

1 RACHEL MEDWOOD
2 BENJAMIN SHAPIRO
3 EMILY WADA
4 GRAHAM YOAKUM
5 LOYOLA & CALTECH, LLP
6 1200 East California Blvd.
7 Pasadena, CA 91125

8 Attorneys for Defendants
9 DANIEL BALTIMORE, JOHN JOHNSON, SUNDANCE LAW, and
10 CALIFORNIA INSTITUTE OF TECHNOLOGY (“Caltech”).

11 SPECIALLY APPEARING AS OF COUNSEL:

12 ROBERT CORBIN - #75445
13 CORBIN & FITZGERALD LLP
14 601 W 5th St #1150
15 Los Angeles, CA 90071-2024
16 FRED VON LOHMANN - # 192657
17 ELECTRONIC FRONTIER FOUNDATION
18 454 Shotwell St
19 San Francisco, CA 94110-1914

20 UNITED STATES DISTRICT COURT
21 WESTERN DISTRICT OF CALIFORNIA

22 UNITED STATES OF AMERICA,)	Case No.: RL-04-9999
)	
23 Prosecution,)	WITNESS STATEMENT OF DEFENSE
)	EXPERT SETH SCHOEN
24 vs.)	
)	
25 DR. DANIEL BALTIMORE,)	Date: May 21, 2004
26 PROFESSOR SUNDANCE LAW, JOHN)	Time: 2:15 pm
27 JOHNSON, AND THE CALCULATING)	Courtroom: Beckman Auditorium
28 INSTITUTE OF TECHNOLOGY,)	
)	
Defendants.)	

I, Seth Schoen, declare as follows:

1. I make this declaration for defendants on my own personal knowledge. I currently hold the position of Staff Technologist with the Electronic Frontier Foundation, and have attached hereto a current curriculum vitae.

I. CRYPTOGRAPH AND CRYPTOGRAPHY RESEARCH

2. Cryptography is a field of mathematics that includes, among other things, the transformation of information to provide confidentiality or integrity of messages, together with cryptanalysis, or attacks on the security of cryptosystems.

3. Cryptography includes the use of mathematical methods called ciphers to transform messages using a value called a key, with the goal of making a message unintelligible to anyone who does not know the relevant key. This is valuable for security because it allows the difficult problem of assuring the security of messages to be reduced to the problem of assuring the security of keys, which is often easier.

4. Some ciphers, such as so-called "one-time pads", can be shown mathematically to provide no conceivable useful information at all to an attacker. That is, it can be demonstrated that a message properly encrypted with such a cipher would not provide any basis for the attacker to believe that any one possible original message was intended more probably than any other was. A cipher that provides no useful information at all is called "unconditionally secure".

5. No purely cryptanalytic attack against an unconditionally secure cipher can ever succeed. However, an attacker might discover some useful information by other means. For instance, the attacker might examine the presence, source and destination, length, or timing of a message, and draw inferences from any of these. In some cases, the fact that a message of a certain length was sent at a certain time might in itself be sufficient to produce relevant information, much as law enforcement officers sometimes seek to obtain "pen/trap orders" to find out the patterns of

1 communications, but not the contents of communications, among suspects. This process is known
2 as traffic analysis.

3 6. Unconditionally secure ciphers are rarely used for communications, because they require
4 vast amounts of key material, which must never be re-used and the secrecy of which must be
5 carefully maintained. One-time pads are sometimes used for extremely sensitive military or
6 diplomatic communications.
7

8 7. Ciphers that are not unconditionally secure may still be extremely useful. In many cases,
9 knowledgeable cryptographers may form a consensus that a successful cryptanalytic attack against a
10 particular cipher appears to be humanly impossible, or unreasonably expensive, based on the current
11 mathematical state of the art. While such an attack is still logically possible, experts may be unable
12 to imagine any practical way of carrying it out.
13

14 8. This distinction is illustrated nicely in a 1981 paper entitled "Mental Poker" by Adi Shamir,
15 Ronald L. Rivest, and Leonard M. Adleman. These three cryptographers are the co-inventors of an
16 important and widely used cryptosystem called RSA. Shamir, Rivest, and Adleman use their
17 cryptosystem to try to solve the "Mental Poker" problem: "two players [...] want to play poker over
18 the telephone" in such a way that neither can cheat. The cryptographers devise "[a]n elegant
19 protocol for dealing the cards that permits one to play a fair game of Mental Poker", but
20 simultaneously offer a mathematically "rigorous proof that it is theoretically impossible [to do so]".
21 The tension between these two results is ultimately resolved by "the enormous computational
22 difficulty of [cheating] by 'breaking' the code". That is, cheating at Mental Poker is theoretically
23 possible, but nobody can imagine how to build a machine that would perform the necessary
24 computations.
25
26
27
28

1 9. Cryptographers have often wished to produce formal mathematical proofs of the level of
2 security provided by particular ciphers, but so far, they have not been able to find many conclusive
3 proofs. Instead, they have shown in some cases that attacking some given cipher is harder than
4 solving some other particular mathematical problem, which is a relative and not an absolute proof
5 of difficulty.
6

7 10. Because of the difficulty of formal proofs of security, the cryptographic community has
8 employed an alternative: the extensive study of the family of attacks against proposed security
9 systems -- a form of scientific peer review.
10

11 11. Traditionally, the U.S. National Security Agency conducted a kind of internal, classified
12 review of security systems, while the public cryptographic community conducted an open, public
13 review; according to cryptographer Bruce Schneier, no other organizations in the U.S. have
14 generally had adequate resources to perform their own satisfactory security assessments of newly
15 proposed cryptographic techniques.
16

17 12. For those who, like most prospective users of cryptography, lack relevant security clearance,
18 the best we can do to evaluate claims of strength for some security system is to see how it fares
19 when subjected to public scrutiny and attack by those skilled in the arts of cryptanalysis.
20

21 13. Cryptosystems that lack unconditional security can generally be attacked by "brute force",
22 which is to say by trying every possible key. "Brute force" is a pejorative term because brute force
23 attacks may not use mathematical subtlety; like chess players, cryptographers admire cleverness.
24

25 14. Against a particular system, there many other attacks employing clever mathematics to
26 obtain certain information about the key or the message. For example, a mathematically skilled
27 observer might deduce that one or more key bits in a particular cryptosystem can be calculated
28 directly from some particular property of an encrypted message.

1 15. However, some of these attacks will merely offer a particular solution (a "speed-up over
2 brute force") that allows certain keys to be ruled out quickly; to reduce the attacks to practice, it
3 would still be necessary to mount a brute force attack. Thus, many successful attacks have a brute-
4 force element together with a clever mathematically oriented discovery or group of discoveries that
5 allow many possible keys to be eliminated rapidly.
6

7 16. When an attack contains a brute force element, there must be some way of recognizing when
8 the attack has been successful. This might take the form of a small amount of "known plaintext" (for
9 example, an attacker might expect a business letter to begin with "Dear" or an e-mail message to
10 start with "From"), or might include some statistical test to see whether a candidate decryption
11 appears to resemble English text or other usable data.
12

13 **II. CONTROVERSIES OVER REAL-WORLD CRYPTOSYSTEMS**

14 17. Valuable information has often been gained from attacks against actual cryptosystems.
15 Although, for reasons discussed earlier, the failure of a particular attack does not prove that a
16 system is secure, the success of an attack can prove that the system is not secure. In some cases, the
17 failure of an attack may also help provide a concrete estimate of how effective any similar attack
18 might be.
19

20 18. The tradition of creating challenge messages dates back at least to 1977, when Rivest,
21 Shamir, and Adleman published a message encrypted with their RSA system as a challenge with a
22 \$100 prize. The message, 9686961375462206147714092225435588290575999112457431987469
23 5120930816298225145708356931476622883989628013391990551829945157815154, was
24 published in Scientific American in August 1977. The challenge was not solved until 1994, when a
25 team of cryptographers used a distributed Internet search with help from volunteers to determine the
26 original plaintext, "THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE". The attack
27
28

1 provided a useful benchmark of the difficulty involved in attacking the RSA cryptosystem when
2 used with keys of a particular length.

3 19. RSA Data Security, Inc., a company founded to commercialize the RSA technology,
4 continued the tradition by offering a series of prizes designed to induce people to mount attacks
5 against its own cryptosystem, as well as to solve certain other mathematical problems. RSA's goals
6 in offering these prizes apparently included expressing its own confidence in the strength of its
7 system, gathering empirical results about the state of the art in attacks against RSA, and
8 demonstrating to the public that certain attacks against RSA were relatively difficult.
9

10 20. Another cryptosystem, called the Data Encryption Standard (DES), was widely used
11 throughout the past two decades. It was adopted as a standard in 1977 and recommended by the
12 U.S. government through the National Bureau of Standards (subsequently National Institute for
13 Standards and Technology). Ever since its creation, the security of DES was the subject of great
14 controversy, because of the non-transparent process employed in the creation and selection of the
15 system, and because of persistent rumors about the role of the National Security Agency in the
16 creation of DES.
17

18 21. Many people believed that NSA, which performs cryptanalysis of intercepted
19 communications, had somehow attempted to reduce the security of DES, perhaps by adding some
20 kind of flaw known to DES, or perhaps by reducing the specified key length, among other
21 possibilities.
22

23 22. Other things being equal, ciphers that use shorter key lengths are much easier to attack by
24 brute force. Each additional key bit in a symmetric cipher like DES doubles the number of key
25 possibilities and so roughly doubles the amount of time that would be consumed for a successful
26 brute force search.
27
28

1 23. DES, as specified by the government, uses a 56-bit key.

2 24. Completely separate from their views about whether NSA had influenced the design of DES
3 and whether DES contained any cryptographic design flaws that might facilitate cryptanalytic
4 attack, many cryptographers voiced concerned during the early 1990s that DES would be vulnerable
5 to a brute force attack, perhaps using a specially constructed DES-cracking machine.
6

7 25. Some skeptics of the security of DES pointed to Moore's Law, an observation by the
8 semiconductor pioneer Gordon Moore about improvements in microchip technology. While Moore
9 did not specifically address improvements in processor speed, Moore's Law has often been
10 colloquially paraphrased as an observation that "available processor speed doubles every eighteen
11 months". If correct, this would suggest that the processor power available to an attacker for a
12 constant cost would also tend to double every eighteen months because of improvements in
13 technology. (Equivalently, the attacker could generally successfully attack a symmetric cipher with
14 one additional key bit every eighteen months for a constant cost.) Published papers in the early
15 1990s suggested that DES should probably no longer be considered secure against brute force
16 attack, or that it was approaching the end of its useful lifetime and ought to be replaced by a more
17 modern cipher with a substantially larger key length.
18
19

20 26. RSA Data Security was also interested in assessing the security of DES and offered prizes
21 for the successful decryption of various messages encrypted with DES, as well as several other
22 symmetric ciphers. By offering these prizes, RSA hoped to establish the approximate difficulty of
23 brute force attacks against these ciphers.
24

25 27. The first challenge was won in June 1997 by a team of computer enthusiasts collaborating
26 over the Internet and coordinated by Rocke C. Verser. Verser's project, called DESChall, was the
27
28

1 first time anyone had ever publicly demonstrated the capability of breaking DES, although it took
2 his group several months to decrypt a single message.

3 28. I participated in the DESChall project by contributing computer power. That is, I instructed
4 various computers to which I had legitimate access to attempt to help Verser crack DES when they
5 had nothing else to do. I did this because I wanted to help demonstrate that DES was no longer
6 secure by modern standards and ought to be replaced, and because I liked the idea of collaboration
7 by Internet users to solve difficult mathematical problems.
8

9 29. The participating computers would contact Verser's server, which would instruct them to
10 attempt to decrypt RSA's message using various candidate keys. The participating computers
11 would then advise Verser of whether or not they had been successful. When one computer was
12 finally successful in its attempt, it advised Verser, who then contacted RSA. Thus, the computer
13 power of all these computers (which were owned and operated by people who had never met and
14 who had no formal association with one another) was jointly harnessed to demonstrate the ability to
15 crack DES.
16

17 30. Although this technique had previously been used to solve other mathematical problems,
18 such as the original challenge by Rivest, Shamir, and Adleman themselves, the DESChall project
19 enjoyed an unusual amount of public attention. It was the first time I had the opportunity to
20 participate in such a "distributed computing" project. I will discuss other distributed computing
21 projects and their significance below.
22

23 31. RSA conducted more challenges in which it invited people to crack DES faster than Verser's
24 team had cracked it. Because some government representatives, especially law enforcement,
25 continued to claim incorrectly that DES offered a very high level of security and did not need to be
26
27
28

1 replaced, my current employer, the Electronic Frontier Foundation, became involved. (I was not
2 employed by EFF at that time and learned about the facts I describe here from books and articles.)

3 32. EFF constructed a purpose-built DES-cracking machine that was specifically designed to
4 decrypt messages that had been encrypted with DES. The cost of this machine was something over
5 \$200,000, but most of the expense was associated with the design of the machine, not with parts or
6 assembly. EFF subsequently published the complete schematics for the machine and dedicated
7 them to the public domain, which would allow other interested parties to build equivalent machines
8 much more inexpensively.
9

10 33. The EFF DES Cracker successfully demonstrated an ability to crack DES by brute force in
11 just 56 hours of search in July 1998. EFF's DES Cracker was much faster than all of the computers
12 of the volunteers in Verser's project put together, but only when used to decrypt DES; it could not
13 be used for any other purpose.
14

15 34. This effort led to the publication of a book (Cracking DES: Secrets of Encryption Research,
16 Wiretap Politics, and Chip Design; O'Reilly and Associates, 1998) which included schematics for
17 the machine and source code together with historical and contemporary papers on the economics of
18 brute force attack against DES. This book was an important advance in the state of public
19 understanding about the security of DES and similar systems, and the design and demonstration had
20 validated the speculations of researchers about the efficacy of brute force attack.
21

22 35. These attacks against DES, and the publication of Cracking DES, undermined public
23 confidence in DES. This was an appropriate outcome, because the attacks (along with additional
24 attacks carried out in 1999) demonstrated that DES really was not adequately secure; they
25 demonstrated what the capabilities of a malicious attacker might be, for example. The attacks, as
26
27
28

1 Cracking DES explained, did not make the DES any more or less secure than it had been, but did
2 reveal much more accurate information about the level of security it enjoyed.

3 36. While the cryptographic literature on key lengths had already suggested this information, a
4 concrete demonstration not only advanced the science of cryptography but also provided valuable
5 publicity and a more concrete desire among DES users, especially those who had been unfamiliar
6 with the research literature, for improved alternatives.

7
8 37. At about the same time as the first of the public attacks against DES, the National Institute
9 of Standards and Technology promptly sought to develop a replacement for DES. NIST employed
10 an open and transparent process for the selection and validation of the new government-
11 recommended encryption algorithm. This process involved and invited attacks on candidate
12 ciphers. The cipher NIST eventually selected, called the Advanced Encryption Standard (AES),
13 supports substantially larger key lengths and enjoys broad public confidence. AES was adopted by
14 the government in 2000 and was quickly implemented by many software developers. For many
15 applications, including securing financial transactions, private e-mail, and trade secrets, AES has
16 been replacing DES.
17

18
19 38. I believe that the replacement of DES by AES is an objective improvement in computer
20 security that would likely have been further delayed without high profile and realistic
21 demonstrations of the insecurity of DES.

22 39. After 1998, I observed what I interpret as a consensus among cryptographers that symmetric
23 ciphers with key lengths around 56 bits and below should be considered "weak" and not deployed in
24 new applications in which a skilled adversary might perform a brute force attack. NIST's
25 recommendation of AES has also been interpreted as an endorsement by the government of this
26 view. As NIST recommended, AES key lengths start at 128 bits; that is, the least secure way to use
27
28

1 AES correctly is with a 128-bit key. Since each key bit doubles the number of possible keys, a 128-
2 bit symmetric key is 2^{72} or 4,722,366,482,869,645,213,696 times as hard to attack by brute force
3 as a 56-bit key.

4 **III. THE CONTINUED IMPORTANCE OF DISTRIBUTED COMPUTING**

5
6 40. Not only have the technologies developed in the course of attacks on RSA, DES, and other
7 systems (including RSA's RC4 and RC5 ciphers) advanced cryptographic science, they have also
8 demonstrated the power of distributed computing technology and provided instructive early
9 examples of how to deploy and manage widespread distributed computations. Aside from attracting
10 attention to the possibilities of distributed computing, they have provided engineering case studies
11 that help future developers understand how to create distributed systems that scale well, that resist
12 attack, and that can defend themselves appropriately when participants try to cheat by returning
13 false or corrupt data.
14

15 41. The success of DESChall and of another group called Distributed.Net in solving RSA's
16 cryptographic challenges inspired a number of other distributed computing projects, not all of which
17 were related to cryptography.
18

19 42. For example, researchers at the Space Sciences Laboratory at UC Berkeley built on the
20 success of Distributed.Net to implement an earlier plan for what they referred to as "public-resource
21 computing" to analyze recorded data from radio telescopes for statistical patterns that might indicate
22 transmissions by intelligent civilizations on other planets. Their SETI@Home project is ongoing
23 and remains enormously popular.
24

25 43. Although it had begun in 1996, the Great Internet Mersenne Prime Search received renewed
26 attention from the Internet community after DESChall's and Distributed.Net's successes inspired
27 more Internet users to devote their computer resources to solving difficult mathematical problems.
28 The Mersenne Prime Search attempts to identify the largest prime numbers ever discovered by

1 performing sophisticated tests on certain numbers to discover whether or not they are prime. This
2 project has significantly advanced the science of number theory, and has also achieved several
3 world records for the discovery of large primes. Since 1997, the Mersenne Prime Search has held
4 the record for the discovery of the largest known prime. In March 1999, an anonymous donor,
5 recognizing the potential of distributed computing to solve additional mathematical problems,
6 endowed \$500,000 worth of prizes to encourage the discovery of extremely large prime numbers by
7 distributed computing systems; these prizes are administered by EFF as the EFF Co-operative
8 Computing Awards. The first of four awards has now been made to the Mersenne Prime Search,
9 which has demonstrated the vitality of distributed computing as a means of solving challenging
10 computational problems. (Other mathematics research on somewhat more obscure problems, such
11 as the discovery of abstract objects known as "optimal Golomb rulers", is also on going.)

14 44. Many researchers are considering the possibilities of using "grid computing" to share
15 computational resources for scientific applications and of "cluster computing" to replace
16 supercomputers by networks of smaller, cheaper personal computers working together. Different
17 kinds of mathematical problems are amenable to solution by different kinds of clusters; for some
18 problems, the computers should be identical and connected by a fast network at a single physical
19 location, while other problems can be solved by a heterogeneous collection of computers spread all
20 around the world. Distributed computing projects such as cryptography-related collaborations are
21 helping to reveal which kinds of problems can be solved by which sorts of distributed computing
22 clusters.
23

25 45. When I worked at the National Energy Research Scientific Computing Center at Lawrence
26 Berkeley National Laboratory in 1998, I learned that the United States Department of Energy was
27 extremely interested in grid computing and cluster computing and was considering deploying
28

1 clusters of personal computers to replace supercomputers for particular applications. Since then, the
2 Department of Energy has actually purchased and built enormous cluster systems that are being
3 used for simulations of the natural world, including nuclear weapons simulations and medical
4 research. DOE has also funded research into grid computing and the sharing of computing
5 resources across large distances. For technical reasons, systems like DESChall and Distributed.Net
6 will never be efficient for physics simulations, but they can be extremely effective for other
7 research tasks such as analyzing the results of experiments. (Indeed, SETI@Home is essentially
8 allowing home users to participate in analyzing the results of an enormous radio astronomy
9 experiment.) I believe that insights from projects such as DESChall and Distributed.Net are
10 continuing to bear fruit in showing how to build large and reliable distributed computing systems,
11 and what sorts of problems may be solved efficiently by such systems.
12
13

14 **IV. DRM SYSTEMS**

15 46. An extremely controversial contemporary application of cryptography is in the creation of
16 so-called "digital rights management" (DRM) systems.

17 47. DRM systems attempt to apply and enforce policies that restrict the use of some information
18 in digital form.

19 48. Typically, rather than merely attempting to limit the people or organizations to which some
20 information will be intelligible, DRM systems attempt to limit the devices or computer programs to
21 which it will be intelligible. For example, a DRM system designer may believe that a particular
22 program (perhaps written by himself or herself) enforces some policy, whereas other programs do
23 not. The designer may take steps to try to make encrypted documents intelligible to that program
24 and not to other programs.

25 49. DRM systems have been controversial not only because of their effects, with which my
26 employer, EFF, has long been concerned, but because of their design. Several cryptographers have
27
28

1 argued that DRM systems generally violate the so-called Kerckhoffs criterion or Kerckhoffs rule, a
2 foundation of modern cryptographic methods. Named for pioneering security expert Auguste
3 Kerckhoffs, the criterion states that a cryptographer must assume that a third party, attempting to
4 intercept and decode a communication, has access to the encryption method being used; the security
5 of the encryption relies on the secrecy of the key, a piece of information which must be kept secret
6 from an adversary. But since the adversary in a DRM system is the legitimate end-user, the
7 Kerckhoffs criterion has arguably been violated by the distribution of the secret key to the adversary.
8 After all, DRM systems typically include decryption keys in hardware or software, and a user, by
9 studying either, can recover these keys -- a category of attack that simply does not exist in
10 traditional cryptographic applications.
11

12
13 50. Indeed, such attacks against DRM have been routine. For example, Jon Lech Johansen and
14 his associates created the popular DeCSS software simply by studying software that implemented a
15 DRM system and learning its "secrets" -- secrets that had been distributed directly to many millions
16 of end users. (I criticize the DRM system in question, CSS, for its key length below, but the key
17 length was not a factor in the successful attack by Johansen et al.; instead, the attack was possible
18 because the DRM developers caused the relevant keys and other information to be published inside
19 every single DVD player.)
20

21 51. In the same sense, DTCP, which I describe briefly below, could be successfully attacked
22 without any sort of cryptanalysis, because the necessary information is distributed to the public
23 within every DTCP implementation. DTLA demands that DTCP implementers use certain
24 measures to make it difficult for purchasers of devices that implement DTCP to study those devices,
25 but it is unclear what effect these measures will have against intrepid researchers. However, that
26 attack is not the particular attack employed in the present case.
27
28

1 52. Generally, DRM systems work by encrypting both a document and associated policy (here
2 referred to as "CCI", or "copy control information", which may be too narrow a term because
3 policies may restrict many activities other than copying). DRM developers attempt to ensure that a
4 relevant decryption key will only be available to devices or software that are somehow known to be
5 expected to implement or enforce the policy. Then devices or software that will not enforce the
6 policy cannot decrypt the document, and, conversely, certain devices or software that will enforce
7 the policy can decrypt it.

9 53. Since commercial publishers renewed their interest in DRM systems in the mid-1990s, the
10 DRM field has exploded and many researchers and vendors have explored DRM technology. As a
11 result, DRM is a much larger subject than it is possible to treat in detail here, and encompasses
12 many implementation details, means of conveying and expressing policies, etc., that are beyond the
13 scope of this report.

15 54. Importantly, DRM systems generally depend on various "cryptographic primitives", such as
16 ciphers. If those cryptographic techniques can be attacked, the attacks against them may be used in
17 turn to attack an entire DRM system.

19 55. Many commercial publishers have begun to use DRM to try to restrict certain uses of some
20 of their published works.

21 **V. DTCP AND THE SUCCESSFUL ATTACK**

22 56. The Digital Transmission Content Protection (DTCP) specification is a relatively widely
23 deployed proprietary DRM scheme developed by five companies (Hitachi, Intel, Matsushita,
24 Toshiba, and Sony). The companies (and, by metonymy, the DRM scheme itself) are sometimes
25 collectively referred to as "5C".

27 57. DTCP is favored by various major U.S. motion picture studios, which have sought to
28 encourage its commercial adoption.

1 58. DTCP is a link encryption technology that specifies a means of encrypting data (typically
2 digital video data) as it is transferred from a "source" device to a "sink" device. Most commonly,
3 DTCP is used to interconnect consumer electronics devices using an IEEE 1394 (or "FireWire")
4 connector, if the devices to be connected have some contractual, statutory, or regulatory reason to
5 enforce publishers' policies against the users of the devices. DTCP can also be used over various
6 interconnections other than IEEE 1394.
7

8 59. The five companies that developed DTCP sent up a legal entity called the Digital
9 Transmission Licensing Administrator (DTLA), which enters into contracts with various
10 manufacturers regarding the implementation of the DTCP specification. DTLA and its member
11 companies assert that no one can lawfully manufacture DTCP implementations without a license
12 from DTLA.
13

14 60. DTLA publishes portions of the DTCP specification, and maintains certain secrets that are
15 needed in order to create interoperable DTCP implementations. I believe that DTLA provides
16 certain of these secrets to its licensees pursuant to non-disclosure agreements. I have never had any
17 reason or opportunity to learn any of DTLA's confidential information.
18

19 61. If a DTCP source device is to send encrypted video to a DTCP sink device, the devices first
20 participate in an authentication protocol by which they attempt to recognize one another, as part of
21 the process of enforcing publishers' policies. To my knowledge, if I connected a non-DTCP sink
22 device to a DTCP source device, the DTCP source device would be able to recognize that my sink
23 device did not implement DTCP, and consequently the source device could refuse to transmit
24 certain encrypted video across the link. (In general, whether the video would be transmitted even to
25 a DTCP sink device depends on the "copy control state" information maintained by the source
26 device.)
27
28

1 62. When a DTCP source device transmits video to a DTCP sink device, the video is "encrypted
2 on the wire"; this is what is meant by "link encryption".

3 63. The general parameters of this communication -- though not the encryption keys involved --
4 are published by the relevant IEEE 1394 standardization bodies and by DTLA. This means that it is
5 possible, using only published information, to make a device that records the entirety of the
6 encrypted video transfer from source device to sink device. This transfer can then be saved to a
7 hard drive. But since it is encrypted, it would not be meaningful or useful to anyone in that form.
8

9 64. Furthermore, DTCP uses cryptography in a standard and well-known way to prevent a
10 "replay attack" in which the data recorded as described above is played back into a sink device. The
11 sink device would be able to tell that the recording of an earlier communication was not "live", and
12 it would refuse to accept it. These techniques are widely used in many cryptographic applications,
13 not just DRM applications.
14

15 65. It appears to me from my examination of the facts that defendant Prof. Law and
16 subsequently other unidentified parties used a technique similar to what I have described to obtain a
17 recording of what is essentially a conversation between two DTCP devices. That recording could
18 have been obtained using only general-purpose technologies and public information, but, as I have
19 noted, since it would be encrypted, it would be difficult to use it for anything. It appears that Prof.
20 Law and other parties were able to use the decryption service at issue successfully to decrypt such
21 recordings. While it is not at all surprising to learn that DTCP was successfully attacked, this is the
22 first successful attack on DTCP of which I am aware. (The allure of attacking a real deployed
23 system might have attracted a particularly large number of people to participate in contributing their
24 computer power to the attack.)
25
26
27
28

1 66. It is worth noting that DTCP's link encryption uses a symmetric cipher with a 56-bit key. As
2 I have noted above, the use of such ciphers are not consistent with the state of the art in computer
3 security and it is reasonable to expect that a skilled attacker would be able to decrypt data encrypted
4 with such a cipher.
5

6 67. I tried to determine why DTLA or its member companies would have chosen to use such
7 weak encryption.

8 68. I considered the earlier example of the Contents Scramble System (CSS), which is used to
9 encrypt some commercially released DVD video discs, uses only 40-bit keys. In 1997, Ian
10 Goldberg, then a graduate student at the University of California, Berkeley, publicly demonstrated a
11 successful brute force attack against a different 40-bit cipher in only 210 minutes, using the
12 resources of a single university research network. The feasibility of this sort of attack would likely
13 have been obvious to any computer scientist even before Goldberg's demonstration.
14

15 69. An industry representative at a conference told me that CSS developers, despite their
16 awareness of the ease with which attacks could be performed, chose 40-bit keys because developers
17 of mobile devices, such as portable DVD players, preferred to produce small devices with long
18 battery life. Weak cryptosystems, compared to strong cryptosystems, may sometimes be
19 implemented in hardware using microchips that consume less power. Thus, the player
20 manufacturers hoped to economize their devices' power consumption by deliberately encouraging
21 the use of easier-to-attack encryption.
22

23 70. Industry representatives at other events have said that CSS used weak 40-bit keys because of
24 government-imposed export controls on the export of strong cryptography. Prior to successful legal
25 and regulatory advocacy campaigns by EFF and others, the U.S. government extensively regulated
26
27
28

1 the export of devices and software that could be used to achieve confidentiality of messages with
2 strong encryption.

3 71. However, I understand that the U.S. export regulations did not in general control the export
4 of strong cryptography when it was used solely for DRM purposes. Because other countries had
5 and have different export control regulations, it is possible that the use of weak cryptography in
6 DRM products has been viewed as desirable or preferable under the export laws or other
7 cryptographic regulations of some other nation.

8
9 72. I have not learned with certainty whether similar considerations motivated the selection of
10 56-bit keys for DTCP. However, I know that DTCP was invented after successful attacks had
11 already been demonstrated against other systems that used keys of around that length. I believe it is
12 reasonable to conclude that the inventors of DTCP chose 56-bit keys for reasons analogous to those
13 I have discussed above: to satisfy non-security-related wishes of device manufacturers, and/or to
14 attempt to comply with some nation's legal regulations applied to cryptography.
15

16 **VI. CONCLUSION**

17 73. Systems like those devised by Johnson are part of an important tradition in computer
18 security research that has yielded important insights about what is or is not possible with a
19 particular security system, insights which have significantly improved computer security. Generic
20 cryptanalytic and distributed computing tools and techniques are valuable contributions to science.
21

22 74. This declaration is true and correct to the best of my knowledge and was executed in San
23 Francisco, California.

24 Dated: April 21, 2004

25
26 _____
27 Seth Schoen
28 Declarant

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28