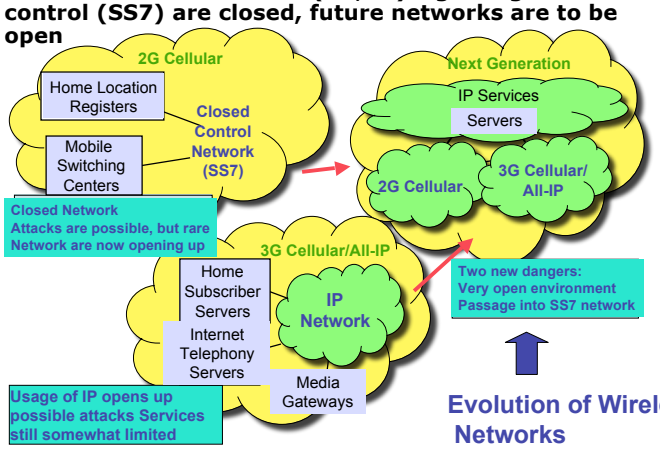
CAT: SDL Based Toolkit for Vulnerability Assessment of 3G networks

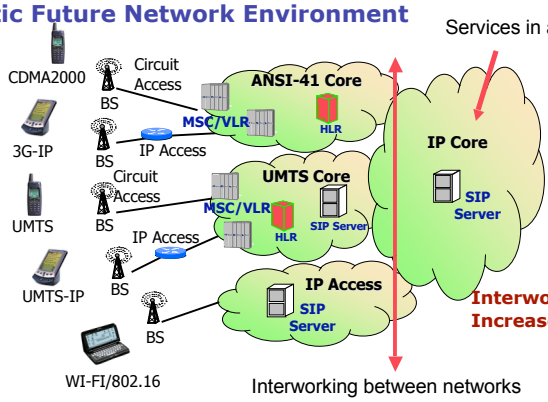
Kameswari Kotapati, Peng Liu, Thomas F. LaPorta

Current telecom network (2G,3G) signaling and control (SS7) are closed, future networks are to be open



Evolution of Wireless Networks

Realistic Future Network Environment



Services in all-IP domain

- Telecom networks use IP for control and services
- Open interfaces for service introduction
- Interworking between networks required

Interworking Architecture ⇒ Increased Vulnerability

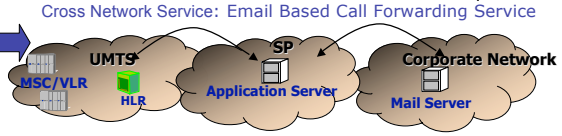
Futuristic Interworking Service: Cross Network Service ⇒ Increased Vulnerability

Cross Network Services will use a combination of Internet based data and data from the wireless telecommunication network provide services to the wireless subscriber

Service description: Forward incoming cell phone calls to voice mail unless caller has email pending for more than 4 hours

Attack: compromise mail server, change time-stamps, deny all calls

Cross Network Service: Email Based Call Forwarding Service



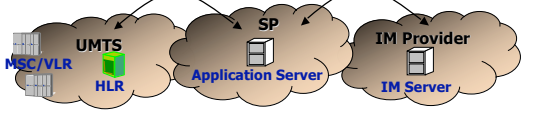
Service description: Location-based Instant Messaging.

Requires cooperation between WSP, IM-provider, and location-based IM provider. Agreements include privacy

Attack: forward subscriber's location unwanted parties, violate privacy

Attack: modify user's IP address, return wrong location, deny service

Cross Network Service: Location based Instant Messaging Service



Cellular Network Vulnerability Assessment Toolkit CAT

GOAL

- Generate graphical trees that capture attack propagation in 3G networks

USER INPUT

- 3G data parameters (Seed/ Goal)
- Seeds: Data that is corrupted by an attacker
- Goals: Data that is *derived* incorrectly

System input

- Freely available Technical telecommunication specification written in Specification and Description Language (SDL).
- System model – show relationship between processing and data.

Output

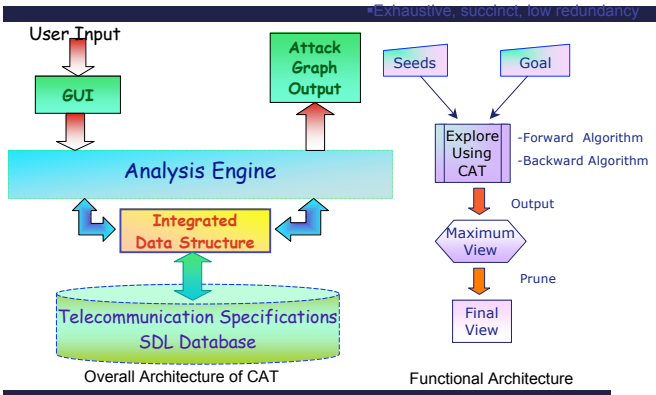
- Attack graph
- Traces seed propagation through the network and impact on services.

Cascading Effect

Spreading of the exploit from one part of the network to another due to the strong relationship between data parameters and the exchanging signals between 3G network elements.

Uniqueness

- Detects cascading effects.
- Detects attacks independent of intruder profile and network configuration.
- Exhaustive, succinct, low redundancy

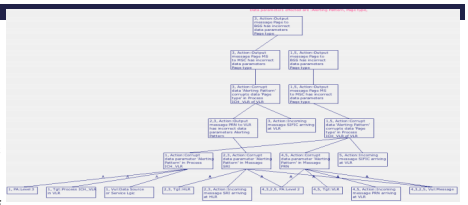


Overall Architecture of CAT

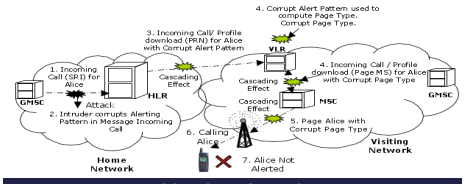
Functional Architecture

CAT detects the following categories of attacks:

- Message based attacks are those attacks where the intruder uses messages to attack the network.
- Server data based attacks are those attacks where the intruder corrupts data stored in the Servers.
- Server level service logic based attacks are those attacks where the intruder corrupts the service logic of Server in the Block.
- Indirect attacks are those attacks in which, given a 3G data parameter d_1 in {D}, where {D} is the set of all 3G data parameters, corruption of d_1 leads to corruption of some other data parameter d_i, which in-turn leads to corruption of some d_j and so on until no other data parameter is corrupt. $d_1 \rightarrow \ldots d_i \rightarrow d_j \rightarrow \ldots \rightarrow d_n$.
- In the Multi-Point attack, corrupting a single data parameter does not lead cause any damage but the corruption of multiple data parameters at multiple points in the network leads to the indirect attacks.

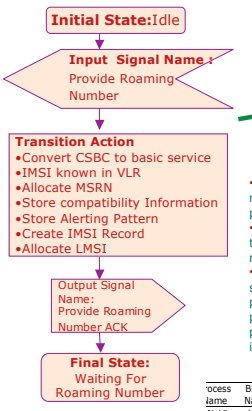


Attack Graph for Alerting Attack



Alerting Attack

Architecture



SDL Fragment of Process Provide Roaming Number in VLR

Table 1:Signaling Message Information

Message Name	Data Elements
PRN	International Mobile Subscriber Identity(IMSI), Mobile Station International ISDN Number(MSISDN), MSC number, Bearer Capability, LMSI, GSM Bearer Capability, ISDN BC, ISDN LLC, ISDN HLC, Pre-paging support, Alerting Pattern

Table 2: SDL Specifications

Process Name	Block Name	Initial State	Input Message	From Entity	Transition Action	Output Message	To Entity	Final State
_VLR	VLR	Idle	PRN	HLR	Convert CSBC to basic service IMSI known in VLR Allocate MSRN Store compatibility Information Store Alerting Pattern Create IMSI Record Allocate LMSI	PRN_ACK	HLR	Idle

Table 2: SDL Specifications

Process Name	Block Name	Initial State	Input Message	From Entity	Action	Output Message	To Entity	Final State
_VLR	VLR	Idle	PRN	HLR	(Bearer Capability~)=Basic Service (IMSI | MSISDN | MSC #)=MSRN (MSISDN ~)=LMSI	PRN_ACK	HLR	Idle

- AND dependency: All `n` data parameters used to compute the resulting data parameter must be corrupt to corrupt the resulting parameter.
- OR dependency: Corruption of any one of `n` data parameters used to compute the resulting data parameter, is sufficient to corrupt the resulting parameter.
- NONE dependency: The output parameter is assigned for a given set of input parameters. Modification or corruption of input parameters will not corrupt the output parameter as the input parameters are not used to compute the output parameter. But retrieval of the output parameter using the corrupt input parameter as a key will result in an incorrect solution.

Converting Telecom SDL specs to CAT System Input

Adversary Model

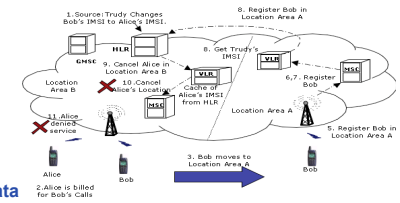
- Detect Message Based Attacks
- Cascading Effects
- Insufficient Data
- Unidentified Relationships
- Requires Expert Input

Identify Data Dependencies

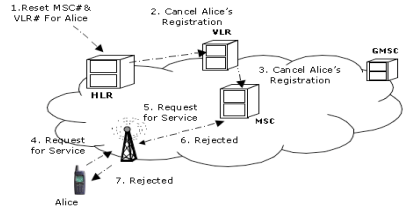
- Intuitive
- Expert Knowledge: Discover up to 60% more attacks

Detects:

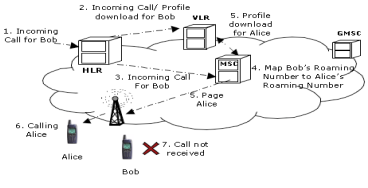
- Indirect Attacks
- Block level Attacks
- Multipoint Attacks
- Cascading Effect



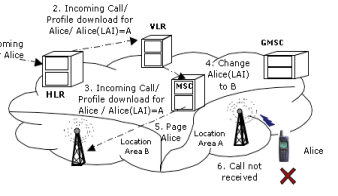
a. Mixed Identity Attack



b. Power-Off Power-On Attack



c. Call Redirection Attack



d. Missed Calls Attack

Interesting Attacks discovered by CAT