Exploring the Landscape of Cybercrime

Zinaida Benenson, Andreas Dewald, Hans-Georg Eßer, Felix C. Freiling, Tilo Müller, Christian Moch,
Stefan Vömel, Sebastian Schinzel, Michael Spreitzenbarth, Ben Stock, Johannes Stüttgen
Friedrich-Alexander-University Erlangen-Nuremberg, Germany
www1.informatik.uni-erlangen.de

***Abstract*—This document gives an overview over current research within the security group at Friedrich-Alexander-University Erlangen-Nuremberg, Germany, and attempts to describe the future research roadmap of the group. This roadmap is structured around the *landscape of cybercrime* with its three main groups of actors (attackers, users and investigators) and their main activities and deficits: attack and evasion for attackers, awareness and education for victims, evidence extraction and analysis for investigators.**

I. Introduction

Cybercrime is a growing phenomenon, however also one that still waits to be fully understood [1], [2]. Roughly speaking, cybercrime is crime in cyberspace, where cyberspace is a social space whose infrastructure is formed by digital internetworked computers.

The amount of crime involving digital systems is steadily increasing. This involves both more traditional crime in which digital systems are merely used as tools (e.g., different types of fraud, blackmailing, hidden communication) as well as new forms of crime in which digital systems are an enabling technology (e.g., computer abuses, malicious software, malicious remote control networks like botnets). Both forms of cybercrime correspond to two types that have been identified in the literature [2], [3]: crime that is more oriented towards people (e.g., cyberstalking) and crime that is more oriented towards computers. We focus on the latter type of cybercrime which is far from being well understood.

Much of cybercrime can be characterized by an economic motivation where cybercriminals "hack for profit", thereby forming an underground economy of considerable size [4], [5]. This, however, makes them behave in a rather rational manner and contrasts cybercrime from notions like cyberwar or cyberterrorism in which crimes either do not make a cost/benefit caluclation or are politically motivated.

This document aims at describing the current and future research roadmap of the security research group at Friedrich-Alexander-University Erlangen-Nuremberg, Germany. The major part of this group was affiliated previously with the University of Mannheim, Germany. The relocation to Erlangen gave us the possibility to re-focus our research agenda and form a new joint group vision which we wish to communicate to the systems security research community.

Our vision is structured around the *landscape of cybercrime* with its three main groups of actors (attackers, users and investigators) and their main activities and deficits:

1) attack and evasion for attackers,
2) awareness and education for users,
3) evidence extraction and analysis for investigators.

II. The Landscape of Cybercrime

As mentioned in the introduction, cybercrime is crime that happens in cyberspace. Cyberspace is here understood as the "digital world" in which many people spend a non-negligible part of their daily life. For simplicity, we visualize cyberspace as an unstructured but clearly distinguishable realm in the landscape of cybercrime (see Fig. 1).

A. Actors

Since crime always relates to the physical world, there is no crime that happens *entirely* in cyberspace. There are always humans that act or are acted upon. In this context, we identify three groups of actors in cyberspace:

1) Attackers: Humans that act in an offensive manner, i.e., practice attack and evasion techniques. Such humans can be cybercriminals or security researchers who impersonate the role of adversaries in order to test certain computer systems for weaknesses (penetration testing).
2) Users: Humans who are acted upon and suffer from the actions of the first group. People belonging to this group are often called victims.
3) Investigators: Humans who try to understand and investigate the activities of the two previous groups. These people can be thought of as security researchers from academia or investigators of law enforcement agencies.

There is no sharp distinction between these three groups. For example, security researchers can belong to all three groups, depending on what they are doing. Although we think that ethics are an important topic, note that in our distinction we try to avoid *malicious intent* as a defining attribute of any of these groups. Nevertheless, any scientific activity should be governed by ethical considerations. This is especially crucial if scientists play the role of attackers, as we explain below.

B. Activities

The classification of the groups described above implies a characteristic set of activities for each participant that we will outline in more detail in the following (see Fig. 1).

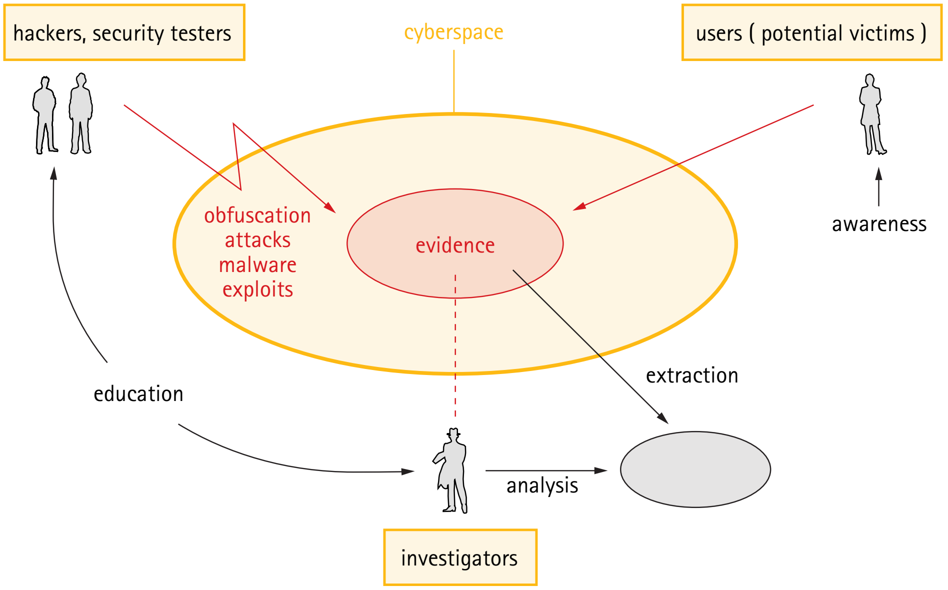

Figure 1. The Landscape of Cybercrime with its Actors.

1) Attackers: Attackers practice offensive thinking, i.e., they look at systems with the intent to break (into) the system. This can result in penetration or security testing, employing techniques like fuzzing or source code analysis, identifying vulnerabilities, and finally producing exploits that can be used to automate attacks with the help of malicious software. Such software must again be protected by evasion or obfuscation methods that may lead to attacks which are hard to detect and mitigate.

2) Users: Users “use” networked digital systems. Depending on their proficiency, they (should) practice reasonable conduct in cyberspace and employ attack detection and attack mitigation techniques (antivirus software, intrusion detection, cryptography, etc.). In case of security incidents, they should also practice basic incident response activities. All this depends on the education and awareness of the users.

3) Investigators: Investigators (pro)actively investigate security incidents in cyberspace. They prepare for incident response through training, they collect evidence created by attackers and users, the analyze said evidence and try to find out what actually happened. Typical activities of investigators are reverse engineering, logfile analysis, development of incident response and digital forensics tools, as well as documentation of their activities.

III. Current and Future Research Areas

We now present relevant research areas which are important to us in current and future research. We structure these areas according to the classes of actors described above.

A. *Develop and Cultivate Offensive Technologies*

This area corresponds to the class of attackers described above. We now describe current research we are currently exploring.

1) Current research activities: Penetration testing is a widely used approach to assess the security of real-world systems by attacking them. The penetration tester tries to actively push the system to an insecure state by accessing it in a way that was not foreseen by the system’s designer. Interestingly, there is little work that passively monitors a system and infers secret information from the behavior of the system. These passive attacks are well known in cryptology under the name “side channnel attacks”, but little known for large systems such as business applications. We investigate the following research questions [6]:

- How to detect side channel information leaks in large software systems?
- How to decode the information leaked through a side channel?
- How to prevent and mitigate information leakage through side channel vulnerabilities?

We also investigate anti-forensic techniques to protect data on disk or in memory. This includes our work on AESSE [7], a system for memory analysis resistant [8]–[10] disk encryption. In this context we also look at obfuscation techniques that extend the capabilities of current malware to withstand reverse engineering.

We also extend the global malware analysis system from the InMAS project [11] and make it accessible through the website mwanalysis.org. The website offers a dynamic malware analysis based on CWSandbox [12] and is a source for a large set of new and interesting malware.

2) Future research directions: Future research directions that interest us are the following:

- Speculate and validate future malware techniques, e.g., in the areas of obfuscation and anti-reverse-engineering. As examples we wish to investigate RAM encryption based on AESSE [7] to improve memory analysis resistance.

- Building systems that resist other specific attacks on disk encryption, e.g., bootkit attacks (stoned bootkit, evil maid attacks).
- Attacking non-standard hardware like real-world sensor network systems [13]. Wireless sensor networks are already being used in such critical domains as monitoring of offshore oil rigs and such networks often turn out to be quite sloppily specified and prorammed.

B. Awareness and Education

This area corresponds to the class of users described above.

1) Current research activities: We investigate issues of the psychology of security. Technical means for achieving IT security have been steadily improving over the decades. Therefore, the main weak point in securing computer systems is shifting from the technology to the psychology [14], [15]. We examine what people think and feel about computer security and why they think and feel this way. The main goals of this research is to understand why people cannot use the current systems in a secure way.

Another aspect of our current research is usable security. Currently, users perceive security mainly as an interruption of their primary tasks [16], [17]. The main goal of our research on usable security is to find out how to make security not a nuisance but a service. How can security goals and methods be communicated in an appealing and understandable way? How can people develop a feeling for security and insecurity in the digital world?

2) Future research directions: In future research we wish to improve research-orientation in training and education so that users (and investigators) are not so much restricted by their tools. We also develop a specifically offensive education curriculum for undergraduate and graduate students.

C. Foundations of Forensic Computing

Forensic computing (sometimes also called *digital forensics*, *computer forensics* or *IT forensics*) is a branch of forensic science pertaining to evidence in cyberspace. Forensic computing aims at identifying, preserving and analyzing digital evidence after a security incident has occurred. As in other forensic sciences, investigators attempt to establish hypotheses about previous actions and try to falsify them based on traces of actions left at the scene of the crime.

Like in other forensic sciences, the emergence of forensic computing was mainly driven by practitioners trying to satisfy immediate needs within concrete digital investigations. Now that many universities, mainly from North America, have started to establish degree programs and research labs in this area, forensic computing is increasingly profiting from research knowledge and the scientific methods developed in computer science, but there is still a lot of potential [18].

1) Current research activities: The current research topics of the group encompass the following activities.

An important benefit of science's participation in digital forensics is the insight that digital forensics has much more in common with traditional forensics than its pioneers assumed. From this perception, we form a foundation of forensic computing and develop new approaches based on the experience of traditional forensic science [19].

In this context we develop tools and techniques in evidence collection and evidence analysis, for example:

- We examine traces of volatile information in main memory. These approaches complement persistent data-oriented techniques and may be of indispensable help when dealing with encrypted disks or sophisticated types of malicious applications that solely reside in RAM. For this purpose, we evaluate existing frameworks for memory acquisition and analysis (e.g., Volatility [20]) and extend their functionality.
- We develop a tool called ADEL [21] for the analysis of smartphones with a major focus on Google's Android platform. ADEL is able to dump and analyze SQLite databases from a connected smartphone.
- We are also developing a technique called *selective imaging*, which is the creation of partial forensic images by selectively acquiring only relevant data from digital devices [22]. While selective imaging has already been researched on a per-file basis [23], we work on achieving arbitrary granularity of selection to enable the application of this technique, even in complicated cases. The resulting evidence containers require accurate provenance documentation [24] and precise verification procedures, which we are currently developing to achieve the same level of reliability as with common sector-wise images [25].

We also investigate techniques to better educate and train investigators, taking the foundations of forensic computing as the primary basis. For this, we are using the Forensic Image Generator Generator tool (Forensig^2) [26]. This is a tool to reduce the creation time of an artificial forensic image to a minimum without losing the "ground truth" of the image content. Therefore the author of the image has to write a script describing the artificial image. The scripting language is similar to Python.

The primary aim of this tool is for education purposes, generating artificial images for apprentice forensic investigators. However, the use of the tool is not limited to this scope, it is also a very handy tool for open research questions. The ability to generate huge amounts of similar but not identical images makes it possible to test the difficulty of a certain forensic problem, to quantify the knowledge of an investigator, to evaluate different teaching approaches, and to answer many more unanswered research questions.

2) Future research directions: Future research directions that interest us are the following:

- Analysis of "non-standard" digital technologies (Solid State Disks, Flash Memory, SCADA systems, sensor networks, Firewire, Thunderbolt, etc.)
- Investigate fundamental tradeoffs in technically unavoidable evidence. The example of caches (in their many forms) shows that there is a tradeoff between performance (using a cache) and not creating evidence (not using a cache).
- The general question of quantification and empirical research of correlations between evidence and actions is still largely open.
- Developing new types of reverse engineering approaches for larger software systems like complex applications (e.g., relating certain actions to evidence) together with the software (re-)engineering community.

References

[1] D. Wall, *Cybercrime*. Cambridge: Polity Press, 2007.

[2] S. W. Brenner, *Cybercrime: criminal threats from cyberspace*. Santa Barbara: Praeger, 2010.

[3] S. Gordon and R. Ford, "On the definition and classification of cybercrime," *Journal in Computer Virology*, vol. 2, no. 1, pp. 13–20, 2006.

[4] R. Thomas and J. Martin, "The underground economy: Priceless," *The USENIX Magazine*, vol. 31, no. 6, pp. 7–16, 2006.

[5] J. Spoenle, "Underground economy," in *Current Issues in IT Security*, M. Bellini, P. Brunst, and J. Jähnke, Eds. Berlin: Duncker & Humblot, 2010, pp. 67–79.

[6] S. Schinzel and F. C. Freiling, "Detecting hidden storage side channel vulnerabilities in networked applications," in *Proceedings of IFIP SEC 2011*, 2011.

[7] T. Müller, A. Dewald, and F. Freiling, "AESSE: A Cold-Boot Resistant Implementation of AES," in *Proceedings of the Third European Workshop on System Security (EUROSEC)*. Paris, France: ACM, Apr. 2010, pp. 42–47.

[8] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest We Remember: Cold Boot Attacks on Encryptions Keys," in *Proceedings of the 17th USENIX Security Symposium*, Princeton University. San Jose, CA: USENIX Association, Aug. 2008, pp. 45–60.

[9] B. D. Carrier and J. Grand, "A Hardware-Based Memory Acquisition Procedure for Digital Investigations," *Digital Investigation* , vol. 1, no. 1, pp. 50–60, Feb. 2004.

[10] M. Becher, M. Dornseif, and C. N. Klein, "FireWire - All Your Memory Are Belong To Us," in *Proceedings of the Annual CanSecWest Applied Security Conference*. Vancouver, British Columbia, Canada, 2005.

[11] M. Engelberth, F. C. Freiling, J. Göbel, C. Gorecki, T. Holz, R. Hund, P. Trinius, and C. Willems, "The InMAS Approach," in *Proceedings 1st European Workshop on Internet Early Warning and Network Intelligence (EWNI)*, 2010.

[12] C. Willems, T. Holz, and F. C. Freiling, "Toward automated dynamic malware analysis using CWSandbox," *IEEE Security & Privacy*, vol. 5, no. 2, pp. 32–39, 2007.

[13] A. Becher, Z. Benenson, and M. Dornseif, "Tampering with motes: Real-world physical attacks on wireless sensor networks," in *Proceedings Security in Pervasive Computing*. Springer, 2006, pp. 104–118.

[14] R. West, "The psychology of security," *Commun. ACM*, vol. 51, pp. 34–40, April 2008. [Online]. Available: http://doi.acm.org/10.1145/1330311.1330320

[15] B. Schneier, "The psychology of security," http://www.schneier.com/essay-155.html, 2008.

[16] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[17] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the 28th international conference on Human factors in computing systems (CHI)*. New York, NY, USA: ACM, 2010, pp. 383–392.

[18] S. L. Garfinkel, "Digital forensics research: The next 10 years," in *Proceedings of the Digital Forensics Research Conferencs (DFRWS)*, 2010.

[19] K. Inman and N. Rudin, *Principles and Practice of Criminalistics: The Proefssion of Forensic Science*. Boca Raton: CRC, 2000.

[20] Volatile Systems, LLC, "The volatility framework: Volatile memory artifact extraction utility framework," 2008. [Online]. Available: https://www.volatilesystems.com/default/volatility

[21] F. C. Freiling, S. Schmitt, and M. Spreitzenbarth, "Forensic Analysis of Smartphones: The Android Data Extractor Lite (ADEL)," in *Conference on Digital Forensics, Security and Law*, 2011.

[22] P. Turner, "Selective and intelligent imaging using digital evidence bags," *Digital Investigation*, vol. 3, pp. 59–64, 2006.

[23] M. Bäcker, F. Freiling, and S. Schmitt, "Selektion vor der Sicherung," *Datenschutz und Datensicherheit*, vol. 34, no. 2, pp. 80–85, 2010.

[24] P. Turner, "Digital provenance-interpretation, verification and corroboration," *Digital Investigation*, vol. 2, no. 1, pp. 45–49, 2005.

[25] E. Kenneally and C. Brown, "Risk sensitive digital evidence collection," *Digital Investigation*, vol. 2, no. 2, pp. 101–119, 2005.

[26] C. Moch and F. C. Freiling, "The forensic image generator generator (forensig2)," in *Fifth International Conference on IT Security Incident Management and IT Forensics (IMF)*, IEEE Computer Society, 2009, pp. 78–93.