eNAC

The Cybex Initiative | e-NEWSLETTER ON THE FIGHT AGAINST CYBERCRIME

www.cybex.es
Nº6· DECEMBER · 2009

LEGAL

Francois Paget, Senior Research Engineer at McAfee summarizes the cybercriminal organization and their use of 2 key tools: carder forums and crimeware.

DATA PROTECTION

Francesco Testa, Antimafia Public Prosecutor from Catania talks about the Convention of Budapest of 23.XI.2001 including the new regulations of the Data Retention Activities and the protection of Electronic Evidence.

TECHNICAL

Valentín Hernando García and Arturo Rodríguez, members of the Spanish Civil Guard Criminalsitics Service, detail step by step a forensic analysis of an embedded device; an IP camera.

INSTITUTIONAL

Gorarzd BoZic, Team Representative of the SI-CERT (Slovenian Computer Emergency Response Team), talks about the SI-CERT and its methodology for reaction against Cybercrime.

JURISPRUDENCE

In this issue, we consider EU Directive 2007/64/EC on payment services in the internal market and how this will affect the way banks and credit card issues deal with proof when a customer challenges the issue that they did not use their card and electronic signature (PIN).

EVENTS

Selection of conferences for the months of December 2009 and January 2010 that might be of benefit to lawyers, prosecutors, technicians, judges, computer forensic specialists, law enforcement bodies or any person that deals with Cybercrime and electronic evidence.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

eNAC
e-NEWSLETTER ON THE FIGHT AGAINST CYBERCRIME
www.cybex.es
Nº6 · DECEMBER · 2009

Index

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

eNAC

e-NEWSLETTER ON THE FIGHT AGAINST CYBERCRIME

Dear readers,

We would like to thank you for all your positive comments regarding the Electronic Newsletter on the Fight Against Cybercrime (ENAC).

It is a pleasure for the ENAC team to realize that its objective of producing an e-Newsletter which provides, from one hand, a professional approach on the current problem of cybercrime from different perspectives -legal, data protection, technical, law enforcement, institutional and jurisprudence-, and on the other hand, the exchange of information and share of knowledge between professionals and updates on electronic evidence legislation around the world is being successfully accomplished.

But the effort being done by the ENAC team, Cybex, and the European Commission's Directorate General Freedom, Justice and Security would be senseless without a close relation with the project cornerstone, our readers. The ENAC has been thought, developed and prepared for you, so from the ENAC team we would like to welcome you to send us your feedback, your ideas or your requests so that they can be evaluated and taken into account.

We truly appreciate your support!

Enjoy the read,

Mrs. FREDESVINDA INSA
Project Director
finsa@cybex.es

Mrs. MIREIA CASANOVAS
Project Coordinator and Chief Editor
mcasanovas@cybex.es

Cybex
Plaza Cataluña 20, 9ª floor · 08002 · Barcelona · España
tel. +34 93 272 20 41 · fax. +34 93 215 50 72

Go to Russian version of the ENAC
Available on December 15th

Go to Spanish version of the ENAC

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

FRANCOIS PAGET
McAFee Avert Labs Senior Research Engineer

CYBERCRIME: TODAY'S ORGANIZATION, TOMORROW'S FUTURE?

François Paget is a senior malware research engineer at McAfee Avert Labs in France. He has been involved in malware research since 1990 and was a founding member of Avert Labs in 1995. Paget is a regular conference speaker at French and international security events, author of a book and numerous articles, and general secretary of the French Information Security Club (CLUSIF).

Introduction

Globalization offers many benefits to consumers and businesses. Unfortunately it also offers plenty of opportunities to organized crime. Globalization has promoted and strengthened the economics of illegal activities; offenders have become international entrepreneurs. The Internet, a globalized medium by design, provides money and information to all sorts of customers and businesses. It is notably the home of virtual worlds and their economies, which have attracted many people, including criminals. The unholy marriage of the Internet and crime has created two forms of "cybercrime": network attacks, and using those networks as a playing field for other activities. The criminals are also better organized thanks to the ease of global communication. Spanning borders and taking multiple forms, cybercrime poses new challenges that endanger citizens, our collective security, and the economy of every nation on the planet. There are many factors which make cybercrime successful. Among them, poor economies whose citizens can make better money in such criminals enterprises. This excerpt is from a new McAfee report, **Cybercrime and Hactivism**, whose main goal of this report is to show the extent to which organized groups will go when motivated by profit or political ideology. The report also explores the motivations that may lead an individual to fall into such illegal activities. For the purposes of this newsletter, we summarize the cybercriminal organization and the use of 2 key tools: carder forums and crimeware. You can read more details about online crime and other threat information in our full report and in other reports at McAfee's Threat Center, http://www.mcafee.com/us/threat_center/default.asp .

Organization and Glorification

Around the world, individuals and groups of pirates, activists, and mafia carry out illegal acts on the Net, often in the hope of becoming rich. Rather than going it alone, many Internet users join groups or they create new ones. Whether the reasons are economic, cultural, or technical, the motivations behind joining the virtual criminal universe are plentiful.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

In Russia, the hacking boom took place after the 1998 financial crisis. Myriads of small and large companies closed down, leaving programmers and developers out of work and hungry. In Bulgaria, a similar phenomenon occurred in the early 1990s, when an army of young, highly qualified, tech-savvy individuals could not find work. "Virus factories" became a big topic at that time. Besides the many unemployed yet skilled computer workers, corruption and economic decline fueled the emergence of cybercrime. Although some traditional criminal organizations attracted new recruits, other enterprising individuals started their own businesses.

Over the years, the business has become more and more methodical. Cybercrime companies that were created from nothing are now the IT division of the Russian mafia. Headed by technology or business school graduates from good families, the companies were seen as IT start-ups, just like any others. Otherwise poorly positioned, the hardened mafia members provided the capital. Uncertain in the area of management and business, hackers are far from the management teams, employed simply as labor when needed. Many of these companies benefit from the leniency—and even the protection—of the Russian Federal Security Service (FSB), especially against Interpol and extraditions to the United States and Europe. In return, they promise to never attack government IT infrastructures. This is an unspoken agreement that has been fully respected for nearly ten years. If these hackers are arrested, the secret services may offer the cybercriminals an alternative to prison by offering them jobs in the FSB[1].

Today, still, more than 75 percent of Russian science and technology students cannot find a job after graduating from university. To make ends meet, they or their tutors open shkola hackerov ("hacker schools"). At their homes, they provide lessons in hacking and then direct their students to crime channels that will allow them to earn two to three times more than they would if they led honest lives.

In Russia, traumatized by ultraviolent crime, society is likely to ignore cyberpiracy, which doesn't bring bloodshed to the streets and hardly affects public order. Some cybercrime syndicates are viewed by the public as Russia's new brainpower in the digital era. The criminals are also seen as Robin Hood figures, who can adequately support their families and share the spoils with the police by extorting spare change from the overly rich West. In China, a survey conducted in 2005 by the Shanghai Academy of Social Sciences shows that hackers and rock stars are looked upon with exactly the same esteem in the country. 43 percent of elementary school students said that they "love" hackers.

In the 1990s, as numerous graduates struggled to find work, some disillusioned programmers in Bulgaria wrote viruses. Although the term *virus factories* was used to describe their efforts, they had no employers and received no remuneration at the time. Often, the virus writers were motivated only by their dissatisfaction. Although high-quality malicious programs and related services sometimes earn a programmer up to US$1,000, the low wages do not attract computer specialists.

[1] Ruth Alvey, "Russian hackers for hire: the rise of the e-mercenary," Jane's Intelligence Review, July 1, 2001 p.2

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

In March 2001, the Russian hacker Igor Kovalyev spoke in an interview with *Wired Magazine*: "Here hacking is a good job, one of the few good jobs left."[2] The criminal path offers a way out and a chance for upward mobility. Skilled developers no longer hesitate to get closer to mafia organizations, which have become increasingly more interested in the Internet. Today, programmers easily agree to work with the mafia for remuneration.

In Asia, with the help of specialists and with great discretion, the Chinese triads have also discovered IT pirating. They have implemented modern forms of extortion—distributed denial of service (DDoS) attacks for ransom, for example—against commercial sites. Meanwhile, during the past decade, Chinese authorities have come to understand the growing dependence of modern armies on computers. The People's Liberation Army thus decided to establish the means for a future cyberwar. In 1998, during a speech before Congress, CIA Director George J. Tenet stated that China was looking to circumvent the U.S. Army's technological lead by using cyberwarfare as a tactic.[3]

Even in the United States, hackers or malware creators can sometimes find legitimate employment. The latest example occurred in April 2009. The author of the Twitter worm (JS/Twettir) was offered a job a few days after he was identified.[4]Thus the hacker becomes a winner. The cult of the hacker is dangerous, however. It gives everyone within it a positive image of delinquency, even though their acts are illegal. This celebrity could attract its supporters into carrying out criminal acts with less laudable motives than highlighting software flaws.

Alongside the mafias that are concentrated in particular areas, many groups form around timely opportunities. Some last several years, while others survive only a few months. Fraud such as the TJX scam, covered in more detail in the report, also involves groups of individuals who specialize in using counterfeit credit cards with previously stolen data. These groups come together and break up on a moment's notice. In March 2007, Florida police pursued one such group and made several arrests. Those questioned had cleaned out electronics stores and jewelers by using gift vouchers previously purchased with counterfeit cards that a partner had supplied to them. This money-laundering technique allowed them to make more than US$225,000 in purchases, as shown in a summary in *USA Today*. [5] In June, a second group of individuals was arrested. They held more than 200,000 credit cards from TJX and Polo Ralph Lauren.

Crimeware

Malware is often presented as ready-to-use tools that are user friendly. The crimeware market, in which malware is used to perpetrate crime, has undoubtedly converted some conventional branches of crime to digital. In 2009, the attack tools available for sale are more sophisticated. They require some expertise and in-depth network knowledge from their users. Today there are low-end products with prices driven down by competition, and high-end products which remain expensive.

[2] Inside Russia's Hacking Culture: http://www.wired.com/culture/lifestyle/news/2001/03/42346
[3] CIA Director, Testimony Before the Senate Committee on Government Affairs, June 24, 1998
[4] Twitter worm author gets a job at exqSoft Solutions: http://blogs.zdnet.com/security/?p=3170
[5] TJX data theft leads to money-laundering scam:: http://www.usatoday.com/money/2007-06-11-tjx-data-theft_N.htm

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

In China, it seems that a half-dozen groups are behind the crimeware industry. The information is sometimes contradictory, and it can be difficult to obtain a translation of their names. One of the groups, which TheDarkVisitor calls the "Crab Group", is said to be the source of spectacular infections, including some that are believed to have affected more than 30 million machines. Citing a Kingsoft Anti-Virus report, Scott Henderson says that "within hacker circles, the majority of money is earned by establishing viral dissemination chains. While a virus author may earn a salary of one million Yuan a year (approx USD 150,000), it was possible for a viral dissemination group to earn ten million Yuan (approx USD 1.5 million) yearly."[6] Other groups now seem to be limiting their actions in their own territory.

Since 2003 in Eastern Europe, ProdexTeam has served as the online storefront for an individual with the pseudonym of Corpse. He is known for having developed and sold Trojans, including Haxdoor and Nuclear Grabber. Globally, this was the first malware associated with rootkits and capable of intercepting financial data. In 2006, the Swedish bank Nordea lost US$1.1 million because of one of these variants. Although the individual stated in October 2006 that he stopped his activities, he is said to still be involved in cybercrime and carding.

To gain market share in the field of crimeware, as in Corpse's situation, criminal offices have multiplied. Some are known through a group name that their members give themselves, while others are known through the pseudonym of an individual, who does not seem to work in isolation.

Communication Tools and Carder Forums

Specialized sites and forums continue to support crimeware offerings and services. The easiest ones to access contain nothing more than harmless information for establishing an initial contact.

After a few exchanges which to not bind you to anything, you are sometimes directed to more secure sites where sponsorship is generally required. In the East and the West alike, preferred contact method is ICQ. In China, however, cybercriminals tend to use rarely IRC to communicate. They prefer web-based BBS (Bulletin Board Systems), particularly the Baidu Post Bar (post.baidu.com), or QQ instant messaging.

In May 2001, 150 criminals from Eastern Europe held a meeting in an Odessa, Ukraine restaurant. They understood that the Internet created new opportunities for money laundering and profit making, so they hatched the criminal organization CarderPlanet. The visible part of the organization is a forum dedicated mainly to trafficking banking data. From the United States or Great Britain, hackers come and sell what they gather from their extortions. This data feeds into offices that made fake credit cards onsite. The cards can then change hands, return to the West or, for a commission, be used for all sorts of fraud.The organization is set up like a mafia. At the top of the pyramid are the top-level dignitaries, some in the role of the godfather.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

[6] The "Crab Group" virus dissemination family: http://www.thedarkvisitor.com/2009/02/the-crab-group-virus-dissemination-family/

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

The TJX case gives us an example of the success of these forums. Between 2005 and 2007, the credit card numbers of 94 million North American and United Kingdom TJX customers were stolen. In August 2008, eleven people were arrested, including three American citizens, one Estonian, two Chinese, one Byelorussian, and three Ukrainians.[3] The media reported that they were part of an international hacker network. Among them were the hackers who penetrated the Wi-Fi network and some top-level intermediaries. In fact, they were people who regularly posted on carding forums created using the CarderPlanet model, with members from around the world. Besides the inevitable "full info" and card dumps, vendors offered to sell fake passports, traveler's checks, and sometimes even fake school diplomas. Among the most famous forums are Mazafaka (more than 9,000 registered), ShadowCrew (more than 4,000), DarkMarket (more than 2,000), and the International Association for the Advancement of Criminal Activity.

Such carder forums have become more popular as a way for online criminals to trade their expertise and products. Every day, thousands of pieces of information related to stolen, misappropriated, and sometimes even fake credit cards are sold by cybercriminals. Specialized forums put carders and buyers into contact with one another. They first buy a trial, test it, and if they are satisfied, carry out a larger purchase (between 10 and 100 units). For fifteen years, groups specializing in credit card fraud have used various platforms that, for the most part, have been very quickly infiltrated by the secret services of many countries, who periodically conduct wide-scale operations in these environments. A review of the main sites, including the many international arrests of members of the forums, is included in the full report. One such forum was ShadowCrew. Operational from August 2002 to October 2004, this forum offered its members a place to find information and mostly to buy and sell digital personal and banking data (SSNs, dumps, CCV2 codes, etc.) and counterfeit documents. The site, originally created by dissident members of CounterfeitLibrary.com, is hosted in the United States. The members acquired privileges through their active participation in discussions and their contribution of tutorials. The forums offered content in English and Russian, and without distinction, they supported members from the U.S. and the countries of Eastern Europe. The United States specialised in hacking, while Russia and Romania became experts in manufacturing fake cards.

The many infiltrations conducted by law enforcement services have made cybercriminals cautious. They hope to avoid repeated FBI inspections, like the ones against ShadowCrew and DarkMarket.[8]

Conclusion and Predictions

Each year for more than five years, we have continued to announce the increasing professionalism of attacks, ever increasing quantity of malware, and increasingly loftier revenue objectives. The exploitation of long lists of banking-related domains, like those discovered in June 2003 in version B of W32/Bugbear@MM, is sadly no longer a surprise.

7 Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers: http://www.usdoj.gov/criminal/cybercrime/gonzalezIndict.pdf
8 Q&A: FBI agent looks back on time posing as a cybercriminal: http://news.cnet.com/8301-1009_3-10234872-83.html

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Besides these regular findings, other trends are expected to emerge over the next few years.

·First of all, **cybercrime will become more like conventional crime to the point that they become one of the same.**
·**The same relationship will continue between organised financial and economic crime.**
·**These changes will go hand in hand with an escalation of violence against those who get in the way of cybercrime.** Without qualms, some of them already use methods from their predecessors.
·**The operation of offshore centres housing online banking services and virtual casinos that are nearly illegal or outright criminal will continue to grow.** Despite efforts by international organisations, cybercriminals will be even more sophisticated than ever in exploiting vulnerabilities in international standards. There will be new opportunities available to money launderers and those involved in international online financial crime.
·Finally, cybercrime, rogue states, and non state-owned transnational entities will come together. Rumours of cyberattacks led by or encouraged by nationalist, corrupt or authoritarian regimes are getting more and more precise. While the concept of cyberwar is no longer reserved to science fiction, **it is not unlikely that unstable regimes, anti-Western states, and terrorist or radical (eco-terrorism) states may turn to methods of digital crime.** Until now, such states have always denied their involvement in this type of attack. It may not be long before we see undeniable proof of their participation.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Section Editors: Esther George and Pedro Verdelho

The legal section of the newsletter aims to describe and discuss the most relevant subjects both at the international and internal level specially in Europe, but also in Latin America, Asia and AFrica, referring to the evolution of cybercrime and the new adopted legislations. All contribution provided by readers is welcome, by comments or by submitting articles for publication. If you have any legal issue to present, please contact the Editors.

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

FRANCESCO TESTA
Antimafia Public Prosecutor, Catania

INTERNATIONAL COOPERATION: THE CONVENTION OF BUDAPEST OF 23.XI.2001. THE NEW REGULATIONS OF THE DATA RETENTION ACTIVITIES AND THE PROTECTION OF THE ELECTRONIC EVIDENCE. THE PRINCIPLE OF "NE BIS IN IDEM IN INTERNATIONAL JURISDICTION"

Due to the "universality" of computer crimes that we have already described, the European Union has recognised the need to complete the existing agreements – multilateral or bilateral treaties among Member States; the European Convention on Extradition, opened for signature in Paris, on 13 December 1957; the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959; the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 – and to provide specific regulations in order to foster cooperation in the criminal matters, for combating Cybercrime.

The Convention on Cybercrime, opened for signature in Budapest on 23 November 2001, was signed with the purpose to pursue a common policy for the protection of the confidentiality, integrity and availability of computer systems, networks and computer data, for safety in electronic communications, and to prosecute the behaviours that endanger – even with fraud – such juridical interests.

Article 1 of the Convention provides the "basic" definition of a "computer system". It is "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data". As we can see, this is a much simpler definition than the one provided by the Italian jurisprudence. However, this corresponds with the Italian definition at least in the basic profile, which is the ability of processing "computer data" automatically. The computer data is also completely defined as "representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function".

The Convention prescribes the obligation for the States signatory to adequate their substantive criminal law, by introducing legislative measures aimed to punish some "typical" actions of attack on computer systems, such as the "cases" of illegal access (Article 2), the attempt to the data and to the integrity of a system (Articles 4 and 5), and the misuse of devices (Article 6).

Furthermore, it prescribes the same obligation for the case of attack to other protected goods, if this attack is made through computer systems, such as illegal interception (Article 3), computer-related forgery (Article 7), computer-related fraud (Article 8), child pornography (Article 9), and the offences related to the protection of intellectual property (Article 10).

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

The Convention reserves a specific attention to the need that each Member State must adopt very severe regulations for the repression. In fact, it does not only require "effective, proportionate and dissuasive sanctions", but also expressly requires – with no precedents in this sense – to include deprivation of liberty (Article 13).
The severe principles of the Convention also apply to legal persons in whose benefit a natural person may have committed a criminal offence described in the Convention, or who have made possible the commission of one of the mentioned criminal offences by a natural person submitted to their authority, due to the lack of supervision or control.

According to the domestic legislation of each State, the liability of a legal person may be criminal, civil or administrative (Article 12 Section 3), provided that the consequent sanctions, even if monetary, are proportionate and dissuasive (Article 12 Section 2).

The Budapest Convention must be noticed above all for the modern procedural instruments offered, both for the pre-trial investigations and for the instruments of international cooperation. For the first aspect, we need to outline the regulations of Articles 16-19, which prescribe the obligation to provide:

1)the possibility for National authorities involved in combating computer crimes, to order the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, where there are grounds to believe that the computer data is particularly vulnerable to loss or modification (Article 16 Section 1);
2)to oblige the person who preserves the data to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, and to keep the secret on the orders received. A Party may provide for such an order to be subsequently renewed (in Italy, up to 6 months).
3)the said authorities can order to submit specified computer data stored in a computer system or a computer-data storage medium, both if such data is available to a private person located and if the data is available to a service provider offering its services in the same territory. This formula, given its extensiveness, seems to foresee more possibilities of operation in the production order. This way, the order can be associated to data regarding individuals and clients located abroad, provided that they are subscribed to a service provider that offers its services also in Italy (Article 18).
4)the possibility to proceed to the search and to access computer systems, data and media, as well as their seizure (Article 19). The Convention also duly provides that the regulations that allow the search or the access to a computer system must also provide the possibility to "expeditiously extend" the operations also to other computer systems connected, if the authorities have grounds to believe that the data sought is no longer in the initial system.
5)real-time collection of traffic data associated with specified communications in its territory transmitted by means of a computer system, as well as – only with regard to the most serious offences to be defined in each domestic legal system – the interception and the recording of the data regarding such communications (Articles 20 and 21).

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

Two regulations contained in Article 22, which regard the competence (or better, the jurisdiction) of the authorities of each Party, are very important.

Section one prescribes that each Party must provide the possibility of prosecuting the offences indicated in the Convention not only when they are committed in its territory, on board of its ships or on board of its aircrafts, but also "by one of its citizens, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State".

This regulation is very innovative for the Italian legal system that, as we have seen, currently provides a similar extension of the jurisdiction of the Italian judiciary authority only for the offences of exploitation of child prostitution and pornography, and against sexual freedom (Article 604 of the Criminal Code). The intention of this regulation is to reduce the area of non-punishable actions because of the "delocalisation" of computer crimes.
Since the Convention aims to create a sort of "common judiciary space" for the offences that occupy some of this space, the obvious consequence is the possibility that more Parties can claim jurisdiction over the same criminal fact and on the same person.

Section 5 of Article 22 considers this case, but perhaps solves it too quickly: "When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution".
At this point, the matter of the "ne bis in idem internazionale" applies. This principle has been neglected for a long time in Italy. Its purpose is to prevent that a fact or a behaviour that is the object of a final condemnation in a Member State can be prosecuted again in another Member State.

In fact, the obstacle in the Italian legal system for the recognition of this principle is given by Article 11 of the Criminal Code, which prescribes to repeat the trial against a national or a foreigner who has already been tried for the same fact abroad.

In the past our jurisprudence (even the constitutional jurisprudence: see the judgments 48/1967 and 69/1976) has denied this principle several times in our system. However, they have specified that the regulations of Article 11 are subordinate to the international regulations coming from Conventions that bind the State to comply to the principle of ne bis in idem.

This way, at least in Europe, the jurisprudence has finally given the priority to Articles 54-58 of the Convention of 19 June 1990 for the application of the Schengen Accord (implemented by Italy with the Act 388/1993). A recent decision of the Supreme Court (Supreme Court I no. 28299 of 23.06.2004) has recognised the applicability of the principle with regard to the judgments made by the Judicial authorities of the other States that adhered to the Accord. The Court said that, according to this principle, no procedure can be started in Italy against a person who has received a final condemnation or acquittal for the same fact in one of the above-mentioned States, provided that:

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

1) it needs the facts are exactly the same;
2) the statement must be a definitive one, and it must follow the analysis into the merit of the fact;
3) in the case of condemnation, the penalty must be executed or in execution, or at least it couldn't be executable according to the law of the Party who condemned the person.

However, some situations will arise out of the "common judiciary space" created by the Schengen Protocol, which will cause a double committal. With regard to these situations, the indications provided by Article 22 Section 5 do not appear adequate.

Also with regard to international cooperation the Convention of Budapest shows very new profiles, even if the approach is traditional.

First of all, I think that some regulations are very interesting about the reasons that can authorise the requested Party to refuse the assistance (Article 25 Section 4 and Article 27 Section 4). Other than the usual cases of political offences and the case that the fulfilment of the request can prejudice the sovereignty or undermine its security or order, the Convention excludes that the requested Party can refuse the assistance pretending that the offence being prosecuted by the requesting Party must be considered a fiscal offence.

Furthermore, particular attention is paid on the rapidity in the procedures of exchange of information (even spontaneous: Article 26) and of transmission of the requests of mutual assistance and of the consequent responses. The use of the modern communication instruments is authorised (Article 25 Section 3) in the transmission of letters rogatory, provided that they give appropriate guarantees of security and authentication (for instance, digital or electronic signature). The requests for assistance of the Judicial authority of the requesting Party can be directly forwarded to the requested Party, subject to the obligation of sending a copy to the central authority (Article 27 Section 9).

Each Party can accept to forward spontaneous information or requests for mutual assistance only subject to the condition that the circumstances and the data object of the request are kept "confidential" by the other Party (Article 26 Section 2; Article 27 Section 8).

Of course, the object of the mutual legal assistance consists of all the investigation activities that the Convention considers as "typically" necessary for combating computer crimes. This is the search and the access to computer systems located abroad, their seizure, the storage of traffic data in real time, and the interception of the contents of the communications sent through a computer system (Articles 31, 33, and 34).

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

I would like to outline two important innovations introduced by the Convention in setting the assistance instruments. The first innovation (Article 29) is the possibility for one Party to request, before submitting a letter rogatory, to request and obtain from the other party the temporary measure of the expeditious preservation of computer data stored through a computer system located abroad. The preservation of such data must be made by the authorities of the requested Party for at least 60 days, before the requesting Party submits a request for mutual assistance for the search, the access to a computer system, or for the seizure of the data being examined. This regulation will be very useful in international investigations, and will make them quicker. This is indispensable for an effective contrast of the "volatility" of the evidence of crimes against computer systems, or the evidence of the crimes committed using computer systems.

Another innovative regulation (Article 32) is the one regarding the trans-border access to computer data stored in computer systems located abroad. This is an "adaptation" to the investigations in this subject of an instrument that has already been introduced by the Protocol of adhesion to the Schengen Accord (Article 41 of the Act 388/1993), which regards the trans-border prosecution with no need to have a previous authorisation of the Authorities of the Contracting Party in whose territory the prosecution must be continued. This regards a person found in flagrante delicto for some serious crimes specified in Section 4 of the same Article. The Convention of Budapest authorises the Authorities of one Party, with no need to have the authorisation of the other Party, to the "virtual" access to the computer data stored and available to the public, regardless of the geographical location of such data. It also authorises the "virtual" access (and also to receive it) – with a computer system located in its territory – to computer data located in another State, only if the individual (normally the providers) who has the authority to disclose such data "legally and voluntarily" agrees to do so.

Section Editor: Mrs. Elena Domínguez Peco

This section will expose the different realities regarding the data protection policies in different countries. You are welcome to collaborate in the development of the section or give us your opinion by contacting the Editor.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

VALENTÍN HERNANDO GARCÍA, ARTURO RODRÍGUEZ OLMEDO

Criminalistics Service of the Civil Guard. Engineering Department (Computing Area)
TECHNICAL COMPLEXITY IIIII

FORENSIC ANALYSIS OF AN EMBEDDED DEVICE: AN IP CAMERA*

1 The devide to be analysed

The device (IP camera) has an embedded operating system that needs to be accessed for a forensic analysis. The device does not provide access to its embedded operating system or to the administration web interface, since the system requires user authentication. We do not know who the system users are, their privileges or passwords.

The system is in operation and, after examining its specifications, it does not have a permanent storage device. Consequently, if it is turned off, part of the information of interest that is stored in the RAM would be lost.

2 Preliminary study

The device is an IP camera of the ERZIC-IPTIR02P make by the company A-MTK. It is fitted with a Prolific ARM9v4 - PL1029 micro with 32 MB of RAM and a 4 MB EPROM NOR flash memory. It has a CMOS OV7725 sensor, a Prolific I2C recording device and a Prolific Audio AC97 recording device, as well as a Realtek RTL8139 Fast Ethernet network interface.

*Technical complexity rating shows the technological experience level needed to easily undestand the article contents. Level for this interview is HIGH IIIII.
* Original article language: Spanish. The article may be found at the following link

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

The device is supplied with software called IPWIZARD II, which locates and identifies the cameras on the network

After looking for information on the Internet, we discovered that this type of device uses an embedded Linux operating system and is capable of configuring HTTP, FTP and DHCP servers. It uses RTSP video and audio streaming protocols and can be administrated remotely via a TELNET session. Information was also obtained on three user access levels in two environments: web and console.

Web environment users can have 2 types of privileges: administrators (admin), who can configure the device, display, create users and update the firmware; and viewer users, who can only see what the camera is recording. The root user of the operating system is the only user who can access via the console, but he/she cannot connect using the web environment.

We considered the following options for accessing the camera:

-Using a weakness that has not been patched on this system.
-Carrying out a brute force or dictionary attack.
-Sniffing the network in the device search process using the IP camera software and then analysing the packets that are captured.
-Capturing the memory of the IPWIZARD II application process when it searches for and identifies devices and then analysing the information.
-Studying the device firmware updates in local mode and online.
-And studying the file packaged with the firmware in case it contains information of interest on the users and their passwords.

3 Initial studies and their results

Another camera of the same make and model was previously acquired to perform the aforementioned studies on it to avoid altering the original device.

The studies to be performed are as follows:

a) Study of the device weaknesses that have not been patched:

We used version 7.9.7 of the Shadow Security Scanner software and scanned the device in search of known weaknesses, locating the ports that were open and any services that may be running, etc.

The result obtained was that no known weaknesses were found on the device. However, we discovered its IP address (192.168.0.100) and confirmed part of the information obtained on the Internet, i.e. that ports 21 (FTP), 23 (TELNET), 80 (HTTP) and 554 (RTSP) were open.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

b) Brute force or dictionary attacks:

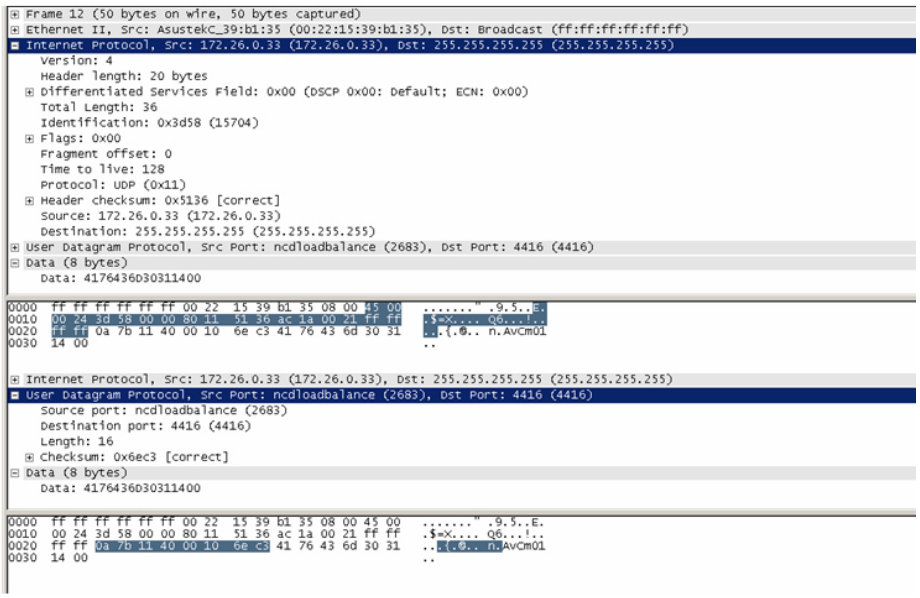
Various tests were performed to determine the possibility of succeeding with a brute force or dictionary attack in the FTP, TELNET and HTTP session authentications. The Brutus program was used. After carrying out various tests, it was concluded that this type of technique was not viable in view of the estimated time indicated by the programme, which was one year to complete an attack on a root user with an eight-digit password.

We performed various other tests using a variety of dictionaries and the result was very similar to the previous test. Consequently, this option was discarded.

c) Study of weaknesses in the IPWIZARD II software:

We looked for a weakness or vulnerability in the camera's IPWIZARD II software. We used a sniffer (Wireshark, version 1.2.1) to capture network communication packets during the process for locating and identifying cameras on the network.

Click to enlarge

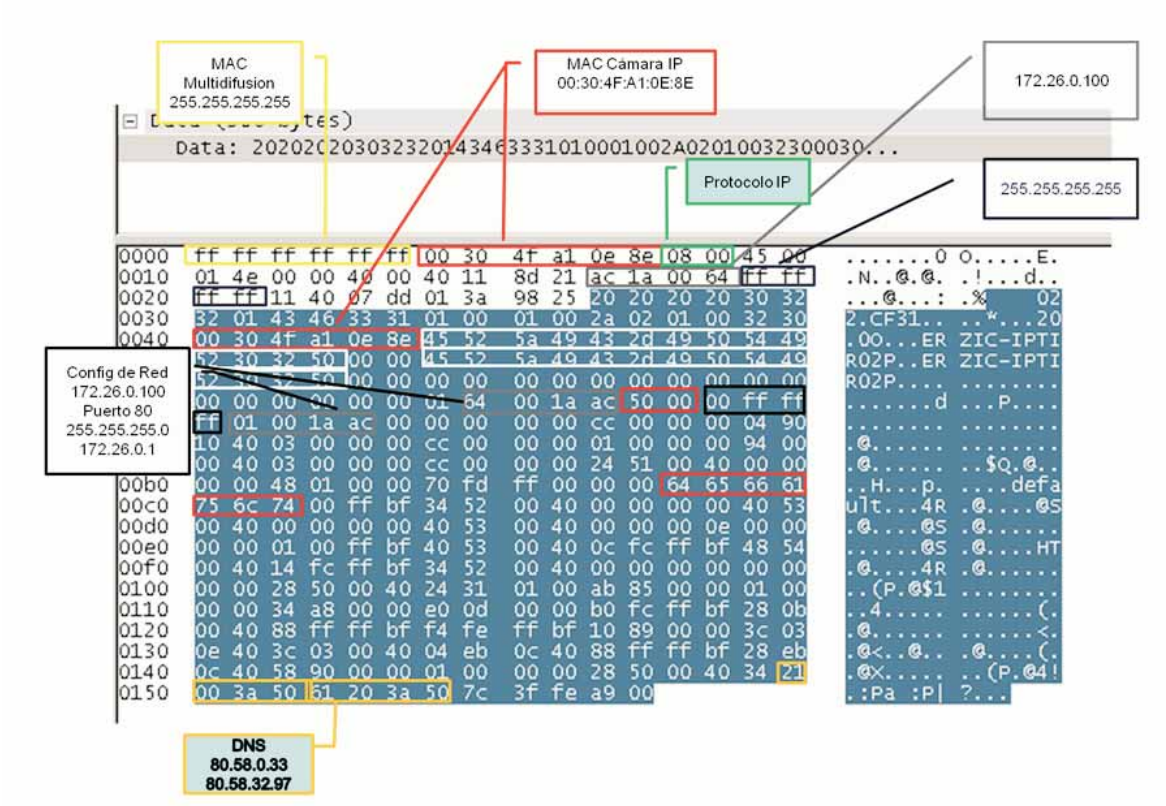


Response from the embedded device

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

The result obtained showed that there was no authentication between the computer and the camera since only one UDP packet is sent with a value in the specific DATA field (AvCm01) and the camera returned the basic information on the network configuration and the name of the device in another UDP packet. This was shown on the graphic interface of the IPWIZARD II application, although it was not clear and had to be interpreted.



Interpretation of the information provided by the IPWizard utility through the sniffer

d) Study of the IPWIZARD II process in memory:

The WinHex software was used to dump the information in the area(s) of the memory used by the IPWizard in case it provided data about any of the authentication processes or the interpretation of the information sent in the UDP packet returned by the camera.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

```
IP Wizard II
rtsp:// :554/mpeg4/media.amp?resolution=1024x768
http://%s:%d

GET /param.cgi?action=list&group=Network.Interface.I1
HTTP/1.1
Authorization:Basic %s

 Network
Network.Interface.I1.Link.BootProto=
Network.Interface.I1.Link.BootProto= dhcp
Network.Interface.I1.Manual.IPAddress=
Network.Interface.I1.Manual.IPAddress=
Network.Interface.I1.Manual.SubnetMask=
Network.Interface.I1.Manual.SubnetMask=
Network.Interface.I1.Manual.DefaultRouter=
Network.Interface.I1.Manual.DefaultRouter=
Network.Interface.I1.Active.MACAddress=
Network.Interface.I1.Active.MACAddress= ON OFF
Communication... %s %s &
```

```
Network.Wireless.ESSID=%s &
Network.Wireless.BSSID=%s &
Network.Wireless.Mode=managed &
Network.Wireless.Mode=ad-hoc &
Network.Wireless.Channel=auto  &
Network.Wireless.Channel=%d  &
Network.Wireless.SecurityMode=none &
Network.Wireless.SecurityMode=wep &
Network.Wireless.SecurityMode=wpa-psk &
Network.Wireless.WEP.Authentication=open &
Network.Wireless.WEP.Authentication=shared &
Network.Wireless.WEP.ActiveKey=%d %s %s &
Network.Wireless.WEP.Key%d=%s &
Network.Wireless.WEP.GenerationMethod=ASCII  &
Network.Wireless.WEP.GenerationMethod=manual  %s %s &
Network.Wireless.W0.Key=%s &
Network.Interface.I1.Link.BootProto=dhcp &
Network.Interface.I1.Link.BootProto=none &
Network.Interface.I1.Manual.IPAddress=%s &
Network.Interface.I1.Manual.SubnetMask=%s  &
Network.Interface.I1.Manual.DefaultRouter=%s  %s:%s
```

Part of the information obtained from the IPWizard process memory

After analysing the dump of this process in memory, it only provided us with information that included the use of basic authorisation in the HTTP communication. In other words, it confirmed that the authentication credentials were encoded in BASE64, that the RTSP protocol was used for the streaming and that the camera returned information about the network configuration of the device at positions in the packet that were associated with the variables interpreted and displayed by the graphic interface, but no information was found on any of the authentication processes.

4 Study of the IP camera firmware updates and results

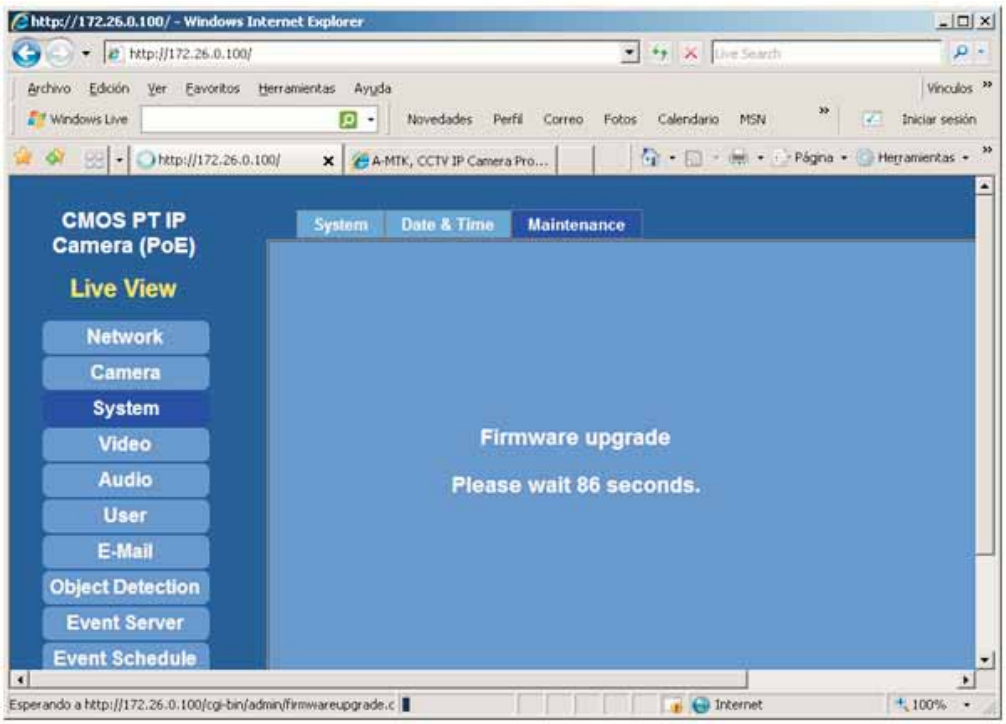
In view of the result obtained so far, we considered studying the camera firmware updates. We considered two possible options: the online update and the update in local mode.

We started this study by considering the possibility of performing an online update (autoupdate) from the manufacturer's website and sniffing the communications during the process; however, it was not possible since, when this study was performed, this option was not available on the manufacturer's website. It was only possible to perform this operation in local mode from the web environment and, to do so, administration privileges were required (admin).

The latest version of the firmware was requested from the manufacturer of the camera that had been acquired, together with the previous version, to study the update process in local mode. They were sent to us by e-mail, since they were not available for download from the manufacturer's website.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security



Update in local mode

After capturing the communications during the firmware update process, it was confirmed that no authentication could be performed with the device, since the firmware was sent to the device via an FTP session in passive mode and the update process took place on the embedded device. It was verified that the authentication process in the web environment encoded the users' credentials in Base64.

Similarly, the study of the communications confirmed the possibility of obtaining the credentials of the users that were using the camera from the web environment, owing to the format in which the data were encoded (Base64). However, none of these users would allow us to connect to the device console with root privileges.

5 Study of the IP camera update firmware in local mode and results

In view of the results obtained, the only option remaining was to study the update firmware and analyse its content. The file packaged with the firmware we had been sent was not encrypted or compressed, which would make its study possible without too many additional difficulties. It comprised three binary packets: the one corresponding to the RAMdisk with the system required for updating the firmware; the kernel of the Linux operating system embedded in the device; and the root file system.

During the update process, the new kernels and root file system were transferred to the EPROM memory of the system embedded in the camera.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

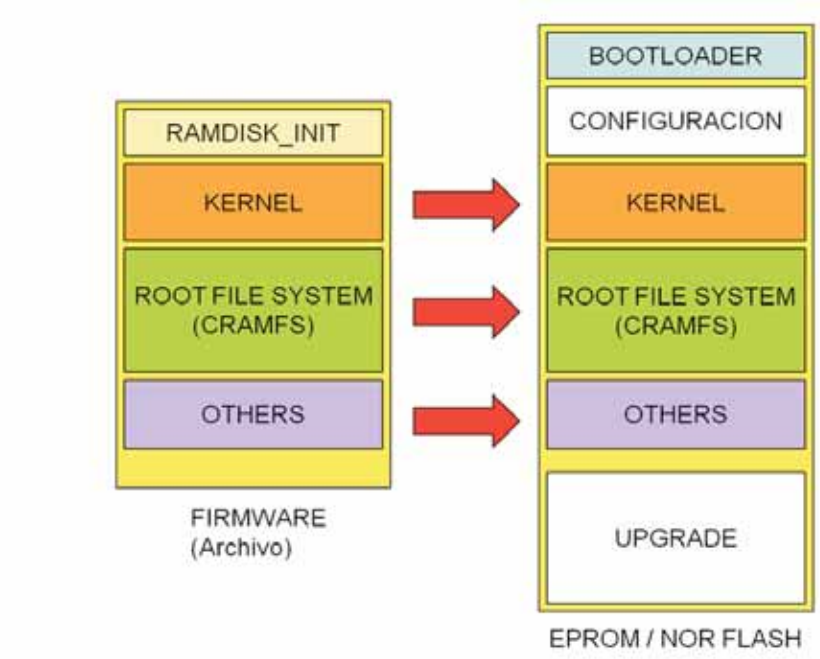
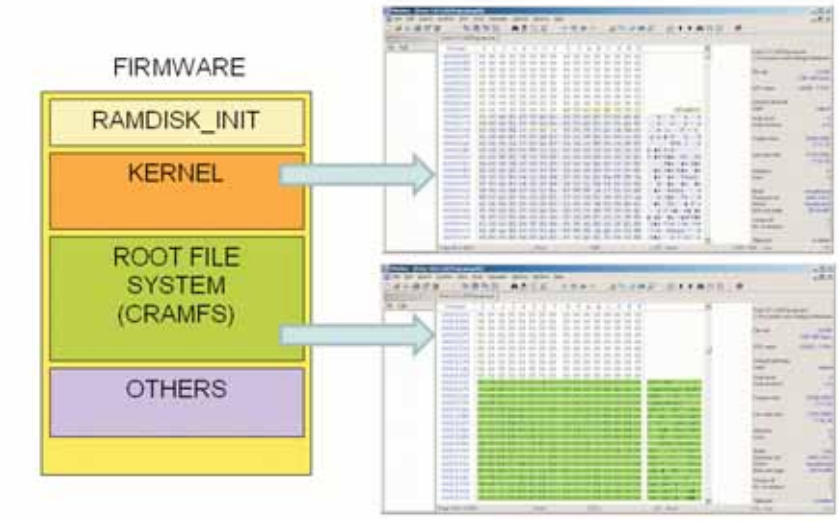


Diagram of the firmware update process

After locating the packets in the firmware file and extracting them, it was verified that the kernel was in zImage format (compressed) and that the root file system was of the CRAMFS type (file system in compressed RAM).

Click to enlarge

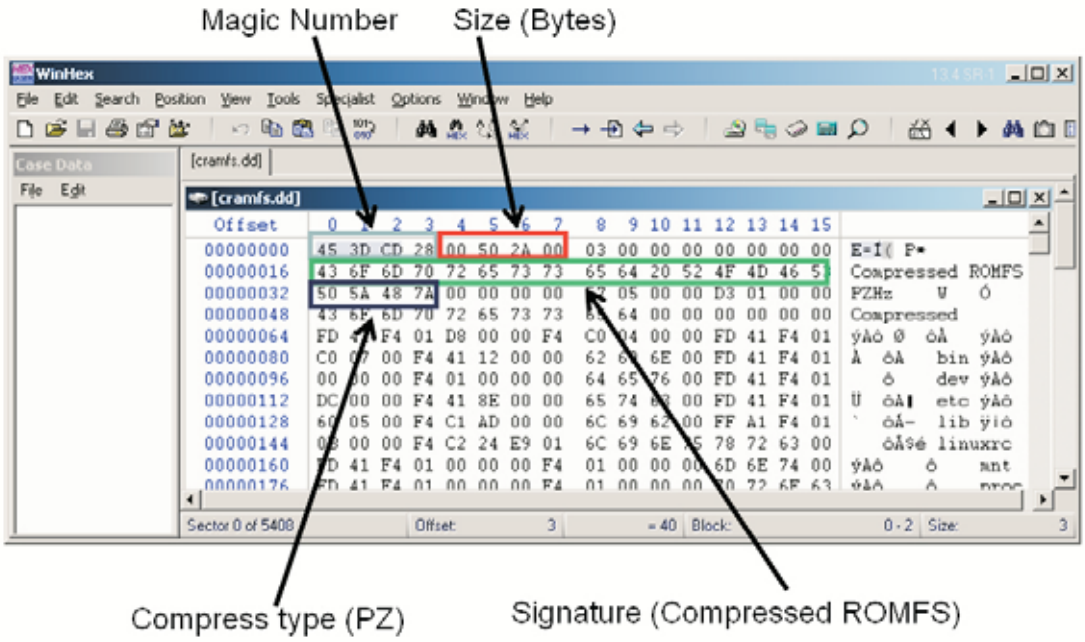


Location of the binary packets of the kernel and the root file system (CRAMFS)

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Of these two files, the one corresponding to the root file system was considered to be of greater interest and the study focused on it to locate the "/etc/passwd" file in the file system. This file would contain the credentials of the device users and, in particular, that of the root user, which would allow us to connect to the device using a telnet session.



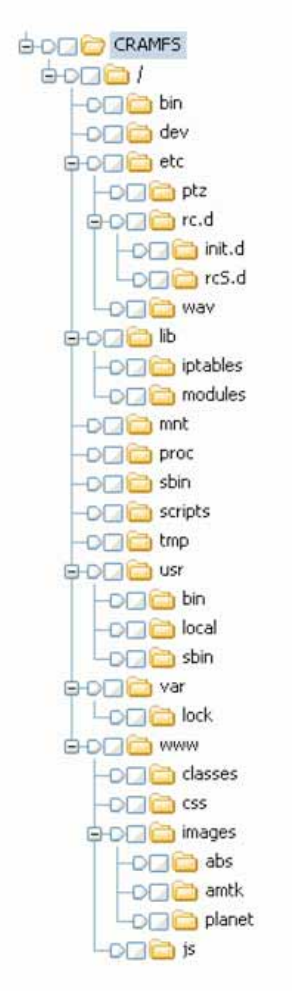
Structure of the header and information that identifies a file system (CRAMFS)

Using the Linux operating system, this file system was mounted using the loopback devices to access and analyse the content. For this purpose, the following command line was executed:

```
# mount –t cramfs –o ro,noexec,nodev,nosuid,loop /ruta_imagen/cramfs_erize.dd    /punto_montaje
```

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

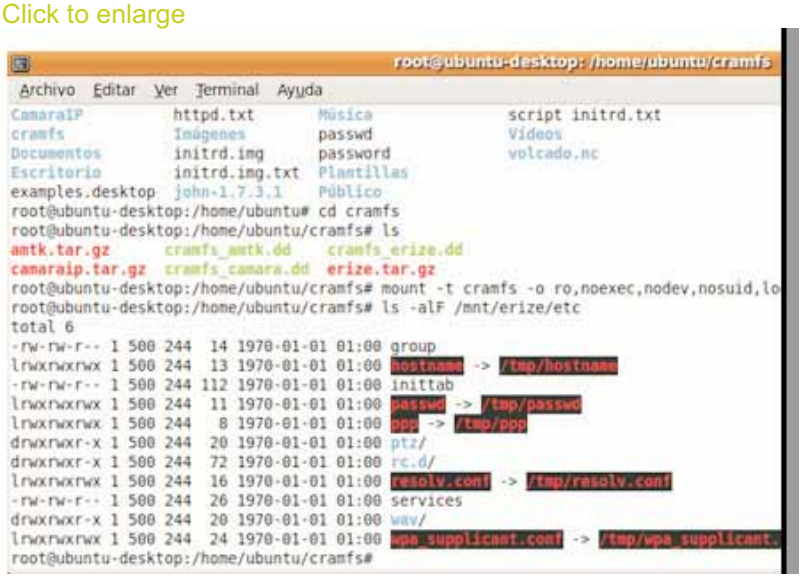


After the content of this file system had been examined, the following files were not found in the "/etc/" folder: passwd, hostname or resolv.conf, among others, which are necessary for configuring Linux system and which, in our case, were links to others in the "/tmp/" folder. Similarly, it was verified that it did not contain any file, as was expected.

In usual circumstances and as occurs in certain embedded systems in network NAS or routers, for example, the "/etc/passwd" file would be part of the root file system.

Consequently, if the files are not in the "/etc/" folder of the cramfs, but there are links to others with the same names in the "/tmp/" folder, they have to be created when the system is booted.

Click to enlarge



The files in the /etc/ folder in the CRAMFS file system

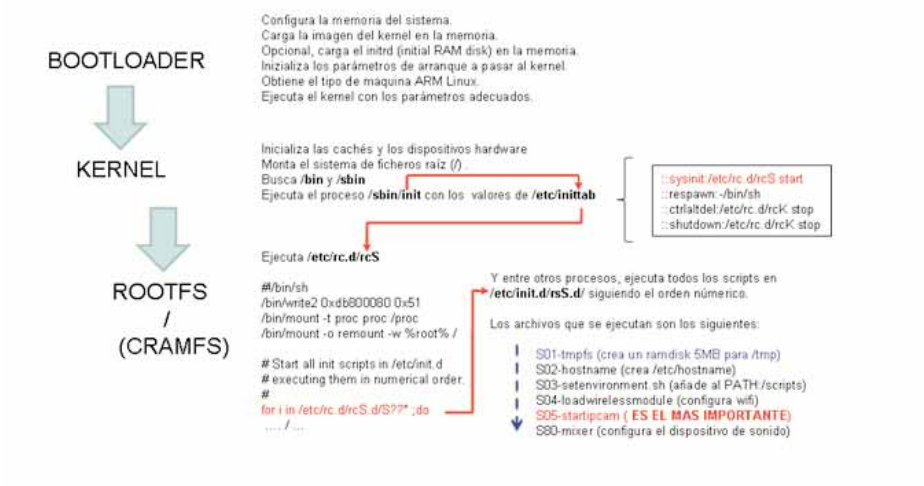
In short, the boot of a Linux system starts with the bootloader, which loads the kernel and the ramdisk in memory, mounts the root file system and launches the start scripts.

Therefore, we continued the study by analysing the boot of the embedded system and focused on the start scripts.

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

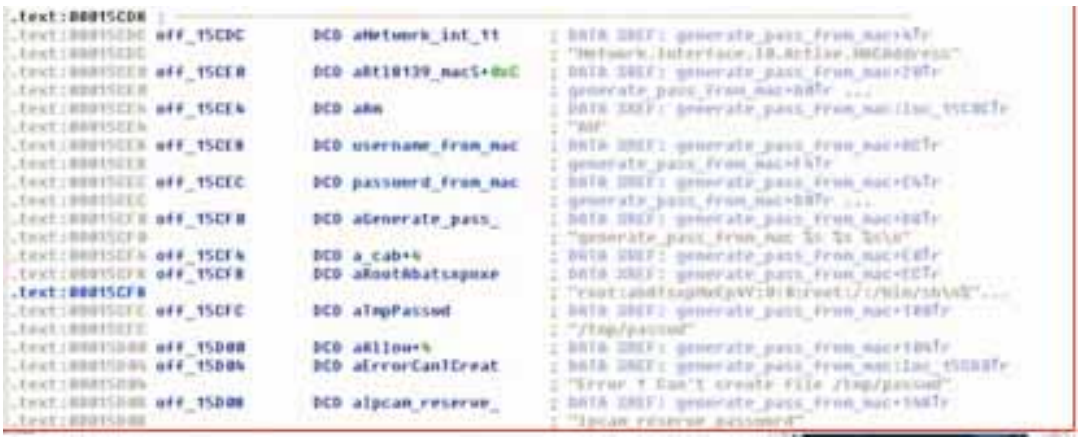
Click to enlarge



We examined the fifth script in "/etc/rc.d/rcS.d/" in detail (S05-startipcam) and we analysed its content. The file configures different drivers of the device and starts the system, launching, among others, the telnetd and httpd demons, as well as configuring the network and other devices.

We used the IDA32 program to disassemble the "/bin/httpd" file and compared it with another with a similar distribution. We found that the file in the CRAMFS file system had been modified and had at least one additional function in its code, called "generate_pass_from_mac".

Click to enlarge

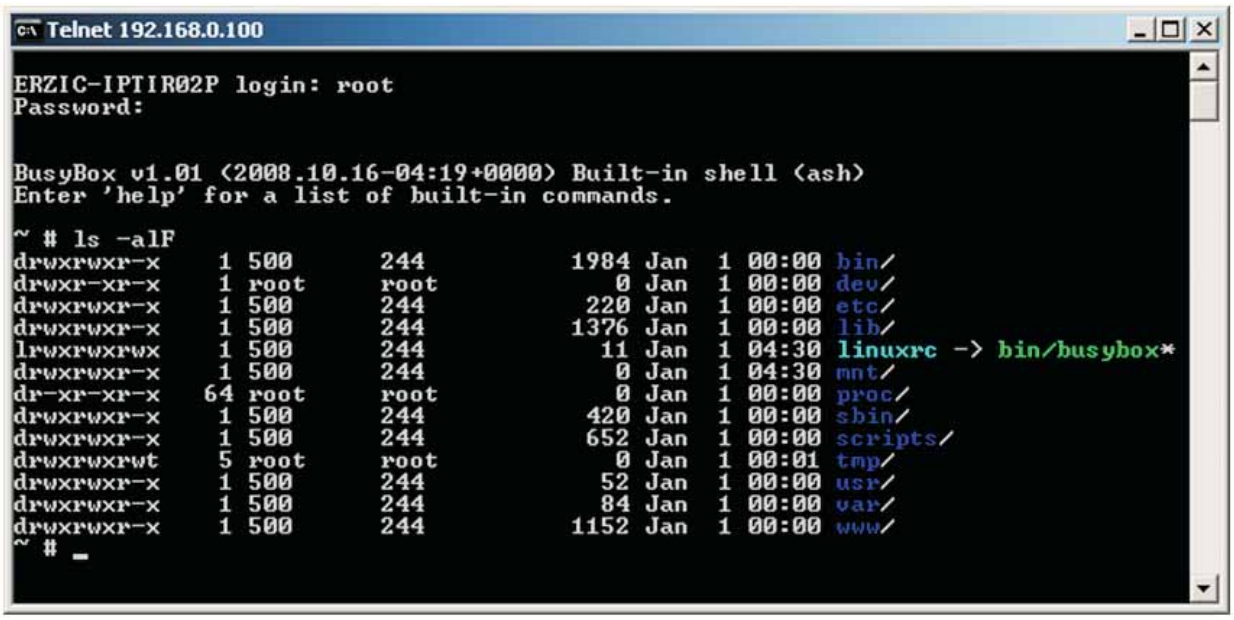


Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

We analysed this function and found that it contained a subroutine for generating a system user and the corresponding password using the MAC address of the device and that it also created the file "/tmp/passwd" during the execution time with the entries of the user and the one corresponding to the root user with a legible text chain.

We used the John The Ripper program to crack the password and gained access to the device we had acquired with a Telnet session.

We verified the existing users on the device, confirming the existence of the aforementioned two: root and 4FA10E8ES (the user created through the IP camera MAC).



Similarly, we found that when the httpd demon is booted, the "/tmp/passwd" file is created with the aforementioned two users and the password was obtained for the user generated with the MAC.

Other searches were performed in the cramfs file system with the expression ":root:" and no other files with this chain appeared, except for the aforementioned httpd.

Similarly, using the "nram getall" command, the information on the embedded system configuration that remained in the EPROM memory was retrieved.

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

6 Dump of the information of interest on the embedded system of the IP camera and results

We examined the Linux operating system of the IP camera and verified the existence of the dd and nc commands, etc., which were in the busybox command interpreter that was being executed on the system and which would allow us to dump the information of the device to be analysed by our forensic team in the laboratory.

After performing various tests with our (confirmed) IP camera, we started a telnet session for the (unconfirmed) camera that was to be analysed with the root user credentials that were obtained and we performed a dump of the RAM memory (/dev/mem and/proc/kcore), the root file system (/dev/norblock/disco/disc), the content of the "/tmp/" folder, the device boot and configuration parameters and various files located in "/proc/".

VOLCADO DEL DISPOSITIVO DE MEMORIA RAM

nc –l –p 9000 | tee imagen_mem.dd | md5sum >hash_mem.md5	dd if=/dev/mem bs=4096 | nc 192.168.0.200 9000

VOLCADO DEL DISPOSITIVO DE MEMORIA (FORMATO ELF)

nc –l –p 9000 | tee imagen_kcore.dd | md5sum > hash_kcore.md5	dd if=/proc/kcore bs=4096 | nc 192.168.0.200 9000

VOLCADO DEL ROOT FILE SYSTEM (CRAMFS)

nc –l –p 9000 | tee imagen_cramfs.dd | md5sum > hash_cramfs.md5	dd if=/dev/norblock/disc0/disc bs=4096 | nc 192.168.0.200 9000

VOLCADO DE LA CARPETA /TMP/

nc –l –p 9000 | tee tmp.gz | md5sum > hash_tmp.gz.md5	tar –cvzf /tmp/tmp.gz /tmp ; dd if=/tmp/tmp.gz | nc 192.168.0.200 9000

VOLCADO DE LA ZONA DE CONFIGURACION DE LA EPROM

nc –l –p 9000 | tee configuracion.txt | md5sum > hash_configuracion.txt.md5	nvram getall 2>&1 | nc 192.168.0.200 9000

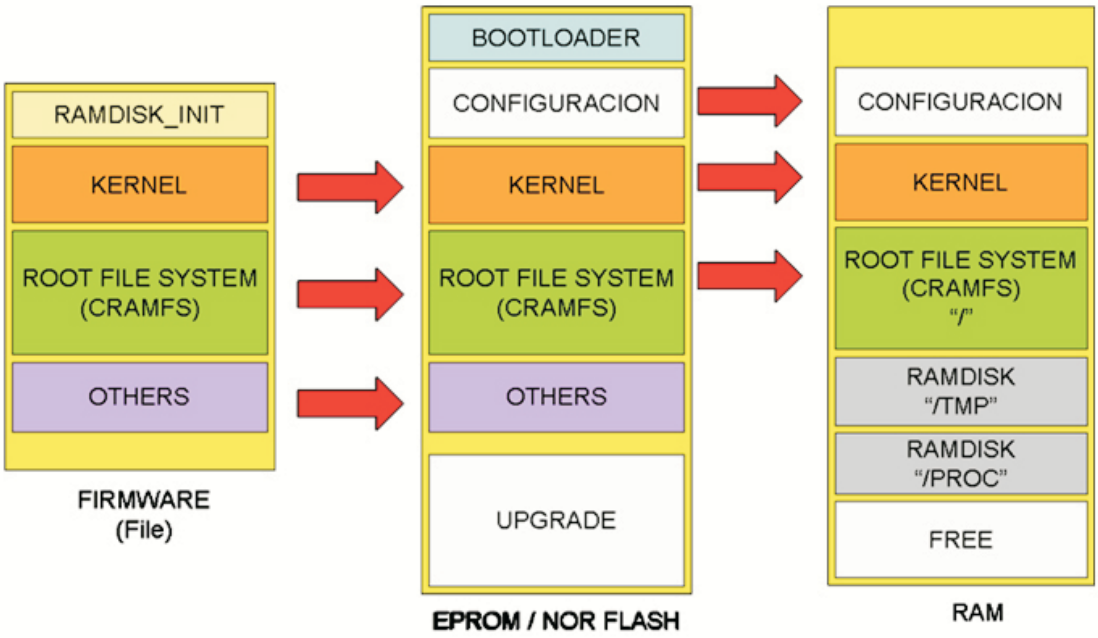
We analysed the files that were obtained and located the information that was required for solving the problem that was posed.

In other words, as might be expected, during the boot of the embedded device, the information in the NOR Flash

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

memory (kernel, cramfs and boot or configuration parameters) is sent to the RAM memory of the device. In our device, two ramdisks are also created. These ramdisks are used by the virtual file systems of the "/tmp/" and "/proc/" folders, which contain important information (logs, the passwd files and host, etc.) and can only be accessed when it is in execution. If the equipment were turned off, this important information would be lost.



Information flow studied: Firmware NOR Flash RAM

Until then, the solution was more than acceptable, since there was no need to turn off the embedded device and lose certain information of interest located in the RAM memory. However, we decided to go even further in this study and considered the possibility of verifying what happened during the firmware update in the EPROM memory and how the memory was structured.

7 Study of the EPROM memory of the embedded system of the IP camera and results

The structure of the NOR Flash memory of an embedded system is divided into several regions in a way that is similar to other storage devices on which operating systems are installed on a computer. These regions are as follows:

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

· The bootloader.
· The store for the permanent configuration of the device (CONFIGURATION and BOOT PARAMETERS).
· The operating system kernel (KERNEL).
· The root file system (ROOT_FS).
· It may also have other areas for updates or other functions determined by the designer.

Structure of a NOR Flash memory that contains an operating system

To perform this verification, a bit-by-bit copy was made of the information on the storage device. To do so, the NOR Flash memory of the board of the IP camera under study was dismounted. It was a TSOP 48-pin type memory with the following specifications:

32-Megabit EON make, model EN29LV320A
(4096K x 8-bit / 2048K x 16-bit)
Flash Memory, with Boot Sector Flash Memory, CMOS 3.0 Volt-only

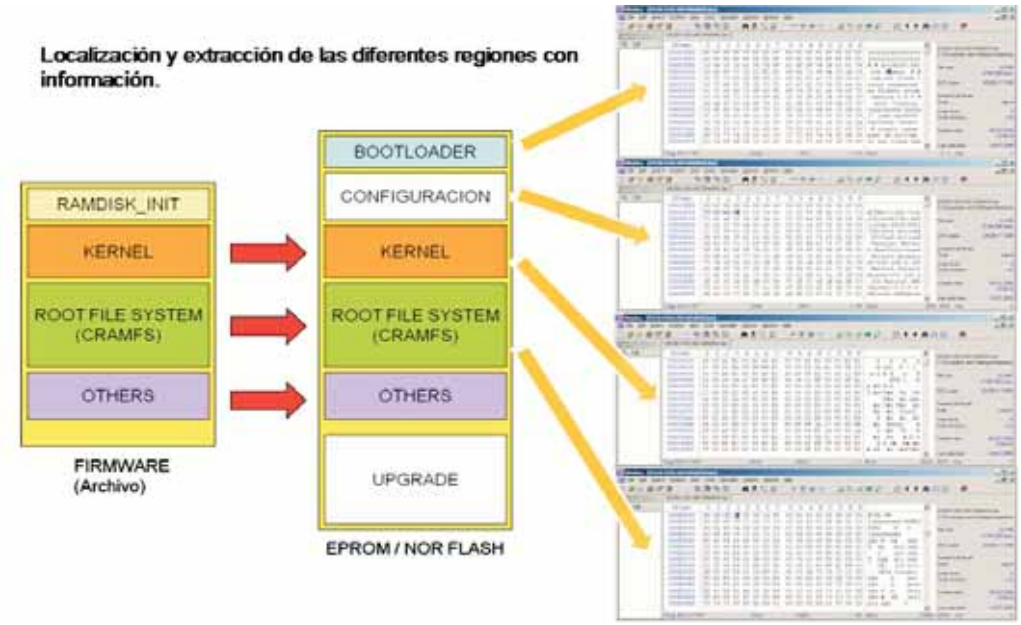
The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Using a memory reader/programmer device and a slot that is appropriate for this type of NOR Flash memory, a binary image of the content stored was made for subsequent study.

We used the WinHex hexadecimal editor to examine the file obtained from the dump and extracted the fragments corresponding to the BOOTLOADER, CONFIGURATION, KERNEL and ROOT_FS regions into four files.

Click to enlarge



We analysed the bootloader and found that it had at two-stage boot and that the areas of memory that contained the binary code for the boot also contained the region with the information about the CONFIGURATION.

We also found the device ID chain.

This was followed by the KERNEL, which corresponded exactly to the one in the firmware with which we updated our unconfirmed IP camera.

And, finally, we found the cramfs-type ROOT_FS with content that was identical to the one in the firmware and the one obtained in the dump of the embedded system under analysis.
This analysis, which was complementary to the others, allowed us to confirm what we knew about the EPROM memory firmware update process for an embedded device.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

The study confirmed the existence of the root file system (CRAMFS) in both the file with the firmware and in the RAM memory of the device in operation, as well as in the NOR Flash memory used as a permanent storage device for information about the embedded system, i.e. the IP camera.

8 Conclusions

This article provides details about the steps followed to access an IP camera with an embedded system in operation to guarantee that the information obtained has complied with the standards required by forensic analysis methods. Consequently, it specifies a method that has been referred to as "live forensics".

The above was also complemented with the dump and subsequent analysis of the NOR Flash memory with which the aforementioned IP camera is fitted. This made it possible to clarify how the camera firmware was updated.

9 References

Embedded Linux Primer: A Practical, Real-World Approach
By Christopher Hallinan
Published: Prentice Hall, September 2006

Embedded Linux
By John Lombardo
Published: NewRiders, June 2001

ARM Developer Suite Assembler Guide, version 1.2.

Building Embedded Linux Systems, Second Edition
By Karim Yaghmour, Jon Masters, Gilad Ben-Yossef, and Philippe Gerum
Published: O'Reilly Media, August 2008

Reference websites:
http://www.embeddedrelated.com
http://www.kernel.org
http://www.gzip.org/zlib/rfc-gzip.html#file-format

Section Editor: Matías Bevilacqua

This section will focus on the technical side of cybercrime and electronic evidence. The reader is highly encouraged to contribute to this section. Given the technical complexity rating system used, we are open to divulgative introduction articles on technology, state-of-the-art white papers and everything in between. Please contact the Editor if you'd like to contribute to this section.

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

GORAZD BOŽIC
Team Representative · SI-CERT
SI-CERT, SLOVENIAN COMPUTER EMERGENCY RESPONSE TEAM

Gorazd Božic has graduated from University of Ljubljana with B.Sc. in Computer Science in 1994. Immediately after his employment at ARNES, he initiated the formation of SI-CERT, the Slovenian Computer Emergency Response Team, which he is leading today. Being active in various cooperation groups, he was appointed the Chair of the European CERT group, TERENA TF-CSIRT in 2000 and served four two-year terms. Gorazd Boži• also participates in awareness-raising activities within the local Safer Internet programme, SAFE-SI. He is a representative of Slovenia on the Management Board of ENISA (European Network and Information Security Agency).

SI-CERT was established in 1995 within the auspices of the Academic and Research Network of Slovenia. It was in September that year that SI-CERT handled its first incident, an unprotected NFS[1] file system at the university lab being exported to the whole of internet. The spread of internet outside of the academic community has barely started and as in many European countries, a CERT was another service that a local NREN offered. Today SI-CERT is available to general public in its main role as a coordinator of network security incident handling. Apart from publishing public notices and bulletins, the team also participates in the local Safer Internet project, SAFE-SI (www.safe.si) and organizes local introductory workshops on topics such as malware and network traffic analysis.

The focus of SI-CERT work has gone through similar stages as I guess is the case for most other CERTs: from investigating computer break-ins in late 1990s, to chasing bot-herders on rogue IRC[2] servers and bouncers (with a little help from malware analysis), fighting major denial-of-service attacks to present time where we react to phishing attacks and help victims of various fraudulent schemes (oh, I forgot to mention a bit with SSH dictionary attacks in between). This focus will no doubt change again in the future as the attackers shift their interest to more profitable schemes. But there is an underlying mechanism that enables CERTs to do their work: co-operation.

CERT co-operation

By very nature of their work, CERTs always seek cooperation with each other that will enable achieving results when handling an incident. One of the first results of such cooperation was FIRST, the Forum of Incident Response and Security Teams (www.first.org). Established in 1990, just two years after the Morris Worm[3] incident, it is today truly "the premier organization and recognized global leader in incident response." FIRST organizes an annual conference that is a must for teams from all over the world.

[1] NFS, Network File System is a protocol that enables access to a remote file system over the network by moutning it on a local system. Microsoft's SMB is nowadays mainly used for the same purpose.
[2] Internet Relay Chat grew out of the BBS community and enables group chat over a network of connected IRC servers. It was a precursor to modern IM systems and flexible enough to serve as a command-and-control communication channel for large botnets.
[3] The Morris Worm was the first computer worm that spread over the internet. One of the results of this incident was the formation of the first CERT, now CERT/CC. See http://en.wikipedia.org/wiki/Morris_worm for more information.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Apart from that, regular exchanges of information on the mailing list and other internal on-line communication channels give many chances to share experience and seek advice from fellow teams. Even though there are formal procedures and a detailed membership process, human networking at conferences and technical colloquia as well as on-line is crucial.

In parallel to FIRST, European teams started with different ideas of a regional European-wide collaboration platform already in the mid-1990s. The final outcome (from today's perspective, of course) was the TERENA TF-CISRT task force established in May 2000 which is still active today. It is established under the auspices of the TERENA[4] Technical Programme to promote the collaboration between Computer Security Incident Response Teams (CSIRTs) in Europe. TF-CSIRT's "Terms of Reference" document defines aims of the TF-CSIRT, participation, it's chair and secretary, deliverables of the task force and it's mandate. It also specifies that participants meet in face-to-face meetings three times a year, while between meetings all discussions are carried out on the TF-CSIRT's mailing list. Meetings are hosted by participant's organizations on a voluntary basis (this approach has proven itself quite successful). Each meeting is divided in two days: the first day is dedicated to seminar sessions with speakers both from within the group as well as invited speakers not normally involved in TF-CSIRT, while the second day is dedicated to a meeting where work of the group is evaluated, issues are discussed, and future work is decided on.

Some of the early results of the TF-CSIRT include the idea of IODEF (Incident Object Description and Exchange Format) a common data format and common exchange procedures for sharing information needed to handle an incident between different CSIRTs, that would allow both known and new types of incidents to be formatted and exchanged. Another deliverable of the TF-CSIRT group is the RIPE IRT object[5] which allows a European CERT to define its constituency in the RIPE database. With one query you can find out which CERT to contact for a specific IP address or range (of course if the references have been put in the database by either the CERT itself or the constituent's network administrators).[6]

Members of TF-CSIRT also developed material for two-day courses in different modules, covering operational, legal, technical, organizational and vulnerability issues. European Commission has at the start funded delivery and development of the materials for three years, as well as the two courses a year. The materials are available for others to use on a non-commercial basis, subject to certain conditions to ensure quality, and there have been at least as many courses held under these rules as under the EC ones. The TRANSITS courses are now amongst others being facilitated and supported by ENISA.[7]

[4] Trans-European Research and Education Networking Association, www.terena.org
[5] http://www.ripe.net/ripe/docs/irt-object.html
[6] For an example, check the query
http://www.db.ripe.net/whois?form_type=simple&full_query_string=&searchtext=193.2.1.66&submit.x=8&submit.y=8&submit=Search
[7] http://www.enisa.europa.eu/act/cert/support/guide/training/transits

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

European CERTs have also established the so-called "Trusted Introducer" framework[8] which addresses a common problem in a regular operational work of a CERT, namely that of recognizing who is known to the community (and therefore you can decide to trust them more) and who is not. With a handful of CERTs that in itself was not a problem as we all more or less knew each other directly, but as the number of European teams grew this accreditation scheme became very useful. Teams can support other teams when they apply for accreditation or can raise objections against "rogue" teams (although this happens rarely). The framework can be extended to cover more requirements and different grades and such possibilities are at the moment under discussion. More information is available at the Trusted Introducer web site www.trusted-introducer.org where you can also find a list of all known European teams. ENISA uses this information to update the "CERTs in Europe" map[9] (check the map also to see which teams use the RIPE IRT objects).

The Estonian attack

The denial-of-service attacks on Estonian targets in 2007 are nowadays a frequently mentioned example on how countries must prepare for a suitable cyber-defense. It was a coincidence that the attacks started only a couple of days before a scheduled meeting of TF-CSIRT in Prague. When at that meeting the team representative of the Estonian CERT-EE presented the difficult operational situation they were facing, other teams were of course ready to help where they could. Calls for assistance were issued immediately to both the TF-CSIRT group as well as members of FIRST to check for offending traffic from within their networks and limit it where possible. As the Estonian colleague noticed, the effects were visible within hours.[10] I dare say that CERTs were among the first (if not the very first) that helped with operational measures. Even though many of the teams have not been preparing exactly for such an event, the benefit of experience with operational handling of network incidents was enough to fight the first tide. It is my strong opinion that a cooperation framework that has grown to be so effective and is not burdened by stringent formalisms that try to define every aspect of what to do when bad things eventually happen, is one that should be taken as a role model for other forms of international cooperation on operational issues.

Cooperation with the "outside world"

But in the end CERTs can only do so much. When crime happens, the law-enforcement needs to step in with their procedures and powers of investigation. In other cases, government offices need to regulate the virtual world (punishing spamming companies, protecting one's privacy and so on), while in some cases even non-governmental organizations can do their share. Just to briefly illustrate this last point: earlier this year, a web site www.specialphones.eu was offering advanced phones for half the regular price. It was soon discovered that this site was registered to a company that used a non-existent address in Tallinn.

8 http://www.trusted-introducer.org/
9 http://www.enisa.europa.eu/act/cert/background/inv
10 see http://www.terena.org/news/fullstory.php?news_id=2103 for the press release with more details

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Victims from Slovenia turned to the local consumer protection organization. SI-CERT then worked with them and while they have contacted their Estonian sister organization through the European Consumer Centre framework, we have been discussing options with the Estonian CERT-EE on what the possibilities are to limit the number of victims. Together we have been successful to quickly take the site down.

But most of the time, CERTs need good contacts with ISPs in the country where they operate and with the local law-enforcement agencies. These had to adapt and learn with the spread of the internet (and mobile phone networks) at the turn of the century. They needed new experts and were mostly eager to learn from CERTs. I personally think that today the police is well equipped with knowledge to investigate computer-related crime, but is on the other hand sometimes burdened by procedures that are out-dated or were brought in from the past era of paper documents, faxes and old phone networks.

Conclusion

Today we are dealing with internet fraud that is either technologically very simple and uses mostly social-engineering attacks, or with sophisticated malware and fast-flux networks that are used for spamming, phishing attacks and trojan attacks. To fight these we need cooperation frameworks that will enable us to investigate and react in a more efficient manner. In my opinion, more surveillance, internet filtering and similar big-brother measures are not the way to fight today's internet crime. What we need instead is a network of operational institutions that can quickly exchange information and agree on how to limit the damage and secure evidence so the law-enforcement wheels can start turning to collect it.

It is also not sensible to wait one whole year for a response on the official court request directed to law-enforcement agencies in another country. The sensible thing is to change that, so we don't needlessly loose time while papers are passed from one table drawer to another. Formal procedures are indeed established for a reason and protect one's rights, which is the correct thing to do! But I don't think it is these procedures that cause delays but instead it's more a combination of bureaucracy, work overload and sometimes even downright sloppiness. And these things can be addresses and eventually corrected.

Section Editor: Liljana Selinsek

The reader is invited to contact the Editor to present his or her Institution's activities in reference to the fight against cybercrime, or any other contribution regarding this topic.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

STEPHEN MASON
Section Editor and Barrister · Chambers of Stephen Mason

This issue deals with the provisions of Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC Text with EEA relevance Official Journal L 319, 05/12/2007 P. 0001 - 0036.

Article 94 provides that 'Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 1 November 2009.' This is an important Directive that will affect everybody in the EU that has a credit or debit card, and will affect the evidence that card issuers must provide if a customer claims that money has been removed from their account by way of an ATM or Point of Sale terminal (PoS) across the EU. The relevant article is article 59, which is set out below:-

> Evidence on authentication and execution of payment transactions
>
> 1. Member States shall require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for his payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency.
> 2. Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of his obligations under Article 56 [included below for reference].
>
> Article 56
>
> Obligations of the payment service user in relation to payment instruments
>
> 1. The payment service user entitled to use a payment instrument shall have the following obligations:
> (a) to use the payment instrument in accordance with the terms governing the issue and use of the payment instrument; and
> (b) to notify the payment service provider, or the entity specified by the latter, without undue delay on becoming aware of loss, theft or misappropriation of the payment instrument or of its unauthorised use.
> 2. For the purposes of paragraph 1(a), the payment service user shall, in particular, as soon as he receives a payment instrument, take all reasonable steps to keep its personalised security features safe.

In this issue, consideration will be given to five cases across the EU that have dealt with ATM and electronic signature (PIN) complaints brought by customers against banks.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

Country: Greece
Case citation: No. 5526/1999
Court: Athens Court of First Instance

Keywords: ATM · electronic signature (PIN) · burden of proof · liability

SUMMARY

After a debit card was issued to the complainant, a thief broke into his vehicle and stole a number of items, including the recently issued debit card (the document that mentioned his PIN was not removed). The claimant informed the bank and the police within a few minutes of the theft, but as a result of the negligence shown by the banks, the account was not suspended and the thieves removed 1,200.000 drachmas from his account. The bank refused to refund the money. The bank was ordered to refund the customer, and the learned judge indicated that it is for the bank to provide for the security and secrecy of the PIN, not for the customer to prove it was not them that took the money from the ATM.

COMMENTARY

It is suggested that the learned judge, Gavalas Dimitrios, was correct in this decision. Although the amount of evidence that the card issuer is now required to provide under article 59 of the Directive is greater than provided in this case, nevertheless the learned judge indicated clearly that there is a deadly game being played between the banks, who insist on using poor quality technology, and the criminals, who know how to out-wit the banks. The customer is caught in the middle. Whilst it is true that some customers do make false claims of loss against the banks, it is for the banks to provide for better security.

Source: For a complete translation of this case into English, see Anastasia Fylla, 'Court Decision No. 5526/1999', *Digital Evidence and Electronic Signature Law Review*, 4 (2007) 89 - 90.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Country: Austria
Case citation: OGH judgment of 29.06.2000, 2 Ob 133/99v
Court: Oberste Gerichtshof (Supreme Court)

Keywords: Liability - bank cards - ATM - misuse - electronic signature (PIN)

SUMMARY

The claimant took action (he assigned his claim to the consumers' association which brought the action) for the defendant to be ordered to pay the sum of ATS 10,000.00 plus costs for debiting his account improperly following repeated ATM card misuse. On 12 June 1990, a person in the branch of the claimant's bank called him by telephone to inform him that his account was ATS 09,000.00 over its overdraft limit, because two amounts of ATS 5,000.00 had been taken out via two ATMs. The claimant was adamant that the original ATM card was in his possession at all times, and, more particularly, at the time of the alleged withdrawals. It could not be established whether the two withdrawals of ATS 5,000.00 each, on 8 June 1990 and 9 June 1990, when the transaction were made.

The question for the courts was whether the bank was entitled to demand that the customer should indemnify it for its costs incurred as a result of the the amounts withdrawn, or whether it had to credit the customer for the money removed from the ATMs because the customer was not responsible for effecting the transactions. The learned judges reached the conclusion that the banks used complex equipment and technology, thus it was for the bank to prove the case, not for the customer to prove it was not them.

COMMENTARY

The members of the Court indicated there was a difference between excluding the liability of the bank for misusing ATM cards technically and excluding liability for misuse due to the loss of a card. In this instance, the bank could not prove that the card issued to the customer was used in the ATMs in question. The members of the court also discussed the burden of proof in such cases.

Source: For a complete translation of this case into English, see, 'OGH judgment of 29.06.2000, 2 Ob 133/99v', *Digital Evidence and Electronic Signature Law Review*, 6 (2009) 223 - 231 (with a commentary by Dr Clemens Thiele, attorney-at-law, LLM Tax (GGU).

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Country: Germany
Case: 5 October 2004, XI ZR 210/03
Court: Bundesgerichtshof (Federal Court of Justice)

Keywords: Electronic signature (PIN) - ATM - card holder - theft of card - subsequently used by thief - liability

SUMMARY

The claimant had a current account with the defendant, a German savings bank. The bank had issued an EC-Card with a personal identification number (PIN). On two consecutive days, two amounts of DM 500 and one amount of DM 1,000 were withdrawn before the card was blocked on the third day. The card holder claimed the card had been stolen at a local festival. She alleged that she had neither written the PIN onto the card nor stored the PIN together with the card. She claimed that the thief must have deciphered the PIN or must have taken advantage of defects in the security mechanisms in place to keep the bank's institutional key secret. The amount withdrawn was debited to the account. The card holder sued the bank for payment of DM 2,000.00. The bank argued that it was impossible for the PIN to be found, and the claimant must have written her PIN on the card or the PIN was recorded near the card for the thief to use the ATM with the correct PIN. The members of the Court held that if cash is withdrawn from an ATM shortly after the theft of a card by using the stolen card and the correct PIN, a prima facie presumption applies that the card holder had noted the PIN on the card or stored the PIN together with the card.

COMMENTARY

The decision in this case has been severely criticized in Germany by academics, lawyers and consumer's associations. (See also Dr. Martin Eßer 'Germany' (chapter 7) in Stephen Mason, Electronic Signatures in Law (2nd edition, Tottel, 2007)). Of significance was the reliance placed by the members of the Court on the assertion by the Federal Office for information security (Bundesamt für die Sicherheit in der Informationstechnik) that it is mathematically impossible to generate the PIN of an individual card by means of information present on the card without prior knowledge of the bank's cryptographic key.

Source: For a complete translation of this case into English, see '5 October 2004, XI ZR 210/03', Digital Evidence and Electronic Signature Law Review, 6 (2009) 248 - 252; commentaries are also provided by Dr. Martin Eßer and Dr. Thomas Kritter, 252 - 254; for a detailed discussion of the case law in Germany in English, see Assistant Professor DDr. Gerwin Haybäck, 'Civil law liability for unauthorized withdrawals at ATMs in Germany', Digital Evidence and Electronic Signature Law Review, 6 (2009) 57 - 66.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Country: England & Wales
Case: Job v Halifax PLC (not reported) case number 7BQ00307
Court: Nottingham County Court

Keywords: ATM - electronic signature (PIN) - proof for civil proceedings

SUMMARY

Seven cash withdrawals totalling £2,100 were made from Mr Job's account in February 2006 by way of two ATMs in Reading. Mr Job said he did not make the withdrawals, and he claimed that he did not authorize any third party to make them. He also denied that his card had ever left his possession and that he had never allowed anyone else to know his PIN. Mr Job subsequently complained to his bank, who rejected his claim. He took his case to the Financial Ombudsman Service, who also rejected his claim. Mr Job subsequently began legal proceedings to recover the money in February 2007 as a litigant in person. Mr Job began to be legally represented in the winter of 2008 on behalf of the Bar Pro Bono Unit.

The bank relied upon one item of evidence - a print-out of internal logging software. This is secondary evidence, that is, the evidence recorded in the log consisted of information sent to it from other sources, in turn processed by other software components, and subject to the usual problems of inaccuracy regarding any digital data that is highly processed. The learned judge concluded that Halifax had discharged its burden and proved that Mr Job's card was used in the ATMs. He did not reach any conclusion as to how the withdrawals were made, only that they were made by Mr Job, or by someone authorised by him, or by gross negligence.

COMMENTARY

This case illustrates two dangers that litigants face when considering initiating legal action in England & Wales. First, Mr Job could have forced the bank to reveal more evidence at the pleadings and disclosure stage of the proceedings, but because he was not legally represented, he did not know the significance of the procedural rules and how, by failing to use them effectively, the bank would have faced compelling arguments to produce relevant additional evidence at disclosure. This meant the case was heard on the basis of only one item of evidence when it was eventually tried. Second, under the procedural rules, cases are either allocated to the Small Claims track (in this track, neither party is liable for the costs of the other party, so a litigant in person will not be liable for the costs of the other party, even if they fail in their case), and Fast Track. Cases are allocated to Fast Track where the facts may be complex, but the claimant then looses the shield against a costs order - which occurred in this case. Had Mr Job been legally represented at the time the decision was taken to transfer the case from Small Claims to Fast Track, it could have been argued that such a decision was unfair.

Source: The judgment is printed in full with the permission of the learned trial judge in Digital Evidence and Electronic

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security
cybex
The Digital Forensic Company

Country: Lithuania
Case citation: Ž.Š. v Lietuvos taupomasis bankas, civil case No. 3K-3-390/2002
Court: Lietuvos Aukščiausiasis Teismas (Supreme Court of Lithuania)

Keywords: ATM - electronic signature (PIN) - liability of the bank

SUMMARY

The applicant deposited 800 Litas in cash into the bank account connected to the payment card issued by the bank, and on 27 August 1999 the applicant deposited a further 48,200 Litas to the same account. On 29 August 1999 almost all the money was withdrawn from the account connected to the payment card using various ATM machines in Poland. The applicant claimed that he did not perform these operations. The bank refused to restore the sums of money that had been withdrawn. The members of the Court considered liability and burden of proof, and concluded that the lower courts, each of which had found in favour of the bank, had not applied the burden of proof correctly.

COMMENTARY

The members of the Court took a realistic and robust view of the risks inherent in the technology used by banks, and made it abundantly clear that the banks have to produce a significant amount of evidence to prove their case (they listed a large number of items of evidence that should be provided by a bank, listed in detail on pages 260-261 of the translation). The comments made by the learned judges in this Supreme Court decision are very valuable, and of all the cases mentioned in this eNewsletter, this case more accurately reflects the position that the card issuer finds themselves in since the EU Directive should have entered into force in Member States.

Source: For a complete translation of this case into English, see Sergejs Trofimovs, 'Ž.Š. v Lietuvos taupomasis bankas', Digital Evidence and Electronic Signature Law Review, 6 (2009) 255 – 262.

Section Editor: Mr. Stephen Mason

The reader is invited to send details of cases (both civil and criminal, reported and not reported) that have relevance to digital evidence direct to the Editor. Please provide the correct citation as it would be in your own country, together with a full copy of the judgment. Translations into English will be appreciated if it is possible. Also, if there are any significant items of legislation that are of interest, please inform the Editor of any such changes. It is important to understand that because digital evidence moves over physical borders with ease, the changes to national legislation dealing with digital evidence and cyber crimes affects all other nation states.

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

• CONFERENCES

1-3 December 2009
7th Australian Digital Forensics Conference
Kings Perth Hotel, Perth, Australia

Purpose: The aim of the conference is to bring together IT managers, system and network administrators, security specialists, academics, security solutions vendors, practitioners and anyone interested in computer forensics its role and application; techniques in detecting, responding and investigating computer and related security incidents, and sharing their views, experiences and knowledge with those involved in the forensic computing field.

Web site: http://ocs.scss.ecu.edu.au/index.php/adf/7th

6-9 December 2009
First IEEE Workshop on Information Forensics and Security sponsored by the IEEE Signal Processing Society
London, United Kingdom

Purpose: The proposed workshop differentiates itself by encompassing a broad range of disciplines associated with information security. It is intended to provide a forum for the exchange of ideas between the various disparate communities that constitute information security. By so doing, it is hoped that researchers will identify new opportunities for collaboration across disciplines and gain new perspectives.

Web site: http://www.wifs09.org/

9-11 December 2009
8th International Information and Telecommunication Technologies Symposium I2TS 2009
Federal University of Santa Catarina, Santa Catarina Island, Brazil

Purpose: Given its multi-disciplinary nature, I2TS intends to provide a broad range of topics for audience communities in: Analog and Digital Telecommunication, Wireless Networks, Information Technologies and Applied Statistics, Free Software, Distributed Computing and Real-Time Systems, Wired Computer Networks, Computational Security, Pervasive and Ubiquitous Computing, Telemedicine and Information Systems and Medical, Research and Development for

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company

Innovative Technologies. I2TS serves as an international forum for people from academia, industry, research laboratories, for presenting recent research results in information and telecommunication technologies and applications.

Web site: http://www.i2ts.org/

10-11 December 2009.
IBWAS09, Iberic Web Application Security conference
Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Universidad Politécnica de Madrid, Spain

Purpose: This conference aims to bring together application security experts, researchers, educators and practitioners from the industry, academia and international communities such as OWASP, in order to discuss open problems and new solutions in application security. In the context of this track academic researchers will be able to combine interesting results with the experience of practitioners and software engineers.

Web site: http://www.ibwas.com/

12-14 December 2009
2009 International Workshop on Security in Cloud Computing (SCC'09)
Chengdu, Sichuan, China

Purpose: SCC'09 will bring researchers and experts together to present and discuss the latest developments and technical solutions covering various aspects of security issues in Cloud Computing. SCC'09 seeks original unpublished papers focusing on theoretical analysis, emerging applications, novel system architecture construction and designing, experimental study, and social impacts of the Cloud Computing. Both review/survey papers and technical papers are expected. Both review/survey papers and technical papers are expected.

Web site: http://bingweb.binghamton.edu/~ychen/SCC09.htm

14-16 December 2009
28th IEEE International Performance Computing and Communications Conference
Phoenix, Arizona, USA

Purpose: Topics include Grid and cloud computing; Internet Services and Network Management Network protocols; Network Information Assurance, and Security Multi- and single- core processor architecture; Cache, Memory, and Disk Storage Systems; Workload Characterization and its Impact on Architecture Design Embedded Systems; Ubiquitous computing Mobile ad hoc, Sensor and Mesh Networks; Parallel and Distributed Systems Performance Evaluation and Modeling Performance Tools and Techniques.

Web site: http://ipccc.org/ipccc2009/main.php?page=6#workshop3

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

3-6 January 2010
Sixth Annual IFIP WG 11.9 International Conference on Digital Forensics
University of Hong Kong, Hong Kong

Purpose: IFIP Working Group 11.9 on Digital Forensics is an active international community of scientists, engineers and practitioners dedicated to advancing the state of the art of research and practice in the emerging field of digital forensics.

Web site: http://www.ifip119.org/Conferences/

22-29 January 2010
US Department of Defence Cyber Crime Conference
St Louis, Missouri, USA

Purpose: This conference focuses on all aspects of computer crime: intrusion investigations, cyber crime law, digital forensics, information assurance, as well as the research, development, testing, and evaluation of digital forensic tools.

Web site: http://www.dodcybercrime.com/10CC/

• LEGAL TRAINING

14-17 December 2009
European Certificate on the fight against Cybercrime and Electronic Evidence (ECCE)
Lithuania
Web site: http://www.advoco.lt and http://www.cybex.es/ecce/en/

Section Editor: Mr. Stephen Mason

The reader is invited to send details of conferences, university degree courses, legal training seminars and vendor seminars direct to the editor for inclusion in future issues of the eNewsletter. By submitting your event or course, you accept that it will not necessarily be included in a future issue of the eNewsletter. The inclusion of events and courses is at the sole discretion of the Editor. The criteria for inclusion of events and courses focuses on what, if any, relevance it will have for judges, lawyers and digital evidence specialists within the legal framework.

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Editors

A team of seven Editors has been engaged to create the European Electronic Newsletter on the Fight Against Cybercrime, each one being an Expert on the ENAC Section of which they are responsible.

The Editors are in charge of recruiting writers and articles and reviewing and selecting the most appropriate to be included in the ENAC.

According to the order of appearance of their Sections in the ENAC, the Editors are the following:

Mr. PEDRO VERDELHO
Public Prosecutor and trainer
pedro.verdelho@gmail.com

Mrs. ESTHER GEORGE
Senior Policy Advisor, Crown Advocate
Crown Prosecution Service
Esther.George@cps.gsi.gov.uk

Mrs. ELENA DOMÍNGUEZ PECO
Public Prosecutor and Collaborator
for the Spanish Data Protection Agency
elena.dominguez@comjib.org

Mr. MATIAS BEVILACQUA
Computer Forensic Expert
IT Manager
Cybex
mbevilacqua@cybex.es

Mr. NIGEL JONES
Director
Technology Risk Limited
nigel.jones@technologyrisklimited.co.uk

Mrs. LILJANA SELINSEK
Assistant Professor at the
Law Faculty of University of Maribor
liljana.selinsek@uni-mb.si

STEPHEN MASON
Barrister
Chambers of Stephen Mason
stephenmason@stephenmason.eu

Mrs. MIREIA CASANOVAS
Chief Editor
Cybex
mcasanovas@cybex.es

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Distributors

To ensure the widest possible diffusion of the Electronic Newsletter on the Fight Against Cybercrime, the ENAC counts with the collaboration of Distributor Institutions and Organizations, who will distribute the ENAC monthly to their contacts database.

If you are interested in being a Distributor partner please contact the Project Coordinator Mrs. Mireia Casanovas at mcasanovas@cybex.es.

The Distributors of the ENAC Project are the following:

- Actuar Asociación Civil
- Agencia Española de Protección de Datos
- Alba Advisors LTD
- Altmark and Brenna
- Ambassade du Costa Rica
- Asia Pacific Cyberlaw, Cybercrime and Internet Security Institute (Waseda)
- Asociación de Jueces, Justicia y Opinión
- Association of Prosecutors of Republic of Serbia
- Attorney-General's Department Sri Lanka
- Centro de Estudios Judiciários
- CERT-LEXSI
- Ciberdelincuencia.org
- Comisión Interinstitucional Sobre Terrorismo CISTE
- Consejo General de la Abogacía Española
- Conselho Distrital de Lisboa da Ordem dos Advogados

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Council of Europe

Crown Prosecution Service United Kingdom

Cuerpo Nacional de Policía Española

Cyprus Police Cyber Crime Task Force

Department for International and European Affairs Hungary

Directorate for Investigation of Organized Crime and Terrorism. Prosecutor's Office · High Court of Cassation and Justice

Cristian Driga Cabinet de Avocat Romania

Ebay

Escuela de Juristas Bolivia

Escuela Judicial del Consejo General del Poder Judicial

Espion LTD

Estonian Public Service Academy (EPSA)

EUROJUST

Federal Judicial Police Computer Crime Unit DJF/FCCU Belgium

Federal Judicial Police Brazil

Fiscalía General del Estado Ecuador

Fiscalía General del Estado España

Guardia Civil Española Grupo de Delitos Telemáticos

Home Office United Kingdom

Institute for Arbitration and Mediation

Institute of Criminal Sciences Croatia

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Institute of Criminology
Faculty of Law · Ljubljana

Institutio Nacional de Tecnologías de la Comunicación INTECO

International Training and Methodology Centre for Financial Monitoring

Ledjit Consulting

Lithuanian Bar Association

Malta Police Force

Microsoft

Ministerio della Giustizia
Dipartimento per gli Affari di Giustizia

Ministry of Justice
and Citizens Liberties
Romania

Ministerio Público de Chile
Unidad Especializada en Lavado de Dinero, Delitos Económicos y Crimen Organizado

Ministry of Justice
of the Slovak Republic

Morenets Consulting

National Institute of Criminology
Budapest

National Prosecuting Authority of South Africa

National Public Prosecutor's Office of the Republic of Poland

National School for the Judiciary
France

North American Consumer Project on Electronic Commerce

Organization for Security and Cooperation in Europe

PAD-ORION

Policía Federal Preventive
Delegación Coyoacán

Portaley Nuevas Tecnologías
Spain

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

Procuradoría General de la República Dominicana

Risk Analysis Consultants s.r.o. · RAC

Serious Organised Crime Agency (SOCA)

Sindicatos dos Magistrados do Ministerio Publico Portugal

State Prosecutor Department of Justice Philippines

Superintendencia de Servicios de Certificación Electrónica

Technology Risk Limited

Telecommunication Authority Turkey

TEUTAS srl

The Voivodeship Headquarters of the Police Krakow

The Society For The Policing Of Cyberspace

United Nations Interregional Crime and Justice Research Institute · UNICRI

University of Buenos Aires

University of Edinburgh

University of Maribor

University of Verona

United Nations Office on Drugrs and Crime

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

eNAC
e-NEWSLETTER ON THE FIGHT AGAINST CYBERCRIME

The ENAC project is funded by Cybex and the European Commission's Directorate General Freedom, Security and Justice, within the framework of the Criminal Justice Programme 2008

Disclaimer:

ENAC e-newsletter provides news and opinion articles as a service to the readers. Statements and opinions expressed in these articles are solely those of the author or authors and may not be shared by the ENAC Board of Editors, Cybex management or the European Commission.

The translations included in the ENAC newsletter were prepared with the utmost care. However, ENAC Board of Editors, Cybex management or the European Commission do not accept any liability for the accuracy and completeness of the compilation and content of these translations, or the direct or indirect consequences of acting or failing to act based on these translations.

DL: B.25824-2009
ISSN: 2013-5327

Criminal Justice 2008
With financial support from Criminal Justice Programme
European Commision - Directorate - General Justice, Freedom and Security

cybex
The Digital Forensic Company