

ATTACKS FROM THE LOGICAL TO THE PHYSICAL WORLD

"This article has been inspired by Bruce Sterling's book "Distraction", and by Bruce Schneier's CryptoGram article , <http://www.counterpane.com/crypto-gram0304.html#1>".

Authors

Román Ramírez <rramirez@chasethesun.com>
Managing Director, Chase The Sun

Jesús Arnáiz <jarnaiz@chasethesun.com>
Technology Director and Operations Director, Chase The Sun

This article in .PDF:

<http://www.chasethesun.es/docs/logicoafisico.pdf> [Español]
<http://www.chasethesun.com/docs/logictophysic.pdf> [English]

This article in .RTF:

<http://www.chasethesun.es/docs/logicoafisico.rtf> [Español]
<http://www.chasethesun.com/docs/logictophysic.rtf> [English]

Introduction

Traditionally, the valuation and quantification of attacks to logic goods has been done based in the logical havoc caused by them. We speak of figures in the millions of euros or dollars, exclusively taking into the picture denial of service and other purely logical factors.

However, all this logical damage implies certain repercussion over the physical world, and there are many more implications and potential vulnerabilities yet to be exploited, which will probably be so in the near future.

Throughout some paragraphs in this article, it may seem to the reader we are exaggerating or taking the issues in it to the extreme, issues that nowadays don't pose any threat at all, nor will they to the common observer in the near future.

Actually, it is not our aim to induce paranoia, but we do want to give evidence of the potential dangers existing TODAY, which we will probably see materialise into real cases in the more than near future.

Direct and side effects of a logical attack

The propagation of an Internet worm like CodeRed, Nimda or Slammer, generally causes damage to the quality of service, damage to critical services (such as web and databases) and, additionally, monetary losses associated to the disbursement for the recovery of casualties.

Among the physical effects caused by these attacks as resonancy, we can immediately list: loss of production hours, stalled employees waiting for the solution, corporate image problems, after-incident time dedicated in coming to a solution, potential hardware replacement costs.

Looking through the cases we know, which conforms our body of knowledge in our estimations in damage control, we often overlook the attacks we currently suffer are actually simple and little sophisticated. The direct and immediate damage that most of the attacks or worms leverage can be repaired in short time, and in most of the cases their effects have been minimised or restricted to just some workstations of the network.

But, what happens when a particular attack affects a device acting as a link between the logical and physical worlds? The most straight-forward and basic example is a computer managing a set of relays (electronically controlled switches), and also possessing a "modern" and permanent network connection, such as DSL, WiFi or cable.

Physical attacks coming from the logical world

Snail Mail

We won't go into much detail about the issue discussed in Bruce Schneier's article dealing with the attacks coming through snail mail, but we would like to do some remarks on the parcel services.

As Schneier himself explains, if we launch automated attacks using some particular programs (you can find additional details in the article of Simon Byers, Avi Rubin and Dave Kormann, <http://www.avirubin.com/scripted.attacks.pdf>), we can force massive subscriptions to paper publications, that once delivered might overflow anyone's -physical- postbox.

Let's imagine an attacker could cancel important and urgent parcels, such as documents, goods or, taking it to the extreme, transfusion grade blood, or organs to be transplanted.

It may seem the occurrence these two last cases may be highly remote, but it may be not, moreover if we bear in mind that most surely a high percentage of hospitals will have specific distribution agreements with parcel delivery companies (specialised in this kind of assignments), which, at the end of the day, may as well be vulnerable.

Damage to personal and public image

This sort of attacks can affect the relationships of individuals with their social environments. Let's imagine the case of an exemplary citizen that out of the blue starts to see its mail flooded by hardcore pornographic publications. In large communities, a common citizen enjoys a certain level of privacy, but in smaller communities we can ascertain the postman is most probably another member of the community, which may or may not talk to others about the tone of an individual's mail.

Also, if our postbox is outside our home, some types of parcels can easily be linked to the us, let alone the ones we have to pick up from the post office.

How much could it affect your image in your community this kind of mail or parcels?

- Politically incorrect subscriptions: It is an immediate example, and it is a case frequently seen; porn magazines roguely sent to relevant members of the community. Specially known are the cases of "jokes" whose victims were the priests of local churchs.
- Acquisition and shipping of compromising materials: We have heard of many cases of credit card theft on the Internet. With a stolen card and the victim's personal information, an attacker can do a lot of harm. For instance, by buying explicit sexual material and sending it to the address of an innocent member of the community, or even with more elaborated attacks, like offensive letters on behalf of others, etc.

Changes in client profiles

More and more firms strive to improve their information systems on an everyday basis, to enable the client to manage or update his/her data over the Internet or over the phone.

Let's think what sort of changes could an attacker infer to our registries in those entities was he capable of impersonating us and faking an update operation.

In most customer care lines we are requested personal information that an attacker could obtain should he have the intention to do so.

For instance, many of them request the reference ID of the latest bill (which could have been stolen from our postbox), or they request our complete name and social security number (which may be obtained from the records of our university).

- Corruption of the information: for instance, the redirection of our snail mail to an address where we would never receive it, or where it could be stolen by our attacker, so he can freely use our identity. Change our account number, giving a bogus number, so every payment would be automatically rejected (which in the end could cause the shut down of the service due to impayment), or modifications to the secondary details of the client, which could enable the attacker to counterfeit a card (e.g. a debit card from a supermarkets chain).
- Deactivation of services: the most annoying case we might face is when the attacker decides on our behalf to shut down services that we much need. For instance, mobile

telephone, or even medical insurance. Telephone, Internet connection, necessary subscriptions, etc. All these services and many others can be prey of attacks.

Fraudulent consumption of physical resources

“Trojan Horses” are one of the most current problems presently. They can manipulate the dial-up configuration of an account, so the user is fooled into making calls through a premium number with higher charges.

On many occasions, the victim is not even aware that he is making calls to premium and highly charged numbers, even though he may have the phone bill in front of him.

It is common practice among many porn websites to try and insert this type of Trojans in the systems of potential victims.

In the section we will dedicate to mobile phones we will see that a Trojan Horse which redirects our calls to this premium numbers can be extremely harmful.

Even widely known Trojan Horses like Cydoor, Alexa and others, whose principal task is the capture of each and every movement of the user, and the learning of his customs so personalised advertising can be carried through later, could become tools that link the virtual alter ego of a user with his real personality in the everyday world.

Imagine a Trojan Horse that, after learning the habits and customs of the user, assumed the task of arranging personalised postal marketing to be sent to the user, perfectly suited to his preferences.

Being this bad enough, it could worsen if these systems captured the mailing address from, for instance, his e-mail program, and distributed it among avid advertisers in the porn industry.

Vulnerable equipment and hardware

- Computing equipment: there is no doubt computing equipment is vulnerable to logical attacks. To date, attacks of any type and condition have been observed, mainly classified in three groups; denial of service attacks, intrusions (where manipulation may happen or may not), and information theft. But the near future will bring to use eager and tangible threats, such as new worms with artificial intelligence abilities that, as an example, would know how to adapt themselves to the different platforms, with the ability to learn new assault techniques, and generate its own dynasty of new worms with limited (or not) means of attack. An example comes to mind, a worm that keeps a permanent connection to a remote system, which gives him access to a daily updated database of new vulnerabilities or 0d (Zero Day) exploits, so this worm would modify its behavioural pattern from time to time. This same worm could even incorporate its own compiler, which will enable it to generate its own binaries. It would give birth to this binaries, that would include modifications, making them invisible to Antivirus tools or IDSes. TinyC, <http://fabrice.bellard.free.fr/tcc/> is an example of a compiler weighting less than a MegaByte. Even with TinyC itself, worms with the ability to interpret C source code could be created. Thus, without the need to compile, their abilities could be

endless. We must be prepared for the true cases of polymorphic and mutable attacks, as new software applications, and so worms, are growing in genetical capabilities.

- Mobile phones, PDAs and PAN networks: nowadays almost everybody has got a mobile telephone, in professional environments as in personal ones, among the elderly as among the youngsters and teens. Most of them carry their mobile phone 24 hours a day and indeed here in the Western countries most people buy a mobile phone over a computer. Needless to say, the up and coming PAN networks (Personal Area Networks), will open many doors of attack to the "virtual space" of a user. Currently, using Bluetooth technology any user can build her own "personal technology bubble", wrapping herself inside a communications network that links every electronic device around her, creating a vast range of functionalities (and of potential vulnerabilities). The functionalities delivered by current mobile phones or PDAs are overwhelming, ranging from the ability of geographical location via GPS (or directly, through the position of the handset in relation to the GSM network cells), international calls, calendar, integrated phonebook, audio and video recording capabilities, the ability of taking and processing photos, and many more. If, in addition to this, we bear in mind we are starting to see devices like mobile-enabled watches, such as the "Spot" from Microsoft, and that most of these new devices will probably end up using the advanced functionalities of GPRS and UMTS networks, we have to ask ourselves about the future of these devices and their effects upon us in case we suffer a security incident. The service options of SMS and MMS (multimedia messages) may allow effects as odd as the denial of service on a phone through message flooding. We will possibly witness the appearance of a new generation of abusive uses and attacks launched through these multimedia options in MMS. The abuse of the geographical location service could occur in cases ranging from hijacking and stalking incidents, to companies recording, not just where people buy online, but which physical stores they enter (let's recall Tom Cruise's film, "Minority Report", <http://us.imdb.com/Title?0181689>), when they stop to have an ice cream, which days of the week they meet for coffee and with whom (crossing the records of every person involved), when and with whom do particular individuals have relations, even "bosses" that check when do their employees enter or leave the office, leave their desk, go to the toilet, etc. The current error margins of mobile geographical location range from three to ten metres. Most mobile operators even provide services that enable a user to find out when does another user switch her mobile phone on or off, with the immediate effect upon the privacy of the latest. The special multimedia options, such as the video and sound recorder, and photo camera, could become "spy" tools at the service of a potential attacker. Being the user's phone or PDA previously infected with a Trojan Horse, it could remotely activate the microphone, the photo camera or the video recorder, tainting the privacy of a user as a concept to be verified. Mobile phones and PDAs are nowadays the first computer humans constantly carry on, almost stuck to their skin (in some cases taking advantage of human features to, for instance, transmit a business card, <http://www.almaden.ibm.com/cs/user/pan/pan.html>). It is the first computer many humans voluntarily and willingly carry, to the point they identify themselves with it, and extend the personalisation and customisation of their images to the mobile phone, as though it was an extension of themselves. What can be the consequences of suffering an "intrusion" in our mobile? The loss of our secret payment keys, could possible be one of the most serious, and let's think that if there are people that identify themselves with their mobiles, it may be possible they put all their trust on them. They are, at the end of the day, like any other computer, and they suffer from the same security problems. What could be the economic cost of being infected with a Trojan Horse that forces a mobile phone to launch every call through a special

international or premium number? Could an attacker use our handset as an intermediate assault point to make calls hiding the real origin of them?

- Electrical appliances: nowadays domotics is a commonly used discipline (back in the 80s and 90s there was an explosion in the general interest in home process automation). Presently, we can find appliances ranging from washing machines and fridges that can be managed from the Internet (just look at the Siemens or Ariston Digital models), to complex television systems such as satellite channels or devices like TiVO. An attack affecting the IT systems of any home, could cause serious effects upon the operation of these devices. Let's remember the vulnerabilities found in the SNMP managers SNMP (CERT, <http://www.cert.org/advisories/CA-2002-03.html>), and let's imagine an attack against the manager of one of these home devices, causing malfunction and, among other consequences, the overflow of a washing machine, the unfreezing in the fridge, or, in a more spectacular fashion, the projection of pornography (and/or ads) through TiVO (it would be trivial to modify the configuration and preferences of the user of a service like TiVO, provided we have privileged access to his device). Which other devices are we going to see "connected" in the future? Ovens? Heating? Ventilation systems? Specialised medical equipment?
- Printers and Faxes: In the 90s a simple attack against Fax devices was extremely popular: it consisted of the use of a black paper sheet, that once placed inside the Fax, was converted to an endless paper stripe by pasting with tape the extremes of the sheet, so when a fax was sent, the receiver ran out of ink. This was a simple but destructive attack, as it caused a "denial of service" to the fax, and obviously a disbursement for the replacement of the ink cartridge. Currently, many SMEs have integrated Fax and printer devices, and in many occasions they also integrate a tiny modem that simulates the complete office (ie. Integrated within a laptop). How secure or vulnerable are these complete solutions for the portable office? Chances are if we enable our Fax simulator we are opening the door for potential remote attacks.
- Closed Circuit Video surveillance: In big cities like London, Paris and Madrid, there are CCTV controlled urban areas. Due to security or law enforcement concerns these areas and streets are controlled through complex structures of cameras and control panels. Also, we can find surveillance cameras inside most ATMs, that periodically and continually capture the scene of the ATMs (which may not have people inside, opposite to the cameras). Many vendors (for instance, Axis, 3Com, Cisco ...) sell WiFi devices that in some way or another can be used together with a camera to send the captured images over the waves (with the inherent risk of eavesdropping or interference). Let's imagine a potential attacker that gained access to these CCTV surveillance systems, who would use them to his profit, to say, control the movements of particular citizens or important political representatives (the "24 hours" series, starring Kiefer Sutherland, demonstrates the fraudulent and criminal use consequence of abusing a CCTV system). Other fiction plots, such as "Sliver" (starring Sharon Stone), demonstrate how the abusive use of a building's CCTV provides unlimited might to a "voyeur", that closely surveys the movements of all of his neighbours. A chapter of the "CSI" series dealt with the case of a stalker who

controlled his victims by installing cameras, thanks to his privileged access his condition of cable installer provided him ("CSI", 42nd chapter). Imagine how vulnerable can we be if organised criminals could access the surveillance systems inside our homes, offices or streets. The combination of access to multiple CCTV systems, could help these criminal groups to planify the assault of armoured vans, military convoys, or the tracking of a victim.

- Computer controlled machinery: There are hundreds of devices that depend upon a computerised controller or that connect and send information to some kind of computerised manager. In enterprise frameworks, SAP R/3 systems and MRP technology encompass any stage of the production chain, starting down on every production point, thus we can affirm each step is controlled by an information system. Many factories keep process and assembly chains attended by complex robots, whose management is done through computers, and even many basic infrastructures that serve citizens depend on computers (water supply systems, electricity, waste disposal ...). A logical attack that could affect these sort of infrastructures could cause mayhem. The topic of damages to basic infrastructures is thoroughly discussed in the website of eEye Digital Security, <http://www.eeye.com/html/Research/Papers/DS20020724.html>, authored by Marc Maiffret. These are the potential victims of attacks to computer-controlled machinery:
 - Traffic lights: let's think in the implications of an attack that could affect traffic control systems, traffic lights, en-route warning systems ... The potential risk is huge.
 - Lifts: in tall buildings and skyscrapers, the control of the lifts depends upon a central computer. The access to this computer can keep all the people inside building from accessing the lifts.
 - Fire: the fire response system is frequently connected to a computerised management system. Should an attacker be able of remotely activating it, how much money would be loss to damage from water or foam spilt by the fire extinction systems?
 - Industrial systems: many manufacturing plants depend upon the production chain management system (petriNets, for instance). Which effects could arise from an attack to these automated systems?
 - Industrial scale urban services: waste disposal, water supply, electricity supply, fuel distribution, underground air recycling systems, etc.
 - Others: you name it, it is vulnerable.

Derivation of criminal authorship

This is traditionally done by IPspoofing techniques or "reflection" over third party information systems. What the attacker will try is to mask its origin address when launching an attack to a remote system, presenting instead the addresses of other systems, by launching the attacks through them (e.g. via proxy), or using advanced techniques to hide his direction.

But, what if what the attacker intends is to hide his social identity? We can find on the Internet multiple examples of databases that record citizen information, being it university records, population surveys, newspapers that contain articles that mentioning a citizen ...

A criminal could intend to use a different identity to buy over the Internet, to register an alternative address (to be used to pick up the goods illegally acquired on behalf of the victim), or in pursuit of many other purposes.

Among these intentions, we can include the previously discussed examples, like the use of stolen credit cards, which in fact can serve as a simulated personality in any payment operation, or, worse enough, may enable a potential attacker to clone the complete identity of a different citizen.

In the United States and other countries, there are no national identity cards in use, which makes possible to anyone with enough will and means to create a false document (say a driving license), just by accessing the birth records of a citizen (this has been done many times, using the personal information of deceased people, or of children that died at birth time).

Induction to crime via logical methods

In Bruce Sterling's book, "Distraction", a technique is discussed where crime can be induced through the net.

The goal is to create in a set of potential killers (serial killers for instance) the need to criminally act against a victim. This technique is executed starting from a large database containing data of people with homicidal tendencies, that would be bombarded with constant information about the victim to be harm.

Although it is a theory proper of a novel, we must not forget there is strong speculation about figures like the "dormants", the "Manchu killers", and, among others, about the book "The Catcher in the Rye" by J.D. Salinger, ISBN: 8420634093. Over the years this book has been linked to the murders of John Lennon (Mark David Chapman), the attempt to kill Ronald Reagan (John Hinckley) and others.

Inside the CIA, mind control experiments were carried for a long time, as project BLUEBIRD and project ARTICHOKE (which went on to be named MKULTRA) demonstrated.

In the film "Conspiracy Theory", starring Mel Gibson, we find direct references to the book "The Catcher in the Rye" as the trigger for homicidal conducts.

Is it possible to induce predisposed people to commit a crime? It is complex to answer this question, and it should be analysed by specialised professionals.

It is clear though, none of us would be worry free should we know someone can be actively sending our information to recognised or potential murderers.

References and notes

[1] "Distraction" - Bruce Sterling, ISBN: 84-8421-280-7

[2] "Automated Denial-of-Service Attack Using the U.S. Post Office" - Bruce Schneier, <http://www.counterpane.com/crypto-gram-0304.html#1>

[3] "The Catcher in the Rye" - J.D. Salinger, ISBN: 84-2063-409-3

[4] "Tiny C", <http://fabrice.bellard.free.fr/tcc/>

[5] Project MKULTRA, <http://www.medals.org.uk/unosir/archives/mkultra.htm>



- [6] Chase The Sun, <http://www.chasesun.com>
[7] eEye Digital Security, <http://www.eeye.com>
[8] "CHO's Testimony on the Nation's Infrastructure Systems for a Congressional Subcommittee Hearing", by Marc Maiffret, <http://www.eeye.com/html/Research/Papers/DS20020724.html>
[9] "PAN FACT SHEET", by Thomas Zimmerman, <http://www.almaden.ibm.com/cs/user/pan/pan.html>

Madrid, April the 18th, 2003