



The Greek Wiretaps

Vassilis Prevelakis

Technische Universität Braunschweig

Diomidis Spinellis

Athens University of Economics and Business



A bad day in March

- March 4, 2005: Vodafone - Greece realize that their network had been infiltrated.
 - Foreign code had been installed in exchanges.
 - Cellphones of Vodafone's customers were being bugged.
 - High level persons including the Greek PM were victims.



Overview of talk

- Introduction of the cast and timeline
- Analysis of incident
 - Background
 - Rogue Software
 - Discovery - Response
- Discussion



Major Actors

- Vodafone - Greece
 - One of three mobile operators in Greece.
- Ericsson
 - Supplies AXE exchanges for two Greek mobile nets.
- Intracom
 - Contracted by Ericsson to develop s/w for AXE.
- ADAE
 - Independent authority for information and telecommunication privacy and security.



Timeline 1

- 2003: ADAE established.
- March 2004: General Elections
 - conservatives win the elections replacing the then governing socialists
- June 2004: Illegal activities commence
- Aug. 2004: Athens Olympics
- Jan. 2005: SMS-related errors are logged
 - Vodafone asks Ericsson to investigate the errors
 - ADAE publishes “secrecy assurance regulations” for telecom companies operating in Greece.



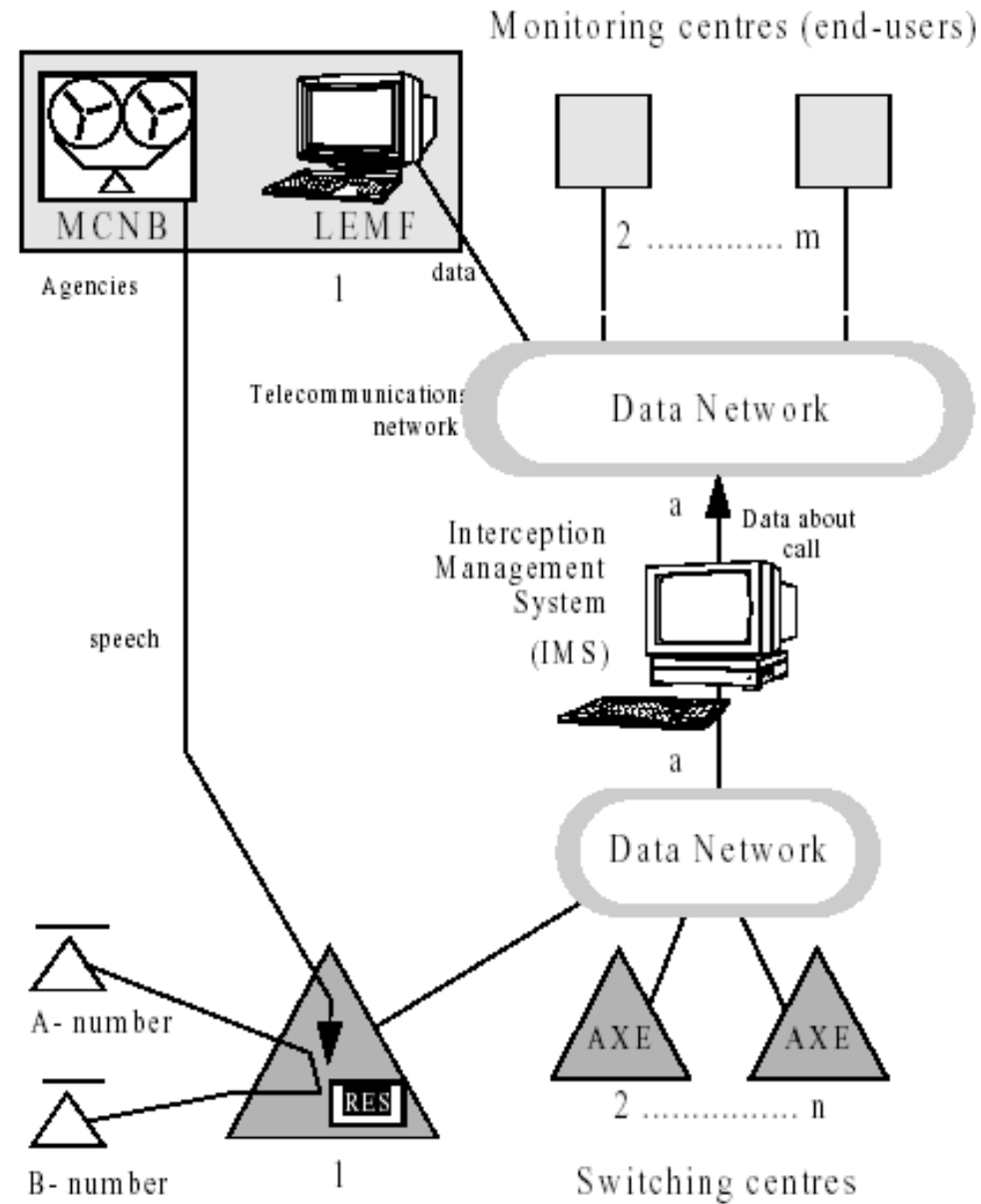
Timeline 2

- Mar. 2005: Ericsson notifies Vodafone of the rogue software
 - shadow phones stop making calls
 - Vodafone removes rogue software
 - Greek PM notified - investigation begins
- Feb. 2006: Investigation is concluded
 - Greek Government releases details
- March 2006: ADAE presents confidential report
- June 2006: Vodafone fined 76 million Euros.



Analysis of Incident

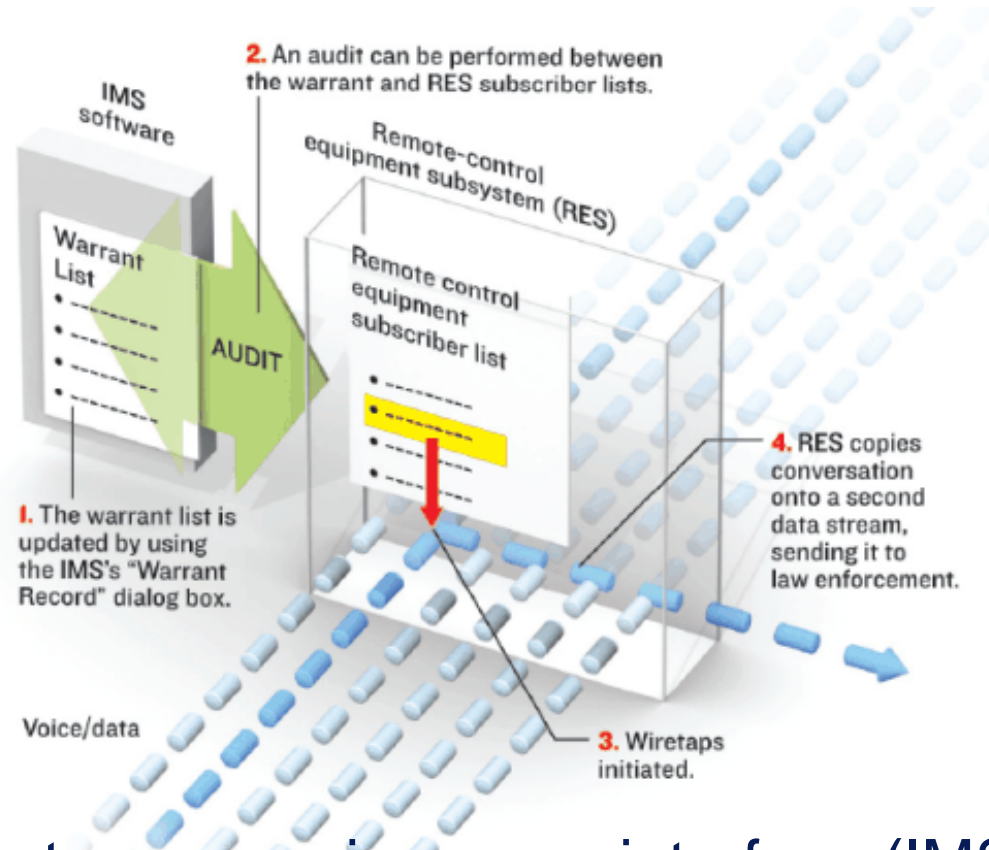
- Background
 - AXE Lawful wiretaps
 - Ericsson Software Update Mechanism
- Rogue Software
 - Installation - Operation
 - Main Features
- Discovery
 - Innocuous error causes Ericsson to investigate
 - Incident Response



AXE Telecommunications Interception Model 8



Intercepting a Call



LI system comprises user interface (IMS) and Remote-control Equipment Subsystem (RES)

Analysis->Background



AXE Updates

Information word	Block number
Software unit identification	SUID
Signal distribution table	Entry address for signal M
	⋮
	Entry address for signal 1
Signal distribution table	Instruction set version
	Destination for signal 1
	⋮
Patch	Destination for signal N
	Program code
	⋮
New code	JMP correction area address
	⋮
	Correction area
	⋮
	Alternative instructions

- code was patched in place
- updates applied on live-systems
- changed modules identified via
 - metadata
 - checksums

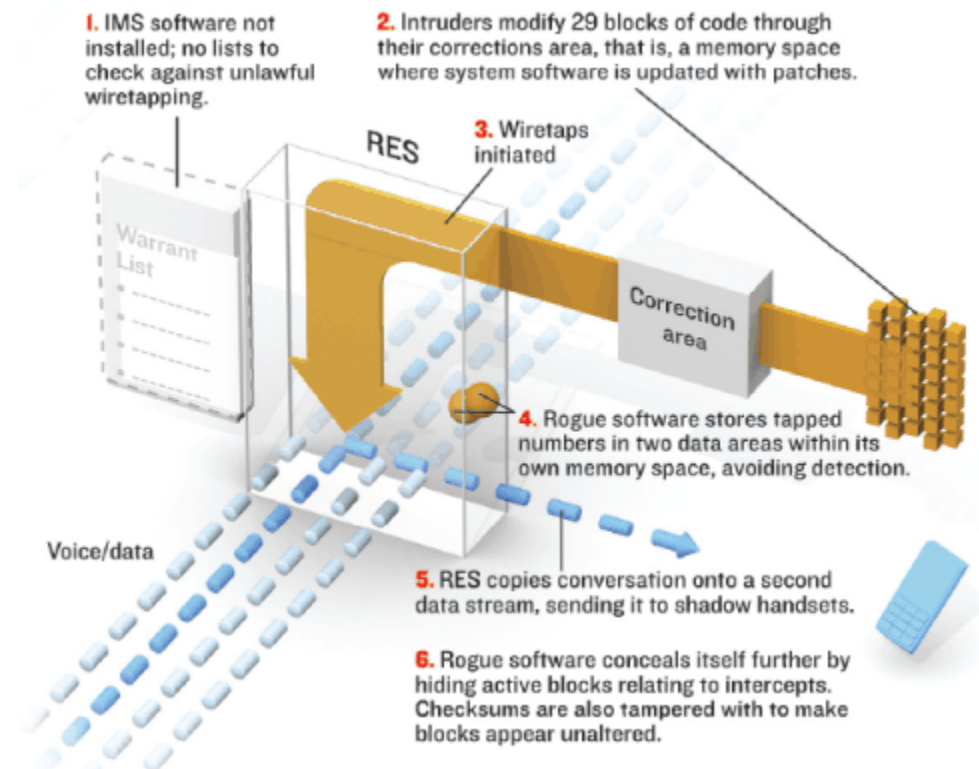


Analysis of Incident

- Background
 - AXE Lawful wiretaps
 - Ericsson Software Update Mechanism
- Rogue Software
 - Installation - Operation
 - Main Features
- Discovery
 - Innocuous error causes Ericsson to investigate
 - Incident Response



Operation of Rogue SW



- Rogue software allowed intercepts to be carried out without any formal record.

Analysis->SW



Rogue SW: Features

- Activated LI functionality already present in exchanges
- Concealed its presence
 - module list command
 - checksums
- Added new account
- Allowed logged-on user to suspend logging
 - six spaces at the end of command
- Used SMS to report traffic - location info of tapped numbers



Analysis of Incident

- Background
 - AXE Lawful wiretaps
 - Ericsson Software Update Mechanism
- Rogue Software
 - Installation - Operation
 - Main Features
- Discovery
 - Innocuous error causes Ericsson to investigate
 - Incident Response



All good things ...

- Intruders attempted to install software on another exchange triggering a burst of error reports
 - this was probably due to differences in the configuration of last exchange with previous ones.
- Vodafone opened a ticket with Ericsson to investigate the errors.
- Ericsson notified Vodafone of the existence of unauthorized software.
 - Note that the same day Vodafone was notified, calls between shadow phones ceased.



Incident Response

Fear, Uncertainty and Doubt

- Vodafone
 - failed to follow proper (or even reasonable) procedures for notifying authorities after the intrusion was detected
 - destroyed evidence (visitor records and logical access logs)
- Greek Law enforcement
 - uncertainty over jurisdiction caused multiple investigations and contributed to loss of forensic evidence
- ADAE
 - fined Vodafone for failing to notify customers of tapped cell phones.



Incident Response

- Concerns about the continued operation of the network apparently prevailed over the collection of forensic evidence
- ADAE was new - still trying to establish itself
- Legal framework was also immature
 - was being developed as the wiretaps were taking place.



Discussion

- What can we learn about the Athens affair?
 - planning is necessary
 - debate about whether Vodafone should have disabled the software obscures fact that they did not have incident response procedures in place.
 - continued vigilance
 - don't shoot the messenger (or the victim)
- Can it happen again?
 - **front-line** services need explicit protection



Other things to consider

- End-to-end security in telephony
 - is it feasible?
 - do we want it?
- Is trust in the PSTN justified?
- What you don't know can't harm you (really!)
 - we need openness in order to assess risks
- Issue is not confined to utilities
 - more and more entities collect personal and private information without any clue on how to protect them (or themselves from litigation)



Questions?
