Who is “n3td3v”?

Hacker Factor Solutions

White Paper

Release 1.4.1, 12-October-2006

Hacker Factor
P.O. Box 270033
Fort Collins, CO
80527-0033
www.hackerfactor.com

Table of Contents

1 Introduction

On 2-August-2006, Neal Krawetz from Hacker Factor Solutions presented "You Are What You Type: Non-Classical Computer Forensics" at the Black Hat Briefings security conference. This talk covered a variety of techniques for identifying individuals and physical characteristics based on how people write and the keys they use. The profiling approach uses solid scientific research from the linguistic and physical development fields.

A few days before the conference, the presentation was discussed with a small group of security professionals. One person, Valdis Kletnieks, offered a challenge: identify "n3td3v" – an individual who was frequently offensive on the Full Disclosure mailing list.

In three minutes, writing samples from n3td3v were collected. Two minutes later, it was determined that n3td3v was not a "he" but a "they": at least three distinct individuals, two males (one European) and a female. Another researcher (Jim McCown) mentioned that the trolling[1] reminded him of the postings made by Gobbles Security. Dr. Krawetz had met the primary members of Gobbles Security many years ago and knew that they consisted of three people: two males (one is Eastern European) and a female.[2]

This document shows techniques used to identify writing characteristics and concludes that the core people behind Gobbles Security are strong contenders for being the people behind n3td3v.

1.1 Analysis Approach

Five different word-based methods are used for identifying individuals, analyzing each individual's writing samples, and comparing author attributes. Each method is a profiling approach; while not expected to be 100% accurate, they are usually correct. These approaches identify and analyze habitual behaviors – in this case, word usage. The methods are as follows:

- **Gender determination**. Different sexes use different word frequencies. Based on the observed frequency of specific words in the writing samples, the author's gender can be approximated. This system is roughly 60-70% accurate. In situations where it is wrong, it is consistently wrong. For example, a male classified as having a female writing style will be consistently classified as having a female writing style. This is because the system measures habitual word usage and not actual gender. The system is tuned toward American English; other dialects such as British English and Commonwealth English will have "weak" scores, suggesting a possible European. In this paper, gender determination is also used to identify multiple authors within a single document since each author has a different habitual style.
- **Mental lexicon analysis**. The *mental lexicon* is a basic theory in linguistic analysis. Put plainly, you only use the words you know. If an author has never heard of a word, then he will not use it. If an author has heard of a word but does not know the meaning, then he will use the word incorrectly. Although normally used for testing vocabulary and comprehension, this theory also forms the basis of a vocabulary approximation: it can be used to determine if a speaker is a native English speaker. In addition, it can be used to determine foreign language and advanced education attributes. This system has consistently passed blind tests with an accuracy rate greater than 80%.
- **Vocabulary histogram and core words**. When people communicate, they use some words more often than others. Words that are heavily used by the speaker form a core vocabulary. Different speakers have different cores. While this system is very accurate at determining a core vocabulary, the likelihood of two arbitrary people from the same country having the same cores is around 40% (i.e., 60% distinct), although some cores can be very distinct. Cores are based on word repetition and are influenced by their environment. Thus, a vocabulary histogram can be used to approximate nationality.

[1] People who post messages only for the purpose of irritating others are referred to as "trolls" in online communities.

[2] The initial analysis was completed in less than five minutes; most of this paper was written on 4-August-2006. The author apologize for the delay in releasing this paper, and offers his sincerest thanks to the technical reviewers for checking the methods, questioning conclusions, and providing feedback.

- **Punctuation frequencies**. Similar to core words, punctuation usage is also habitual, repetitive, and distinct. While it is not uncommon for two arbitrary people to have the same punctuation frequencies, the likelihood of two distinct samples having the same author is very unlikely.
- **Preferred sentence lengths**. When writing, people have an internal sense of cadence; they know what sentence length feels right. People also have preferred sentence structures, leading to similar sentence lengths. While some people may hyper-focus on a particular sentence length or range of lengths, other people prefer a variety and a near-even distribution. These habitual behaviors are distinct. While not as accurate as punctuation frequencies, sentence lengths can be used to identify whether two different authors wrote two different samples. This system has a high degree of false positives, indicating that the authors could be the same person, but a low degree of false negatives, where the two distinct authors are actually the same person.

Each of these profiling approaches generates distinct profiling attributes. It is very important to remember that “distinct” is not “unique”. Multiple people can and do have similar or identical attributes. While “unique” means that a specific attribute is restricted to a specific individual, “distinct” means that it is quantifiable. Saying “a human who breathes air” is not distinct since all people breathe air. In contrast, “a human who is left-handed” is distinct since not all people are left-handed.

1.2 Analysis and Errors

A thorough study of the accuracy rates for these analysis methods has not been completed. The initial tests of each method varies from 60%-70% accurate for gender determination and sentence length, to over 80% accurate for lexical analysis, core words, and punctuation frequency analysis. Taken independently, it is very possible for any of the five analysis methods to generate a false conclusion. For example, assuming each method is 70% accurate yields a 30% chance of error for any single profiling method[3]. When combined, it becomes very unlikely for all five methods to be incorrect. The likelihood of a completely wrong profile is 0.30^5, or 0.24% (less than 1%)[4]. As detailed in this document, we are identifying three people, not one. The odds of completely misidentifying all attributes of all three people are approximately 1 in 100,000,000.

Even though the probability suggests that at least one of the profile methods will be correct, there is only a 16.8% chance (0.70^5) of all profiled attributes being correct for a single person. For example, the profile may indicate a female that is European and holds an advanced (college) education, while in reality the person may be *male*, European, and a college graduate. Fortunately for this paper, the profiles *do not need to be accurate* – the profiles *only need to be consistent*. Multiple writing samples by the same person should generate the same profile – if the person is evaluated as having a female writing style, then all writing samples by this person should indicate a female. The consistent profile is used to identify individual authors.

1.3 Duplicate Profiles

The approximated 70% values from Section 1.2 identifies whether the profile is accurate, but it does not identify the likelihood of two people having the same profile. Each of the analysis methods evaluates multiple variables. For example, gender determination measures the usage of 25 distinct words (informal writing; formal writing evaluates 33 distinct words) to determine one of three values (male, female, or weak score). Assuming a completely random and evenly distributed sample, the likelihood of two people having the same results is 1 in 3, or 33%.[5] The other

[3] The different analysis methods have different levels of accuracy. For simplicity, they can be assumed to be 70% accurate. In actuality, gender determination and sentence lengths are the least accurate methods; lexical analysis, core words, and punctuation frequency are more accurate. Including all of the different accuracy metrics will create much more complicated computations and not demonstrate a significantly different degree of error.

[4] This combination assumes that the each analysis method is independent. For completeness, this is not necessarily a safe assumption. The words used for the gender determination algorithm are also used for the lexical analysis. Similarly, sentence length has a correlation with punctuation frequency. In addition, each algorithm uses the same data set; a biased data set can skew the results from all of the profiling methods.

[5] This 33% metric is actually a simplistic value. The gender determination odds from a truly random sample are 40% male, 40% female, and 20% weak score. Other analysis methods have more complicated results. The 33% statistic is only used to show that, even in a relatively simple case, the likelihood of three people having the same consistent profile is extremely unlikely. It is also important to recognize that the standard deviation, skew, and t-statistic values also determine the likelihood of a duplicate result. These statistics for the linguistic and gender analysis are available from the references in this document.

analysis methods have lower odds of a random match since they evaluate more variables and generate more possible results.

Knowing that the worst of the analysis methods has about a 33% chance of matching a randomly selected person, we can determine the likelihood of all five results matching a randomly selected person. The percentage is no greater than 0.33^5, or 0.41% (less than 1%). Furthermore, this paper assigns three distinct profiles to three distinct people and then compares the results to another trio of people. The likelihood of all three assigned profiles matching another trio of people is 0.0041^3, or $6.97 \cdot 10^{-6}$% (about 7 in 100,000,000).[6] Although it is possible to falsely match profiles to three pairs of people, it is not probable.

1.4 Analysis Approach Summary

To summarize the analysis approaches:

- Five different profiling methods are used in this paper.
- The results from each method are more likely right than wrong. While some of the profiling values may be incorrect, it is unlikely that all of the profiling results will be wrong.
- Even if the results are incorrect, they will be consistent for multiple samples by the same author. This is because each method measures habitual behaviors.
- It is unlikely for two unrelated and randomly selected people to have similar profiles.
- As unlikely as it is for two people to have the similar profiles, it is much more unlikely to identify three pairs of people who have similar profiles.

As demonstrated in Section 2 of this paper, n3td3v appears to have three distinct profiles – indicating three distinct people. In addition, the n3td3v profiles are similar to another known trio: Gobbles Security.

[6] Even assuming a 50% chance of a duplicate match per metric, the likelihood of matching all five metrics is only 3% and the likelihood of matching three profiles to three people is 0.003% (about 3 in 100,000).

2 Profiling n3td3v

They way we write and the words we use are distinct. Different people have different vocabularies, word preferences, and even a sense of cadence – a rhythm that determines how many words make a good sentence length. Linguistical forensics and profiling identifies attributes such as preferred words, punctuation usage, and vocabulary size. This form of analysis is based on scientific research from the fields of linguistics, education, and sociology, and it all starts with writing samples.

2.1 Acquiring Samples

The entity identifying itself as “n3td3v” (commonly pronounced “net-dev”) offers plenty of writing samples from postings to newsgroups, blogs, and even the web site “www.n3td3v.com”[7]. Unfortunately, most samples are relatively small – under 300 words. Although linguistic analysis works best with larger samples, single paragraphs still have definable attributes.

There are many tests that can be conducted on writing samples. For this paper, the gender determination, punctuation analysis, sentence lengths, grammatical structure, and lexical approximation analysis methods are applied.

2.2 Gender Determination

Men do not communicate like women. Books such as *You Just Don’t Understand: Women and Men in Conversation* and *Talking 9 to 5* identify many of the communication differences. These differences are not limited to verbal and non-verbal (e.g., body language); the written words we use and how we use them also show gender differences. In 2003, a group of researchers conducted a survey to empirically identify gender-specific writing styles.[8] The researchers identified attributes such as *women use more pronouns while men use more proper nouns* and *women use more adjectives while men use more adverbs*. Their research paper included quantitative differences and also showed that writing attributes varied by genres – a male writing fiction will use different words when writing non-fiction.

A group of people at the BookBlog implemented a system based on the gender determination research. Their tool, the *Gender Genie*, use a very simplified variation of the work – only focusing on a small word list. This tool was 60-70% accurate, better than random guessing but certainly not authoritative. Hacker Factor Solutions used the Gender Genie as a basis for the *Gender Guesser*[9]. While just as accurate at the Gender Genie, the Gender Guesser was adapted to analyze formal and informal writing styles, and to identify possible European authors.

Samples of text attributed to n3td3v were tested using the Gender Guesser. Multiple writing samples from the same author should have similar attributes. Even if the system is wrong, it should be consistently wrong. The n3td3v samples contained three distinct styles, identifying two distinct genders (Table 1).

Each of the text samples from n3td3v are relatively small, adding to variance in the total scores. Yet, n3td3v appears to have three distinct results from the gender analysis. Two people appear to be male – one may be European – and one person uses a female writing style.

[7] This web site is operated by a third-party but contains quotes from n3td3v.

[8] Shlomo Argamon, Moshe Koppel, Jonathan Fine, and Anat Rachel Shimoni, “Gender, Genre, and Writing Style in Formal Written Texts.” 2003.

[9] The Gender Guesser is available online at *http://www.hackerfactor.com/GenderGuesser.html*.

Table 1. Sample text from n3td3v, analyzed using the Gender Guesser.[10]

Sample [including spelling errors]	Analysis	Interpretation

I think if there was a case of vote rigging, however, it would be carried out by my opponents, who are more than willing to carry this anti-n3td3v propaganda way into 2006, to ruin myreputation, and to pollute the list with polls and quotes, seen already in this and past anti-n3td3v threads. Have a good new year i'm sure you'll have no vulnerabilities to disclose, since you're someone who just hates on people who do disclose vulnerabilities to vendors and the security community. setup your own security group, be friends with hundreds of people in multiple scenes, have IM and E-mail contact with some of Yahoo's top security advisors and security engineers, then you can come back to this list and challenge me. FOOL!	Total words: 134
	Genre: Informal
	Female = 105
	Male = 300
	Difference = 195; 74.07%
	Verdict: MALE
		This sample shows a strong score, indicating that the author is likely male.

It is our intelligence that university students and graduates are being approached on campus by evil individuals offering large sums of money to join a cyber devision against governments.	Total words: 29
	Genre: Informal
	Female = 0
	Male = 19
	Difference = 19; 100%
	Verdict: MALE
		A small sample showing another strong male score. The first sample’s author could have written this, or the sample could be too small.

MARK SEIDEN social engineers n3td3v, offers a T-shirt to get home address. He tried to befriend me, but was rude to me, so I told him to never contact me, even though I had never heard of him before he tried to get information. He came into my instant message uninvited.	Total words: 45
	Genre: Informal
	Female = 253
	Male = 0
	Difference = -253; 0%
	Verdict: FEMALE
		This writing sample is very different. It scores with a strong female weight.

I find the folks who talk about filtering individuals actually turn out to be more lame than the folks they were complaining about. Usually the folks complaining about the list have never contributed in any form to the list whatsoever. For me I think the folks people talk about filtering offer a better insight into whats going on than nobody users who complain and ask about content filtering.	Total words: 68
	Genre: Informal
	Female = 129
	Male = 112
	Difference = -17; 46.47%
	Verdict: Weak
		This sample does not show strong gender preferences. This could indicate that the sample is too small, or could suggest that the author is European.

I'm sick of lying for yahoo employees I've gone on for 7 years lying for them I want to tell the police everything I know Someone off list tell me how to report this guy The "n3td3v" group was a joint effort of yahoo and google employees I want to hand them in now Regards, n3td3v I fell out with an employee, thats why i'm going public	Total words: 73
	Genre: Informal
	Female = 83
	Male = 121
	Difference = 38; 59.31%
	Verdict: Weak
		Another sample that appears to be from a European.

[10] The Gender Guesser system, algorithm, and source code (in JavaScript) are available online at *http://www.hackerfactor.com/GenderGuesser.html*. This system measures common word frequencies. Specific words are assigned male or female weights and the total weighted values are added together for gender determination. The ratio of the total male score with the total male and total female word scores determines if the verdict is a weak score. While large samples perform the best results, small samples with many word instances still generate acceptable verdicts.

2.3 Lexical Analysis

The gender determination algorithm is roughly 60-70% accurate, yet the algorithm identifies distinct attributes. For example, if it misclassifies an individual, it is likely to consistently misclassify samples from the same person. In this case, the quotes appear to come from three distinct individuals. Knowing this, the samples can be divided into three categories for lexical analysis.

Although a person may understand a large set of words, they only compose sentences from a small, familiar group of words. This is referred to as a *mental lexicon*[11]. The average adult American male with an advanced education may have a vocabulary of 25,000 words. A comparable person in Britain may use upwards of 75,000 words[12]. By analyzing the words used, the size of the mental lexicon can be approximated, indicating each author’s command of the English language.

Many people apply a core set of words – words they repeat statistically more often than others. In some cases, people may have dual or triple cores, where different word frequencies are clustered into groups. Constructing a histogram of distinct word frequencies and searching for clusters permits core measurements. Cores are usually due to a limited vocabulary in the mental lexicon. Generally speaking, Americans have very small cores and may demonstrate dual or triple cores. This is due to a relatively small mental lexicon. Native-English speaking Europeans, such as those from the U.K., have very large mental lexicons and a wider word selection. This leads to a lack of repetition and either a very large core or no discernable core. Australian English and Canadian English have similar attributes to American English. In contrast, Commonwealth English (Europe, India and other current and previous British territories) are similar to British English – they have large cores when they are discernable.

- Person #1: This person uses a vocabulary estimated at 20,000 words. The author is identified as a probable male and may have an advanced education. A histogram of distinct word usage indicates a clear dual core of preferred words; this is not common for a European.
- Person #2: The person identified as a probable European demonstrates a large vocabulary and complex sentences. The gender determination suggests that this author is using English as a foreign language (EFL), but he is likely fluent in English. This author also uses a high percentage of determiners and a low percentage of conjunctions, suggesting an Eastern European primary language. A histogram of word usage indicates virtually no core set of words. This is also common for most Europeans.
- Person #3: As with Person #1, this person appears to use large vocabulary. This person likely uses English as a primary language. The educational assessment of this individual suggests an advanced education due to very complex sentences, but this assessment is inconclusive due to the limited sample size. Similar to Person #2, this person has no clear set of core words; she may be European or the sample size may be too small.

2.4 Author Profiles

The people behind n3td3v do one thing exceptionally well: they frequently and inconsistently use variations in spelling and grammar. This deters analysis. Fortunately, the location of present and absent punctuation (e.g., end of sentence markers) is obvious from the written text. This can be used to identify preferred sentence lengths and writing profiles (Table 2).

- Person #1: This person shows a preference toward commas and long sentences – including a preference for sentences containing 15-17 words (in these examples, 16 words is most common sentence length, but other writing samples may offset the focal length a little). Conjunctions are common. In addition, this person frequently uses commas in place of end-of-sentence punctuation.
- Person #2: This person rarely uses commas. This is common for Europeans with Slavic or Baltic primary languages.

[11] Oldfield, R.C. (1963) Individual vocabulary and semantic currency: a preliminary study. *British Journal of Social and Clinical Psychology* **2**:122-130.
[12] Carter, R. (1987). *Vocabulary: Applied Linguistic Perspectives*. London: Allen & Unwin.
Bright, William (Ed) (1992) *International Encyclopedia of Linguistics*. Oxford University Press.

- Person #3: This person does use commas but not as often as Person #1. This person also prefers shorter sentences than Person #1. Many of the sentences are missing basic grammar components, such as verbs – the absence is likely intentional. Based strictly on punctuation frequency, word usage histogram, and sentence lengths, Person #2 and Person #3 could be the same person, but Person #1 is distinct.

Table 2. Sample text from n3td3v, using punctuation and sentence length analysis.

Person #1	Person #2	Person #3
# character frequencies: . 31 (31.31%) ? 1 (1.01%) ! 2 (2.02%) , 39 (39.39%) : (0.00%) ; (0.00%) (1 (1.01%)) 1 (1.01%) - 3 (3.03%) " 6 (6.06%)	# character frequencies: . 14 (50.00%) ? (0.00%) ! (0.00%) , 6 (21.43%) : (0.00%) ; (0.00%) ((0.00%)) (0.00%) - (0.00%) " 2 (7.14%)	# character frequencies: . 13 (46.43%) ? (0.00%) ! (0.00%) , 9 (32.14%) : (0.00%) ; (0.00%) ((0.00%)) (0.00%) - 1 (3.57%) " (0.00%)
#Words per sentence, frequency: 53 2 (6.06%) 52 1 (3.03%) 44 1 (3.03%) 43 1 (3.03%) 41 1 (3.03%) 40 1 (3.03%) 34 1 (3.03%) 31 2 (6.06%) 29 2 (6.06%) 28 1 (3.03%) 23 2 (6.06%) 21 1 (3.03%) 20 1 (3.03%) 19 2 (6.06%) 18 1 (3.03%) 17 1 (3.03%) 16 **4** (12.12%) 13 2 (6.06%) 11 2 (6.06%) 10 1 (3.03%) 9 1 (3.03%) 3 1 (3.03%) 1 1 (3.03%)	#Words per sentence, frequency: 28 1 (7.14%) 27 1 (7.14%) 23 1 (7.14%) 18 1 (7.14%) 17 1 (7.14%) 12 1 (7.14%) 11 1 (7.14%) 10 2 (14.29%) 9 2 (14.29%) 7 2 (14.29%) 2 1 (7.14%)	#Words per sentence, frequency: 34 1 (7.69%) 32 1 (7.69%) 26 1 (7.69%) 23 1 (7.69%) 18 1 (7.69%) 14 1 (7.69%) 12 1 (7.69%) 8 1 (7.69%) 7 2 (15.38%) 6 1 (7.69%) 4 2 (15.38%)

2.5 Summary of n3td3v

The group identified as n3td3v appears to consist of at least three distinct individuals. If there are more than three people, then there are at least three primary members who provide most of the n3td3v postings.

The three people are profiled as:

- Person #1: He is likely an American, Australian, or Canadian male with an advanced (college) education. He is inclined to write long sentences.
- Person #2: He appears to be male, European, speaks English as a foreign language, and has a Slavic or Baltic primary language. He is also the most likely member of n3td3v to drop or omit punctuation.
- Person #3: This person is likely a female with an advanced (college) education.

2.6 Additional Associations

Beyond the quantitative assessments, there are observable qualitative distinctions between the different members of n3td3v. These distinctions appear in their semantic constructs and are specific to each individual.

- Person #1: This is the most vocal of the members. He is inclined to write run-on sentences and misuse commas. He frequently insults other people.
- Person #2: This person uses the most authoritative writing style. He is more likely to announce the virtues of n3td3v.
- Person #3: This person is the least active. She commonly uses personal pronouns and proper punctuation. The topics usually contain personal feelings.

3 Profiling Gobbles Security

Numerous people have suggested a possible relationship between n3td3v and Gobbles Security. In 2001, Gobbles was an unidentified entity trolling forums such as BugTraq. Most postings contained insults and lacked technical details. Gobbles made claims as to being multiple people. These appearances and claims are similar to the n3td3v postings in forums such as Full Disclosure and CNet.

In late 2001, Gobbles began releasing zero-day exploits. The initial exploits focused on Yahoo! and Microsoft products. Later Gobbles branched out, covering other companies, operating systems, and products such as Hewlett-Packard, OpenSSH, and BSD. Their range of exploits was impressive.

3.1 Acquiring Samples

People do not always write like they talk, and writing samples are needed in order to determine if Gobbles and n3td3v are the same people. Many of Gobbles’ advisories are available from Attrition.org, and each advisory contains large writing samples.[13]

3.2 Gender Determination

Each of the advisories contains sections that could have been written by different people. Each section was entered into the Gender Guesser for authorship determination.

- **GOBBLES-04.txt**. This advisory discusses issues with the Yahoo! Messenger protocol. The initial “Background” section appears to have been written by a female. The paragraphs from the “Technical Details” section show a different writing style and appear to have been written by a male[14]. A female likely wrote the “Fix” section, while the “Demonstration” section shows a weak score, suggesting a European. This advisory was likely a team effort.

Section: Background
Genre: Informal
Female = 815
Male = 231
Difference = -584; 22.08%
Verdict: FEMALE
	Section: Technical Details
	Genre: Informal
	Female = 210
	Male = 365
	Difference = 155; 63.47%
	Verdict: MALE

Section: Fix
Genre: Informal
Female = 39
Male = 10
Difference = -29; 20.4%
Verdict: FEMALE
	Section: Demonstration
	Genre: Informal
	Female = 64
	Male = 56
	Difference = -8; 46.66%
	Verdict: Weak

- **GOBBLES-05.txt**. This advisory addresses a problem in Netscape Mail. The document appears to have two authors: one is an American[15] male, and the other is likely European.

[13] *http://attrition.org/security/advisory/gobbles/*

[14] The score for the “Technical Details” section (63.47%) is between the ranges associated with both males. The author could be either of the identified males or a third, unidentified male. The variation could also be due to writing sample size and is therefore inconclusive as to the individual assignment. The only conclusion that can be drawn is that the author is likely male. Similar mid-range scores appear in the other writing samples, but it is not consistent enough to distinguish a third male from sampling variation.

[15] As noted above, the author may be American, Australian, Canadian or similar nationality where the English dialect uses a core set of words. This author is unlikely to be British, Indian, or other English-speaking European.

Introduction
Genre: Informal
Female = 380
Male = 455
Difference = 75; 54.49%
Verdict: Weak
	Background
	Genre: Informal
	Female = 49
	Male = 116
	Difference = 67; 70.3%
	Verdict: MALE

Security History
Genre: Informal
Female = 38
Male = 114
Difference = 76; 75%
Verdict: MALE
	The Problem
	Genre: Informal
	Female = 349
	Male = 719
	Difference = 370; 67.32%
	Verdict: MALE

Exploit Details (paragraph, not code)
Genre: Informal
Female = 128
Male = 136
Difference = 8; 51.51%
Verdict: Weak
	Vender Notification
	Genre: Informal
	Female = 182
	Male = 335
	Difference = 153; 64.79%
	Verdict: MALE

- **GOBBLES-06.txt**. This advisory addresses a problem in the Hewlett Packard 48 Series Calculators. The document appears to have two or three authors: one is likely European. The others are likely both American males (scores around 71% and 80% respectively). Unlike the other example advisories, the authors appear to trade off between paragraphs and not just between sections.

Introduction (first two paragraphs)
Genre: Informal
Female = 248
Male = 631
Difference = 383; 71.78%
Verdict: MALE
	Introduction (third paragraph)
	Genre: Informal
	Female = 424
	Male = 285
	Difference = -139; 40.19%
	Verdict: Weak

Security History
Genre: Informal
Female = 354
Male = 895
Difference = 541; 71.65%
Verdict: MALE
	Background
	Genre: Informal
	Female = 86
	Male = 361
	Difference = 275; 80.76%
	Verdict: MALE

Description of Problem (first paragraph)
Genre: Informal
Female = 273
Male = 404
Difference = 131; 59.67%
Verdict: Weak
	Description of Problem (penultimate paragraph)
	Genre: Informal
	Female = 218
	Male = 446
	Difference = 228; 67.16%
	Verdict: MALE

Fixes
Genre: Informal
Female = 64
Male = 227
Difference = 163; 78%
Verdict: MALE
	Vendor Notification
	Genre: Informal
	Female = 33
	Male = 141
	Difference = 108; 81.03%
	Verdict: MALE

- **GOBBLES-07.txt**. This advisory is primarily written by the European. A few of the paragraphs (most notably every “hehehe” paragraph) show attributes suggesting the American male (denoted by a score around 71%).

Most of these advisories have large writing samples, leading to a more accurate determination. The scores are relatively consistent for specific authors. Although this cannot be used to identify “who” the specific authors are, it can be used to segregate samples by author for further analysis.

3.3 Lexical Analysis

The initial advisories produced by Gobbles Security include three authors: one male (Person A) who appears to use American English, one European male (Person B), and one female (Person C). Later advisories excluded the female and introduced a third male (Person D). Each of these samples can be separated by their gender determination results and analyzed for lexical attributes.

- Person A: This person has an active vocabulary estimated at 15,000-20,000 words. This person has a large enough vocabulary range to suggest some college education. Similar to n3td3v’s Person #1, a histogram of word usage shows a clear dual core of preferred words.
- Person B: This person demonstrates a very large vocabulary and no distinct core set of words. This is common for Europeans. The word selections appear similar to n3td3v’s Person #2.
- Person C: Although text examples from this person appear to use broken English and poor grammar, the style is likely intentional. The writing samples attributed to this person include a large variety of words (all used correctly), indicating a native English speaker with a mental lexicon of 15,000-20,000 words. This person has a large enough vocabulary range to suggest some college education. The writing sample has a noticeable lack of determiners, probably due to an intentional attempt at altering her writing style. As with n3td3v’s Person #3, a histogram of distinct word usage does not show any clear core set of preferred words.
- Person D: This person, identified by a gender determination score of 80 (strong male score), demonstrates a large vocabulary usage, indicating a possible advanced (college) education, and he shows a similar dual core of words, suggesting an American. Person D is distinguished from Person A by a consistently stronger gender determination score and a significantly higher percentage of determiners (determiners account for 5% of all words used by for Person A, compared to 9% for Person D).

In all of the Gobbles Security advisories, each author prefers to use “GOBBLES” in place of first-person pronouns. This is likely a convention agreed upon by the different members, or an artifact from an editor’s comments prior to public release. n3td3v does some of this first-person replacement, but not to the same degree as Gobbles Security.

3.4 Author Profiles

The Gobbles Security advisories can be profiled for punctuation and sentence length preferences (Table 3). These results can be compared with the authors from n3td3v.

Based on the punctuation frequency and sentence length preferences, we can identify a few consistent attributes.

1. Strictly based on punctuation and sentence lengths, Person A and Person D have similar styles and could be the same person. The most notable attributes are their similar period-to-comma ratios, and parenthesis usage comprising around 10% of all punctuation. Although they have different sentence frequencies, this could be due to the sample size. Both have gender-based word usage suggesting an American male, and both use “hehehe...” to indicate laughter. But, including the lexical analysis shows that Person A and Person D have very different core vocabularies and are not likely the same person.
2. Person A has different punctuation frequencies and sentence length preferences compared to Person B and Person C. This suggests that Person A is not the same person as Person B, and none of the males are the same as Person C.
3. Person #1 could be Person A. Although there are differences in comma usage; both use commas when being funny, sarcastic, or intentionally offensive. In the samples from n3td3v, all of the quotes are from humorous statements, sarcastic comments, or insults. Both people also show a preference for long sentences and a focus on sentences of length around 16 words: Person #1 prefers sentences with 16 words and Person A prefers 15 words – the difference can be attributed to the writing forum or topic. Both Person #1 and Person A frequently write the humorous, sarcastic, or insulting messages more frequently than the other members.

4. Person #2 could be Person B. Both have a nearly 2:1 ratio of periods to commas, and relatively little other forms of punctuation. Although there are few samples from n3td3v’s Person #2, both people appear to have similar sentence lengths and a preference for shorter sentences. Both Person #2 and Person B frequently discuss their purpose and reason for being.
5. Person #3 could be Person C. Both have similarly high period-to-comma ratios and similar preferences for hyphens. Both people also show a range of sentence lengths indicating a preference toward a variety of sentence structures. Both people also appear to intentionally use broken English in their writings and focus on personal feelings.
6. Person D has no counterpart from the n3td3v writing samples.

Table 3. Sample text from Gobbles, using punctuation and sentence length analysis.

Person A	Person B	Person C	Person D
Character frequencies: . 26 (33.77%) ? 3 (3.90%) ! 13 (16.88%) , 5 (6.49%) : 2 (2.60%) ; 1 (1.30%) (8 (10.39%)) 9 (11.69%) - 1 (1.30%) " 6 (7.79%)	Character frequencies: . 26 (46.43%) ? 1 (1.79%) ! 6 (10.71%) , 14 (25.00%) : 2 (3.57%) ; (0.00%) (3 (5.36%)) 3 (5.36%) - 1 (1.79%) " (0.00%)	Character frequencies: . 13 (40.62%) ? 2 (6.25%) ! 1 (3.12%) , 6 (18.75%) : 1 (3.12%) ; (0.00%) (1 (3.12%)) 1 (3.12%) - 4 (12.50%) " (0.00%)	Character frequencies: . 12 (60.00%) ? (0.00%) ! (0.00%) , 2 (10.00%) : (0.00%) ; (0.00%) (2 (10.00%)) 2 (10.00%) - 2 (10.00%) " (0.00%)
#Words/sentence, freq: 49 1 (2.50%) 48 1 (2.50%) 47 1 (2.50%) 46 1 (2.50%) 45 1 (2.50%) 43 1 (2.50%) 42 2 (5.00%) 40 1 (2.50%) 39 1 (2.50%) 37 2 (5.00%) 36 1 (2.50%) 34 1 (2.50%) 33 1 (2.50%) 32 2 (5.00%) 30 1 (2.50%) 28 1 (2.50%) 26 1 (2.50%) 25 2 (5.00%) 24 1 (2.50%) 23 2 (5.00%) 21 1 (2.50%) 15 **3** (7.50%) 14 2 (5.00%) 12 1 (2.50%) 11 1 (2.50%) 10 1 (2.50%) 7 1 (2.50%) 5 **3** (7.50%)	#Words/sentence, freq: 80 1 (3.03%) 64 1 (3.03%) 60 1 (3.03%) 53 1 (3.03%) 48 1 (3.03%) 44 1 (3.03%) 39 1 (3.03%) 38 1 (3.03%) 37 1 (3.03%) 33 1 (3.03%) 31 2 (6.06%) 30 1 (3.03%) 29 1 (3.03%) 27 1 (3.03%) 24 1 (3.03%) 23 1 (3.03%) 22 **4** (12.12%) 20 1 (3.03%) 18 1 (3.03%) 16 1 (3.03%) 15 1 (3.03%) 13 **3** (9.09%) 10 **3** (9.09%) 9 1 (3.03%) 4 1 (3.03%)	#Words/sentence, freq: 54 1 (6.25%) 41 1 (6.25%) 31 1 (6.25%) 29 2 (12.50%) 28 1 (6.25%) 27 1 (6.25%) 23 1 (6.25%) 21 1 (6.25%) 20 1 (6.25%) 19 1 (6.25%) 14 1 (6.25%) 12 1 (6.25%) 9 1 (6.25%) 8 1 (6.25%) 6 1 (6.25%)	#Words/sentence, freq: 54 1 (10.00%) 51 1 (10.00%) 35 1 (10.00%) 30 2 (20.00%) 23 1 (10.00%) 20 1 (10.00%) 10 2 (20.00%) 7 1 (10.00%)

3.5 Gobbles in Person

Gobbles Security ended their anonymity by giving a presentation at the Defcon 10 hacker conference (Figure 1). Their talk, *Wolves Among Us*, was effectively a rant (albeit, a very funny rant) about various companies in the computer and security industries. Shortly after their public presentation, Gobbles Security stopped posting in forums.

An audio recording of their presentation is available on the Defcon 10 presentation CD[16]. The accents of the speakers and their verbal compositions suggest that “Silvio” (a Gobbles supporter but non-member) is from Australia or New Zealand, “Gobbles” may be an American or Canadian, and “Unix Terrorist” is likely European. During their presentation, Gobbles was most likely to insult other security groups, while Unix Terrorist frequently discussed their purpose and justified their actions.

Unfortunately, people rarely write like they talk. Written words are usually edited and revised before being committed. In contrast, when speaking people rarely refine their wording. Instead, they adapt to their audience and correct themselves after speaking. As a result, an audio transcript of the Gobbles Security Defcon presentation cannot be used for the author analysis methods covered in this paper.

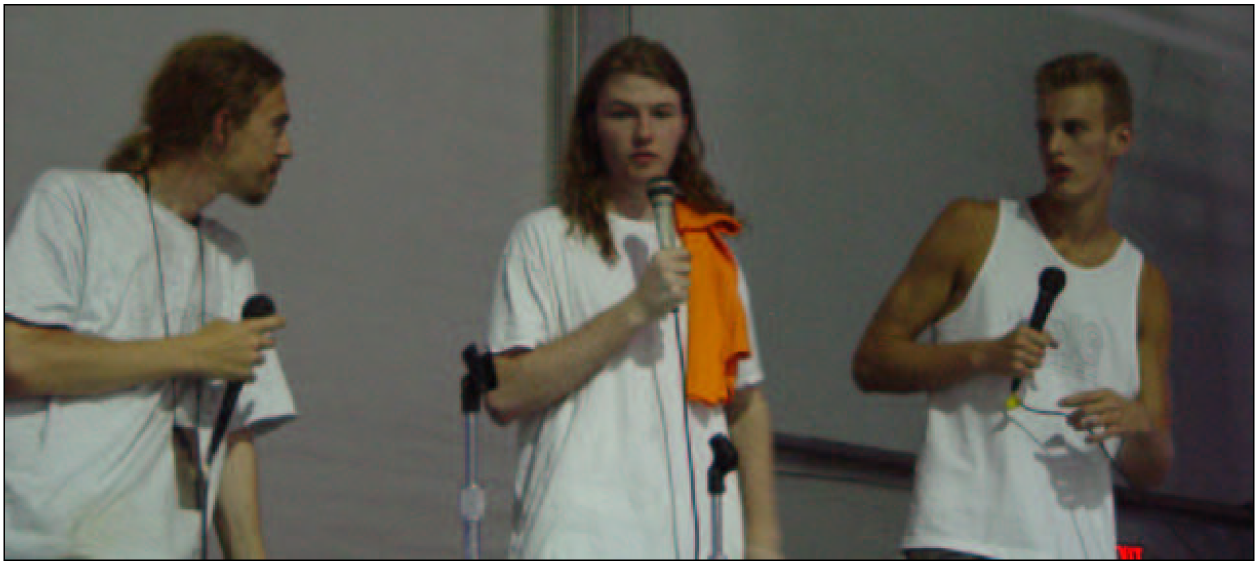

Figure 1. Gobbles Security presentation at Defcon 10. Silvio (left), Gobbles (center) and Unix Terrorist (right). This picture comes courtesy of Grifter, *http://www.defcon.org/images/defcon-10/dc-10-post/dc-10-grifter/gobbles.jpg*.

Meeting Gobbles

Dr. Krawetz first met Gobbles and Unix Terrorist from Gobbles Security at an iDefense party during Defcon 10. The event was held in a crowded bar and there was only one table with an empty seat. Standing at the table were two friendly looking guys; one with long hair and the other was tall. Krawetz walked to the table, but instead of a friendly “hello” or pleasant introduction, the short guy (compared to his counterpart) shouted in an almost rabid fashion: “WHO THE FUCK ARE YOU?”

Krawetz did not know about Gobbles Security at the time. Although the introductions were rough, they proceeded to have a pleasant conversation about responsible disclosure. While their opinions differed from Krawetz’s, both Gobbles and Unix Terrorist were very articulate and their arguments were logical and well thought out – they may act like script kiddies on stage and in online forums, but they are very intelligent.

If Krawetz’s first experiences with full disclosure had been different, he would likely have formed a similar opinion to Gobbles and Unix Terrorist (albeit with a different approach). The approach used by Gobbles Security is novel. They release exploits when they believe companies, governments, or organizations will not disclose or correct risks. Gobbles expressed dissatisfaction with many security groups; while various organizations sound professional, this is merely a verbal façade. The actions by these same large security groups show a lack of technical understanding (e.g., vigorous hand-waving) and a child-like response to security risks. In contrast, Gobbles Security may act and sound immature, but they backup their rhetoric with sophisticated methods. Gobbles Security actively strives to be the *exact* opposite of the “professional security groups” they dislike.

[16] Although the RealVideo stream from the Defcon Archives was not working in August 2006, a copy of the audio files is available online at *http://audio.textfiles.com/cons/dc10/disk_2_of_2/AUDIO/067/*.

3.6 Summary of Gobbles Security Comparison

Gobbles Security consists of at least three core individuals, and possibly another half-dozen less active contributors. The three core individuals have a significant number of common attributes with the unknown n3td3v members.

- Person A: This is likely the person self-identified as “Gobbles.” He has a similar writing style, vocabulary selection, core word list, and punctuation frequency as n3td3v’s Person #1.
- Person B: This is likely the person self-identified as “Unix Terrorist.” He has a similar writing style, vocabulary selection, core word list, and punctuation frequency as n3td3v’s Person #2.
- Person C: This person is likely the same as n3td3v’s Person #3. Both people have similar writing styles, vocabulary selections, core word lists, and punctuation frequencies.

The appearance of n3td3v comes nearly four years after Gobbles Security vanished. Since Person #1 has a larger vocabulary than Person A and Person #3 has a larger vocabulary than Person C, it is probable that both people have since graduated from four-year college programs.

3.7 Additional Associations

Beyond the quantitative assessments, there are observable qualitative distinctions between the different members of Gobbles Security. These distinctions appear to be specific to each individual and correspond with the quantitative profile matches.

- Person A: As with n3td3v’s Person #1, Person A has an abrupt writing style, sarcastic humor, and frequently verbally attacks anything he even vaguely disagrees with.
- Person B: Similar to n3td3v’s Person #2, Person B frequently justifies actions and rationalizes purposes. In addition, both people are less likely to verbally attack other people.
- Person C: Corresponding with n3td3v’s Person #3, Person C’s writings generally carry an emotional aspect and discuss personal feelings. Although not confirmed, this could be Alicia, as identified in a Gobbles cartoon[17].

3.8 Author Analysis Limitations

Profiling techniques are not definitive. Instead, profiling is used to narrow down the range of suspects. Blood typing and DNA are two common profiling methods. In blood typing, there are a limited number of types (A+, AB-, etc.) and a high likelihood of two people having the same type. However, if an actor is known to be type “A+” and a suspect is “AB-”, then the suspect can be immediately dismissed as not being the actor. DNA has many more variables than blood typing. While DNA is virtually unique (excluding identical twins), most tests only check sequence lengths, not actual unique codon sequences; one in 30 million people might appear identical.

The author analysis techniques used in this paper have many more variables than blood typing, but not as many variables as DNA. Personal profiles based on these linguistic approaches are not unique, but are distinct. The distinct attributes of these author analysis techniques falls between DNA and blood typing. These methods cannot be used to positively identify Person #1 as Person A, but can identify that Person #1 is *not* Person B. In this case, any one of the three people could have a doppelganger with the same author profile. However, the likelihood of three distinct people who are known to work together being tested and having extremely similar attributes, skills, and personalities as another distinct trio is extremely unlikely. As shown in section 1.3, the chances of randomly matching three out of three people are extremely slim. Due to the low chance of a false-positive match, it is very likely that the three core members of Gobbles Security are the core founders of n3td3v.

[17] A copy of the cartoon is available from the Internet Archive’s Wayback Machine (*web.archive.org/web/20030605182840/bugtraq.org/art/comic-001.jpg*). The artist has the same verbal characteristics as Person B (Unix Terrorist). Many of the straight lines have a slight sweep, indicated a right-handed artist.

4 Additional Correlations

The feedback and correlations from n3td3v are not limited to their posted comments. There have been other correlations and findings. Consistencies between Gobbles Security and n3td3v involve their appearance and presentation methods.

- Gobbles started by harassing people in the BugTraq and Full Disclosure online forums. Gobbles then branched out to news-related blogs and other comment-feedback systems. n3td3v started by harassing people on the same forums, and then spread to news-related blogs and other comment-feedback systems.
- Gobbles vanished after their presentation at Defcon 10. n3td3v started up after Gobbles vanished; there is no overlap between their appearances. In addition, n3td3v temporarily stopped posting after Defcon 14.
- Both Gobbles and n3td3v have mentioned having a higher purpose than merely insulting people. Gobbles initially harassed people, but then began releasing zero-day exploits. The harassment was likely used to gather a following and achieve a desired attention level. n3td3v seems to be gathering a following and may have a similar mission: they may be waiting for the right time to release a series of zero-day exploits. Considering their dislike toward Microsoft and the impending release of Vista, this is a plausible purpose.

While there have been a few public postings that suggest a relationship between Gobbles Security and n3td3v, the postings have not used any quantifiable analysis. Unfortunately, gut feelings and minority opinions are subjective and not scientific.

4.1 Feedback

In response to a review of Dr. Krawetz’s Black Hat Briefings presentation on author analysis and profiling, n3td3v wrote[18]:

> **artificial intelligence**
> Posted by n3td3v - August 2, 2006 3:31 PM PDT
>
> You really think its as clear cut as that? No, hackers have A.I programs.
> They type their blog entry, forum entry or e-mail and then copy and paste the text into their program.
> The program then generates grammar based on pre-loaded grammar examples of a certain person, or gender.
> Say I want to sound like Joris Evers, I find lots of articles by him, throw the text from those articles into the A.I program engine and the program will translate any of my text into 'Joris Evers speak'.
> I think folks underestimate how sophisticated hackers are now not to be identified via grammar and spelling.
> This is essential, especially when you want to carry out, for example phishing attacks against corporations.
> If I were to type up a fake Paypal site and spam it all around the internet, people would be able to say 'look at the text in this Paypal scam, doesn't this look like n3td3v has written this?'
> Exactly the reason hackers are using A.I to mask their natural grammar style and spelling mistakes.
>
> n3td3v

The people who are identified as likely being behind n3td3v were not at the presentation. (Or they at least were not any of the 400 people in the room and they were not observed walking around the Black Hat Briefings conference floor.) It is clear that this comment is based on a summary from a reporter and not the presentation itself. For example, the presentation explicitly listed the limitations from the use of translation systems and cut-n-paste.

In any case, a male, native English speaker likely wrote the feedback. This author has similar attributes to Person #1 and Person A. The author claims to use an artificial intelligence system to generate text. If this is the case, then the same A.I. system appears to be used by both n3td3v and Gobbles Security. In truth, it is very unlikely that this text was written using an A.I. system – few A.I. systems have ever passed the Turing test. In contrast, it is probable that Gobbles wrote it.

[18] *http://reviews.cnet.com/5530-10921_7-0-10.html?forumID=110&messageID=2108507&threadID=195699* accessed on 4-Aug-2006.

4.2 Who was n3td3v?

On 1-Sept-2006, n3td3v posted a message indicating that the group was ending their online presence.[19]

Full Disclosure posting by n3td3v. All spelling and grammar errors are from the original posting.
Subject: **[Full-disclosure] n3td3v: viva end of n3td3v----and security group** From: n3td3v <xploitable@gmail.com> Date: Fri Sep 1 20:13:50 BST 2006 n3td3v with the beginning Spetember 1st 2006 is the end of n3td3v commentry via Full-Disclosure list or any other medium. This is because n3td3v is moving into the professional scene, so underground hacker scene isn't suitable for the n3td3v agenda. The agenda now is to lay low and say nothing. n3td3v understands the security community needs n3td3v, but n3td3v needs to follow career paths into an academic life style away from the homebred/international hacker community. Thank you Yahoo and Google for being a part of my life during the past 7/half years, its been a blast. Take care security community, the force of n3td3v is with you. Our final death wish is that the security community cross-posts to n3td3v at googlegroups.com, see our mailing list at http://groups.google.com/groups/n3td3v ---all communications for n3td3v group are being passed over to co-commanders,,,,the n3td3v founder and commander in chief is no longer in charge of n3td3v operational decisions-----enjoy the rest of your life. We'll be in touch,,,,,,,,don't forget the power of n3td3v, we're not dead, we're changing command......good bye---for now. Its time for n3td3v to goto academic and move on with the agenda that serves us. Google and Yahoo, good bye, your staff have been briefed on operational detail in private for the following years ahead as we prepare to reduce public relatiions on mailing lists and go fully underground! Add the n3td3v mailing list to your books, this has been a n3td3v production...the rest is upto you to bring the biggest corporations to its knees! rest in peace.......

The text of this document has similar characteristics to n3td3v Person #1 and Gobbles Security Person A. The gender determination is strongly weighted as a male. Although there are few sentences, the sentence lengths and punctuation frequencies[20] are within the range used by Person #1. In addition, the range of words (lexical analysis) indicates a similar vocabulary range to Person #1. This posting was likely written by the person identified as Gobbles.

Gender Analysis	Sentence Lengths	Punctuation Frequency

Genre: Informal
Female = 195
Male = 761
Difference = 566; 79.6%
Verdict: MALE
	`#Sentence word-count/length:`
	`48 1 (25.00%)`
	`34 1 (25.00%)`
	`24 1 (25.00%)`
	`15 1 (25.00%)`
		`# character frequencies:`
		`. 4 (22.22%)`
		`? (0.00%)`
		`! (0.00%)`
		`, 3 (16.67%)`
		`: (0.00%)`
		`; (0.00%)`
		`( (0.00%)`
		`) (0.00%)`
		`- 1 (5.56%)`
		`" 8 (44.44%)`

Following this “final” posting were a several postings by a forth person claiming to be n3td3v.

- 1-Sept-2006: Full-Disclosure mailing list <*http://lists.grok.org.uk/pipermail/full-disclosure/2006-September/049218.html*>. This posting tests as male, but has a distinctly lower gender-weighted score than postings by Person #1. The punctuation frequency appears different and the lexical range appears smaller. In addition, the author did not use the word “n3td3v” in place of personal pronouns and did not use any insulting, inflammatory, or self-appraising vocabulary. This author is unlikely the same as Person #1, Person #2, or Person #3.

[19] *http://lists.grok.org.uk/pipermail/full-disclosure/2006-September/049219.html*

[20] This writing sample uses repeated periods and commas. The duplications were removed before conducting the analysis. With the duplications, the ratio of periods to commas does not significantly change.

- 5-Sept-2006 and 6-Sept-2006: Google Groups N3td3v mailing list. The same posting appears to have been sent twice. Unlike other n3td3v postings, there appears to be only one sentence written by the author; all other texts were pasted from news reports. In addition, these postings were political in nature (not technical; they discussed the British Prime Minister). Even though there is not enough text to analyze, the significant change in content from other n3td3v postings implies a different individual.
- 11-Sept-2006: Google Groups N3td3v mailing list. This was another political posting, with only one sentence and a link to a news site. While this may be by the same author from 5-Sept-2006 and 6-Sept-2006, the author is probably not by Person #1, Person #2, or Person #3.

As of 7-Oct-2006, there have been no other postings by people claiming to be n3td3v. It is very plausible that n3td3v had, in fact, changed hands on 1-Sept-2006 and is no longer active.