The Security of Telephone Networks

A case study of security engineering using
only a knock off latex theme

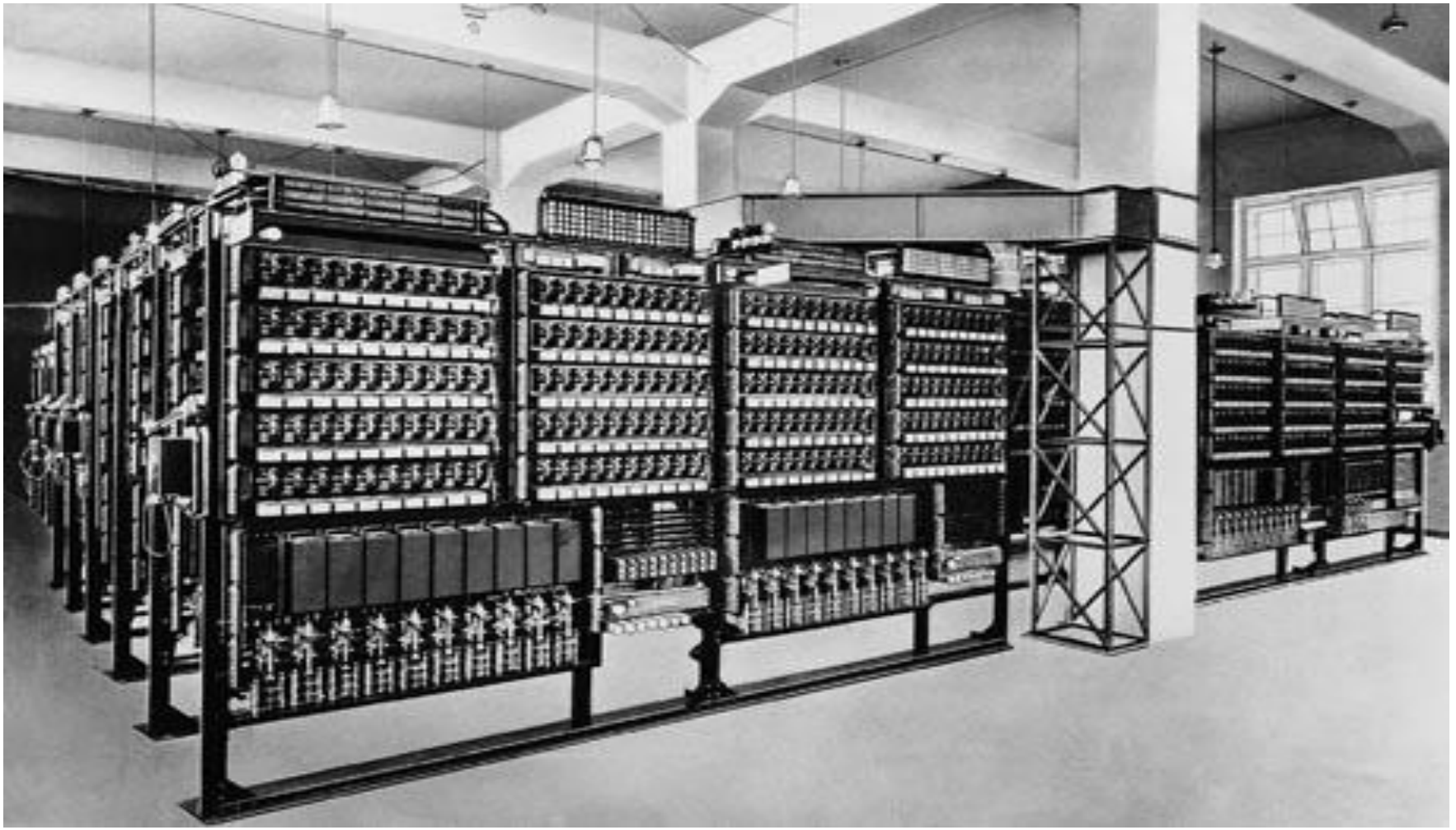
Human operated telephone network exploits

From the first days of telephones up until the 1960s telecoms used human operators to direct calls.

Social engineering attacks to avoid paying for calls.

Fake approval mechanisms on payphone lines to get free calls.

Automated Telephone Switches

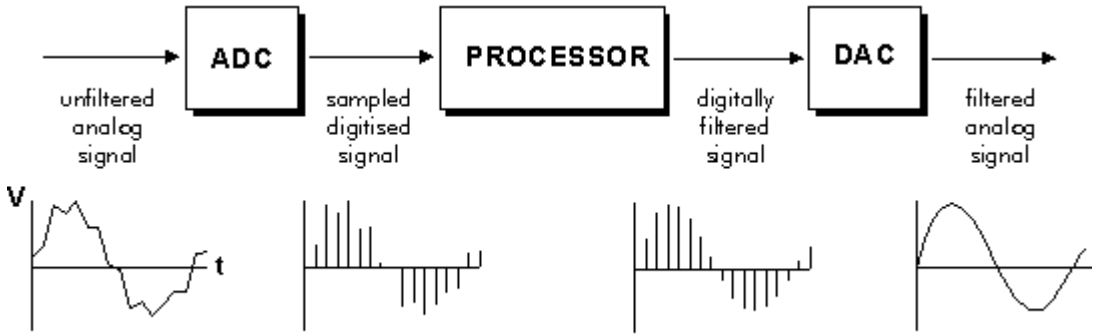


Early Signaling Exploits

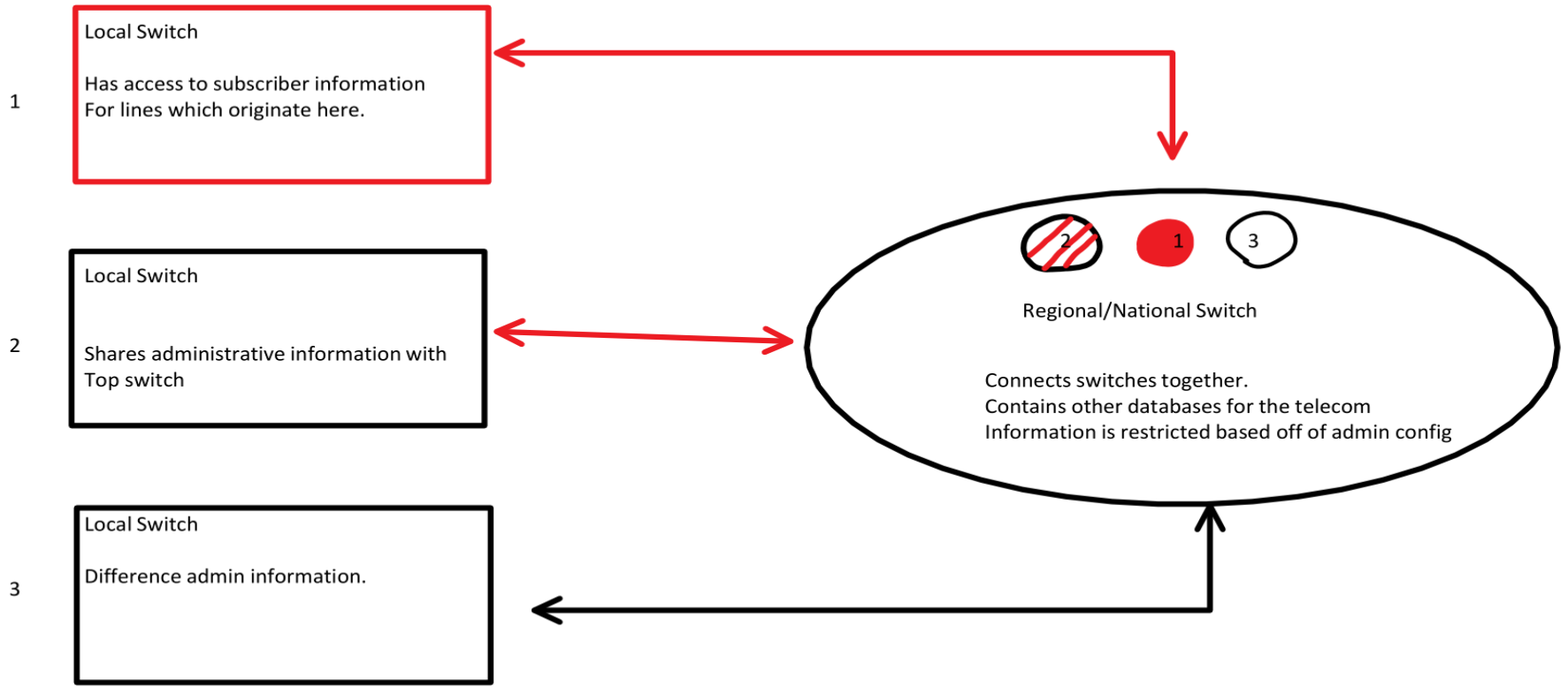
Telephone systems use *in-band signaling*. This means the line you speak on the line commands between nodes are sent on.

Early signals were just sustained frequencies over the line.

Later devices would have their signaling patterns reverse engineered.



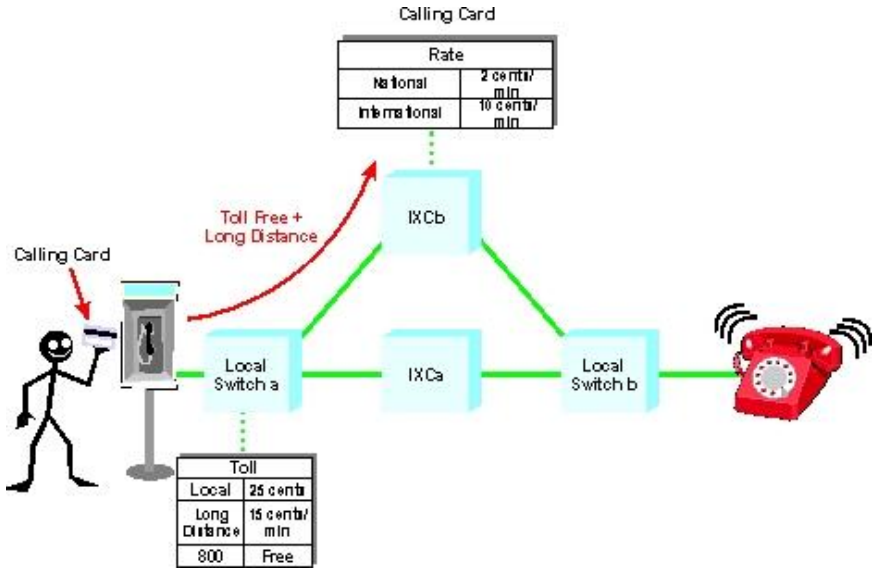
More complex telecom networks



More complex telecom systems (Early pivoting)

As telecoms became larger, more automated, and added features their systems became harder to secure and more valuable to exploit

Permissive security environment. No humans to notice bad requests.



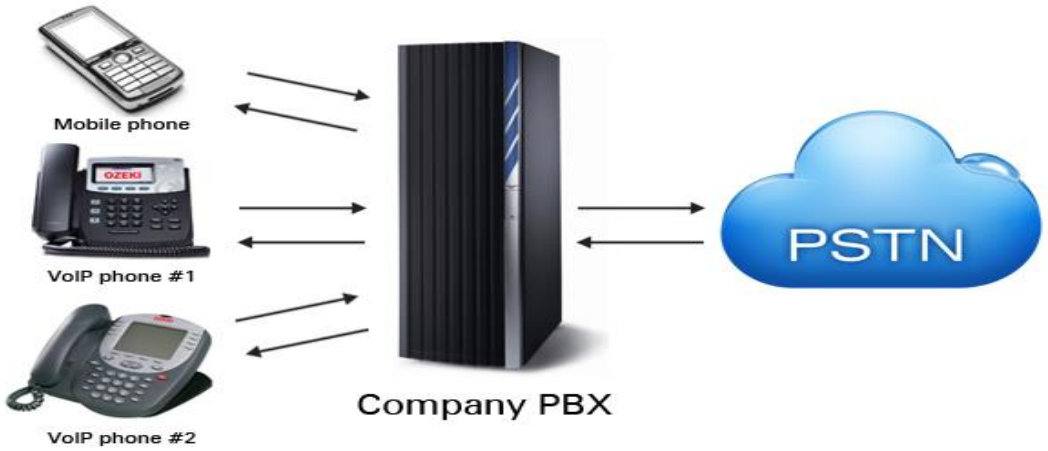
Attacks on other equipment.

Wishing to extend the capabilities of their phone lines businesses and consumers start connecting new devices to phone lines.

PBX hacks are the most notable.

Answering machines were used to organize illicit activities.

Premium rate fraud



Client Side Social Engineering

As telecoms became harder and harder to fool and exploit some people began targeting users.

Claim to be the phone company get personal info.

Get them to subscribe to premium call services.

Security of mobile networks

A case study of security in GSM networks

What problems are mobile networks trying to solve?

While it may seem obvious what mobile networks are trying to solve we should outline they have changed.

- Let anyone with a compatible unit utilize the network to perform some task.
- Prevent people without a subscription from using the network.
- Provide it in such a manner that the network can be operated in a cost effective manner, with reasonable capacity, and phones are of reasonable utility.

Implications of the third statement

Providing a 1 to 1 relation of mobile unit to access points is impossible

Users must share base stations. This is referred to multiple access

The network must be accessible by reasonable hardware

This means that constraints of mobile units we can make, people would like to buy, and can afford must be taken into account.

The network must provide the services which people wish to use

Networks must reconcile the needs of many different use cases in order to provide proper services.

Different schemes of multiple access

FDMA – 0G/1G Networks

FDMA stands for frequency division multiple access, it allowed for a single base station to service multiple phones

Mobile Telephone Service (1950s) – 25 Channels
Improved MTS (1964) – About 32 channels
AMPS (1983) – 416 Channels

Security issues within these networks

These were analog technologies and due to the restrictions of mobile units they provide almost no security.

Mobile cloning was a huge problem. Essentially a return of the fraud seen with the manual/automatic telephone networks.

No eavesdropping protection. Listening into someones conversation was as simple as tuning to the frequency they were talking on.

Systems were again susceptible to in-band signaling attacks for IMTS.

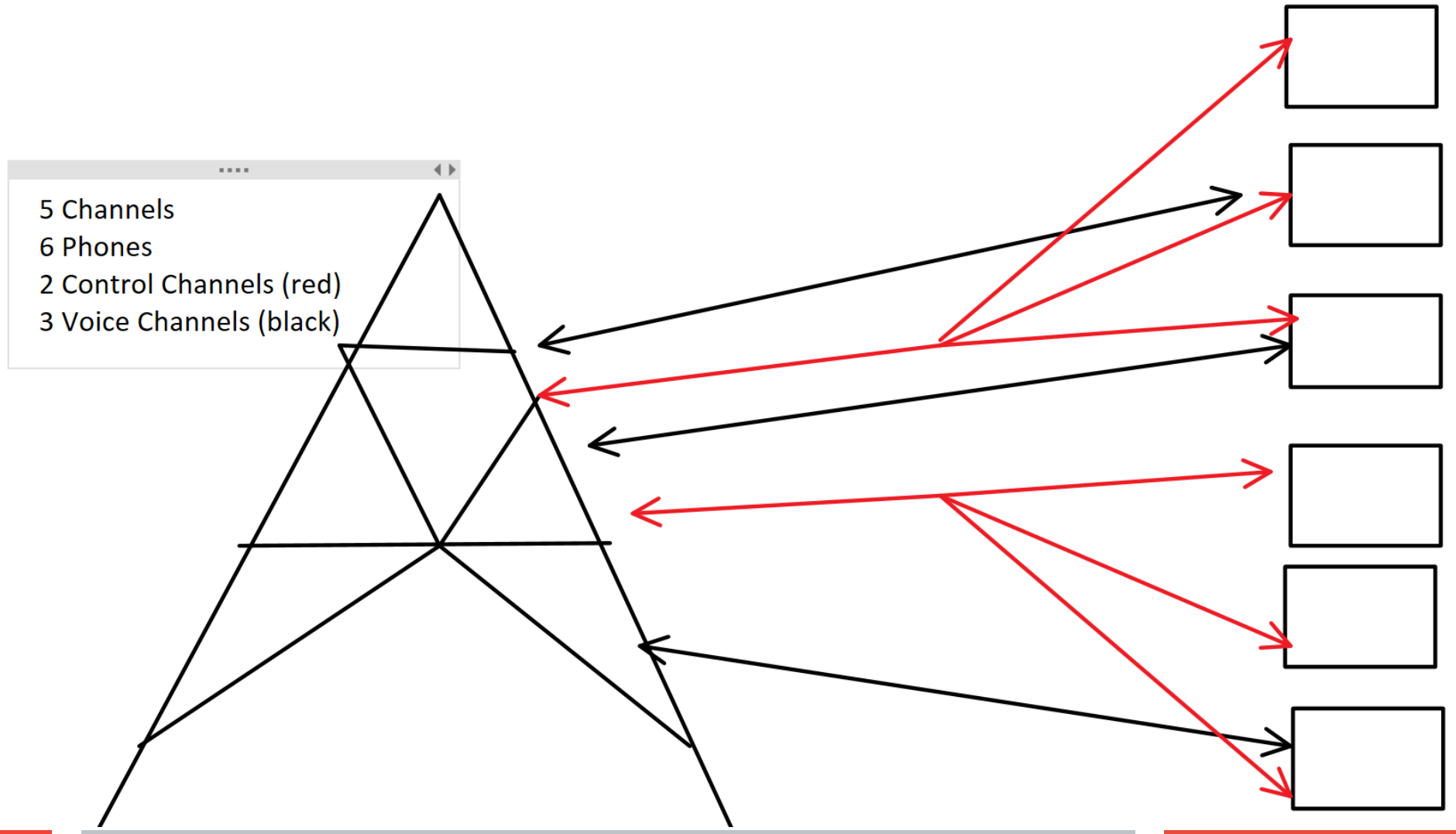
How did AMPS achieve such substainal channel gains?

Control channels, which are special channels used to send/receive commands and information with the mobile unit.

Mobile phones are ALWAYS listening on a control channel and a relatively large amount of information is being transferred within these channels at all times.

They are used to tell units which transmission channel to tune to transmit.

They are used to track which users are connected to which towers within the network.


5 Channels
6 Phones
2 Control Channels (red)
3 Voice Channels (black)

Early 2G Technologies

TDMA – Time division multiple access, divides a channel among devices by having them transmit at a different time over an interval.

CMDA - Code Division Multiple Access, divides a channel among devices by having them transmit a different coding over an interval.

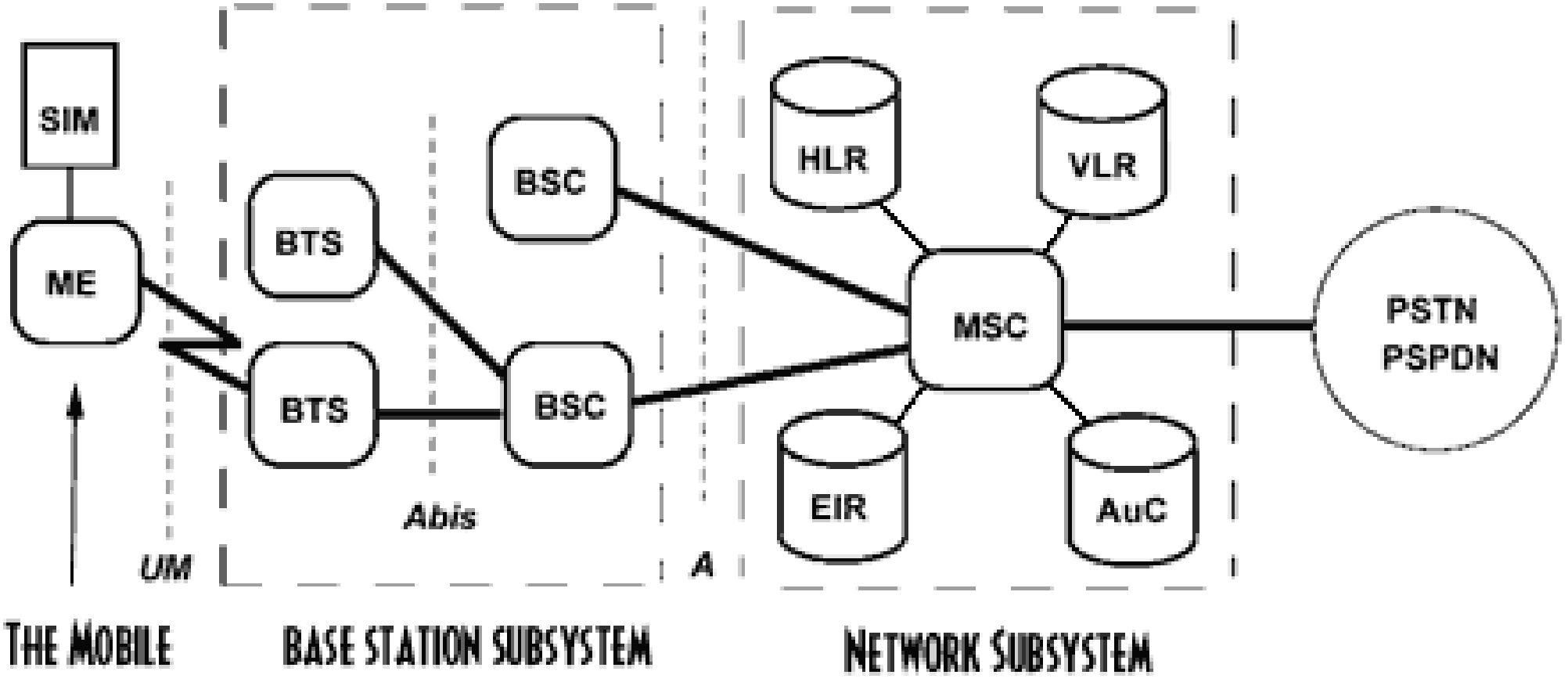
More channels.

Allowed for tower roaming.

Variable tower reach and signal amplification.

Networks were more flexible than their analog forerunners. New services.

2G is relatively complex



Security Concerns of Early 2G Technologies

SMS security (next slide)

Unsecured Control Channels

- Used to transmit call information, GSM service information, issue commands to and from the base station.
- Can be used to impersonate base stations with minimal help.

Algorithm security issues (Security Algorithms Beyond slide)

SMS Design Abstract

Goal: Allow mobile units to send strings and receive strings between each other.

- Should be quick.
- Should not negatively impact device performance when not in use.
- Should work consistently on any network's deployment of 2G infrastructure.
- Should be reasonably secure.

Design Choices in SMS Messages

- **In order to quickly send and receive messages the phone must either be constantly connected or ping the tower every X**
  - Pinging frequently enough to hold a conversation would drain battery life of the more primitive 2G phones
  - Choice made, the phone must be constantly and passively connected
- **What do we use to maintain this connection?**
  - Voice channels are expensive for the network and drastically impact mobile unit performance
  - Phones are already connected to control channels, lets just use those!
- **Too many control channels vs voice channels cause high infrastructure cost**
  - Make messages short enough that they fit in the controls channels!
- **Key negotiation is very expensive in terms of communication due to high packet loss**
  - Ok fine we will only negotiate keys between the two devices at the end of a given physical link
  - Phone to tower, tower to network, network to network, and the reverse.
- **This is the early 90s**
  - Available encryption algos are expensive for handhelds, so we roll our own.

Security implications of these choices

Roll your own algo is hard but GSM was made by a lot of people.

It's even harder when you have to make it for embedded devices.

- GSM ends up using some security by obscurity self-made algo. **CRACKED.**

- **Because critical voice related transmissions take place on control channels 2G-GSM base stations are potentially vulnerable to SMS based DOS attacks**
  - If you block the control line, you break the network.
  - They tried to account for this by basically making it about as easy to DOS with SMS as it would be with voice lines.
- **It's probably close to the best that could have been done in the 90s.**

Failures of 2G security algorithm design.

Security algos in 2G networks face the similar problems to SMS

- Security had to be light on processing power.
- Fit situational constraints.
- Could not really achieve robustness, tried to use false security.
- Enter: A3 (authentication), A5 (communication), A8 (key generation)

A5 Breaks:

- Revision 1: Rainbow table attacks.
  - There is also a general case of the A5/2 attack which works.
- Revision 2: Ciphertext-only attack yield keys.
  - Only requires a few milliseconds of communication and CPU time.
- Revision 3: General form of A5/2 attack.

Security Algorithms Beyond

We often think about security algorithms just being data encryption. In complex systems it is not that simple.

Breaking A3:

- SIM Cloning
  - Identity impersonation in cases where SIM is used as ID.
  - Send commands as a specific client.
- Open access to communication over control channels. (Help break A5):

Breaking A5:

- Open access to communication over voice channels
- With A3 allows someone to impersonate a base station or MU on the fly.

Fun note: This can be used to implement the SMS DOS without MU compromise.

Some security breaks don't just leak data they also lead to loss of network control.

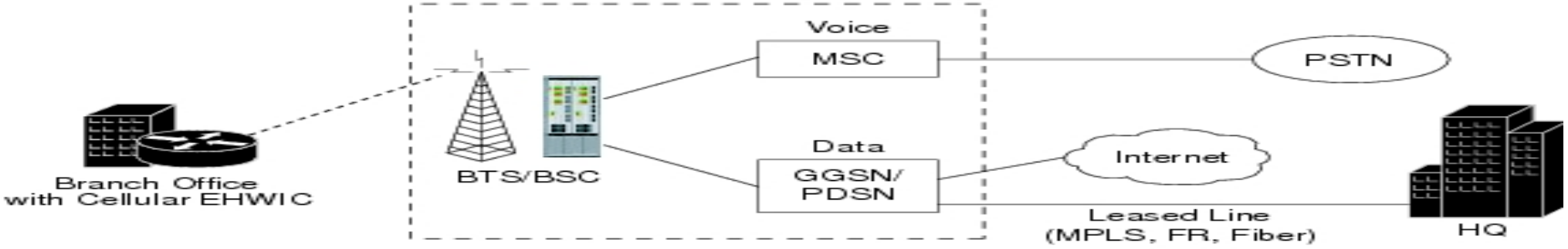
3GPP (2.XG feature additions, 3G/UMTS, 3.XG)

3GPP standards mostly extensions and re-implementations of 2G

- Inherit design flaws
- Make old mistakes
- New mistakes

3.XG and eventually 4G simplifies things

- Layover PTSN for almost all phone calls
- IP based structure for control/packet based services.



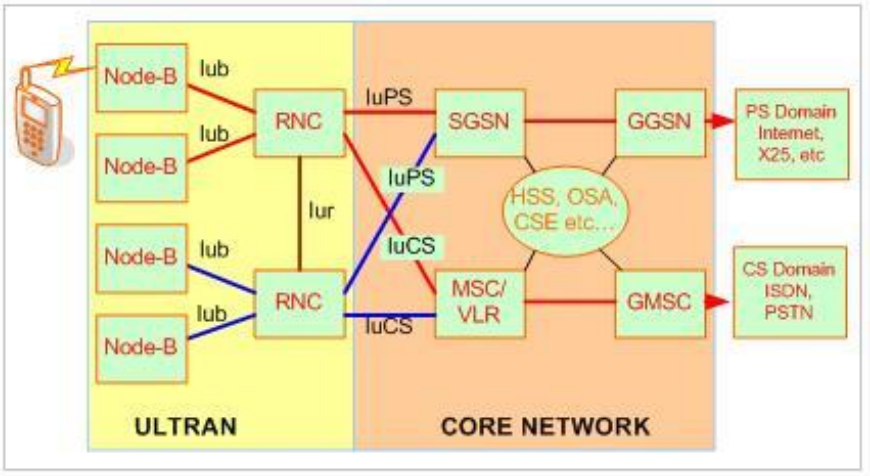
3GPP

Old mistakes and inherited issues

- SMS over control channel constraints inherited.
- Still have the roll your own crypto.

New Issues

- Governments wanted key escrows for new security.
- Longer keys, but only 128 bits.
- SIM cloning



3GPP2 – An exercise in hubris.

Version of 3GPP standards that works on top of 2G CDMA

Published shortly/after 3GPP standards

- Faces same legacy issues as 3GPP
- Chooses to make the same new mistakes as 3GPP even though they had time to correct some.
- Phones use IMSI over SIM which makes cloning worse as you have to replace the MU.

“Attacks always get better; they never get worse.”

- Someone in the NSA

Mobile Unit Security

If the MU compromise is an issue.

- Device OEMs are not very good about providing security updates.
- MU radios can control general purpose device systems.
- Radios are completely closed source and security by obscurity

What have we learned?

Security seems easy within an abstracted view of reality.

- Modern computing has allowed us to forget about the expense of security.
- Today we often have options which fit many needs, **what's important is that we learn from the past what to do when we do not have that luxery.**
- MUs are widely spread, heavily constrained system of devices we can not just write off their short comings and prove constraints cannot be written off.

Do not ever expect to be the exception to a rule.

- Any gains we make from believing we are exceptions are nothing more than deviations in their time to actualization.
- Cell networks got the privilege of reliving the exploits of landline networks.
- Competing standards relived the mistakes of their forerunners and competition.

Security is important, but not easy.