CERIAS

the center for education and research in information assurance and security

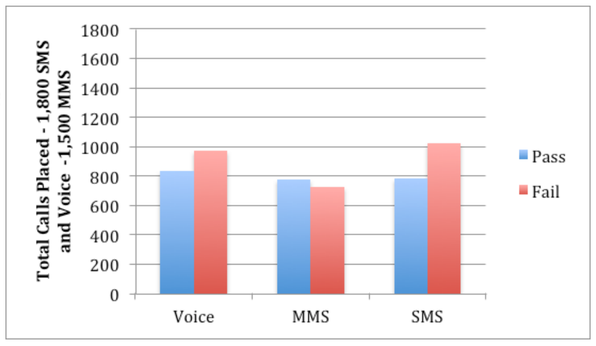
Cyber Forensics

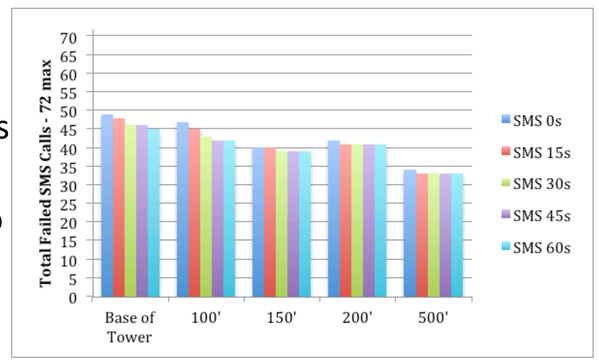
A Field Test of Mobile Phone Shielding Devices

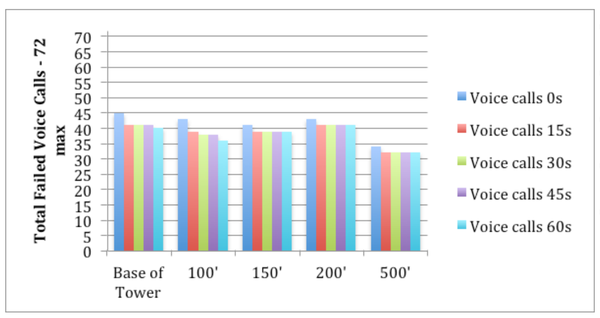
Eric Katz, Rick Mislan, Marc Rogers, Tony Smith

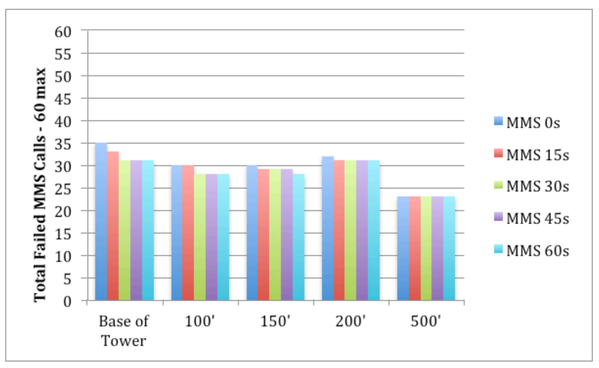
Abstract

Mobile phones are increasingly a source of evidence in criminal investigations. There are many tools that claim to radio isolate a phone in order to preserve evidence. Unfortunately these wireless preservation devices do not always prevent network communication. These devices were tested using mobile phones from both CDMA and GSM services providers. Calls were made to contact the isolated phones using voice, SMS, and MMS at varying distances from the provider's towers. SMS messages were the most likely to penetrate the shields followed by voice calls. MMS were the least likely to penetrate the shields.









Phones Used	
AT&T	
	Apple iPhone 3Gs
	BlackBerry Curve 9300
	Palm Pixi Plus
Sprint	
	BlackBerry Curve 8330
	HTC Hero 2
	Motorola Clutch i465
	Palm Pixi
	Samsung Galaxy S
Verizon	
	Casio G'Zone Ravine
	HTC Droid 2
	HTC Droid Ers
	HTC Imagio

Significance

- Information on a mobile phone is volatile and difficult to forensically recover.
- There are multiple methods a suspect can use to delete evidence.
  - Flooding the phone with calls
  - Remote wipe commands
- Failure represents the potential complete loss of all evidence.
- It is often difficult to tell how far one is from a tower or signal source.

Results

- 53.08% Failure rate overall
- 56.78% Failure to block SMS
- 53.78% Failure to block Voice Calls
- 48.07% Failure to block MMS
- Better results farther from the towers
- No device worked 100% of the time
- **Unacceptable** rates of failure for forensic tools

Shielding Devices
eDEC Black Hole Bag
LessEMF High Performance Silver Mesh
MWT Materials' Wireless Isolation Bag
Paraben StrongHold Bag
Ramsey STE300 - Chest
Ramsey STP1100 - Bag

Implications

As the number of mobile phones taken into custody increases, more standard operating procedures will dictate that mobile phones be isolated in order to protect and preserve the evidence found on them. This study proved that mobile phone shielding devices couldn't be guaranteed to protect evidence on a phone. In a worst-case scenario, any one of these failures could represent the complete loss of all evidence contained on the phone due to a remote wipe command. The American Academy of Science recently berated the entire forensic science community for not following scientific procedure and a lack of failure rates is one of the problems they addressed. More research needs to be done to determine the exact point and frequency of these failures, but this study is a good start. The methodology used for this research will be very useful for developing future studies and methods for investigating the effectiveness of mobile phone shielding devices.

PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center