الفصل السادس
في مكافحة جرائم الموبايل

1. **الإبتكارات**
2. **مكافحة مصادر بعض الجرائم**
3. **شركات الحماية**
4. **منع العبث بالجهاز:**
5. **برامج كشف السرقة**
6. **استخدام برامج الحماية للموبايل**
7. **برنامج**SmitfraudFix .
8. **شركات التصنيع.**
9. **تنمية الوعي الشعبي.**
10. **المكافحة البوليسية.**
11. **الرقابة الجمركية.**
12. **استخدام البصمات الحيوية**
13. **التتبع بالأقمار الصناعية**
14. **كشف تزوير الصورة**
15. **محاربة التزييف**
16. **المكافحة القانونية**

1. **الإبتكارات**:

في الأول من يناير2009 صمم باحثوا العلوم الجنائية الافتراضية جهازاً لاستخلاص ذاكرة الموبايل للتدليل في مسرح الجريمة.وقد وضعت شريحة ذاكرة الموبايل في جهاز حيث بواسطة برنامج كمبيوتري تم استخلاص وفك شفرات المعلومات بإظهار سجل المكالمات والرسائل النصية والبريد الإلكتروني والصور والتسجيلات المرئية (الفيديو) والتواريخ ومن ثم استخدمت هذه المعلومات بواسطة البوليس كأدلة في الجرائم [42].

2. **مكافحة مصادر بعض الجرائم**:

قد تنشأ بعض جرائم الموبايل من الرعونة أوالإهمال أو عدم المعرفة ويستغل أخرون نابهون هذا الإهمال لصاحبهم بارتكاب جرائم ومنشأ بعض هذه الجرائم:

1. بيع الموبايل وترك الذاكرة فيه، وبذلك تكون الصور ورسائل الصور عرضة لمنشأ الإبتزاز بطلب اموال او غيرها خلال نشر صور معينة والتشهير باستخدامها.
2. تخزين الارقام والاتصالات على الهاتف وليس الشريحة وبذلك فان الشريحة تحتوي أسماء أشخاص معينين قد يكونوا مشهورين ويتم استخدامها في الابتزاز او غيره من صور الاحتيال عن طريق اختراق الخصوصية
3. من خلال تصليح الجهاز فقد يتم نسخ او قرصنة المعلومات والتجارة فيها اواستلال الصور والمكالمات او الاحاديث في ارتكاب فعل مجرم.

ولمكافحة مثل هذه الجرائم يجب اتباع الآتي:

2-7 التأكد من خلو الجهاز من أية بيانات حال بيعه.

2-8 تخزين بيانات الإتصال والصور على الشريحة.

2-9 اثبات التاريخ الذي تم فيه تصليح الجهاز واخذ فاتورة بذلك.

3. شركات الحماية:

- الحماية في البنوك Mobile banking (43):

اصبح الأن الموبايل يستخدم في العمليات البنكية كبنوك Citibank, Wachovia, and Bank of America من خلال برامج ووسائل حماية كما لو كان في البنك لنقل الاموال وشركات الموبايل تعمل على إيجاد تكنولوجيا جديدة ووضع الخطط وايجاد تطبيقات جديدة ايضاً. ويجب ان يوافق البنك على الخطة ويستخدم Cingular في البنوك والتعامل بالموبايل في البنوك اصبح دولياً كجزء من التجارة بالموبايلmobile commerce ويتطلب الأمر في

لبتعامل ربما مع أنواع معينة من الموبايلات نظراً للتعدد في أنواع الموبايلات December 2009 ولذلك فان هناك تحديات وسط موجات التزوير والإقتناص (التصيد) وفك الشفرات.ويجب الستيثاق قبل نقل الأموال باستخدام تأمين وسرية ذات مستوي تقني عالي عبر الهواء وباستخدام شفرات سرية. ويمكن حماية المعلومات حالة فقد الموبايل عن طريق خدمات خاصة.

4. منع العبث بالجهاز:

تعطيل الزر الاخضر للاتصال لمنع المتطفلين بالعبث في الموبايل الطريقة:

يتم تعطيل زر الاتصال كالآتي :

1. أذهب إلى القائمية ،ثم الضبط ، ثم ضبط المكالمات ، ثم معاودة الاتصال آلياً فأختر تعمل.
2. عد إلى الشاشة الرئيسية. وأضغط زر النجمه ثلاث مرات فسوف يظهر هذا الحرفP واضغط اتصال فسوف تظهر لك رسالة تقول: (خطا في الاتصال) فانتظر حتى تنتهي معاودة الاتصال ، بعد الانتهاء ستلاحظ ان زر الاتصال لا يعمل.

إعادة الموبايل إلى حالتة الطبيعة يتم كالآتي:

الطريقة الاولى: ان تجعل احد من اصدقائك يتصل بك

والثانية: ان تعيد تشغيل الجهاز..

5. برامج كشف السرقة [34]:

أفضل برنامج لاستعادة موبايلك المسروق

VMS Protection V1.0

أفضل برنامج لحماية الموبايل من السرقه ولاستعادته بعد السرقه

برنامج يجب أن يكون في كل جهاز vms فهو يمكن أن يخفي ويشفر الرسائل والأسماء والصور والفيديو الخ...

إذا سرق موبايلك يتيح لك هذا البرنامج خيار التجسس على نشاطات السارق ومالذي يفعله بجوالك فالبرنامج يرسل تقريراً مفصلاً مثلا سجل المكالمات والرسائل المرسله والاسماء الجديده المضافه والأسماء المعدله.

التقرير يرسل إلى رقم موبايل أنت تحدده من البرنامج مثلا رقم موبايل أخوك أو زميلك أو والدك.

البرنامج يساعدك في استرجاع جهازك المسروق لكن الأهم هو انه يحمي محتويات جوالك من الأيدي العابثه سواء كانت هذه الملفات في ذاكرة الهاتف أو بطاقة الذاكرة شاملة الصور ومقاطع الصوت والفيديو والرسائل والاسماء. حيث يتيح لك خيار تشفير المحتوى (ويجب أتخاذ الحذر عند استخدام هذه الميزه وعدم العبث بها كثيرا).

البرنامج يبدأ في العمل في حالتين:

تفصيل هذه النقطه بمثال:

إذا وضعت رسالة الهجوم في البرنامج مثلا "said" ثم حدثت سرقه لجهازك. فخذ اي جوال من اي شخص في الشارع وأرسل رساله قصيره مكتوب فيها امر الهجوم "said" الى جوالك المسروق عند وصول الرساله لجهازك البرنامج سيعمل تلقائيا على اظهار شاشه على سطح المكتب- طبعاً هذه الشاشه تكون قد كتبت فيها مسبقا ما تري فمثلا ستظهر الشاشه مكتوب فيها التالي:

الموبايل مسروق الرجاء عدم التعامل مع اي حامل لهذا الجهاز والاتصال فوراً بالرقم... وهذه الشاشه لن تذهب نهائيا حتى لو فرمت الجهاز مالم يتم ادخال رمز سري موضوع سابقا من قبل صاحب الموبايل.

كما أن هذه الشاشه يمكن ان تفعل فيها خيار التنبيه هذه الشاشه قد تكون لها فائده أخرى أكبر وأشمل وهي في حال ضياع الجهاز منك فتضع شاشه مكتوب فيها مثلا هذا الموبايل ضائع الرجاء ممن يعثر عليه الاتصال على الرقم....إلخ.

ميزة ثانية بالبرنامج:

هي أن البرنامج ليس له أيقونه في القائمه ولا يظهر من ضمن البرامج يعني مختفي.

الدخول على البرنامج:

الدخول على البرنامج عن طريق ضغط مجموعه من الارقام أو الرموز (الرقم الأصلي 123456) لتظهر لك القائمه الرئيسه للبرنامج. بالطبع تستطيع تغيير هذا الرقم إلى اي رقم يناسبك . ومن خلال التجربة لمهرة ينصح بمحاولة جعل الرقم السري للبرنامج مختلف عن أي رقم سري ممستخدم في جهازك مثل (رمز القفل -رمز المحفظه -رمز برنامج الحارس الذكي) لان اذا كان الرقم السري متشابه فسيسبب لك مشكله بسيطه لانك مثلا عندما تريد فتح برنامج الحارس الذكي والرقم السري للحارس الذكي هو نفس رمز استدعاء البرنامج فسيظهر لك البرنامج ويجب ان تخرج منه لتعود مره اخرى لادخال الرمز لبرنامج الحارس الذكي.

ميزه ثالثة للبرنامج:

لن يستطيع السارق مسح البرنامج أبدا.لأن البرنامج به خاصية uninstall بمعنى انك لن تستطيع مسح البرنامج الا من من البرنامج نفسه وحيث أن السارق لا يعرف كيفية الدخول للبرنامج فسيقف مكتوف الأيدي عاجزا عن فعل أي شئ.

ميزه رابعة للبرنامج:

وهي الأفضل:

بعد ان يرسل لك البرنامج رقم الشريحه الجديده التي وضعها السارق في جهازك تستطيع الاتصال على السارق من أي رقم تحدده سابقا مثل رقم أخوك وهنا الجهاز سيرد تلقائياً على المكالمه دون احساس السارق ويضعها على الـ Speaker مما قد يعطيك الفرصه للتجسس على السارق وهو يتحدث مع شخص أخر والتعرف عليه أو على مكانه .وهذه الميزه يفضل استخدامها بعد سرقة جوالك مباشره. كما يمكن استخدام هذه الميزه للتحدث مع السارق.

1. إذا تم تغيير الشريحه بشريحه أخرى مختلفه وغير مصرح بها من قبل صاحب الموبايل.
2. اذا أرسلت رساله بإمر محدد مسبقاً إلى موبايلك المسروق- وهذا الأمر تحدده أنت قبل ان يسرق الموبايل أو يضيع.

صورة البرنامج

6. استخدام برامج الحماية للموبايل:

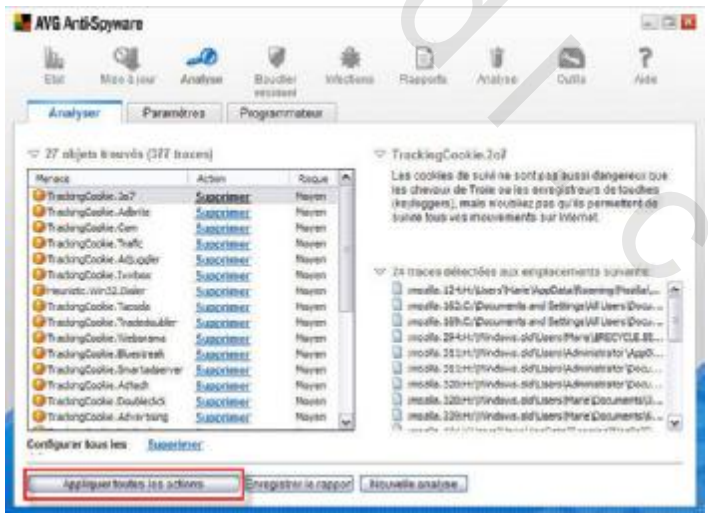
برنامج الحماية الشهير Killer Mobile[44]:

برامج الحماية الشهير

_Killer Mobile

7. **برنامج SmitfraudFix** [45]:

أداة صغيرة تقوم بحذف جميع الفيروسات وملفات التجسس الشهيرة الحجـــم: 1.79 MB



8. شركات التصنيع:

1- جدر النار
2- البوابات
3- برامج الحماية

Cellphone Makers Agree to Universal Charger

The world's ten major mobile phone manufacturers have agreed to produce a universal charger for users across Europe, with the first such chargers expected to be introduced on the EU market next year Read more (June 30, 2009)

www.wirelessguide.org

Home Page Technology Cell Phones All You Wanted to Know About Cell Phone Security

8. شركات الاتصالات :

تسجيل الشرائح واستخدام انظمة طويلة الأجل لتتبع الأجهزة

9. تنمية الوعي الشعبي:

عن طريق نشر الوعي والثقافة العامة للتوعية من أخطار الجهاز ومن جرائمة واستخدامه في الأغراض المفيدة والوقاية من الجريمة.

10. المكافحة البوليسية:

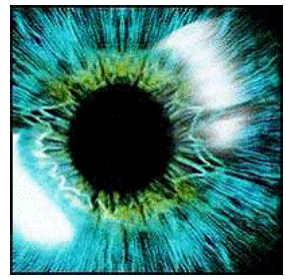
- الرقابة على المحلات.
- مراقبة الغش التجاري.
- التحقيق والمتابعة

11. الرقابة الجمركية:

أذا وجد جهاز رقابي متطور لمراقبة دخول الإجهزة منعا من الغش التجاري فإن الدول التي تقلد أجهزة الموبايل فلتقلد ما تشاء لوالرقابة تشمل المنافذ البرية والحرية والجوية.

12. استخدام البصمات الحيوية [46]:

نهاية التزوير: بصمات القز حية:Iris Recognition يتوقع القضاء على التزوير والتزييف باستخدام آليات غير تقليدية في الحماية مثل استخدام Iris Recognition بصمات القياسات الحيوية مثل بصمة القزحية ويمكن الإستيثاق للدخول ببصمة القزحية لأن البصمة فريدة لكل انسان بما فيها من مميزات.



13. التتبع بالأقمار الصناعية:

August 31, 2009

أنظمة التتبع للجريمة دخلت مرحلة متقدمة باستخدام التقنية والتي بواسطتها يمكن تتبع الموبايل في أي مكان بل ووصلت ليس على مستوي الامكانيات الضخمة في مامكانيلت البوليس بل اصبحت في جهاز الموبايل نفسه ففي التليفون الذكي iPhone وضعت أبل هذه الخاصية Find My iPhone helps track down robbers وكذلك شركات أخري كثيرة ويتم التتبع عن طريق أنظمة يحديد المواقع GPS (Global Postioning Systems) [47]. فيمكن متابعة اللصوص Robbers حالة سرقة الجهاز وفي حالة الجرائم الأخري وبمساعدة البوليس يمكن القبض على اللصوص وهذه الخاصية نظير اشتراك.

متابعة الموبايل بالأقمار الصناعية Mobile Phone Tracking through Satellite

تتبع الموبايل عن طريق تتبع شبكة الـــ GPS GSM mobile phone tracking system via the GPS TRACK satellite network

The system tracks mobile phones using GPS and GSM technology نظام تتبع الموبايل يستخدم تقنية الـــGPS , GSM

مع وجود هامش تقريبي للخأ[48].

هذا النظام على بعد 10 متر للموبايلات في اوروبا وبريطانيا و25 متر في الولايات المتحدة وامريكا الشمالية وكندا بينما 50 مترا في أي مكان فلا يمكن التتبع.GSM اخر والدول التي ليس بها تكنولوجيا الشبكات.

Track a phone number here

United States Select Country

هذا بحث النظام لغرض المعلوماتية فقط ولسنا مسئولين عن اساءة استعماله من المستخدم: Search

IMPORTANT: THE USE OF THIS SYSTEM IS FOR INFORMATIVE PURPOSES ONLY, WE ARE NOT RESPONSIBLE FOR ITS ABUSE BY THE USER.

14. كشف تزوير الصورة [49، 50] :

تتبع التغييرات التي حدثت بالصورة Trak all Changes للوصول الي أصل الصورة بأدوات التعرف على تزوير الصورة من خلال تطوير Adobe

(أ) الصورة الأصلية

(ب) الصورة مع تقليل الدخان

(ج) الصورة مع زيادة لهب

فطرق تزوير الصورة الرقمية هي:

5. الحذف بإخفاء الموجود
6. الإضافة باضافة أرقام أو مقاطع
7. القص (القطع) قص جزء كالأرقام والمقاطع أو الكتابة من صورة

القص واللصق (التركيب) هو أخطر أنواع تزوير الصورة الرقمية لأنه يبدل الصورة الحقيقية بصورة زائفة لم تحدث في مكان أو زمان للشخص المتهم.

15. محاربة التزييف[51]:

Fighting fakes

طبقاً لتقرير الإدارة الصينية للصناعة والتجارة تم رصد 12 نوع من اجهزة الموبايل الغير أصلية في أسواق العاصمة الصينية وهي:

The 12 types of mobile phones are the SnogErisscon W958c, SunyElicssonCECTi658, SunyElicssomP999, SunyElicssonW810i, ScnyEriossonZTC5680, NOKIA6030, NOKIA6630, NOKIA6681, NOKIA8800, NOKIAN70, NOKIAN-Gage, and NOKIAVERTU

وسيتم معاقبة البائعين للأجهزة المزيفة عند التعرف عليهم

Sellers of other fake mobile phones will also be punished once they are identified.

16. المكافحة القانونية:

في معرض الحديث عن جرائم الهاتف الجوال " المحمول" بالاستعانة بما يُعرف بـ "البلوتوث" ورد بجريدة المصري اليوم التي تصدر بجمهورية مصر العربية في عددها 1137 بتاريخ 19 أغسطس 2008 الخبر الذي أكدت فيه د.هدي حامد قشقوش أستاذ القانون الجنائي في كلية الحقوق جامعة عين شمس – إلي وجود فراغ تشريعي في كثير من الجرائم المتعلقة بالمعلوماتية وأكدت أنه لا يوجد قانون خاص بالمعلوماتية ككل باستثناء قانون واحد هو قانون التوقيع الإلكتروني.وفي الخبر نفسه أوضح د إبراهيم عيد نايل أستاذ القانون الجنائي جامعة عين شمس أن هذا النوع من الأفعال يمثل اعتداء على حرمة الحياة الخاص للأفراد وقد جرمه القانون طبقا لنص المادة 39 مكرر من قانون العقوبات[24].

نص نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية في مادته الثالثة على أنه يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد عن 500 ألف ريال أو بإحداهما على كل شخص يرتكب أي من الجرائم المعلوماتية المذكورة بالمادة والتي تضمنت فقرتها الرابعة "المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها[52].

يتطلب الدليل الجنائي الرقمي التقني الحماية اثناء البحث عنه وبعد ضبطه خوفا من العبث به أو الأهمال في تسجيله أو حفظه وتتمثل أجراءات استخراج الدليل في مراحل أربع هي[53]:

1. مرحلة إعداد وتجهيز المعدلت المستخدمة لإستخلاص الدليل.
2. مرحلة ضبط واستخلاص الدليل.
3. مرحلة حماية الدليل من التلف أو العبث بمحتواه.
4. مرحلة تقديم الدليل لأجهزة التحقيق والمحاكم.