

# Wireless Communications Security

Michel Barbeau, Professor  
School of Computer Science  
Carleton University

## Wireless security team

- Profs
  - M. Barbeau, E. Kranakis
- Graduate students
  - P. Boone (Ph.D.), J. Hall (Ph.D.), S. Zou (MCS) *et al.*
- Sponsors: Alcatel, MITACS and NSERC
  - [www.scs.carleton.ca/~cancocom](http://www.scs.carleton.ca/~cancocom)
- Member of the Digital Security Group (P. v. Oorschot)
  - [www.scs.carleton.ca/~dsg](http://www.scs.carleton.ca/~dsg)

# Outline

- Introduction
  - Wireless technologies and security requirements
- Wireless confidentiality
- Wireless availability
- Some challenges

3

# Generations of cellular phones

- 1G
  - AMPS: 1980s, FM, FDMA, handover between cells, limited roaming between networks
- 2G
  - GSM: 1990s, digital-coding of voice, TDMA, Subscriber Identity Module (SIM), data communications
- 3G
  - 3GPP/UMTS: 1998-, WCDMA, global roaming, 2 Mbps data
- 4G
  - All-IP-based, 100 Mbps data

4

## 1G and 2G Networks in Canada

	AMPS	CDMA	GSM/GPRS	iDEN	TDMA
Bell Mobility	X	X			
Rogers Wireless	X		X		X
Telus Mobility	X	X			
Island Telecom		X			
MT&T Mobility		X			
Microcell			X		
Mike Clearnet				X	
Source: www.cellular-news.com					

5

## 3G Wireless in Canada

Name	Price Paid	Est. start date
Bell Mobility	US\$452.7 million	TBA
Rogers Wireless	US\$247.3 million	TBA
Telus	US\$223.7 million	Under trial
W2N	US\$7.16 million	TBA
Thunder Bay Telephone	US\$377,000	TBA
Cost per head of adult population US\$36.45		
Source: www.cellular-news.com		

6

## Security requirements

- Confidentiality
- Availability
- Integrity
- Misbehavior absence
- Participant legitimacy

7

## Why is wireless security difficult?

- Interception easiness
- Medium access uncontrollability
- Topology dynamism
- Evolutional context

8

# Wireless confidentiality

9

# Finding frequencies

The screenshot shows two overlapping Microsoft Internet Explorer browser windows. The top window is displaying the Google search engine homepage with the search term "Georges Bush Radio Frequency" entered in the search box. The bottom window is displaying a search result page from "Military Comms Monitoring". It features two side-by-side photographs of an Airforce One aircraft on a runway, both captioned "Airforce One on Takeoff Roll." Below the photos is a section titled "Secret Service Frequencies 1/30 & 1/31/2002" with the subtext "Bold Frequencies actually heard." This section contains a table with the following data:

Frequency (AM)	Description
32.2300	WHCA Transportation
<b>166.5125</b>	<b>Escort and security</b>
165.7875	Field Offices/Escorts
<b>165.3750</b>	<b>Field Offices Primary/Command post</b>

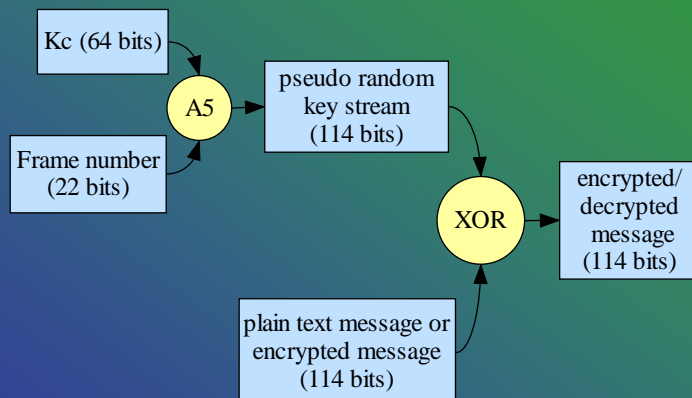
10

## Eavesdropping countermeasures

- Regulations
- Advanced modes
- Encryption

11

## Encryption/Decryption in GSM

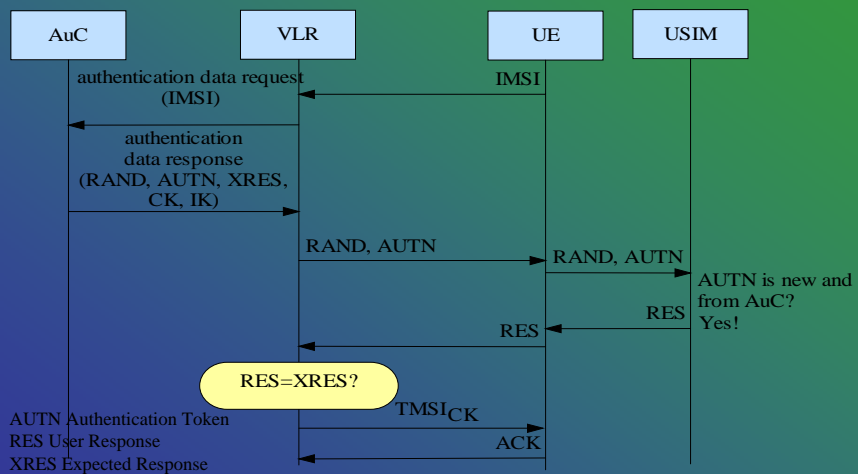


12

# Stream Cipher Weakness

$$\text{Encrypted } (M_1) \oplus \text{Encrypted } (M_2) = M_1 \oplus M_2$$

# Mutual Authentication and Key Agreement in UMTS



## Wireless availability

15

## Why is availability difficult?

- Jamming
- Pile-up

16



## Jamming

Shannon's model:

$$C = W \log \left( 1 + \frac{S}{N} \right)$$

17

## How to Deal With Jamming?

- Increase the power
  - GPS III, planned for 2010
- Use gain antenna
- Increase the bandwidth
  - Spread spectrum
  - Ultra Wide Band
    - Bandwidth greater than 25% center frequency

18

# Pile-up

Images by: J.&G. Naudet (9/11/2001)

19

## Some challenges

- Multimode/hybrid technology devices
- Introduction of new defense methods in existing systems
- Detection/adaptation/resistance to extreme conditions

20