Aalto University
School of Science

Hsin Yi Chen, Sid Rao and Tuomas Aura
Department of Computer Science, Aalto University
In collaboration with Nokia Bell Labs

Threat Modeling Framework for Mobile Communication Systems

Problem Statement

Lack of a common taxonomy and metrics to capture a high-level overview of threats and adversary behaviors specific to mobile communication system

Goal

Create a threat modeling framework to provide a structured way to communicate security issues using a common language and reference framework describing adversary behaviors and threats in telecom networks.

Current Developed Framework

	Attack Mounting			Attack Execution			Attack Results	
Reconnaissance	**Initial Access**	**Persistence**	**Discovery**	**Lateral Movement**	**Standard Protocol Misuse**	**Defense Evasion**	**Collection**	**Impact**
Perimeter mapping of network infrastructure	Access from UE	Infecting UE hardware or software	Operator network mapping	Exploit roaming agreements	SS7-based techniques	Malware anti-detection techniques	Admin,node, and user credentials	Location tracking
Perimeter mapping for mobiles	SIM-based compromised	Infecting network elements	CN-protocol scanning	Abusing interworking functionalities	Diameter-based techniques	Blacklist evasion	User-specific identifiers	Calls eavesdropping
Target intelligence gathering	Access from radio access network	Hard-to-repair vulnerabilities	Target intelligence gathering	Core-network access from compromised base station	GTP-based techniques	Exploit misconfigurations & implementation errors	Communication metadata	SMS and IMS interception
	Access from partner mobile network	Command and control channels	Internal resource search	Exploit platform-& service-specific vulnerabilities	IP-based techniques	Bypass firewall	User data	Data interception
	Access from inside the operator network		UE knocking		Pre-AKA techniques	Bypass homerouting	Operator-specific identifiers	Billing frauds
	Access from operator's IP network infrastructure				SIP-based techniques	Downgrading	Operator data	DoS against the network
	Access from the public Internet					Redirection		DoS against a specific user
	Compromised Insiders and Human Errors					Stealth scanning		Identity-related attacks

Work so far

- Build a webtool to support threat/attack modeling process with the framework
- Model exisiting attacks from literature survey to verify the coverage of the framework and expand threat intelligence knowledge base regarding mobile communication systems
- Framework refinement
- Explore future use cases

Use Case Example – Graph Analysis on Attack Models

Build attack graphs and use graph-theory based analysis to indicate the **importance** of the techniques, the **diversity** of techniques an attacker can use given certain initial access or impact, and **common attack patterns**.