RF CounterSurveillance

• Legal issues – what are they?

• Legalities can vary widely by country and jurisdiction. In Canada, the document that concerns us is the Radio Telecommunications Act.

• For instance, I have heard the rumour that in New York State you are not allowed to scan/monitor any frequencies – it's illegal to own this gear. Could be nonsense though.

• In Canada, however, we are pretty sensible about things. The radio frequency spectrum is publicly owned

• It's like talking in a public park: If it's really *that* secret and you don't want people listening in, either stop talking, go somewhere else and talk, or encrypt it.

• There are, however, some minor restrictions...

9.(1) No person shall
(b) without lawful excuse, interfere with or obstruct any radio communication;
(c) decode an encrypted subscription programming signal or encrypted network feed otherwise than under and in accordance with an authorization from the lawful distributor of the signal or feed;
(d) operate a radio apparatus so as to receive an encrypted subscription programming signal or encrypted network feed that has been decoded in contravention of paragraph (c); or Prohibition(1.1)

Except as prescribed, no person shall make use of or divulge a radio-based telephone communication
(a) if the originator of the communication or the person intended by the originator of the communication to receive it was in Canada when the communication was made; and
(b) unless the originator, or the person intended by the originator to receive the communication consents to the use or divulgence.

9.(2) Except as prescribed, no person shall intercept and make use of, or intercept and divulge, any radio communication, except as permitted by the originator of the communication or the person intended by the originator of the communication to receive it.

RF CounterSurveillance

• Basically, to sum it up, in Canada you can eavesdrop on anything you want, but you are forbidden from decrypting signals

• Anything you hear or find you have to keep to yourself, and you are not allowed to do anything with it, like make a profit. Pretty reasonable, eh?

• These are the same rules that apply to wardriving and make it legal – provided you don't attach to a network and make use of it without permission

• One rumour: you can't drive around in your vehicle with the scanner active – you could use it to evade traffic policing, RIDE spot-checks

• When it comes to the USA you'll want to check what the state regulations are

• Scanners in the USA have to be sold with the cellular phone frequencies blocked – no such regulation exists in Canada.

• The cellular block on some scanner units can be circumvented using easy to find backup software. On restore select a geopolitical/sales region where no block exists. Have an ICOM PCR-1000 in the USA? Back it up but restore it as a Canuck or Aussie unit.

RF CounterSurveillance

• Multiple kinds of Radio Frequency communications in the average business or enterprise

• What springs to the mind of most people is wireless internet as a security concern, maybe Bluetooth, perhaps even wireless keyboards and mice

• I submit that little thought is given to older communications technologies and tools, such as 2-way radio handsets

• Colloquially referred to as 'walkie talkies', Police sometimes refer to them as 'Mitres'

• Don't forget older tech – think holistically - avoid *undue* focus on 'sexy' tools and the future. You live in the here and now.

• Older tech is used a great deal and is important to the safe and efficient operation of society. Old isn't bad – some people out there are still running billing systems on old VAX gear

• Pay attention to the tools used in your enterprise – from top to bottom. Who uses them, and how do they factor into that person's job? How could that person's job affect your security?

• Consider treating any 2-way radio equipped employee as a 'social engineering' vector capable of being remotely exploited

• Physical security is the first, and most important, area you need to protect. Elaborate network security isn't useful if someone walks in and steals the server or your tapes

RF CounterSurveillance

• There is negligible security **actually** in use when it comes to the world of 2-way radio, despite the availability of encryption technology

• Part of this is no doubt due to cost – easy to use and manage crypto is not cheap. Who wants to be taxed more in order to equip police with encrypted radios - which likely offers a negligible ROI? You don't buy just tools, you're buying management and maintenance too

• However, the OPP appears to use encrypted radio. Maybe they get more money from the province, but the TPS gets a harder time from the municipality? The point: **budgets** are the greatest deciding factor in implementing security

• Encryption could affect Interoperability – take the WTC towers as an example. Rescue agencies had a hard time coordinating. Does layering more crypto and management tech sound like it would make this easier or smoother when things are going crazy?

• For these and other reasons, you don't see as much 'true' security as you see obfuscation – use of numbered code phrases (“10-4 Officer 2130”, “What's your 20”) and mis-reliance on technologies such as trunking radio systems

• Trunking radio systems were created so people could make more efficient use of the radio spectrum. The system, base-stations and handsets communicate among themselves and decide what channels to use, and when.

•You never know what frequency you'll be transmitting or receiving on, nor do you have to worry. It's all handled 'automagically' !

RF CounterSurveillance

• The way the spectrum gets chopped up - and how things jump around - is the sole 'security' that trunking (in and of itself) offers. Eavesdropping on a trunking system with a non-trunking scanner usually yields only parts of the conversation before jumps are made to other frequencies

• Not a problem - consumer trunk-tracking scanners are easy to get. Head up to Radioworld (www.radioworld.ca) by Steeles & 400 and drop a few hundred on any Uniden scanner with TRUNKTRACKER I-IV technology. Prices have really come down – this BC346XT only cost $330

• Or the classic method: buy an old trunk-tracking scanner on ebay for cheap, like the Uniden BC780XLT for $99

• Once you own the radio, using easy to obtain/purchase software such as ARC-XT from www.butel.nl, program the radio with the frequencies required for your area.

• These frequencies are public knowledge and easy to locate on the internet. A favourite site is www.radioreference.com which has a huge database of frequencies covering the entire world

• Programming a trunk-tracking radio is more difficult than programming old-school scanners as it uses a different paradigm. It's not a grid, no banks - it's more of a tree of objects

• www.radioreference.com Offers a particularly nice feature with their premium subscription – web services (SOAP) access to the frequency database. ARC-XT can pull from this and program the radio for you

RF CounterSurveillance

RF CounterSurveillance

RadioReference.com
Your Complete Reference Source

Metro Area: Toronto

Toronto County

Separate Agency Pages

Attractions	CYTZ City Centre	Medical/Health
Businesses	CYYZ Pearson Airport	
CYKZ Buttonville Airport	Education	

Categories

EMS	Security	Toronto Police Service
Municipal Government	Toronto Fire Service	Toronto Transit Commission

Radio Reference Module Version 4.1.3109 / Module Last Updated 8/24/2009

RF CounterSurveillance

Toronto Police Service

Conventional Channels

Frequency	Type	Tone	Alpha Tag	Description	Mode	Tag
867.01250		156.7 PL	AA-ITAC2	I-Tac 2	FM	Interop
868.01250		156.7 PL	AB-ITAC4	I-Tac 4	FM	Interop
863.73750	R	110.9 PL	Surveillance	Surveillance	FM	Law Tac
862.93750		110.9 PL	TPS 99-WCITY	Air 4	FM	Law Talk
861.73750		110.9 PL	TPS 9A-ECITY	East City	FM	Law Talk
859.91250			TPS 9B-AIR1	Air 1	FM	Law Talk
866.86250		123.0 PL	TPS 9C-AIR2	Air 2	FM	Law Talk
867.86250		110.9 PL	TPS 9D-AIR3	Air 3	FM	Law Talk
867.51250		156.7 PL	TPS 9D-ITAC3	I-Tac 3	FM	Interop
861.00000		67.0 PL	TPS 9E	Air 5	FM	Law Talk
861.18750		110.9 PL	TPS 9F-LFGD	Lifeguards	FM	Other
860.66250		110.9 PL	TPS B1	Investigative	FM	Law Tac
860.98750		110.9 PL	TPS B2	Investigative	FM	Law Tac
860.48750		110.9 PL	TPS B3	Investigative	FM	Law Tac
860.93750		110.9 PL	TPS B4	Investigative	FM	Law Tac
860.91250		110.9 PL	TPS B5	Investigative	FM	Law Tac
860.18750		110.9 PL	TPS B6	Investigative	FM	Law Tac
151.29500		156.7 PL	TPS EmergNet	Emergency link to all services	FM	Interop
861.68750		110.9 PL	TPS HQ1	HQ/Subway	FM	Law Talk
861.48750		110.9 PL	TPS HQ2	HQ/Subway	FM	Law Talk
861.93750		110.9 PL	TPS HQ3	HQ/Subway	FM	Law Talk
861.66250		110.9 PL	TPS HQ4	HQ/Subway	FM	Law Talk
861.43750		110.9 PL	TPS HQ5	HQ/Subway	FM	Law Talk
860.16250		110.9 PL	TPS MSS 1050	Investigative	FM	Law Tac
860.21250		110.9 PL	TPS MSS 150	Investigative	FM	Law Tac
860.73750		110.9 PL	TPS MSS 250	Investigative	FM	Law Tac
860.23750		110.9 PL	TPS MSS 350	Investigative	FM	Law Tac
860.68750		110.9 PL	TPS MSS 450	Investigative	FM	Law Tac
860.71250		110.9 PL	TPS MSS 550	Investigative	FM	Law Tac
861.16250		110.9 PL	TPS MSS 650	Investigative	FM	Law Tac
860.41250		110.9 PL	TPS MSS 750	Investigative	FM	Law Tac
860.43750		110.9 PL	TPS MSS 850	Investigative	FM	Law Tac
860.46250		110.9 PL	TPS MSS 950	Investigative	FM	Law Tac
857.21250		110.9 PL	TPSA1-ETF-S1	Investigative	FM	Law Tac
857.46250		110.9 PL	TPSA2-ETF-S2	Investigative	FM	Law Tac
857.48750		110.9 PL	TPSA3-SIMP-1	District 1 Simplex	FM	Law Talk
857.18750		110.9 PL	TPSA4-SIMP-2	District 2 Simplex	FM	Law Talk
857.23750		110.9 PL	TPSA5-SIMP-3	District 3 Simplex	FM	Law Talk
857.43750		110.9 PL	TPSA6-SIMP-4	District 4 Simplex	FM	Law Talk
866.01250		156.7 PL	TPSA7-ICALL	I-Call	FM	Interop
857.43750		107.2 PL	TPSA8-CRTSIM	Court Simplex	FM	Law Talk
866.51250		156.7 PL	TPSA8-ITAC1	I-Tac 1	FM	Interop

South Zone	North Zone	East Zone	West Zone
1st Canadian Place	Yonge / Hwy 401	Bell Tower	Winston Churchill Pk
857.1625	861.9125	862.4875	862.1875
857.4125	862.4125	862.9875	862.4375
860.9625	862.4125	863.2375	863.1875
861.2125	862.6625	866.6125	866.2625
861.4625	862.7375	867.1125	866.7625
861.7125	862.9125	867.6125*	867.2625
861.9625	863.1625	868.0875*	867.7625*
862.2125	866.2375		867.9875*
862.4625	866.7375*		
862.7125	867.2375*		
862.9625*			
863.2125*			
866.8875			
867.1625			
867.3875			
867.4625			
867.7375			
867.8875			

From www.reevans.net/scanner/freqs.html

RF CounterSurveillance

• The channels highlighted in red are **Control Channels –** the radios listen to these frequencies to figure out what frequencies to talk on and when. This is *the* distinguishing feature of a trunking system

• You can tell you've hit on a control channel when you listen to it – it makes what some folks like to call a 'buzzsaw' noise. This is the sound of modulated audio

• These are also the channels we are most interested in. We don't need to program the scanner/radio with ALL listed frequencies, just the control channels.

• After programming we use the scanner to monitor the control channels – and poof! – we know who's talking and when, and we can follow them around automatically with no additional work needed

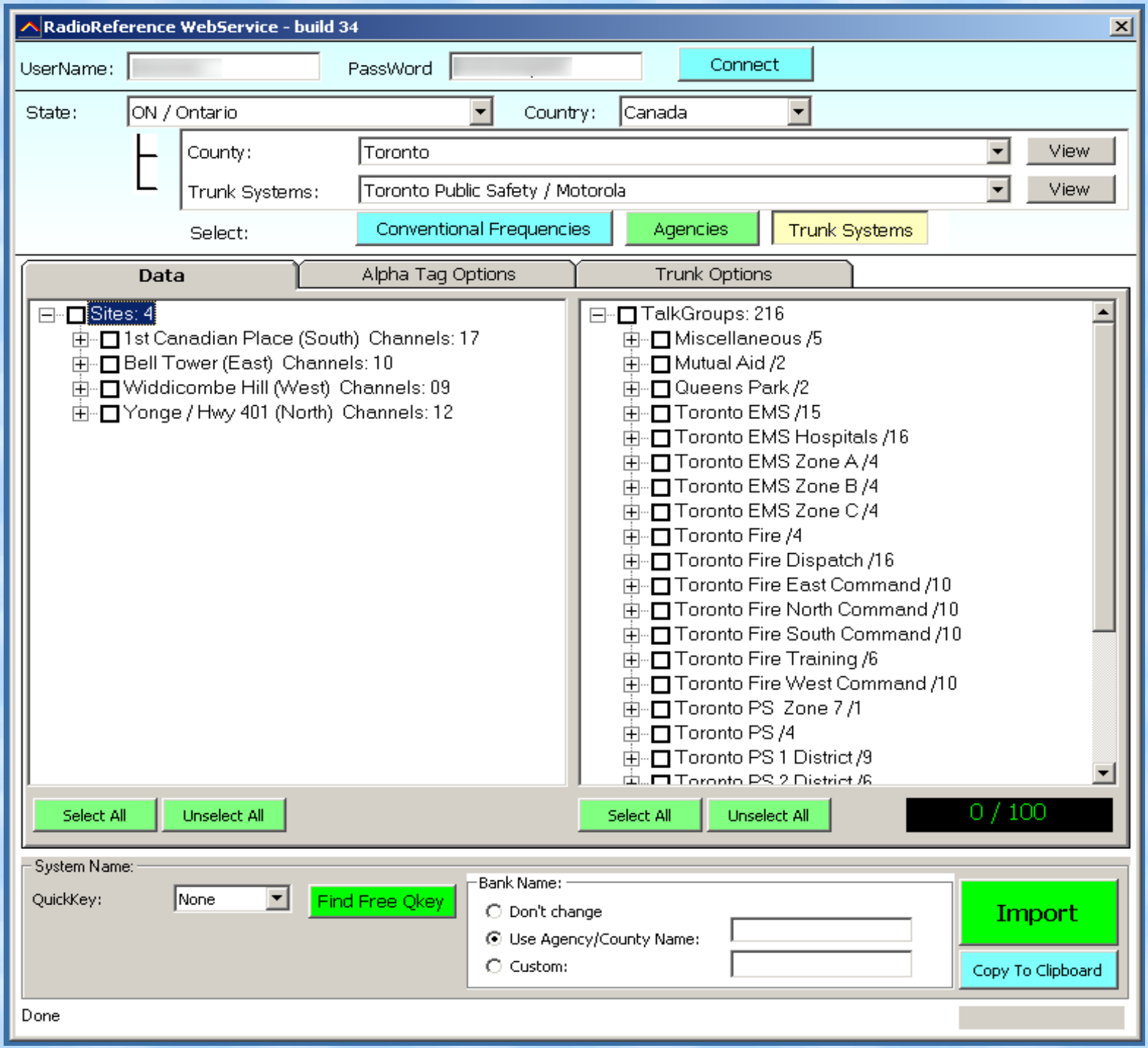
• We're not wasting time monitoring channels that might be unused at that moment – we have guaranteed hits.

• Guaranteed hits, of course, provided that people are using the radios. Some places are quiet – Hamilton on a weekend, for instance, provided surprisingly little.

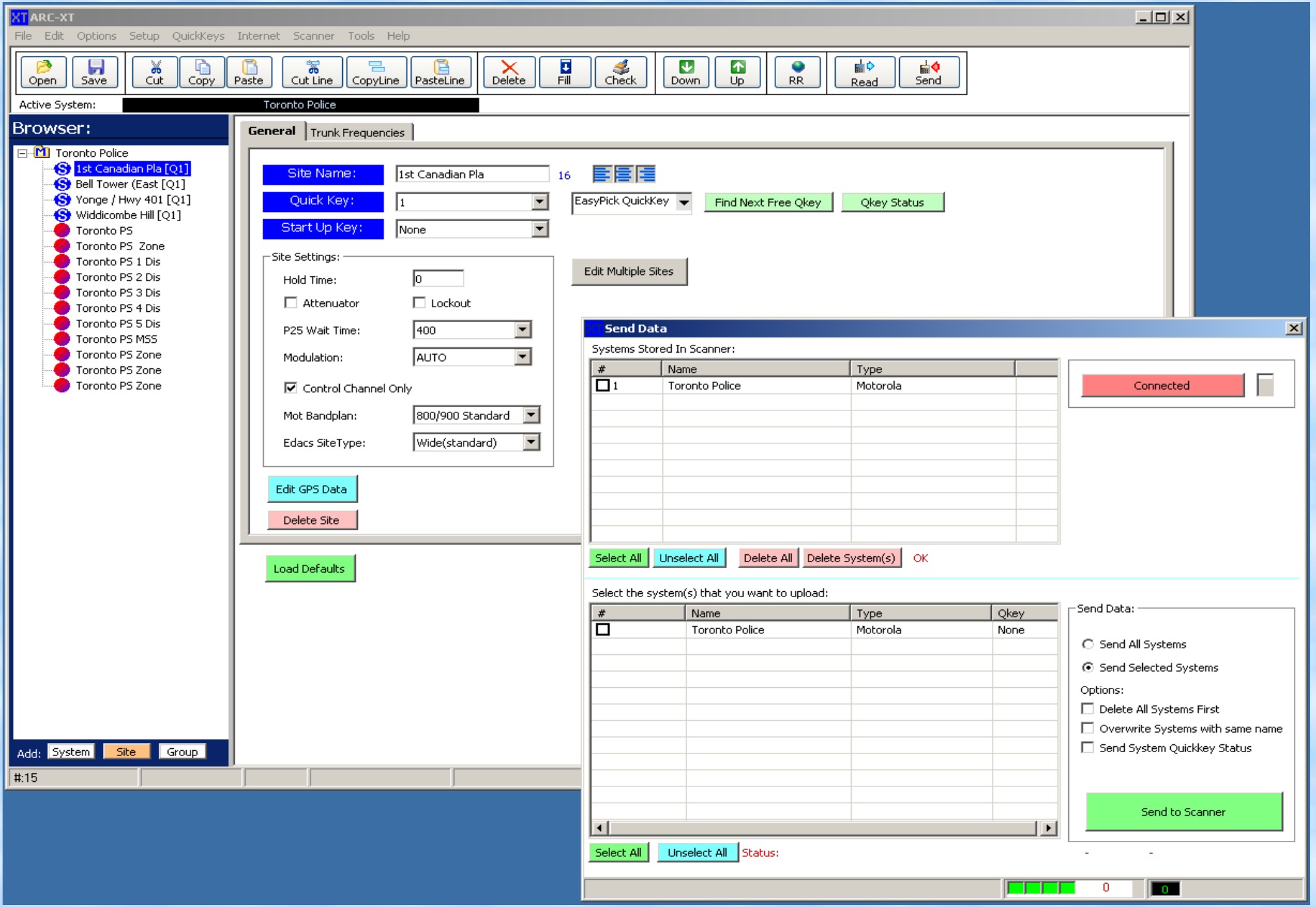
• It's not perfect, however – sometimes noisy radios will hold a channel open for too long, and you'll need to manually 'skip' the channel to get back to scanning for interesting things

• Let's take a look at ARC-XT

RF CounterSurveillance



RF CounterSurveillance



RF CounterSurveillance

• And now we have a scanner programmed to monitor all the police frequencies of interest to us!

• We could just as easily add Fire and EMS to these lists, but I've found these are noisier channels, and the conversation content isn't quite as relevant

• Nonetheless it may be of value to monitor these channels as well – emergency response services tend to respond and work together, providing handy cross-referencing and validation of information. In my experience, firetrucks are usually first on the scene.

• In addition, many private enterprises (office buildings, malls, businesses) maintain their own private 2-way radio networks. Most of these are not trunked.

• They also use different, typically lower, frequencies. These systems are cheaper, easier to manage, and typically have a much smaller range.

• Some of the Uniden scanner models support direct cloning of configurations from handset to handset: you do the hard work of programming just one, then with a cable transfer the info from unit to unit with a few keypresses.

• Scenario: station an agent in each town, when a crew rolls in they meet up and have their radios programmed/customized for the local area

• Let's take a look at lists of trunked and untrunked systems to see what's there

RF CounterSurveillance

All Trunked Radio Systems in Toronto County

System Name	Type	City
AECON Construction and Materials	Motorola Type II Smartnet	Toronto
Air Canada Center	Motorola Type II Smartnet	Toronto
Bell Fleetnet - Ontario Provincial Government Zone 1	Motorola Type II SmartZone	Southwest Zone
Canadian National Exhibition	LTR Standard	Toronto
Eaton Centre	LTR Standard	Toronto
Enbridge Gas Distribution	EDACS Networked Standard	Various
Fleetcom/Lakeshore Electronics	LTR Standard	Toronto
Fleetcom/Lakeshore Electronics # 4	Motorola Type II Smartnet	Toronto
Government of Ontario (GO) Transit	Project 25 Standard	Golden Horseshoe Area
Kelcom (Toronto)	LTR Standard	Toronto
Mobile Business Communications	LTR Standard	Toronto
Mobile Business Communications	LTR Standard	Toronto
Mobile Business Communications Ltd.	EDACS Standard	Toronto
Rogers Centre (formerly the SkyDome)	EDACS Standard	Toronto
Royal Canadian Mounted Police - Portable System	Motorola Type II SmartZone	Various
Ryerson University	LTR Standard	Toronto
Tele-Mobile (Toronto-1)	Motorola Type II Smartnet	Toronto
Tele-Mobile (Toronto-2)	Motorola Type II Smartnet	Toronto
Toronto Hydro	Motorola Type II Smartnet	Toronto
Toronto Public Safety	Motorola Type II SmartZone	Toronto
Toronto TTC Subway	MPT-1327 Standard	Toronto

RF CounterSurveillance

- Some of the following are partial lists – because there's a lot of stuff :)

Businesses

Apartments & Condos

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
451.18750		BM	032 DPL	St James	St James Town Apts (Wellesley & Parliament	FM	Business
451.78750			023 DPL	Menkes	7411 Yonge Maintenance (Menkes Properties)	FM	Business
451.78750			173.8 PL	BrookfldPrpt	Brookfield Property Management Security	FM	Security
452.36250			071 DPL	Menkes	7411 Yonge Security (Menkes Properties)	FM	Security

Construction

Frequency	Input	License	Type	Tone	Alpha Tag	Description	Mode	Tag
151.56500	151.56500	CZX87	BM	162.2 PL	DufferinConc	Dufferin Concrete Div of Holcim	FM	Business
152.03000	151.56500	CZX87	R	162.2 PL	DFFRN CNC	Dufferin Concrete	FM	Business
154.34000				146.2 PL		Dufferin Concrete	FM	Business
154.95000			BM	179.9 PL	Dufferin Cnc	Dufferin Concrete	FM	Business
162.36000				123.0 PL		Lambert Oil	FM	Business
163.05000				179.9 PL	2	Ledcor Construction	FM	Business
165.42000			R	123.0 PL	Dufferin Cnc	Dufferin Concrete (65 Forest Manor, Don Mills)	FM	Business
165.48000				179.9 PL	1	Ledcor Contstruction	FM	Business
167.73000				179.9 PL	3	Ledcor Construction	FM	Business

Couriers

Frequency	Type	Tone	Alpha Tag	Description	Mode	Tag
162.24000	R	146.2 PL	Jesk Entrps	Jesk Enterprises Ltd	FM	Business
163.50000	R	146.2 PL	TransOntario	Trans-Ontario Express	FM	Business
170.85000		CSQ	Jesk Entrps	Jesk Enterprises Ltd	FM	Business
451.83750		136.5 PL		Flying Dutchman	FM	Transportation
452.15000		91.5 PL	ArrowspdDlvr	Arrowspeed Delivery	FM	Transportation
453.96250		151.4 PL	SURETRACK	Sure Track Courier LTD	FM	Transportation
453.96250		151.4 PL		Sure Trac Courier	FM	Transportation
454.22500		210.7 PL		Romark Logistics	FM	Transportation

Hotels

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
408.01250			115 DPL		Holiday Inn (Toronto)	FM	Business
451.78750	XKE248	R	026 DPL	DeltaChelsea	The Delta Chelsea Hotel (33 Gerrard St W)	FM	Business
452.53750			110.9 PL		The Hilton Hotel (TOronto)	FM	Business
452.81250			413 DPL	IntrCntntl	Inter-Continental (220 Bloor W)	FM	Business
453.70000	VCS630	R	203.5 PL	WestinHrbrCs	Westin Harbour Castle	FM	Business
456.78750			173.8 PL		Delta Chelsie Inn (Toronto)	FM	Business
461.03750			107.2 PL		Deys Inn (Toronto)	FM	Business
464.68750			203.5 PL		Valhalla Inn (Toronto)	FM	Business

Mall Security

Frequency	License	Type	Tone	Alpha Tag	Description	Mode	Tag
451.18750			196.2 PL		Malvern Town Center Security	FM	Security
452.06250			179.9 PL		Sherway Gardens Maintenance (Etobicoke)	FM	Security
452.36250			412 DPL	Hazelton Lns	De Bonis Management (Hazelton Lanes)	FM	Business
452.53750			365 DPL		Sherway Gardens Security (Etobicoke)	FM	Security
452.53750			167.9 PL		Fairview Mall Security	FM	Security
452.81250					Woodbine Centre	FM	Security
453.28750					Eaton Centre Security	FM	Security
453.70000					Jane Finch Mall	FM	Security
454.20000			131.8 PL	BVSC SEC	Bayview Village Shopping Centre Security	FM	Security

Rail

Frequency	Type	Tone	Alpha Tag	Description	Mode	Tag
410.56250	R	411 DPL	UnionStnSecr	Union Station Security	FM	Railroad
451.72500		114.8 PL	VIA RAIL	Red Caps/Porters	FM	Railroad
463.96250		103.5 PL	VIA RAIL	Locomotives	FM	Railroad

Security

Frequency	Tone	Alpha Tag	Description	Mode	Tag
165.65000	192.8 PL	YORKDALE SEC	Yorkdale Mall Security	FM	Security
451.66250	331 DPL	MCAS	Metro Childrens Aid Society	FM	Business
460.05000	110.9 PL		Brinks Armoured Cars	FM	Security
464.76250	192.8 PL		Universal ATM Armoured Cars	AM	Security

RF CounterSurveillance

• So what are some of the risks – why should I care?

• People are always the weakest link. Fancy tech is worth less if someone can ring up the company, get through to the help desk, and have the password reset on an account that doesn't belong to them

• Using radios, one can covertly gather all sorts of information – names, phone numbers, times, dates, procedures, perhaps even passphrases. All of this helps an attacker in creating a 'portfolio' which can assist them in social engineering 'attacks' or brute-forcing logins.

• What if the 'attacker' is not interested in quietly obtaining your data? Let's say they want to put a hefty dent in your wallet

• They stake-out your premises and monitor your 2-way radio system. Details about patrols, shifts, and names help them cook up a plan.

• They wait for the day when a couple guards call in sick. At some point the only guard on duty that day has to head down to the loading dock for a couple minutes to handle a delivery. The front entrance is unguarded and unwatched. They head to the elevator, get off at a point close to where your data centre is, then cut cables

• This same sort of thing gets some play in the press or gov't as terrorism concerns, legit or not; knowing names, routines, voices and impersonating an employee to get in the door, scoop an appointment or ambush an outing by listening in, etc.

RF CounterSurveillance

• Robbery – the 'Diamond Heist' scenario

• The place of business is cased – employees are watched, routines determined, scheduled drop-offs and pick-ups noted, etc.

• Attacker #1 sits hidden and/or disguised, scanner in hand, monitoring police & security frequencies. Why? To get a communications baseline so any exceptional incident will be easier to pick out from conversational topics, changes in the amount of talking, etc.

• The targeted business closes for the day

• After some amount of time elapses, Attacker #2 rides by on a bike, and trips the alarm somehow. Attacker #1 scans for and detects communications related to the alarm. Security arrives onsite and determines it's a false alarm.

• This is repeated a few times over the course of the night or some period of time. After a while they get to know the response time and the procedure.

• With each false alarm, it becomes easier for the responders to ignore. With luck, the senior responder might decide it's a waste of money to keep on sending a crew out since it's clearly a false alarm.

• Time to strike: Attacker #2 breaks and enters the premises, knowing there is plenty of time to steal the diamonds. Attacker #1 is keeping watch and can alert to any problems, assuring a safe, clean get-away for everyone

RF CounterSurveillance

- Thank you, and remember... Shop Smart, Shop S-Mart!