Comparison of Cellular Industry (’92) to WiFi Industry (’02)

Vu-graphs are extracts of ones presented at the *CTIA Critical Issues Forum*
15 November 2002

Leslie D. Owens, Booz Allen Hamilton

Presenter Information

Leslie D. Owens (Les)

Booz Allen Hamilton, Wireless Security Lead

703/902-7091 (office)

703/980-3877 (cellular)

Owens_les@ bah.com (email)

les.owens@att.net

WiFi versus 1st Generation Cellular (1)

	WiFi	1st Generation Cellular
Time Period	2002	1992
Incubation period	4 years	4 years
State of industry	Exploding	Exploding
State of security	Poor	Poor (identity-based system)
State of consumers	Perplexed	Perplexed
3rd party response	Many solutions and partial solutions; “marketecture”	Many solutions and partial solutions; “marketecture”
Press activity / Hype	Hog wild	Hog wild
Types of Attacks	Passive and active	Active
Criminal motive	Anonymity and mobility / TBD	Anonymity and mobility

WiFi versus 1st Generation Cellular (2)

	WiFi	1st Generation Cellular
End result of attacks	TBD	Theft of service (fraud) and major criminal activity
Key Law enforcement Agency involved	TBD / USSS?	US Secret Service
Buzzwords	War-driving and war-chalking	Counterfeiting / cloning
Tools of choice	Netstumbler and Airsnort	Curtis ESN reader and Timson software
Detectability	Difficult.	Difficult a priori. Easy after the customer complains
Triage solution	Patched WEP, VPNs	PINs, clone detectors, RF fingerprinting
“Hot” solution to the problem	Switch-based security devices	RF fingerprinting
Government attitude	Very concerned	Somewhat concerned

WiFi versus 1st Generation Cellular (3)

	WiFi	1st Generation Cellular
Industry image	Black eye	Black eye
Loss potential	Astronomical	~$1Billion
Types of losses and pain	Industrial espionage, tarnished image, financial loss, denial-of-service, and information warfare	Theft of service (fraud) and ESN change
Estimated losses	TBD	$1 Million per day
Recipient of losses	Consumers and businesses	Cellular service providers and consumers
Ease of getting tools	Trivial – Internet downloadable tools	Trivial – Can buy / BBS downloadable tools
Entrepreneur criminal products	Sniffers and WEPCrack/TBD	Custom readers, Copy Cat boxes, and Magic phone
Legislation produced	TBD	Title 18 USC 1029

WiFi versus 1st Generation Cellular (4)

	WiFi	1st Generation Cellular
Penalty for attacks	TBD	$10,000 fine and 10 years in prison
Proactive industry association	WiFi Alliance	CTIA
Most proactive government agency	NIST	FCC
Faulty Logic	TBD	“ESN Hardening”
Engaged Entities	Security Officers	Fraud Managers and financial team
Paying attention to problem	TBD	CFO
Problem evolution	TBD	Subscription fraud
Effective first step	Education	Education

WiFi versus 1st Generation Cellular (5)

	WiFi	1st Generation Cellular
How long to bring under control?	TBD	5-6 years
Comprehensive plan	TBD	Fraud Summit and 10-step plan
Ultimate solution that ameliorates the problem	TBD	Single, standardized cryptographic approach

"Those who cannot remember the past are condemned to repeat it."

George Santayana, 1863 - 1952
Spanish-born American poet and philosopher
The Life of Reason