AEGIS
RESEARCH

Secure Telephony
An Oxymoron?

Vassilis Prevelakis

AEGIS RESEARCH

Athens, Greece

AEGIS
RESEARCH

Your Bank is on the phone

- Typical interaction with your bank
  - authentication protocol clearly broken
- Would you use the same protocol on the Internet?

- So you think you can trust the telephone system
  - or at least your bank does...

AEGIS
RESEARCH

Case Study
The Athens Wiretaps

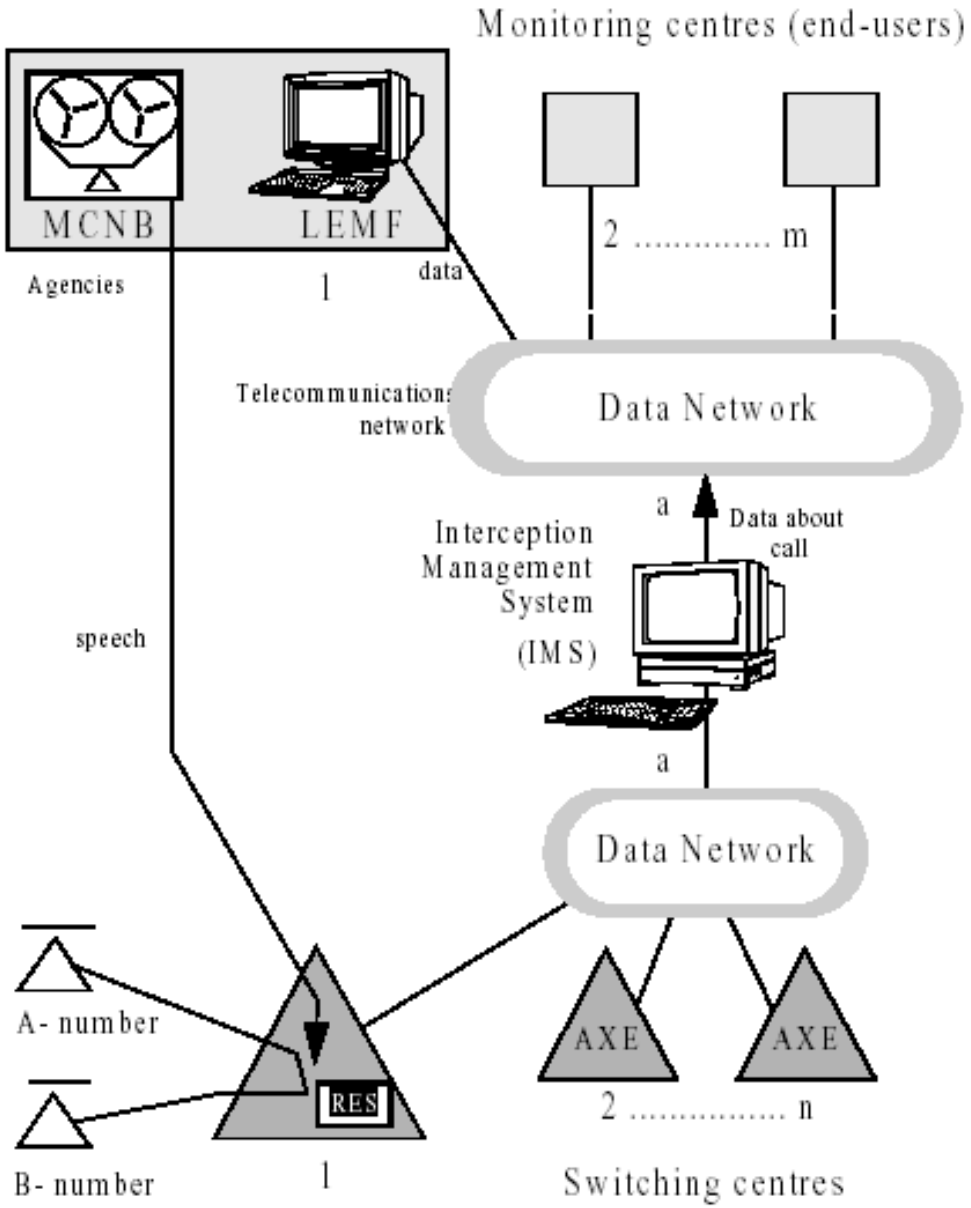
- March 4, 2005: Vodafone - Greece realize that their network had been infiltrated.
- Foreign code had been installed in exchanges.
- Cellphones of Vodafone - Greece customers were being bugged.
- High-level civil servants including the Greek PM were victims.

AEGIS
RESEARCH

Analysis of Incident

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

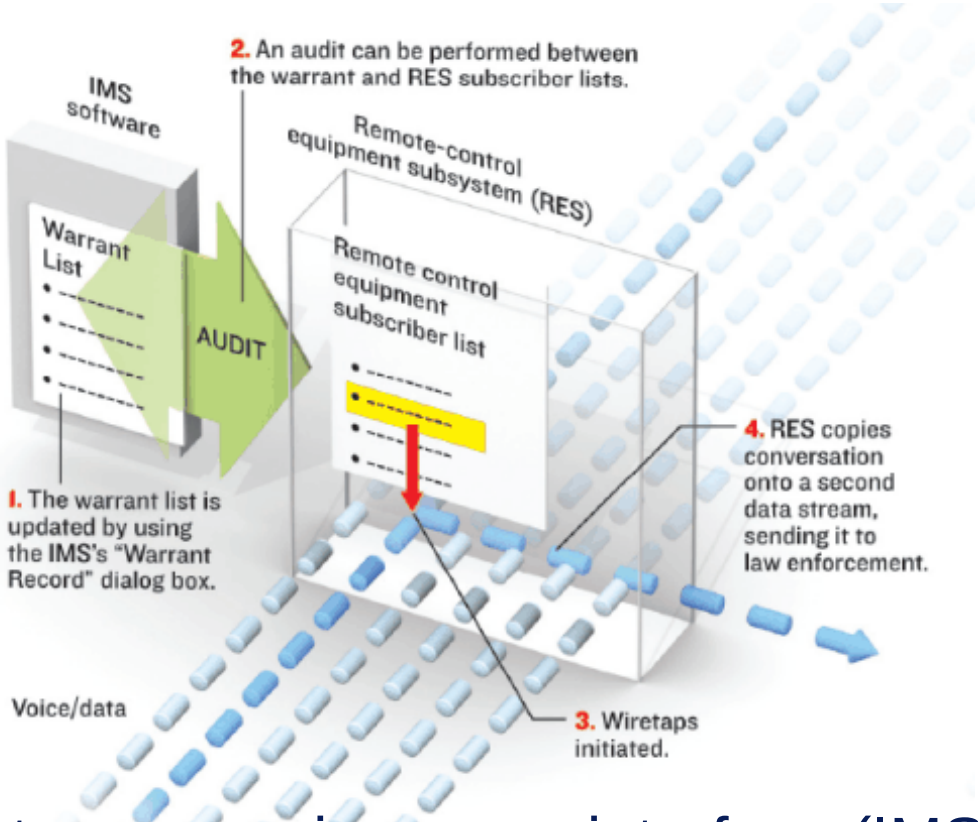
AEGIS
RESEARCH



AXE Telecommunications Interception Model

AEGIS
RESEARCH

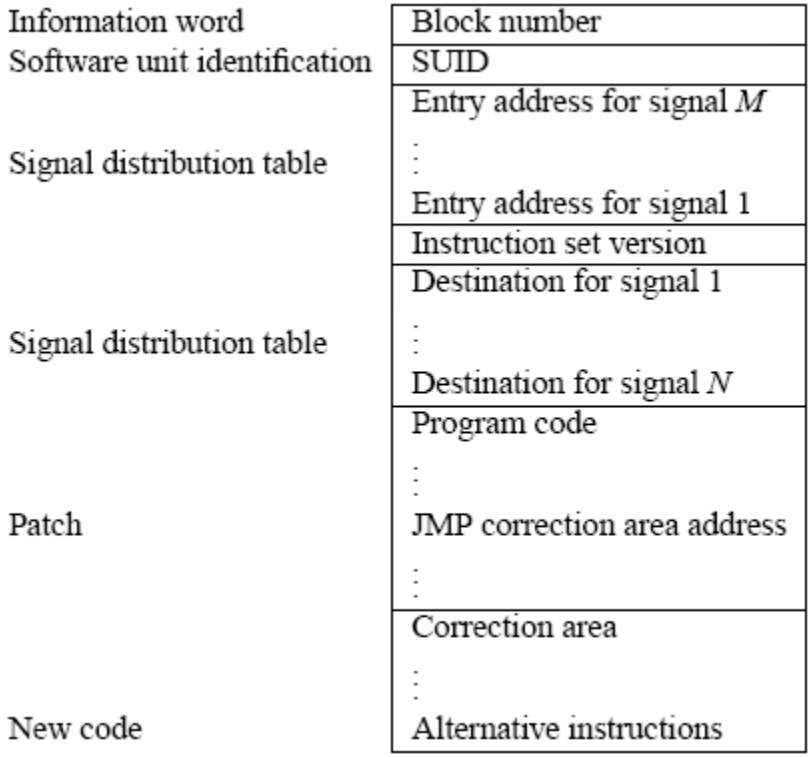
Intercepting a Call



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

AEGIS
RESEARCH

AXE Updates



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

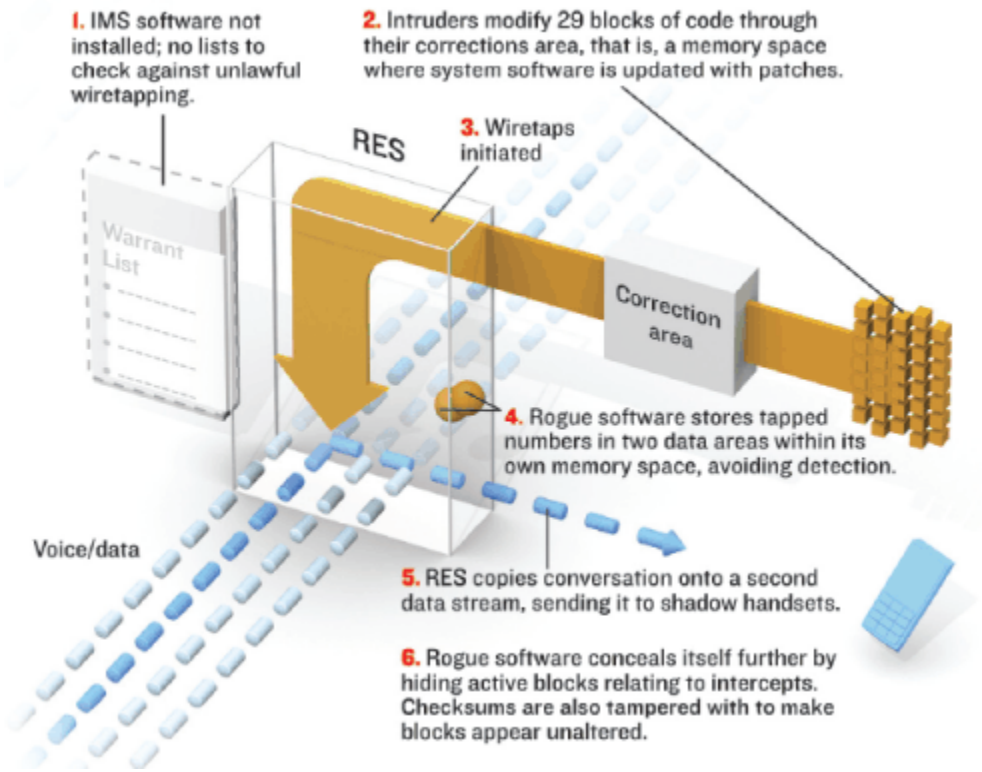
AEGIS
RESEARCH

Analysis of Incident

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

AEGIS
RESEARCH

Operation of Rogue SW



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

AEGIS
RESEARCH

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

AEGIS
RESEARCH

Analysis of Incident

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

AEGIS
RESEARCH

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.

AEGIS
RESEARCH

Observations

- Telephony offers little security
- Public assumes PSTN safer than Internet
  - organizations exploit this to avoid the expense of a more robust solution
    - e.g. whats wrong with using OTP instead of the litany of personal (and usu. irrevocable) information?
- Governments like the status quo
- This carries risks beyond the mere inconvenience of finding your bank account empty.

AEGIS
RESEARCH

Secure Telephony is not a perk

- Once power is granted, it can always be abused
  - e.g. The Prometheus Plan
- Building systems of control is not the same as building secure systems *(Bruce Schneier)*
- Wide scale wiretapping is not only feasible, but widely used.
  - legal limitations in democratic countries usually limit this to international communications

AEGIS
RESEARCH

On the other hand ...

- Governments loath to abandon their ability to monitor communications.
  - When technology made traditional wiretapping difficult, governments asked vendors of telephony systems to add features to enable wiretapping.
  - When the Internet provided a new communications path, again efforts were made to tap it as well.
- Powerful tool in the war against [your-pet-cause]
  - Sounds convincing, but the bad guys are not standing still.
- Requests for new powers must be balanced with the new risks that they create

AEGIS
RESEARCH

Is there any hope?

- It worked for the Internet, so why can't we do the same for secure telephony
- Two classes of security
  - Protect against content disclosure
  - Protect against traffic analysis
- Internet Solutions
  - End-to-end encryption via SSL/TLS (widely accepted)
  - Anonymising services (rather limited appeal)

AEGIS
RESEARCH

Why did the Internet get away with it?

- New technology which needed help to establish itself
  - esp. in the early stages, government-imposed legal restrictions, would have stymied growth
  - Similar pattern to early credit card legislation in the USA
- Public mistrust
  - security was necessary to overcome public concerns
- Profit!
  - lots of institutions wanted to use the Internet to make money
  - pushed for security

AEGIS
RESEARCH

Back to Secure Telephony

- The technology is there (esp. for content), but ...
- Reversing the current status is difficult:
  - no real public interest
  - manufacturers have few incentives to add features
  - governments create legal hurdles
  - no obvious way of making money out of secure telephony.

AEGIS
RESEARCH

Questions?