CISSP Word Puzzle

All of the terms in this puzzle are from topics covered by the CISSP exam.

Solutions to previous puzzles can be found on our website at www.cybersecfirm.com/newsletter/



Across

1 percentage of authorized users denied access (5,9,4)

8 TCP counter (3)

10 radio waves (3)

12 examines multiple headers (3)

13 wireless LAN connection point (2)

15 controls industrial machines (3)

17 group organized for contingency planning (4)

18 tasks before current task (12)

20 transmits temporary session keys (3)

24 vulnerability scanning tool (10)

25 values used to strengthen encryption (2)

26 steady interfering electrical disturbance (5)

27 resource identifier (3)

28 covert channel communicating by relative timing (6,7)

30 Wi-Fi security using LEAP and TKIP (3)

31 program appears useful but has hidden malicious functionality (6,5)

33 noise generated by appliances (3)

35 XML notation for authentication (4)

36 original Microsoft file structure (3)

37 loads the operating system (5)

39 GSM enhancement (4)

40 firewall reacts to events and updates its data to handle future occurrences (7,9)

41 encrypted Internet applications (3)

42 compression algorithm (2)

43 three security principles (3,5)

45 memory exchange without CPU (3)

46 split critical task so that multiple people must complete it together (10,2,6)

50 single event potential loss (3)

51 intelligen code object (5)

52 vulnerability scanner (6)

Down

2 analyzing log files (3)

3 release ambient static electricity (3)

4 exchange of electrons between materials (20)

5 central authority access control (4)

6 dollar value assigned to asset (2)

7 organizational high level security policy (4)

9 converts internal to public IP addresses (3)

10 extension of Wiretap Act (4)

11 backlog of packets in buffers (5)

14 database organized by tables with keys in records (10,8)

15 bootable file copied to external media (3,5)

16 wireless connection requiring authentication (3)

17 video security system (4)

19 percentage loss from an attack (2)

21 dials all numbers in a range looking for modems (3-6)

22 filters traffic between internal network and Internet (8)

23 search warrant scope (8,6)

24 functions performed on objects (7)

25 block cipher used by PGP (4)

29 rules used by firewalls and proxies (7)

32 security bridge between domains (5)

34 private network providing Web services (8)

38 demagnetize media to erase data (7)

40 integrates development, QA, operations (6)

44 layered network defense strategy (3)

45 industrial control network (3)

47 social media (3)

48 alternate source of power (3)

49 uncovers intruders (3)

Taking Care of Business

You are receiving this newsletter because you subscribed at CYBERSECFIRM.COM

Our mailing address is:
CYBERSECFIRM
Street
City, State ZIP

CYBERSECFIRM respects your privacy. We do not sell, rent, or share your information with anybody, and will only use this data to send you the information you have requested.

Subscribe to this newsletter

See previous issues of this newsletter

Contact the editor of this newsletter

Change your subscription email address

Unsubscribe from this mailing list