Course CSC 290A : Introduction to Cryptology

Term Project:
"The Story of Dmitry Sklyarov"

by **Eyal Mush**
emush@cs.rochester.edu
Computer Science, U of R
12/16/2004

Abstruct

Dmitry Skyarov a Russian programmer was arrested in 2001 during his stay in the US, at the request of Adobe Systems, according to the Department of Justice, and charged with distributing a product designed to circumvent copyright protection measures (the AEBPR). Only after two months he was bail out and was permitted to return home to Russia with his family.
The Charges against him had been dropped, as for Elcomsoft, the software company for each he had worked for, still remains subject to prosecution in the US.

Who is ElcomSoft Co.Ltd.?

Established in 1990, ElcomSoft Co. Ltd is a privately owned software company headquartered in Moscow, Russia, specializing in Windows productivity and utility applications for businesses and end users. And develops various security-related products, including password recovery products used by US government agencies to recover all sorts of documents files as included in Microsoft Office suite (Word, Excel, Access ect.), Lotus SmartSuite suite and archiving products (ZIP, RAR, ARJ and ACE). One of their products is the "notorious" advanced eBook Processor (AEBPR). According to the company's website, the software allows eBook owners to translate from Adobe's secure eBook format into a more common Portable Document Format (PDF). The software only works on legitimately purchased eBooks. It has been used by blind people to read otherwise-inaccessible PDF user's manuals, and by people who want to move an eBook from one computer to another.

Who is Dmitry Sklyarov and why he was arrested?

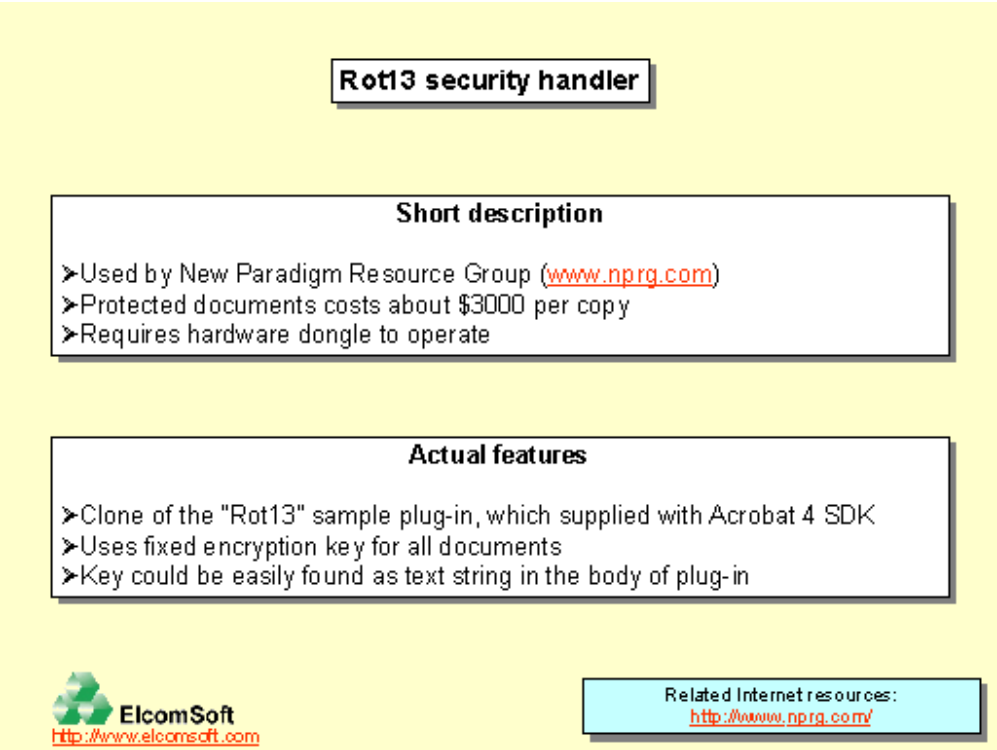
At that time Dmitry was a 27 year-old programmer employed by ElcomSoft, A PH.D student researching cryptanalysis at Moscow State Technical University, a respected cryptographer. He is married and is the father of 2 young children. And helped create the Advanced eBook Processor (AEBPR) software for his employer. The AEBPR has been used by blind people to read otherwise-inaccessible PDF user's manuals, and by people who want to move an eBook from one computer to another.

In July 2001 He was invited to give a presentation at the ***Def Con*** 9, a conference of computer hackers and security experts, at the Alexis Park, in Las Vegas, about the electronic security research work he has performed as part of his PhD research. His presentation concerned the weaknesses and flaws in Adobe's eBook technology software. On July 17, two days after, he was arrested as he was leaving to return to Russia, at the request of Adobe Systems, according to the DOJ **(**Department of Justice) complaint, and charged with distributing a product designed to circumvent copyright protection measures (the AEBPR).

Sklyarov's slide show presentation at DEF CON 9

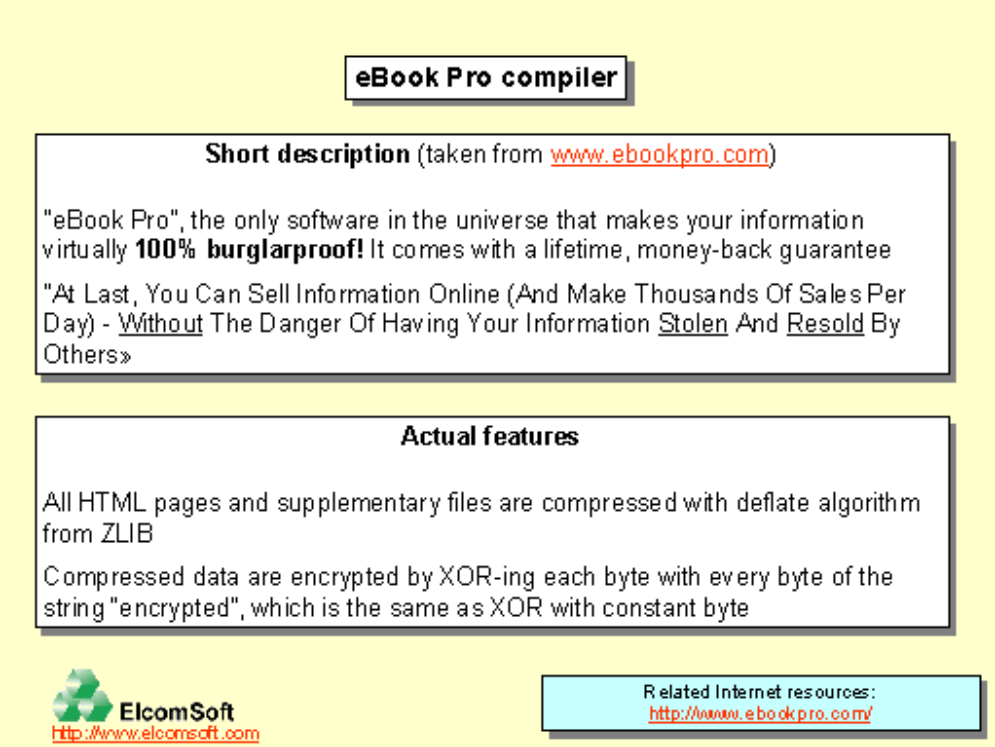
While the big publishing companies, such as Amazon.Com and Barnes & Noble, worry over the potential of illegal copies of their eBooks spreading around the internet, Sklyarov's presentation revealed that they could be ripped off in an unforeseen way: by the producers of stunningly absurd cryptography plugins used in their software. Sklyarov was arrested for revealing these secrets. Publishers encrypt their eBooks to prevent them from being read by anyone except the registered owner. What Sklyarov found out that the encryption software of at least two manufacturers is so weak that it can be broken with ease.

One publisher, New Paradigm Research Group, used a cipher called **rot13** that has been known since Caesar's time, the old plain substitution shift-cipher: for each letter, substitutes the letter that comes 13 places after it in the alphabet - an encryption method so weak that programmers refer to it as the familiar example used in any programming language, the *"Hello World"* of cryptography. Another publisher used to hide the code key by embedding the information inside the document itself, so that the key can be found and used to unlock the document instantly.



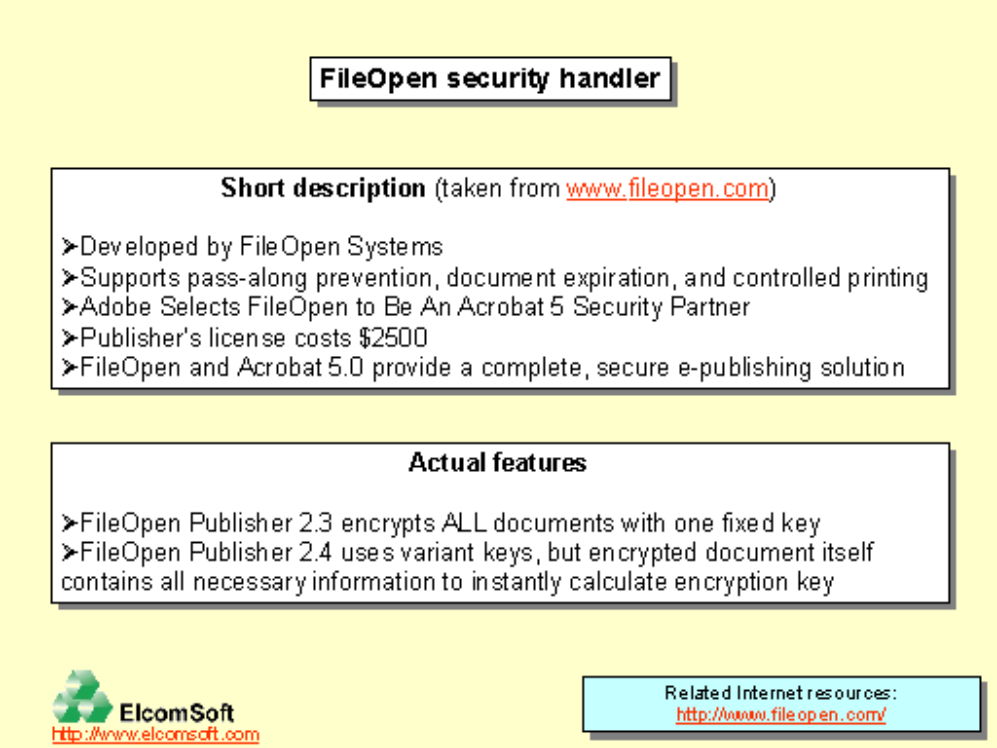
Presentation on DEF CON Nine, July 13th - 15th, 2001
eBooks security theory and practice - Slide 11

On slide 5, Sklyarov's went over the cryptographic algorithm of E-Book Pro, a protection software which was advertised as 100% burglarproof and claimed a list of Fortune 500 companies as its customers. Sklyarov found that the software "encrypts" e-books by mixing each byte of the text with a constant byte. Also, the programmer of this program tried to mix the plaintext with the word "encrypted", mixing with such a short, fixed string of characters would still have been a ridiculously weak encryption method and it probably shouldn't even be called cryptography.



Presentation on DEF CON Nine, July 13th - 15th, 2001
eBooks security theory and practice - Slide 05

On a different slide, Sklyarov's went over weaknesses in the FileOpen Systems e-book security program. Sklyarov found that the FileOpen software, which required a $2500 publisher's license, put the key information in the encrypted document, so that the code can be broken instantly. Although many of this program's customers were known to be scientific and technical journals, they weren't able to determine FileOpen's weakness, because they had no source code and insufficient documentation of FileOpen's internal processes. Sklyarov had to find that out by carefully examining the output of the software in a process of disassembly, reverse-engineering.



Presentation on DEF CON Nine, July 13th - 15th, 2001
eBooks security theory and practice - Slide 12

The best cryptography manufacturers, companies like RSA, publicly disclose their source code and documentation on their cryptographic algorithms, and the resulting encryption still can't be broken in a reasonable amount of time when used correctly. Once the source code is kept secret, it's very easy for the vendor to hide a weak implementation and sell its product to his novice customers.

But it's pointless to attempt to construct a cryptographic means of keeping data from being copied. Encrypted data can be copied as easily as any other data, and then can be viewed by anyone who has the encryption key. In the case of eBooks, one user's key can be used by everyone else, so then encryption us useless.

"He just pointed out that 'the king was naked' - so what's was all the fuss about?"

The Legal aspects

Dmitry Sklyarov and ElcomSoft faced five criminal charges in the indictment, counts of circumvention offenses, trafficking in technology primarily deigned to circumvent technology that protects a right of a copyright owner, and aiding and abetting circumvention offenses, this was a criminal prosecution brought under section 1204 of 17 USC conducted by the U.S. Attorney and the Department of Justice on behalf of the United States government. Basically, they were charged with distributing software that can crack and read encrypted Adobe ebooks in a manner not intended by the publishers. Under those charges, Dmitry faced up to 25 years in prison and a fine of up to $2,250,000, and ElcomSoft, as a corporation, faced a penalty of $2,500,000.

Dmitry Sklyarov and ElcomSoft were not accused of Copyright infringement. ElcomSoft claimed that its Advanced eBook Processor software could not be used by anyone except for people who have already lawfully purchased the right to view the eBooks. Instead, this case depended on constitutionally suspect provisions that were added to the Copyright Act by the DMCA.

Hmm .. what's the **DMCA** again?

DMCA is the Digital Millennium Copyright Act which was enacted in 1998. It has inserted new anti-circumvention provisions into the Copyright statute. These make it an offense to engage in an act of circumvention of a technical protection (section 1201(a)(1)), to develop and provide tools to others which would allow them to access a technologically protected work (section 1201(a)(2)) and to manufacture, import , provide or traffic in tools that would enable another to circumvent protection to copy a protected work (section 1201(b)(1)(A)). The DMCA's anti-circumvention provisions have both civil and criminal penalties carrying a maximum of 5 years' imprisonment and/ or a fine of up to $500,000 for a first offense.

So… these provisions address only the distribution of tools and software or information that can be used for copyright infringement as well as for legitimate non-infringing uses, such as fair use.

Hmm… and **Fair Use** is?

While copyright law grants authors the exclusive right to reproduce their works, the law recognizes an exception to this called fair use. The public's right to make fair use of copyrighted works is an integral part of US copyright law. Fair use rights allow people to make copies of copyrighted works, even when the author or publisher would rather them not. Fair use allows people to make a copy of a work for personal use, or for education, commentary, criticism, parody or other socially beneficial uses.

And ElcomSoft's Advanced eBook Processor (AEBPR) software allows users who have bought a legitimate copy of an eBook from any retailer to exercise the following fair use rights:

1. Make back-up copies and transport eBooks to the user's other pc or a PDA other than the one on which the eBook was first downloaded.
2. Excerpt - users can cut and paste little piece of eBooks for use in academic research, educational and teaching purposes, critiques, commentary and parody.
3. Print the eBook or a section of it, in order to read it.

So the DMCA's anti-circumvention provisions don't prohibit only possession or use of a circumvention technology (copy controls), so it's legal for people in the US to use AEBPR in a non-infringing way. Paradoxically, although it is legal for people to bypass these controls and use their 'fair use' rights, the provision of them is illegal under Section 1201 of the DMCA.

The Medi support for Sklyarov

An expert opinion

Bruce Schneier, founder and CTO of Counterpane Internet Security, in his article 'The Futility of Digital Copy Prevention' (published in the Crypto-Gram Newsletter), describes why it is an impossible task for the entertainment industry to implement widespread copy prevention of digital files, so that people can view or listen to content on their computer but can't copy or distribute it. He explains why the entertainment industry is doomed to fail in trying to use technology to save their existing business because they are contradicting the 4 natural laws of the digital world:

1. Bits are inherently copyable, easily and repeatedly which makes copying on the Internet very different from copying other merchandize as luxury accessories.

2. The ability of software to encapsulate skill. A copy protection scheme is never safe because those one-in-a-thousand hackers which can encode his break into software and then distribute it, and the average user can download it and use it.

3. The lack of political boundaries. The DMCA is a U.S. law which made it illegal to reverse-engineer copy protection schemes, but does not affect any of the hundreds of other countries on the Internet. And while similar laws could be passed in many countries, they would never have the global coverage it needs to be successful.

4. Unrestricted distribution is a natural law of digital content. So The industry need to accept the inevitable and find different ways to make money other than charging for a scarce commodity. They could be funded by advertisers, publicly by regulated taxation or funded by patronage.

Digital files cannot be made uncopyable, and that the public need business models as based on subscription, government licensing and other which respect the natural laws of the digital world.

Schneier also called the public to support in Dmitry in a later article in which he condemned the DMCA saying is unconstitutional, by contradicting the right for Freedom of speech.

The Public support for Dmitry

The site www.freesklyarov.org has followed Dimitry story since beginning, there had been actions organized to free Dimitry, such as Rallies across the country, and Petitions signing which were sent to local senators. After worldwide protests among programmers, Adobe backed away from its support of Sklyarov's prosecution, and government attorneys set aside charges against him in exchange for his testimony in the remaining case against his company.

How the story ended for Sklyarov and ElcomSoft

After Sklyarov was arrested in Las Vegas and held in a local jail briefly, then held in the Oklahoma City Federal Prisoner Transfer Center until August 3, 2001, when he was transferred to the San Jose (CA) Federal building. In total he was incarcerated from July 16 to August 6, 2001, when he was released on $50,000 bail, his bail conditions required him to stay within the federal court district of Northern California. On December 13, 2001 Dmitry Sklyarov was released from U.S. custody and allowed to return home to Moscow back to his family.

Although Sklyarov returned to the United States specifically to testify as a government witness, prosecutors never called him to the stand. Instead the government decided to play an hour-long edited videotape of Sklyarov's deposition instead.

After along year of filing motions and court hearing, a jury acquitted ElcomSoft of all counts against it in the first case to test the criminal provisions of the DMCA, a U.S. law aimed at updating intellectual property rules for the computer age. Although jurors agreed the product was illegal because it was designed to crack antipiracy technology controls, they declined to convict because they didn't believe ElcomSoft intended to break the law.

In one of his interviews, Sklyarov said that if someone would come to him with another project focused on cracking copyright protections he would answer him "if he's sure this is legal." And If the answer would be unclear, Sklyarov said he would suggest the person find a lawyer who could figure it out.

Essets

Skylarov remained in jail for the crime of whistle blowing and distributing a program that allows people to read books, something that should be considered a fundamental human right. There is no question that his software has a legitimate use - anyone should be able to read his own copy of an eBook with any software he wishes to use.
Dmitry just helped to unleash the band over the public eyes and reveal the machinery under the hood of a very common applications used by novice computer user out there, by doing so, he caused the big companies to acknowledge their professional weaknesses, although not explicitly, and make them improve their software security methods by using more advanced cryptography - and yes, math is good for everyone.

As for the DMCA, it is still the law, well at least here in the United States, but I am not bothered with it.

Glosarry:

DEF CON - the world largest underground hacking and security conference which takes place once per year in Las Vegas, Nevada.

DMCA - Digital Millennium Copyright Act

Keywords: Cryptanalysis , Software, Law

Resources:

http://www.freesklyarov.org/
http://www.eff.org
http://www.defcon.org
http://www-2.cs.cmu.edu/~dst/Adobe/Gallery/ds-defcon -Sklyarov's slides

'The Futility of Digital Copy Prevention' article by Bruce Schneier ("Crypto-Gram" Newsletter; May 15, 2001)