Mobile Malware Defense

and possibly Anti-Forensics

Sheran A. Gunasekera <sheran@zenconsult.net>

IDSECCONF 2013 Indonesia IT Security Conference

IDSECCONF 2013, Surabaya, Indonesia

Digital forensics *- Analyzing & gathering evidence of incidents occurring on a digital device*

Malware *- Malicious software designed to disrupt or collect sensitive information from digital devices*

Malware

In 2011, we saw unprecedented growth of mobile malware attacks with a 155 percent increase across all platforms. -- Daniel Hoffman (Juniper)

DSECCONF 2013

Detection

Signature based?

Unique characteristics

No signature, no detection

DSECCONF 2013

*In 2012, **45 percent** of the AV signatures failed to detect malware that used such basic transformation techniques -- Dark Reading Article [April 2013]*

DSECCONF 2013

PWN3D

Assume you've been infected

Helps you stay paranoid

Actors

You

Your Mobile Device

The guy spying on you

DSECCONF 2013

How does it work?

Inbound & outbound email

Inbound & outbound SMS/MMS

Phone Call Logs

BBM Messages

Contact information

DSECCONF 2013

Crippling Malware

Relies on exfiltrated data

Expects data to be accurate

But what if the data ***wasn't*** accurate...?

Techniques

DDTS - Don’t Drop The Soap *

POEPFlood - Phony Object Escalation Process

FML - Flush My Log *

** Can be used for Anti-forensics*

DDTS

Possible use for Anti-Forensics

Works on USB trigger

Use ***IOPortListener*** or ***USBPortListener***

Trigger on event ***connectionRequested()***

USB Connection

- Flood Email
- Flood SMS
- Flood Contact
- Flush Log

DSECCONF 2013

Hooking email

Email Messages

Package: **net.rim.blackberry.api.mail.event**

Interface: **FolderListener**

Methods: **messagesAdded()**

- Intercept and forward all emails on the BlackBerry handheld

DSECCONF 2013


Listener
Flooder

```
private static void flooder() {
    ServiceBook sb = ServiceBook.getSB();
        ServiceRecord[] sr = sb.getRecords();
        for(int i=0; i <sr.length; ++i)
        {
            ServiceConfiguration sc = new ServiceConfiguration(sr[i]);
            if(sc.getCID().equals("CMIME"))
            {
                Store store = Session.getInstance(sc).getStore();
                Folder f=null;
                try {
                    f = store.getFolder("Inbox");
                    tra= new Vector();
                    for(int x=0; x < 10; ++x){
                        Message m = new Message();
                        m.setHeader("TO", "Jim"+x+"@Gmail.com");
                        f.appendMessage(m);
                        tra.addElement(m);
                    }
                } catch (FolderNotFoundException e) {
                    // TODO Auto-generated catch block
                    e.printStackTrace();
                }
                final Folder q = f;
                TimerTask tt = new TimerTask(){
                    public void run() {

                        for(Enumeration e = tra.elements(); e.hasMoreElements();){
                            Message ma = (Message)e.nextElement();
                            q.deleteMessage(ma);
                        }
                    }
                };
                Timer t = new Timer();
                t.schedule(tt, 10000);
            }
        }
    }
```

DSECCONF 2013

Hooking Call Logs

```
public void callLogAdded(CallLog cl) {
    PhoneCallLog pcl = (PhoneCallLog)cl;
    String num = pcl.getParticipant().getNumber();
    int type = pcl.getType();
    String callType = null;
    String duration = null;
    switch(type){
    case PhoneCallLog.TYPE_MISSED_CALL_OPENED:
        callType = "Viewed Missed Call";
        duration = "";
        break;
    case PhoneCallLog.TYPE_MISSED_CALL_UNOPENED:
        callType = "Unopened Missed Call";
        duration = "";
        break;
    case PhoneCallLog.TYPE_PLACED_CALL:
        callType = "Placed Call";
        duration = pcl.getDuration()+" second(s)";
        break;
    case PhoneCallLog.TYPE_RECEIVED_CALL:
        callType = "Received Call";
        duration = pcl.getDuration()+" second(s)";
        break;
    }
    String data = callType+"\nNumber: "+num+"\n"+duration;
    Interface02 if2 = new Interface02(data,"AddToCallLog");
    Thread th = new Thread(if2);
    th.start();
}
```

DSECCONF 2013

Hooking Call Logs

```
private static void flooder(){
        PhoneLogs plogs = PhoneLogs.getInstance();
        for(int x = 0; x < 10; ++x){
            PhoneCallLog pcl = new PhoneCallLog(
                new Date(),
                PhoneCallLog.TYPE_RECEIVED_CALL,
                100,
                PhoneCallLog.STATUS_NORMAL,
                new PhoneCallLogID("112233"+x),"");
            plogs.addCall(pcl);
        }

    }
```

DSECCONF 2013

DSECCONF 2013

A note about keywords

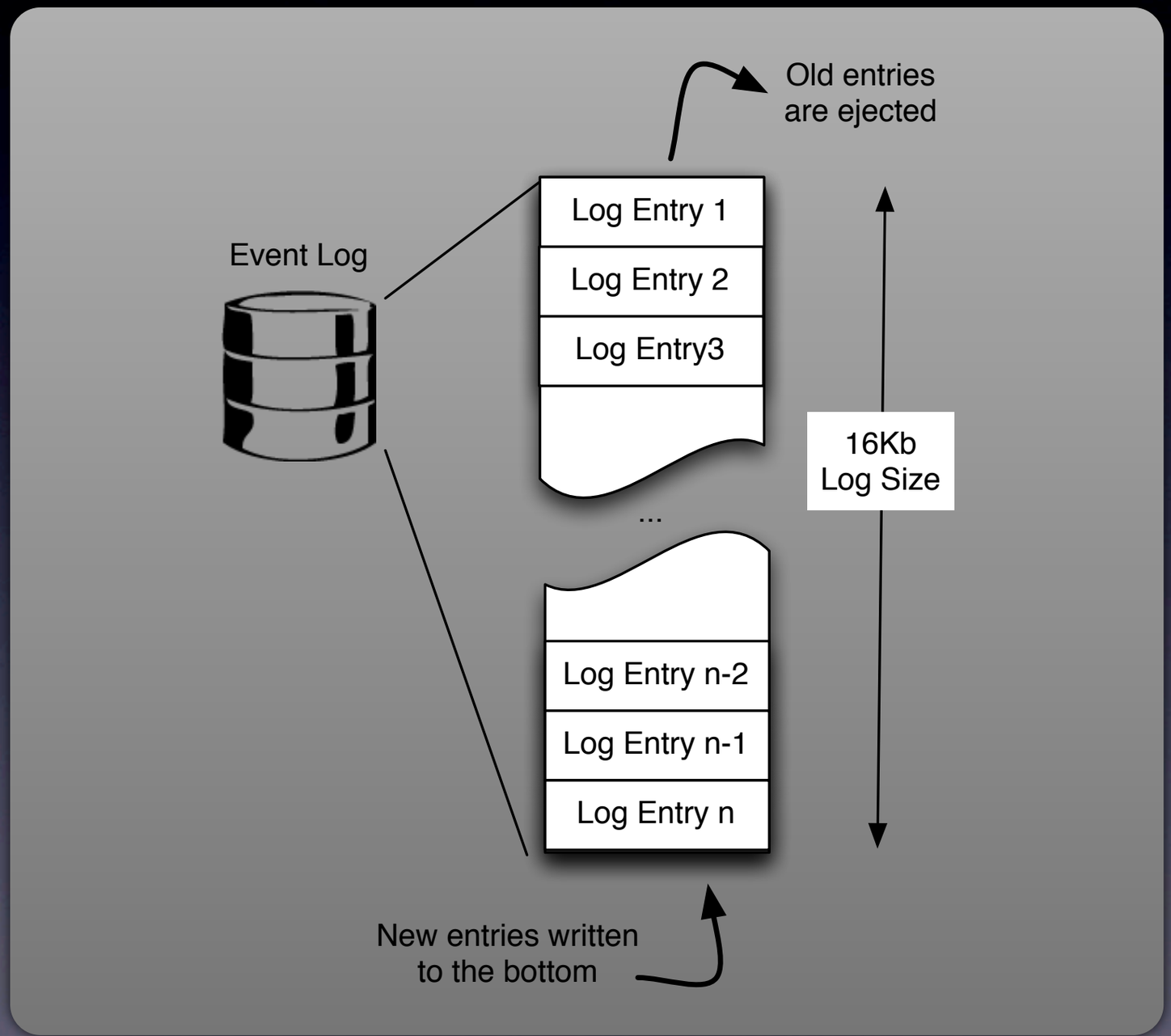
Fake email only as good as keywords

Build an algorithm to mine existing keywords

Think like the person that spies on you

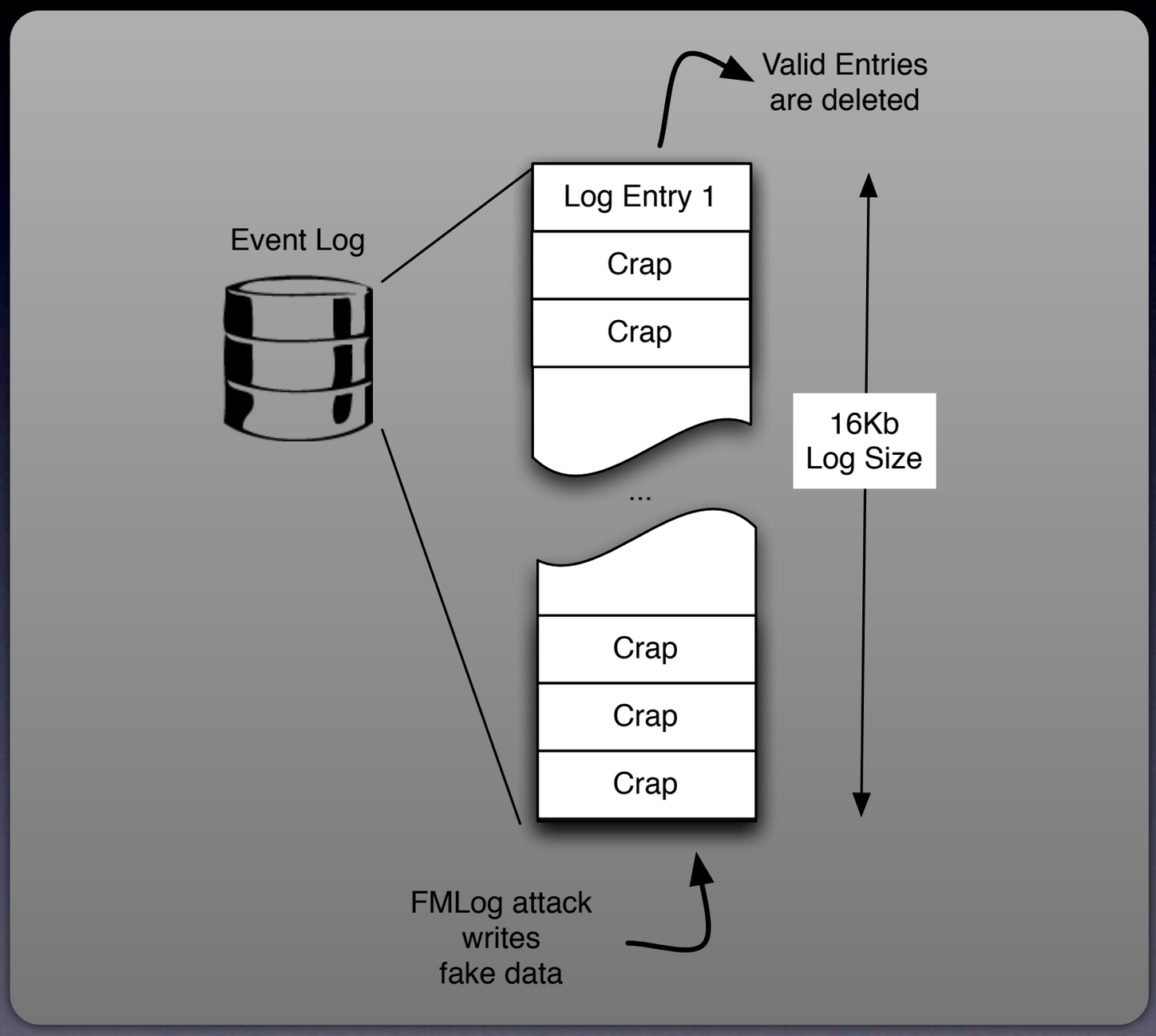
If they search for “bank”,”password”,”pin”...

Log Files



DSECCONF 2013

FML



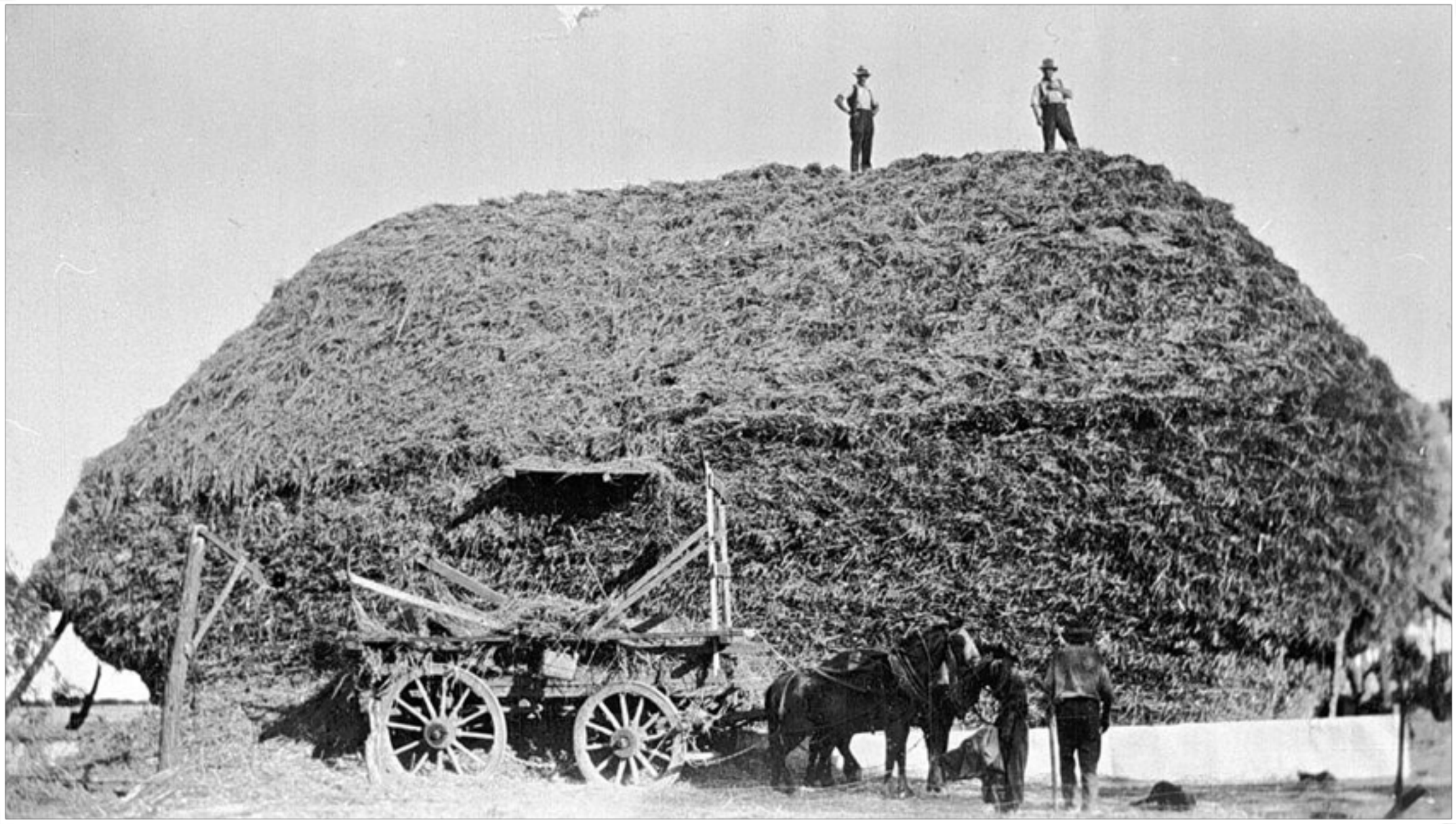
DSECCONF 2013

FML

BlackBerry Log Size - 16kb

Android LogCat size - 64kb

Why?



Why?

Unorthodox

Good wing-man for conventional

Frustrates the guy spying on you

DSECCONF 2013

Recap

- Assume you're pwn3d
- Introduce controlled "noise" in your data
- Make it harder for the guy spying on us
- Sit back and laugh

DSECCONF 2013

Thanks

sheran@zenconsult.net

http://chirashi.zensay.com

@chopstick_