

SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL

Mobile Security from an Information Warfare Perspective

B van Niekerk
MS Maharaj



SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL


Introduction

Concern that cyber security issues and information warfare will migrate to mobile networks.

Paper forms a vulnerability / risk assessment from previous incidents.

Paper outline:

- Background to information warfare and mobile infrastructure.
- Mobile security incidents.
- Preliminary research results.




SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL


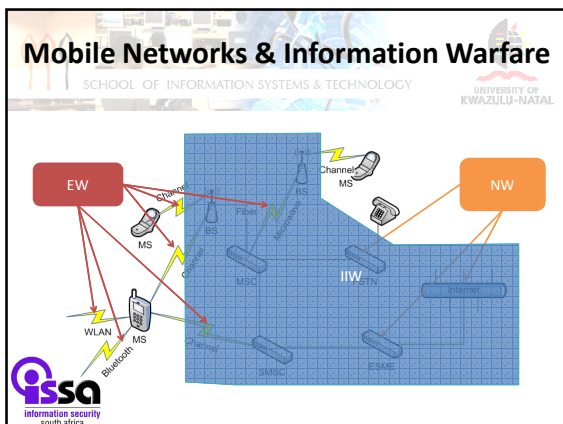
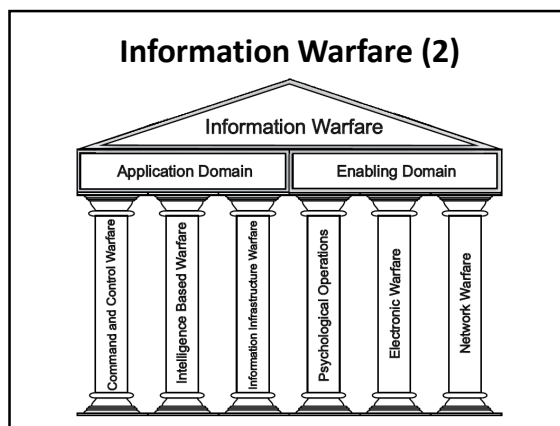
Information Warfare (1)

- Information warfare relevant to political, social, corporate and military spheres.
- Information has value.
- Information and supporting systems are both weapons and targets.

Exploit
Deny
Degrade
Corrupt



Confidentiality
Integrity
Availability

SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL


Incidents (1)

Disgruntled Employee

- Hacked into mobile network, sent fake SMSs
- Responses to SMSs blocked company's phone lines

SMS Banking Scandal

- Gang coerced engineer to assist with providing duplicate SIM cards to exploit banking password SMSs
- Both network and financial institutions compromised




Incidents (2)

SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL

Athens Affair

- Vodaphone Greece's legitimate eavesdropping capabilities exploited.
- Many high-ranking persons had mobile calls monitored.
- Unclear if there was insider help or the network was penetrated from outside.



Incidents (3)


SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL

GSM Project

- 'How-to guide' on cracking A5/1 cipher release on internet.
- Impractical to fully implement.

Malware

- Cabir, Skulls, Commwarrior
- HTC Magic, iPhone
- India bans Chinese mobile products.



Incidents (4)


SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL

Other incidents

- Hate messages distributed via SMS in Kenya.
- Reports of Israel hacking into mobile networks to distribute messages.
- Phishing scams move to mobile.
- iPad 3G details compromised in U.S.

SMS Exploitation


- Exploitation of web-based SMS services for DoS attack.
- SMS injection attack crashes phones.



Incident Summary

SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL

Incident	Tactic	Functional areas
Athens affair	Exploit	Network warfare, information infrastructure warfare, command & control warfare, intelligence-based warfare
GSM Project	Exploit	PSYOP. Electronic warfare&network warfare?
Disgruntled employee	Deny	Network warfare, information infrastructure warfare
SMS banking scandal	Exploit	Intelligence-based warfare, PSYOP
Malware	Exploit, Deny	Network warfare
Israel, Kenya, Phishing	Corrupt	Network warfare, PSYOP
iPad	Exploit	Network warfare
SMS exploitation	Deny	Network warfare, information infrastructure warfare



Preliminary Research Results Simulations


SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL

Background

- Equipment available to jam mobile communications.
- 3G communications uses CDMA which has inherent features that make it difficult to detect and jam.
- It may be possible to estimate the CDMA spreading sequence to subvert the inherent security.

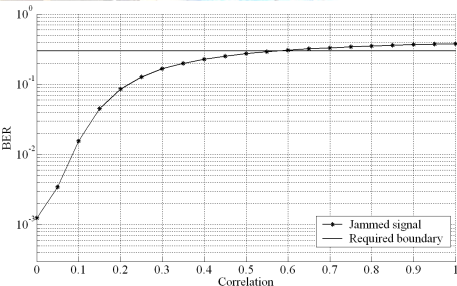
Simulations

- Monte Carlo simulations in Matlab; 100 iterations.
- 6 users, AWGN SNR=10dB, length-31 Gold Codes

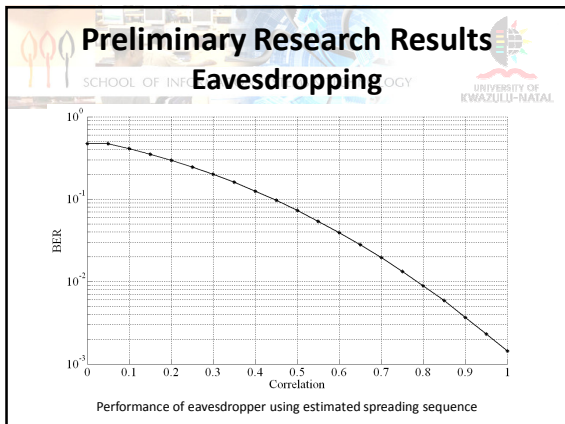


Preliminary Research Results Jamming

SCHOOL OF INFORMATION SYSTEMS & TECHNOLOGY
UNIVERSITY OF KWAZULU-NATAL



Performance of target signal under jamming using estimated spreading sequence

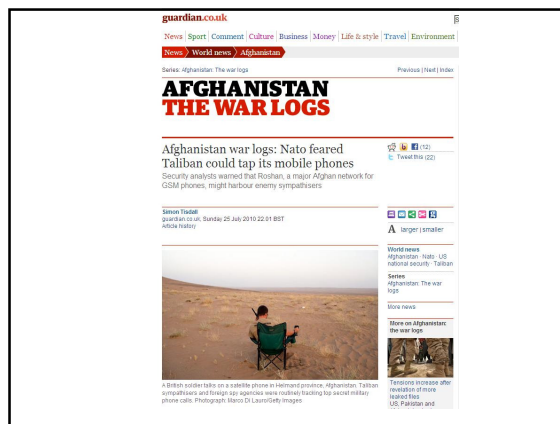



- ### Preliminary Research Results
- #### Interviews (1)
- Prospective respondents identified by their publications
 - 6 international experts approached, 5 responses
 - eDelphi Method
 - Results from these interviews not sufficient by themselves, but will be used in conjunction with local interviews.

- ### Preliminary Research Results
- #### Interviews (2)
- What is the greatest information warfare or security threat to the mobile phone infrastructure?
 - Should the cell phone infrastructure be considered part of the critical information infrastructure, and should cell phones be considered specifically in critical infrastructure and information security policies?
 - How important are cell phones to the following: Large business; small business; military; government; security services; insurgents, terrorists, and criminals.

- ### Preliminary Research Results
- #### Interviews (3)
- 9 keywords received regarding threats to mobile networks:
 - 4 regarding privacy and monitoring
 - dependence, malware, cybercrime, lack of data verification, and smart phones with fewer security controls
 - Mobile networks do form part of the critical information infrastructure - 4 positive, 1 neutral response.
 - Explicit policies for mobile networks - 3 positive, 1 neutral, 1 negative response.



- ### Preliminary Research Results
- #### Interviews (4)
- Importance of mobile communications to:
- Large and small business: 4 positive, 1 neutral
 - Govt, military, security services: 4 positive, 1 negative
 - Malicious actors: 5 positive
- The results indicate there is concern, and that mobile networks are critical.





Conclusion

- There is a concern that mobile networks could become an information warfare battleground.
- The incidents illustrate that information warfare concepts can be used to compromise mobile networks to gather intelligence or deny services.
- Using network warfare may be more beneficial than electronic warfare.
- Initial interview responses again indicates the concern and mobile networks are considered as critical and should be protected



Thank you.

Questions & comments

B van Niekerk	MS Maharaj
991160530@ukzn.ac.za	maharajms@ukzn.ac.za
+27 (0)31 260 8521	+27 (0)31 260 8023

