THE ATHENS AFFAIR

HOW SOME EXTREMELY SMART HACKERS PULLED OFF THE MOST AUDACIOUS CELL-NETWORK BREAK-IN EVER

By Vassilis Prevelakis & Diomidis Spinellis

ON 9 MARCH 2005, a 38-year-old Greek electrical engineer named Costas Tsalikidis was found hanged in his Athens loft apartment, an apparent suicide. It would prove to be merely the first public news of a scandal that would roil Greece for months.

The next day, the prime minister of Greece was told that his cellphone was being bugged, as were those of the mayor of Athens and at least 100 other high-ranking dignitaries, including an employee of the U.S. embassy.

The victims were customers of Athens-based Vodafone-Panafon, generally known as Vodafone Greece, the country's largest cellular service provider; Tsalikidis was in charge of network planning at the company. A connection seemed obvious. Given the list of people and their positions at the time of the tapping, we can only imagine the sensitive political and diplomatic discussions, high-stakes business deals, or even marital indiscretions that may have been routinely overheard and, quite possibly, recorded.

Even before Tsalikidis's death, investigators had found rogue software installed on the Vodafone Greece phone network by parties unknown. Some extraordinarily knowledgeable people either penetrated the network from outside or subverted it from within, aided by an agent or mole. In either case, the software at the heart of the phone system, investigators later discovered, was reprogrammed with a finesse and sophistication rarely seen before or since.

A study of the Athens affair, surely the most bizarre and embarrassing scandal ever to engulf a major cellphone service provider, sheds considerable light on the measures networks can and should take to reduce their vulnerability to hackers and moles.

It's also a rare opportunity to get a glimpse of one of the most elusive of cybercrimes. Major network penetrations of any kind are exceedingly uncommon. They are hard to pull off, and equally hard to investigate.

Even among major criminal infiltrations, the Athens affair stands out because it may have involved state secrets, and it targeted individuals—a combination that, if it had ever occurred before, was not disclosed publicly. The most notorious penetration to compromise state secrets was that of the "Cuckoo's Egg," a name bestowed by the wily network administrator who successfully pursued a German programmer in 1986. The programmer had been selling secrets about the U.S. Strategic Defense Initiative ("Star Wars") to the Soviet KGB.

But unlike the Cuckoo's Egg, the Athens affair targeted the conversations of specific, highly placed government and military officials. Given the ease with which the conversations could have been recorded, it is generally believed that they were. But no one has found any recordings, and we don't know how many of the calls were recorded, or even listened to, by the perpetrators. Though the scope of the activity is to a large extent unknown, it's fair to say that no other computer crime on record has had the same potential for capturing information about affairs of state.

While this is the first major infiltration to involve cellphones, the scheme did not depend on the wireless nature of the network. Basically, the hackers broke into a telephone network and subverted its built-in wiretapping features for their own purposes. That could have been done with any phone account, not just cellular ones. Nevertheless, there are some elements of the Vodafone Greece system that were unique and crucial to the way the crime was pulled off.

We still don't know who committed this crime. A big reason is that the UK-based Vodafone Group, one of the largest cellular providers in the world, bobbled its handling of some key log files. It also reflexively removed the rogue software, instead of letting it continue to run, tipping off the perpetrators that their intrusion had been detected and giving them a chance to run for cover. The company was fined €76 million this past December.

To piece together this story, we have pored through hundreds of pages of depositions, taken by the Greek parliamentary committee investigating the affair, obtained through a freedom of information request filed with the Greek Parliament. We also read through hundreds of pages of documentation and other records, supplemented by publicly available information and interviews with independent experts and sources associated with the case. What emerges are the technical details, if not the motivation, of a devilishly clever and complicated computer infiltration.

THE CELLPHONE BUGGING began sometime during the fevered run-up to the August 2004 Olympic Games in Athens. It remained undetected until 24 January 2005, when one of Vodafone's telephone switches generated a sequence of error messages indicating that text messages originating from another cellphone operator had gone undelivered. The switch is a computer-controlled component of a phone network that connects two telephone lines to complete a telephone call. To diagnose the failures, which seemed highly unusual but reasonably innocuous at the time, Vodafone contacted the maker of the switches, the Swedish telecommunications equipment manufacturer Ericsson.

We now know that the illegally implanted software, which was eventually found in a total of four of

CEOs, MPs & A PM

The illegally wiretapped cellphones in the Athens affair included those of the prime minister, his defense and foreign affairs ministers, top military and law enforcement officials, the Greek EU commissioner, activists, and journalists.

On 6 April 2006, **BILL ZIKOU**, CEO of Ericsson Hellas, was summoned to give evidence before a parliamentary committee looking into the scandal. His company provided the telecommunications switching equipment that rogue programmers broke into.

Vodafone Greece CEO **GIORGOS KORONIAS** ordered the removal of the surveillance program, because, as he explained in a February 2006 newspaper interview, "the company had to react immediately." Removing the program is thought to have tipped off the perpetrators and helped them evade capture.

Greek Prime Minister **COSTAS KARAMANLIS** was only the most notable of the 100 or so individuals illegally wiretapped, which, besides the country's political, law enforcement, and military elite, included Karamanlis's wife.

COSTAS TSALIKIDIS was found hanged, an apparent suicide, just before the Athens affair became public. As a telecommunications engineer in charge of network planning at Vodafone, he was ideally placed to be either an inside accomplice or discoverer of the digital break-in. But his involvement in the case has never been established.

GIORGOS VOULGARAKIS was the first government official to whom Koronias disclosed the case. Giannis Angelou, the director of the Prime Minister's political office, was also present.

OPPOSITE PAGE: ARCHIVBERLIN FOTOAGENTUR/ALAMY; FROM TOP: KOSTAS TSIRONIS/AP PHOTO(2); JOHANNA LEGUERRE/AFP/GETTY IMAGES; AFP/GETTY IMAGES; LOUISA GOULIAMAKI/AFP/GETTY IMAGES

Vodafone's Greek switches, created parallel streams of digitized voice for the tapped phone calls. One stream was the ordinary one, between the two calling parties. The other stream, an exact copy, was directed to other cellphones, allowing the tappers to listen in on the conversations on the cellphones, and probably also to record them. The software also routed location and other information about those phone calls to these shadow handsets via automated text messages.

Five weeks after the first messaging failures, on 4 March 2005, Ericsson alerted Vodafone that unauthorized software had been installed in two of Vodafone's central offices. Three days later, Vodafone technicians isolated the rogue code. The next day, 8 March, the CEO of Vodafone Greece, Giorgos Koronias, ordered technicians to remove the software.

Then events took a deadly turn. On 9 March, Tsalikidis, who was to be married in three months, was found hanged in his apartment. No one knows whether his apparent suicide was related to the case, but many observers have speculated that it was.

The day after Tsalikidis's body was discovered, CEO Koronias met with the director of the Greek prime minister's political office. Yiannis Angelou, and the minister of public order, Giorgos Voulgarakis. Koronias told them that rogue software used the lawful wiretapping mechanisms of Vodafone's digital switches to tap about 100 phones and handed over a list of bugged numbers. Besides the prime minister and his wife, phones belonging to the ministers of national defense, foreign affairs, and justice, the mayor of Athens, and the Greek European Union commissioner were all compromised. Others belonged to members of civil rights organizations, peace activists, and antiglobalization groups; senior staff at the ministries of National Defense, Public Order, Merchant Marine, and Foreign Affairs; the New Democracy ruling party; the Hellenic Navy general staff; and a Greek-American employee at the United States Embassy in Athens.

Within weeks of the initial discovery of the tapping scheme, Greek government and independent authorities launched five different investigations aimed at answering three main questions: Who was responsible for the bugging? Was Tsalikidis's death related to the scandal? And how did the perpetrators pull off this audacious scheme?

TO UNDERSTAND HOW someone could secretly listen to the conversations of Greece's most senior officials, we have to look at the infrastructure that makes it possible.

First, consider how a phone call, yours or a prime minister's, gets completed. Long before you dial a number on your handset, your cellphone has been communicating with nearby cellular base stations. One of those stations, usually the nearest, has agreed to be the intermediary between your phone and the network as a whole. Your telephone handset converts your words into a stream of digital data that is sent to a transceiver at the base station.

The base station's activities are governed by a base station controller, a special-purpose computer within the station that allocates radio channels and helps coordinate handovers between the transceivers under its control.

This controller in turn communicates with a mobile switching center that takes phone calls and connects them to call recipients within the same switching center, other switching centers within the company, or special exchanges that act as gateways to foreign networks, routing calls to other telephone networks (mobile or landline). The mobile switching centers are particularly important to the Athens affair because they hosted the rogue phone-tapping software, and it is there that the eavesdropping originated. They were the logical choice, because they are at the heart of the network; the intruders needed to take over only a few of them in order to carry out their attack.

Both the base station controllers and the switching centers are built around a large computer, known as a switch, capable of creating a dedicated communications path between a phone within its network and, in principle, any other phone in the world. Switches are holdovers from the 1970s, an era when powerful computers filled rooms

FROM ALPHA TO OMEGA

ERICSSON

31 Jan Ericsson provides Vodafone with the details of its R9.1 software, which includes lawful interception (LI) capability.

6 Jun Accounts for first two shadow phones are created.

9 Jun Three more shadow phones are registered.

29 Jun One shadow phone makes two outgoing calls.

20 Jan Shadow phones operate in Lycabettus restaurant in Athens.

24 Jan–1 Feb Two test numbers are configured for interception at a fourth exchange, MEAPA.

24 Jan The MEAPA exchange begins logging forlopp errors.

25 Jan The MEAPA exchange stops logging forlopp errors.

27 Jan Credits are added to the shadow phone accounts.

31 Jan Shadow phones make one call and forward another. The call recipient then sends an SMS message to itself.

11 Feb MEAKF upgrades from R9.1 to R10 software, destroying the rogue code.

18 Feb Credits are added to the shadow phone accounts.

18 Feb Shadow phones operate in Lycabettus restaurant.

JAN 2002 | JAN 2003 | JAN 2004 | MAR | MAY | JUL | SEP | NOV | JAN 2005

vodafone

20 Jan Ericsson delivers R9.1 system software containing partial LI functionality to Vodafone.

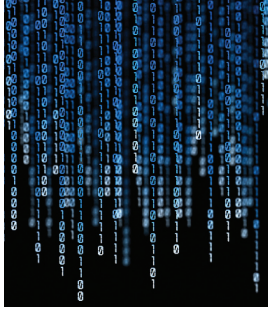
4 Aug Nine more shadow phones are registered.

4–10 Aug Rogue software is installed in three exchanges: MEAKS, MEAKF, MEAPS.

9–11 Aug Rogue software is configured with interception numbers.

13 Aug Opening ceremony of the Athens 2004 Olympic Games.

27–29 Oct Rogue software is installed in the MEAPA exchange but is not used for monitoring.



and were built around proprietary hardware and software. Though these computers are smaller nowadays, the system's basic architecture remains largely unchanged.

Like most phone companies, Vodafone Greece uses the same kind of computer for both its mobile switching centers and its base station controllers—Ericsson's AXE line of switches. A central processor coordinates the switch's operations and directs the switch to set up a speech or data path from one phone to another and then routes a call through it. Logs of network activity and billing records are stored on disk by a separate unit, called a management processor.

The key to understanding the hack at the heart of the Athens affair is knowing how the Ericsson AXE allows lawful intercepts—what are popularly called "wiretaps." Though the details differ from country to country, in Greece, as in most places, the process starts when a law enforcement official goes to a court and obtains a warrant, which is then presented to the phone company whose customer is to be tapped.

Nowadays, all wiretaps are carried out at the central office. In AXE exchanges a remote-control equipment subsystem, or RES, carries out the phone tap by monitoring the speech and data streams of switched calls. It is a software subsystem typically used for setting up wiretaps, which only law officers are supposed to have access to. When the wiretapped phone makes a call, the RES copies the conversation into a second data stream and diverts that copy to a phone line used by law enforcement officials.

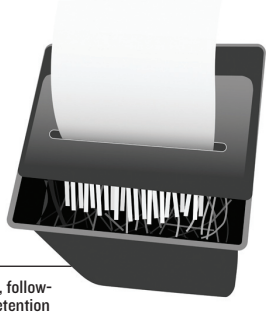
Ericsson optionally provides an interception management system (IMS), through which lawful call intercepts are set up and managed. When a court order is presented to the phone company, its operators initiate an intercept by filling out a dialog box in the IMS software. The optional IMS in the operator interface and the RES in the exchange each contain a list of wiretaps: wiretap requests in the case of the IMS, actual taps in the RES. Only IMS-initiated wiretaps should be active in the RES, so a wiretap in the RES without a request for a tap in the IMS is a pretty good indicator that an unauthorized tap has occurred. An audit procedure can be used to find any discrepancies between them.

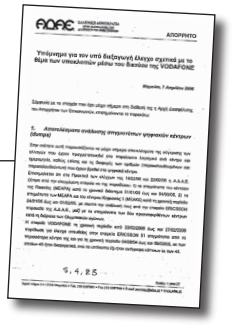
It turns out Vodafone had not purchased the lawful intercept option at the time of the illegal wiretaps, and the IMS phone-tapping management software was not installed on Vodafone's systems. But in early 2003, Vodafone technicians upgraded the Greek switches to release R9.1 of the AXE software suite. That upgrade included the RES software, according to a letter from Ericsson that accompanied the upgrade. So after the upgrade, the Vodafone system contained the software code necessary to intercept calls using the RES, even though it lacked the high-level user interface in the IMS normally used to facilitate such intercepts.

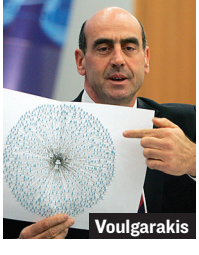
That odd circumstance would turn out to play a role in letting the Athens hackers illegally listen in on calls and yet escape detection for months and months.

IT TOOK GUILE and some serious programming chops to manipulate the lawful call-intercept functions in Vodafone's mobile switching centers. The intruders' task was particularly complicated because they needed to install and operate the wiretapping software on the exchanges without being detected by Vodafone or Ericsson system administrators. From time to time the intruders needed access to the rogue software to update the lists of monitored numbers and shadow phones. These activities had to be kept off all logs, while the software itself had to be invisible to the system administrators conducting routine maintenance activities. The intruders achieved all these objectives.

They took advantage of the fact that the AXE allows new software to be installed without rebooting the system, an important feature when any interruption would disconnect phone calls, lose text mes-







4 Mar Ericsson informs Vodafone of the existence of rogue software.

4 Mar Shadow phones make no further calls.

7 Mar Vodafone locates the rogue software.

8 Mar Vodafone extracts a list of logged phone numbers from MEAKS.

8 Mar Vodafone Greece CEO Giorgos Koronias orders removal of the rogue software.

Jul Vodafone, following its data retention policies, destroys the visitor sign-in books at one exchange facility.

Jul Vodafone upgrades two of the access servers, wiping out access logs.

31 Oct Vodafone places an order with Ericsson for LI software.

18 Nov Ericsson delivers LI software to Vodafone.

8 Mar The government security agency, ADAE, presents its first interim report on the case to the Parliament Committee on Institutions and Transparency.

23 Mar ADAE performs a simulation of the rogue software.

7 Apr ADAE publishes its second interim report on the case.

MAR MAY JUL SEP NOV JAN MAR MAY NOV

9 Mar Costas Tsalikidis, head of network planning of Vodafone Greece is found hanged in his apartment.

10 Mar Koronias briefs Giannis Angelou, director of the prime minister's political office.

10 Mar The Greek presidential decree specifying lawful interception procedures takes effect.

16 Mar Vodafone sends e-mail to Ericsson asking for the return of all exchange backup data.

2006

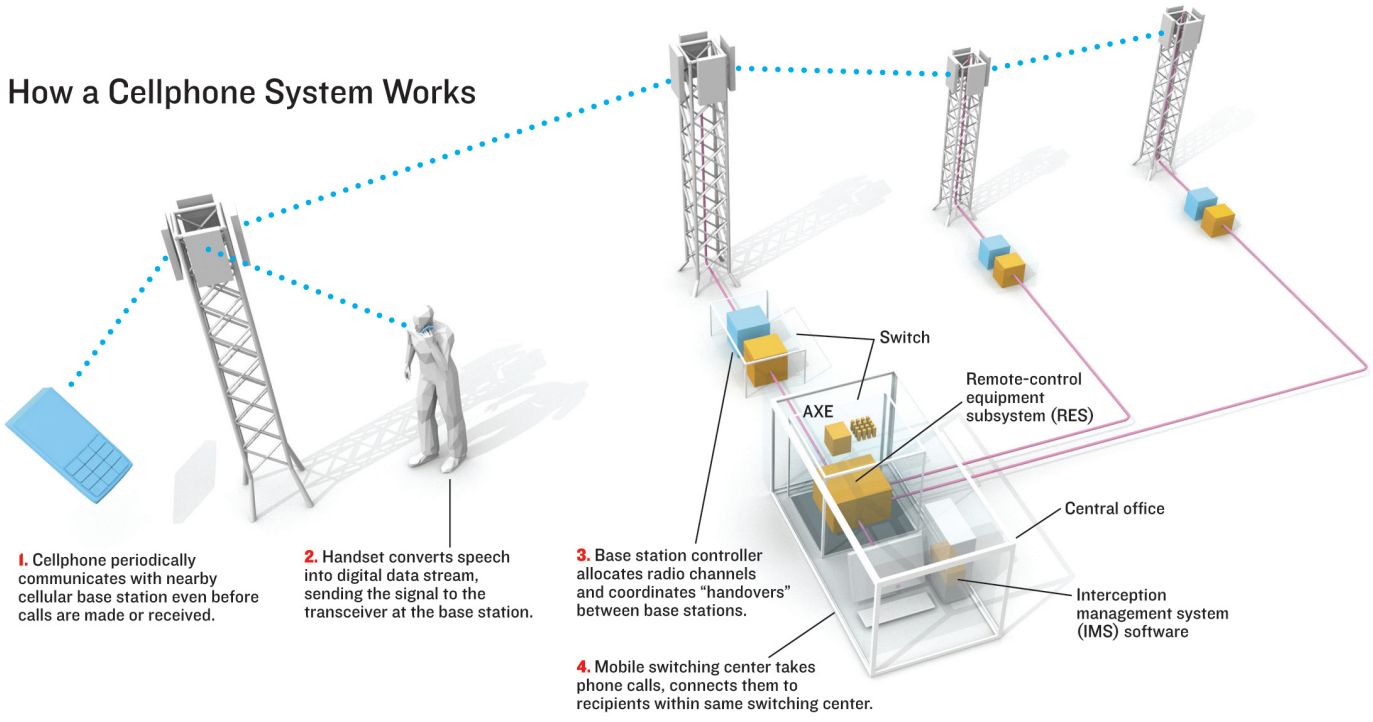
1 Feb Public prosecutor of the Supreme Court finishes the preliminary investigation.

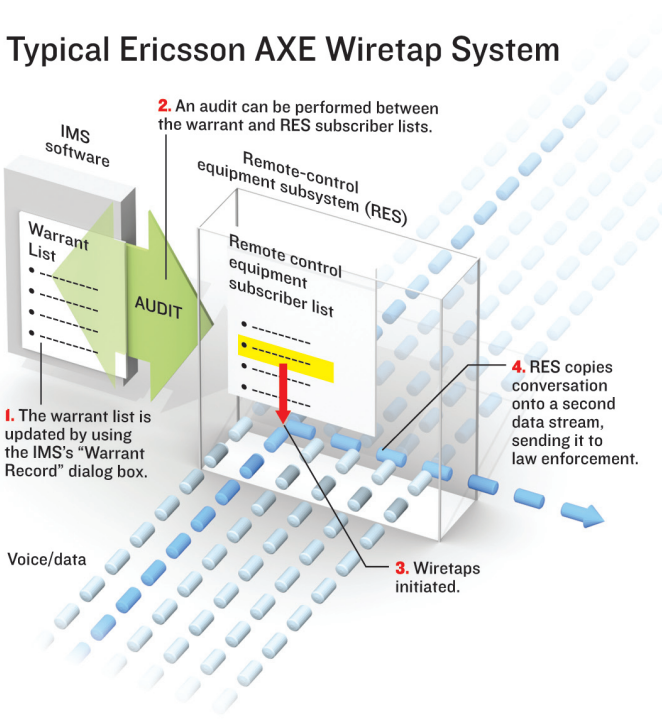
2 Feb The government provides details of the case in a press conference.

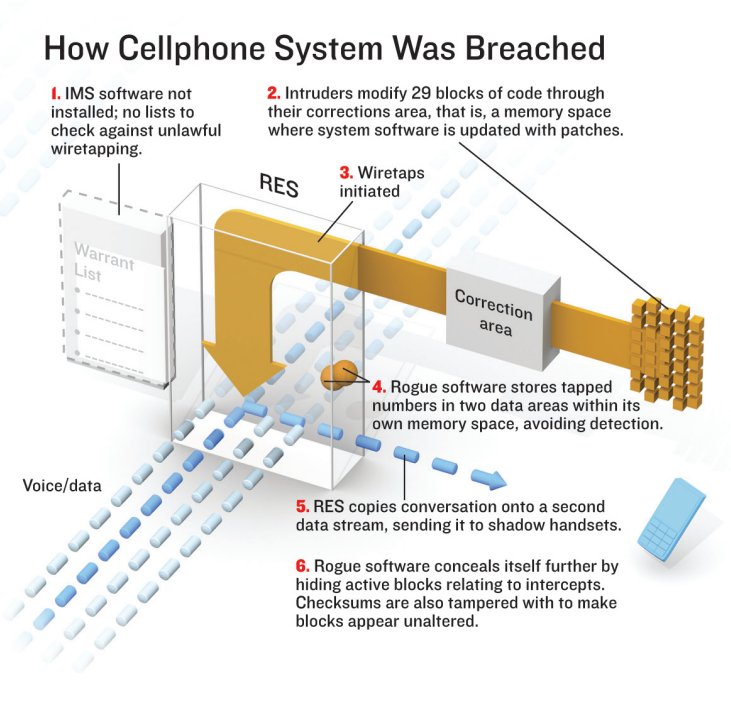
2 Feb Criminal prosecution for the violation of communications privacy and possibly spying is ordered.

14 Dec ADAE fines Vodafone €76 million (US $99.4 million).

CLOCKWISE FROM TOP LEFT: ERICSSON; KOSTAS TSIRONIS/AP PHOTO; MICHAEL BROWN/ISTOCKPHOTO; ADAE; VODAFONE; LOUISA GOULIAMAKI/AFP/GETTY IMAGES; AFP/GETTY IMAGES; ANDREY PROKHOROV/ISTOCKPHOTO







sages, and render emergency services unreachable. To let an AXE exchange run continuously for decades, as many of them do, Ericsson's software uses several techniques for handling failures and upgrading an exchange's software without suspending its operation. These techniques allow the direct patching of code loaded in the central processor, in effect altering the operating system on the fly.

Modern GSM systems, such as Vodafone's, secure the wireless links with a sophisticated encryption mechanism. A call to another cellphone will be re-encrypted between the remote cellphone and its closest base station, but it is not protected while it transits the provider's core network. For this reason—and for the ease of monitoring calls from the comfort of their lair—the perpetrators of the Vodafone wiretaps attacked the core switches of the Vodafone network. Encrypting communications from the start of the chain to its end—as banks, for example, do—makes it very difficult to implement legal wiretaps.

To simplify software maintenance, the AXE has detailed rules for directly patching software running on its central processor. The AXE's existing code is structured around independent blocks, or program modules, which are stored in the central processor's memory. The release being used in 2004 consisted of about 1760 blocks. Each contains a small "correction area," used whenever software is updated with a patch.

Let's say you're patching in code to force the computer to do a new function, Z, in situations where it has been doing a different function, Y. So, for example, where the original software had an instruction, "If X, then do Y" the patched software says, in effect, "If X, then go to the correction area

BRYAN CHRISTIE DESIGN

location L." The software goes to location L and executes the instructions it finds there, that is, Z. In other words, a software patch works by replacing an instruction at the area of the code to be fixed with an instruction that diverts the program to a memory location in the correction area containing the new version of the code.

The challenge faced by the intruders was to use the RES's capabilities to duplicate and divert the bits of a call stream without using the dialog-box interface to the IMS, which would create auditable logs of their activities. The intruders pulled this off by installing a series of patches to 29 separate blocks of code, according to Ericsson officials who testified before the Greek parliamentary committee that investigated the wiretaps. This rogue software modified the central processor's software to directly initiate a wiretap, using the RES's capabilities. Best of all, for them, the taps were not visible to the operators, because the IMS and its user interface weren't used.

THE ROGUE SOFTWARE STORED BUGGED PHONE NUMBERS IN ITS OWN MEMORY SPACE

The full version of the software would have recorded the phone numbers being tapped in an official registry within the exchange. And, as we noted, an audit could then find a discrepancy between the numbers monitored by the exchange and the warrants active in the IMS. But the rogue software bypassed the IMS. Instead, it cleverly stored the bugged numbers in two data areas that were part of the rogue software's own memory space, which was within the switch's memory but isolated and not made known to the rest of the switch.

That by itself put the rogue software a long way toward escaping detection. But the perpetrators hid their own tracks in a number of other ways as well. There were a variety of circumstances by which Vodafone technicians could have discovered the alterations to the AXE's software blocks. For example, they could have taken a listing of all the blocks, which would show all the active processes running within the AXE—similar to the task manager output in Microsoft Windows or the process status (ps) output in Unix. They then would have seen that some processes were active, though they shouldn't have been. But the rogue software apparently modified the commands that list the active blocks in a way that omitted certain blocks—the ones that related to intercepts—from any such listing.

In addition, the rogue software might have been discovered during a software upgrade or even when Vodafone technicians installed a minor patch. It is standard practice in the telecommunications industry for technicians to verify the existing block contents before performing an upgrade or patch. We don't know why the rogue software was not detected in this way, but we suspect that the software also modified the operation of the command used to print the checksums—codes that create a kind of signature against which the integrity of the existing blocks can be validated. One way or another, the blocks appeared unaltered to the operators.

Finally, the software included a back door to allow the perpetrators to control it in the future. This, too, was cleverly constructed to avoid detection. A report by the Hellenic Authority for the Information and Communication Security and Privacy (the Greek abbreviation is ADAE) indicates that the rogue software modified the exchange's command parser—a routine that accepts commands from a person with system administrator status—so that innocuous commands followed by six spaces would deactivate the exchange's transaction log and the alarm associated with its deactivation, and allow the execution of commands associated with the lawful interception subsystem. In effect, it was a signal to allow operations associated with the wiretaps but leave no trace of them. It also added a new user name and password to the system, which could be used to obtain access to the exchange.

Software that not only alters operating system code but also hides its tracks is called a "rootkit." The term is known to the public—if at all—because of one that the record label Sony BMG Music Entertainment included on some music CDs released in 2005. The Sony rootkit restricted copying of CDs; it burrowed into the Windows operating system on PCs and then hid its existence from the owner. (Sony stopped using rootkits because of a general public outcry.) Security experts have also discovered other rootkits for general-purpose operating systems, such as Linux, Windows, and Solaris, but to our knowledge this is the first time a rootkit has been observed on a special-purpose system, in this case an Ericsson telephone switch.

WITH ALL OF THIS SOPHISTICATED subterfuge, how then was the rogue software finally discovered? On 24 January 2005, the perpetrators updated their planted software. That upgrade interfered with the forwarding of text messages, which went undelivered. These undelivered text messages, in turn, triggered an automated failure report.

At this point, the hackers' abilities to keep their modifications to the switch's AXE software suite secret met their limits, as it's almost impossible to hide secrets in somebody else's system.

The AXE, like most large software systems, logs all manner of network activity. System administrators can review the log files, and any events they can't account for as ordinary usage can be investigated.

It's impossible to overstate the importance of logging. For example, in the 1986 Cuckoo's Egg intrusion, the wily network administrator, Clifford Stoll, was asked to investigate a 75 U.S. cents accounting error. Stoll spent 10 months looking for the hacker, who had penetrated deep into the networks of Lawrence Livermore National Laboratory, a U.S. nuclear weapons lab in California. Much of that time he spent poring over thousands of log report pages.

The AXE, like most sophisticated systems nowadays, can help operators find the nuggets of useful information within the voluminous logs it generates. It is programmed to report anomalous activity on its own, in the form of error or failure reports. In addition, at regular intervals the switching center generates a snapshot of itself—a copy, or dump, of all its programs and data.

Dumps are most commonly consulted for recovery and diagnostic purposes, but they can be used in security investigations. So when Ericsson's investigators were called in because of the undelivered text messages, the first thing they did was look closely at the periodic dumps. They found two areas containing all the phone numbers being monitored and retrieved a list of them.

The investigators examined the dumps more thoroughly and found the rogue programs. What they found though, was in the form of executable code—in other words, code in the binary language that microprocessors directly execute. Executable code is what results when a software compiler turns source code—in the case of the AXE, programs written in the PLEX language—into the binary machine code that a computer processor executes. So the investigators painstakingly reconstructed an approximation of the original PLEX source files that the intruders developed. It turned out to be the equivalent of about 6500 lines of code, a surprisingly substantial piece of software.

AN INSIDE JOB?

By Steven Cherry & Harry Goldstein

No mystery novel is complete without the reader finding out "who done it," but real life is usually messier than fiction. In the Athens affair, we can only speculate about who may have been behind the most spectacular cell-system penetration ever.

The hackers' facility with the esoteric art of programming the Ericsson AXE central-office switch convinced some that the criminals were either employees of Vodafone Greece or of Intracom Telecom.

Intracom has aroused suspicion because it provided key software to Ericsson and because the Greek company is a major telecommunications equipment supplier to Greece's dominant carrier, OTE Group. Given that the majority of OTE's shares are owned by the Greek state, a business having large dealings with OTE would have had a strong incentive to tap the phones of the ruling party in order to check on whether any of the deals it or OTE had set up under the previous government were in danger of being derailed. Under this theory, phone taps for Arabs and members of antiauthoritarian groups were installed to send investigators on a wild goose chase.

But what really raised eyebrows was the fact that one of the hacked Vodafone exchanges was located on the campus of the main Intracom facility. Anyone wishing to enter that particular Vodafone facility would have had to go through the Intracom gates, meaning that visitors to the Vodafone exchange would have been logged twice. Unfortunately, the visitor records for the exchange were destroyed by Vodafone in accord with routine procedures, despite the extraordinary circumstances. So investigators had only the Intracom visitor records, which would not record any visits to the Vodafone exchange by Intracom personnel.

The leading cause for suspecting the employees of Vodafone Greece is the suicide of its head of network planning, Costas Tsalikidis. Yet the deceased's family questions whether it was a suicide at all. The family's attorney, Themistokles Sofos, has stated, "I am certain that Costas Tsalikidis did not commit suicide, and that makes me believe he probably gained knowledge of the phone tapping through his diligence with all matters professional." Thus, speculation is divided between theories that say Tsalikidis committed suicide because his involvement was about to be discovered and those that argue that Tsalikidis was murdered because he had discovered, or was about to discover, who the perpetrators were.

Another popular theory posits that the U.S. National Security Agency, Central Intelligence Agency, or some other U.S. spy agency did it. The location of the monitored phones correlates nicely with apartments and other property under the control of the U.S. Embassy in Athens.

Under this theory, phone taps of Arabs and members of antiauthoritarian groups were installed because of fears of a terrorist attack on the Athens Olympics. It is widely believed that these U.S. agencies, particularly the NSA, have all the necessary tools and expertise for mounting such an attack. ■

The investigators ran the modules in simulated environments to better understand their behavior. The result of all this investigative effort was the discovery of the data areas holding the tapped numbers and the time stamps of recent intercepts.

With this information on hand, the investigators could go back and look at earlier dumps to establish the time interval during which the wiretaps were in effect and to get the full list of intercepted numbers and call data for the tapped conversations—who called whom, when, and for how long. (The actual conversations were not stored in the logs.)

While the hack was complex, the taps themselves were straightforward. When the prime minister, for example, initiated or received a call on his cellphone, the exchange would establish the same kind of connection used in a lawful wiretap—a connection to a shadow number allowing it to listen in on the conversation.

Creating the rogue software so that it would remain undetected required a lot of expertise in writing AXE code, an esoteric competency that isn't readily available in most places. But as it happens, for the past 15 years, a considerable part of Ericsson's software development for the AXE has been done under contract by a Greek company based in Athens, Intracom Telecom, part of Intracom Holdings. The necessary know-how was available locally and was spread over a large number of present and past Intracom developers. So could this have been an inside job?

The early stages of the infiltration would have been much easier to pull off with the assistance of someone inside Vodafone, but there is no conclusive evidence to support that scenario. The infiltration could have been carried out remotely and, indeed, according to a state report, in the case of the failed text messages where the exact time of the event is known, the last person to access the exchange had been issued a visitor's badge.

Similarly, we may never know whether Tsalikidis had anything to do with the wiretaps. Many observers have found the timing of his death highly suggestive, but to this day no connection has been uncovered. Nor can observers do more than speculate as to the motives of the infiltrators. [See the sidebar, "An Inside Job?" for a summary of the leading speculation; we can neither endorse nor refute the theories presented.]

Just as we cannot now know for certain who was behind the Athens affair or what their motives were, we can only speculate about various approaches that the intruders may have followed to carry out their attack. That's because key material has been lost or was never collected. For instance, in July 2005, while the investigation was taking place, Vodafone upgraded two of the three servers used for accessing the exchange management system. This upgrade wiped out the access logs and, contrary to company policy, no backups were retained. Some time later a six-month retention period for visitor sign-in books lapsed, and Vodafone destroyed the books corresponding to the period where the rogue software was modified, triggering the text-message errors.

Traces of the rogue software installation might have been recorded on the exchange's transaction logs. However, due to a paucity of storage space in the exchange's management systems, the logs were retained for only five days, because Vodafone considers billing data, which competes for the same space, a lot more important. Most crucially, Vodafone's deactivation of the rogue software on 7 March 2005 almost certainly alerted the conspirators, giving them a chance to switch off the shadow phones. As a result investigators missed the opportunity of triangulating the location of the shadow phones and catching the perpetrators in the act.

SO WHAT CAN THIS AFFAIR teach us about how to protect phone networks?

Once the infiltration was discovered, Vodafone had to balance the need for the continued operation of the network with the discovery and prosecution of the guilty parties. Unfortunately, the responses of Vodafone and that of Greek

law enforcement were both inadequate. Through Vodafone's actions, critical data were lost or destroyed, while the perpetrators not only received a warning that their scheme had been discovered but also had sufficient time to disappear.

In the telecommunications industry, prevailing best practices require that the operator's policies include procedures for responding to an infiltration, such as a virus attack: retain all data, isolate the part of the system that's been broken into as much as possible, coordinate activities with law enforcement.

Greek federal telecom regulations also specify that operators have security policies that detail the measures they will take to ensure the confidentiality of customer communications and the privacy of network users. However, Vodafone's response indicates that such policies, if they existed, were ignored. If not for press conferences and public investigations, law enforcement could have watched the behavior of the shadow cellphones surreptitiously. Physical logbooks of visitors were lost and data logs were destroyed. In addition, neither law enforcement authorities nor the ADAE, the independent security and privacy authority, was contacted directly. Instead, Vodafone Greece communicated through a political channel—the prime minister's office. It should be noted the ADAE was a fairly new organization at the time, formed in 2003.

PHYSICAL LOGBOOKS OF VISITORS WERE LOST AND DATA LOGS WERE DESTROYED

The response of Greek law enforcement officials also left a lot to be desired. Police could have secured evidence by impounding all of Vodafone's telecommunications and computer equipment involved in the incident. Instead it appears that concerns about disruption to the operation of the mobile telephone network led the authorities to take a more light-handed approach—essentially interviewing employees and collecting information provided by Vodafone—that ultimately led to the loss of forensic evidence. They eventually started leveling accusations at both the operator (Vodafone) and the vendor (Ericsson), turning the victims into defendants and losing their good will, which further hampered their investigation.

Of course, in countries where such high-tech crimes are rare, it is unreasonable to expect to find a crack team of investigators. Could a rapid deployment force be set up to handle such high-profile and highly technical incidents? We'd like to see the international police organization Interpol create a cyberforensics response team that countries could call on to handle such incidents.

Telephone exchanges have evolved over the decades into software-based systems, and therefore the task of analyzing them for vulnerabilities has become very difficult. Even as new software features, such as conferencing, number portability, and caller identification, have been loaded onto the exchanges, the old software remains in place. Complex interactions between subsystems and baroque coding styles (some of them remnants of programs written 20 or 30 years ago) confound developers and auditors alike.

Yet an effective defense against viruses, worms, and rootkits depends crucially on in-depth analysis that can penetrate source code in all its baroque heterogeneity. For example, a statistical analysis of the call logs might have revealed a correlation between the calls to the shadow numbers and calls to the monitored numbers. Telephone companies already carry out extensive analysis on these sorts of data to spot customer trends. But from the security perspective, this analysis is done for the wrong reasons and by the wrong people—marketing as opposed to security. By training security personnel to use these tools and allowing them access to these data, customer trend analysis can become an effective countermeasure against rogue software.

Additional clues could be uncovered by merging call records generated by the exchange with billing and accounting information. Doing so, though, involves consolidating distinct data sets currently owned by different entities within the telecom organization.

Another defense is regular auditing of the type that allowed Ericsson to discover the rogue software by scrutinizing the offline dumps. However, in this case, as well as in the data analysis case, we have to be sure that any rogue software cannot modify the information stored in the logs or the dumps, such as by using a separate monitoring computer running its own software.

Digital systems generate enormous volumes of information. Ericsson and Vodafone Greece had at their fingertips all the information they needed to discover the penetration of Vodafone's network long before an undelivered text message sent them looking. As in other industries, the challenge now is to come up with ways to use this information. If one company's technicians and one country's police force cannot meet this challenge, a response team that can needs to be created.

It is particularly important not to turn the investigation into a witch hunt. Especially in cases where the perpetrators are unlikely to be identified, it is often politically expedient to use the telecom operator as a convenient scapegoat. This only encourages operators and their employees to brush incidents under the carpet, and turns them into adversaries of law enforcement. Rather than looking for someone to blame (and punish), it is far better to determine exactly what went wrong and how it can be fixed, not only for that particular operator, but for the industry as a whole.

Merely saying—or even legislating—that system vendors and network operators should not allow something like this to occur is pointless, because there is little that can be done to these companies after the fact. Instead, proactive measures should be taken to ensure that such systems are developed and operated safely. Perhaps we can borrow a few pages from aviation safety, where both aircraft manufacturers and airline companies are closely monitored by national and international agencies to ensure the safety of airline passengers. ■

ABOUT THE AUTHORS

VASSILIS PREVELAKIS, an IEEE member, is an assistant professor of computer science at Drexel University, in Philadelphia. His current research is on automation network security and secure software design. He has published widely in these areas and is actively involved in standards bodies such as the Internet Engineering Task Force.

DIOMIDIS SPINELLIS, an IEEE member, is an associate professor in the department of management science and technology at the Athens University of Economics and Business and the author of *Code Quality: The Open Source Perspective* (Addison-Wesley, 2006). He blogs at http://www.spinellis.gr/blog.

TO PROBE FURTHER

The Wikipedia article http://en.wikipedia.org/wiki/Greek_telephone_tapping_case_2004-2005 contains additional links to press stories and background material.

Ericsson's Interception Management System user manual (marked confidential) is available on the Web through a Google search: http://www.google.com/search?q=IMS+ericsson+manual or at http://cryptome.org/ericsson-ims.htm.