



**Digital
Forensics
Investigation
Research Laboratory**



Linux and Law Enforcement Challenges and Opportunities

Dr. Joshua I. James

Digital Forensic Investigation Research Laboratory

SoonChunHyang University

Joshua@cybercrimemtech.com



<http://forensics.sch.ac.kr>
<http://dfire.ucd.ie/>

whoami



- Dr. Joshua I. James
 - Full-time Linux user for past 6 years
 - Develop “foss” tools for digital investigators [<http://cybercrimetechnology.com>]
 - Lecturer/Researcher SCH, KU, KNPU
 - Consultant: UNODC, INTERPOL, KNPA
 - Have trained Police / Prosecutors / Judges from over 100 countries on Digital Crime & Investigation
 - Focus on the automation of digital investigation processes



Overview



- What is 'normal' cybercrime?
- Linux for Criminals
- Linux for Law Enforcement
- Linux and Legal Systems
- The Law Enforcement *community*
- GitHub's impact on Law Enforcement
- Linux Education for Law Enforcement
- Conclusions



General Cyber Crime



- Cyber crime often targets **mass markets**
 - # of attacks against systems correlate to market share
 - Desktop: MS Windows to target users, OSX gaining attention
 - Servers: Linux-based & MS Windows-based
 - Mobile: Linux-based, iOS
 - Other embedded: Linux-based



General Cyber Crime



- Attacks against Linux-based systems
 - (Servers / Embedded) Mostly configuration issues
 - Software: Not enough app security testing in the community
 - Pick a community app, and fuzz it
 - Security testing is not easy
 - Client-side: Social engineering works great!
 - Mobile-device app permissions, sometimes helpful
 - Android targeted by an estimated 97% of malware in 2013[1] (third-party app stores, apk downloads)



General Cyber Crime



- For the average user, they don't notice they are infected until...
 - Their system stops working
 - Their bank account loses money
 - Phone bill is much higher than expected
- For the average SMB, they don't notice they are infected until...
 - Another company / org tells them
 - Their customers tell them
- Most people are infected, and will never know as long as the malware does not affect their 1) money or 2) user experience (much)



General Cyber Crime



- “Normal” cybercrime is actually pretty boring
 - Low-tech
 - Basic Fraud / IP theft / Illegal Content
- Advanced cybercrime usually related to organized crime and / or Governments
- Most advanced cybercrime is not detected / reported
- Police will normally only look at crimes their citizens are interested in



General Cyber Crime



- Advanced attacks don't necessarily mean advanced techniques

NEWS

Snowden accused of using hacking's greatest weapon to access NSA files: wget

Exfiltrated data said to be using previously unknown port 80. Experts remain amused by media hype.

<http://www.csoonline.com/article/2137013/network-security/snowden-accused-of-using-hacking-s-greatest-weapon-to-access-nsa-files--wget.html>



Linux for Criminals



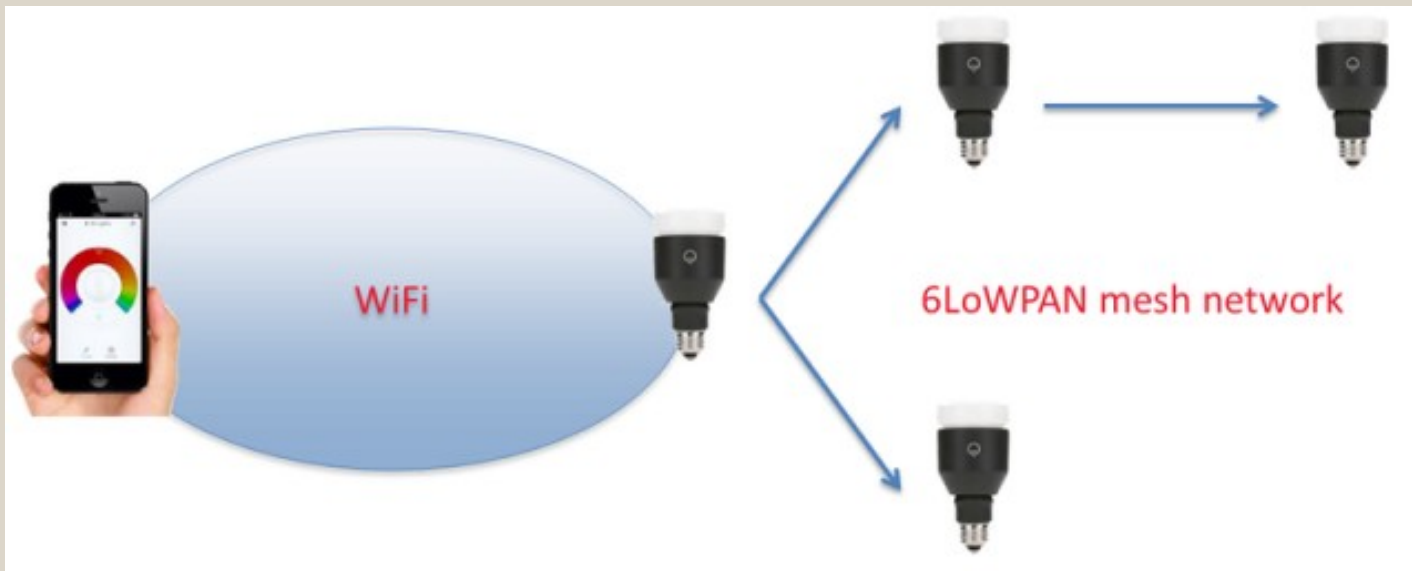
- Linux is perfect for criminals!
 - Extremely powerful
 - Completely customizable
 - Runs on almost anything
 - Excellent for automation
- Basic Linux understanding gives you all the tools you need to mess with systems / networks
- Network policies are normally applied to MS Windows systems – Linux lockdown is an afterthought (maybe)



Linux for Criminals



- Now everything is connected, and is used for illegal compute, information stealing, and just messing with people
- DDoS or full control of IoT networks so far is not difficult with basic sniffing ability (made easy in Linux): TV / Lights / Drones



<http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/>

Linux for Criminals



- Linux pre-configured for hacking (pen-testing)
 - Kali Linux [<http://www.kali.org/>]
 - It is awesome! / It is scary!
 - Anyone, even as a hobby, can easily learn basic security testing (and break stuff)
 - Netizens, hactivists and organized crime are learning
 - Governments and businesses are not



Linux for Criminals



- Criminals:
 - Have an interest in becoming *experts* at the technology
 - Linux / Unix / Windows / Phones / etc
 - Have incentive (money) to become experts
 - Individuals
 - Organized crime



Linux for Law Enforcement



- Law Enforcement:
 - Some have an interest in becoming *experts* in the technology
 - Expert level LE normally move to corporate
 - Many want minimum knowledge to do their job
 - Usually no extra incentive to learn new technologies
 - Many countries do not recognize / invest in cybercrime investigation
 - Many countries have corruption problems
 - Altruism only goes so far



Linux for Law Enforcement



- Law Enforcement:
 - Knowledge greatly depends on region, funding and level of country development
 - Incentives depend on Government
 - Investigation technology sometimes dictated by government or legislation
 - Always behind



Linux for Law Enforcement



- For cybercrime and digital forensics investigation, most countries are locked into MS Windows
 - Three most popular investigation toolkits are Windows-based
 - Most investigation tools are closed-source, commercial



Perception of Linux by LE / Gov.



- Law Enforcement in many countries believe commercial, MS Windows-based software is better for investigations
 - Point and click – easy to do a basic “investigation”
 - Easy to understand commercial software licensing and business models



Perception of Linux by LE / Gov.



- Practical:
 - Linux is HARD
 - What is this CLI stuff?
 - Too many commands - “so hard to remember!”
 - Piping?
 - “I am not a programmer!”
 - Not easy to get started
 - Communities can be very good and very bad



Perception of Linux by LE / Gov.



- Legal:
 - Evidence derived from Linux / Open Source tools *might* be accepted in court
 - Depends on the country
 - Depends on the confidence / competence of the investigators
 - Difficult to trust Linux
 - Who will stand up for Linux in court?
 - Belief that Linux is made by hackers in their mom's basement
 - Community models and licensing models are really, really confusing



Perception of Linux by LE / Gov.



- Legal (cont):
 - Some (few) countries actually **prefer** Open Source tools for investigations
 - **Italy**: gives priority to free and open source tools for investigations
 - Why? We can check the source to see exactly what the code is doing
 - Third-parties can verify the code is working as expected

For an interesting discussion, please see: http://www.digital-evidence.org/papers/opensrc_legal.pdf



Linux for Law Enforcement



- Investigators using Linux:
 - Tend to develop their own tools / systems
 - Automate more of their work
 - Are very active in investigation and learning
 - Have support from management
- Expert investigators choose whatever tool works best, regardless of platform (for some tasks commercial, closed-source is necessary)



Linux for Law Enforcement



- Cybercrime Investigation
 - Usually involves understanding network traffic and routing
 - Linux systems have a lot of tools available for network analysis
 - Systems can easily be employed to collect network traffic (good or bad)
 - Many of the VPN/Proxy/Tor/Web servers from which LE get their logs are Linux/Unix-based



Linux for Law Enforcement



- Digital Forensic Investigation
 - Normally involves text / data analysis
 - Must be able to analyze many different data structures
 - Need to sort massive amounts of data for each case
 - Linux has free, built-in tools that are better for some types of digital forensic analysis than expensive commercial tools
 - Experimental digital investigation tools are normally developed on (or compatible with) Linux systems
 - Scripting languages (Perl/Python) very popular with LE



Law Enforcement Community



- Quite closed
 - Difficult to share information
 - Difficult to share data
 - Many tools and courses developed “for Law Enforcement only”
- Many LE believe that criminals don't know their techniques
 - Criminals are way ahead



Law Enforcement Community



- Open Source Law Enforcement community is gaining popularity
- Many open source / FOSS projects are being created for digital investigation purposes
- Part of the popularity comes from the “Open Source Digital Forensics Conference” (OSDFcon) held by Basis Technology (USA)[2]
- Increased interest is also coming from
 - Open Source Hardware projects
 - Easier consumer-level customization
 - Better online instructions



Open Source Tools



- A number of the most popular Linux-based open source tools include:
 - The Sleuth Kit <http://www.sleuthkit.org/>
 - Guymager <http://guymager.sourceforge.net/>
 - Digital Forensics Framework <http://www.digital-forensic.org/>
- Live CD distributions:
 - DEFT <http://www.deftlinux.net/>
 - CAINE <http://www.caine-live.net/>
 - KALI <http://www.kali.org/>
- Many “investigation automation programs” are built on top these systems
- Linux can already handle a lot of investigation tasks 'out-of-the-box'
- Again, many popular tools are cross-platform
 - Investigators need to support data collection and analysis on every kind of device



Open Source [Hardware] Tools



- As hardware components become less expensive, investigators can begin to build custom devices for investigation
- FIREBrick <http://digitalFIRE.ucd.ie>
 - Hardware write blocker
 - Disk imaging up to 5Gb/min
 - Internal storage mirroring and encryption
 - Free, Open source firmware
 - Fully customizable
 - Can be built for ~185USD
 - Comparable commercial kits ~1,500USD



FIREBrick Forensic Write Blocker



Open Source [Software] Tools



- Automated Network Triage (ANT)
 - Based on Ubuntu
 - Uses gPXE to boot systems over the network
 - Automates keyword and hash search on all network-booted systems
 - Basically a collection of bash scripts
 - Minor client kernel mod (no disk write)
 - More advanced than many systems available today
 - Free and Open Source... but Law Enforcement only



How GitHub has changed things



- GitHub has (unknowingly?) helped police get easier access to new software tools that can be used for their investigation
 - If they know how to look
- GitHub interface is (arguably) easier and more approachable than other versioning systems
- It is easier to get in contact with developers that started projects
- Unless you use the paid service, projects must be public
 - Academics likely to make most repositories public
 - Practitioners more likely to share code since GitHub is easy (depends on culture)
- BUT: contributing back is still a challenge



Linux and LE Education



- Linux / Tech. Education
 - Helps improve investigations (justice)
 - Help improve societies (trust)
 - Helps improve global economy (cooperation)



Linux and LE Education



- Global Linux / Open Source education for Law Enforcement is not easy:
 - Language
 - Time
 - Starting ability
 - Support
 - Cost
- Great course: edX – LFS101x.2 (Linux Foundation)
<https://www.edx.org/course/linuxfoundationx>
 - Excitement from European LE
 - U.S. has good support
 - What about the rest of the world's LE? How can we include them?



Linux and LE Education



- Training courses:
 - Teach free, open source investigation tools for investigators
 - Usually very difficult at beginning
 - A lot of resistance (show us X commercial tool instead)
 - Commercial tools have associated certifications; home-grown FOSS investigation tools don't
 - What is the benefit to the investigator for taking extra time to learn Linux?



Conclusions



- Few Law Enforcement organizations (Govs) understand what Linux is, and what it can do for them
 - Power / Flexibility / Cost Reduction / Security
- Few Investigators are confident enough about their Linux abilities to support it (or FOSS) in court
- Linux support for LE needs to be more formalized than 'geek' interest communities
- Linux needs to be advocated to top-level Government officials / judges for better acceptance



Conclusions



Most importantly, a real community of Linux professionals - with a goal to include Law Enforcement - needs to be promoted and supported

- Such a community somewhat exists in U.S. and Europe
- Cybercrime is global, and Linux is the perfect tool to help fight it, regardless of available budgets



References

- 1) <http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/>
- 2) <http://www.basistech.com/osdfcon/>

