New Comprehensive Taxonomies on Mobile Security and Malware Analysis

Gürol Canbek[1,2], Seref Sagiroglu[3] and Nazife Baykal[2]

[1]HAVELSAN, Mustafa Kemal Mh. 2120 Cd. No:39
06510 Cankaya, Ankara, Turkey. Tel: +90-312-2195787. e-mail: gcanbek@havelsan.com.tr
[2] Informatics Institute, Middle East Technical University, Universiteler Mh. No:1
06800, Cankaya, Ankara, Turkey. e-mail: baykal@metu.edu.tr
[3]Computer Eng. Dept., Gazi University, 06500, Maltape, Ankara, Turkey. e-mail: ss@gazi.edu.tr

Abstract—Taxonomies are known to provide a systematic classification of elements in a particular domain and can be efficiently used to express concepts in a structural manner. Unfortunately, security literature witnesses a few taxonomies having about 40 nodes on average in mostly a narrowed scope and maximum of 25 nodes on mobile scope only. This study surveyed security related taxonomies with quality criteria and proposes new comprehensive mobile security taxonomy and mobile malware analysis subtaxonomy having over 1,300 nodes from not only defensive but also offensive point of view. We have developed new leveling scheme and taxonomic enumeration notation for taxonomies in general and proposed a new definite method to build security taxonomies. We have also visualized our taxonomies for researchers, security professionals, practitioners and even common end users to provide comprehensible, well structured, and handy maps and provided two real-case examples illustrating their application. As privacy and security threats and vulnerabilities dynamically increase and diversify, these new taxonomies would help to see the entire perspective of mobile security without losing any details and present new practical perspective to bring mobile computing and cyber security disciplines closer.

Keywords—Taxonomy, Mobile Security, Mobile Malware Analysis, Cyber Security, Visualization.

1. Introduction

Mobile computing combines many inventions that are useful for humankind into a single platform. While all these technological advances mobile computing further and people use mobile devices in everywhere, unprecedented security risks also arise. According to the report published by World Economic Forum [1], "unforeseen consequences of new life science technologies" such as mobile technologies along with "cyber attacks" such as mobile malware were two of the global increasing risks from 2012 to 2013. The perception became even greater in 2015; the risk of cyber attacks with data fraud or theft increases [2]. In the latest report [3], mobile Internet and machine-to-machine connections are two under-protected areas and large-scale malware could cause large damages in economic, geopolitical, and the trust in the Internet. In another annual report [4], mobile applications becoming the main route for compromise are the 6th prominent threat estimated in 2016.

While the diversity in the capabilities as well as the convergence in mobile platforms obviously present many opportunities to users, they also ex-

pose a very large attack surface to malicious people. Therefore, mobile security should be the critical and indispensable part of information or cyber security in general. The subject, which we shall call as 'mobile security', is actually the security for mobile computing, technology, environments, platforms and devices.

Achieving a certain level of mobile security is not easy. The asymmetry between attacking and securing mobile environments necessitates seeing the whole. As Sun Tzu's 'know the enemy and know yourself' concise philosophy indicates, attackers and their techniques should also be focused. In brief, mobile security should be a holistic process that requires seeing the big picture all the time.

Taxonomy is known as a systematic method to define the big picture. As elaborated in Section 2, security taxonomies in the literature could not go beyond a guide including just a basic level of orientation to a main subject. Unexpectedly, we have encountered many studies titled as taxonomy but they actually enumerate just a few elements, whereas taxonomies on such broad phenomena should provide enough breadth and depth level. Unlike the previous studies, the aim of this study is to provide a new perception on taxonomy for mobile security and mobile malware analysis from not only defensive but also offensive points with a well-established terminology and a visual representation. To the best of our knowledge, this is the first attempt to analyze mobile security systematically together with malware analysis with such a broad scope and even covering many aspects of information security or cyber security at the same time.

Significantly, we have also proposed a comprehensive taxonomy that establishes basic set of concepts and a common language, which are essential for providing 'shared understanding in security community to test the hypotheses and to validate the concepts' [5].

The main contributions of this article are summarized as follows:

- surveyed 28 taxonomy studies of 25 years on security with their quality criteria and limitations,
- developed a new leveling scheme, adopted a new notation and templates for taxonomic enumerations which can be used not only for security but also other domains,
- suggested a novel definite method as a UML like use and misuse case diagram to systematically design a (mobile) security taxonomy,
- proposed new two taxonomies on mobile security with defensive and offensive aspects in 1,322 nodes namely 'mobile security taxonomy' including 'mobile malware analysis subtaxonomy' with extensive list of mobile specific assets and payloads,
- employed visualization techniques on the taxonomies for enhancing understanding and usability, and finally
- demonstrated some real-case examples on taxonomy usage for security practitioners.

The rest of the paper organized as follows. Section 2 surveys the existing 28 security taxonomies about attacks, incidents, malware, security, threat, and vulnerabilities mostly in the last 25 years. It explains our new leveling scheme and taxonomic enumeration notation proposals employed in taxonomies in general, describes the quality criteria of security taxonomies and discusses the major obstacles to achieving a truly useful mobile security taxonomy. Section 3 describes our novel definite method employed in our mobile security taxonomy design. Section 4 summarizes the high-level structure of the proposed taxonomy. The section also introduces the conceptual mobile security classes underlying the mobile security taxonomy and core

classes in detail with different visual representations including a big mind map of the taxonomy for the first time. Section 5 summarizes the proposed subtaxonomy on mobile malware analysis. Section 6 gives two detailed examples of real-case scenario to understand the usage of the taxonomies. Section 7 expresses the results and gives some statistics about the size of taxonomic elements. This section also compares the proposed taxonomies with other taxonomies in a quantitative and qualitative manner. Section 8 provides the discussion on the benefits, limitations, potentials, and challenges of the proposed taxonomies and the possible future works. The last section summarizes the contribution of this study and draws some conclusions.

2. Security Taxonomy Survey

In the literature, there are few examples of taxonomy studies on security, whether named as information security, mobile security, or cyber security. The summary below lists the taxonomies of the 28 studies from 1993 to 2015 and their contents. Before interpreting these taxonomies, let us now look at a specific unaddressed problem regarding to structuring the taxonomy and enumerating (i.e stating or listing) the taxonomy contents verbally rather than visually.

2.1. New Taxonomy Leveling Scheme and Taxonomic Enumeration Notation Proposal

In biological classification, where the first examples of taxonomies were used, there are eight ranks (i.e. relative level of a biological units) in a taxonomic hierarchy namely ‘domain’, ‘kingdom’, ‘phylum’, ‘class’, ‘order’, ‘family’, ‘genus’, and ‘species’ from top to bottom based on Linnean’s work [6]. Taxonomies in general consist of classes under which lower level contents exist. We have not found a specific approach for presenting the taxonomies verbally in our literature review.

The reviewed studies present taxonomy contents in a simple hierarchical chart visually or in a table or bullet points verbally. They do not follow a specific leveling scheme. However, a compact and standardized form is important for especially large taxonomies.

We have developed a new leveling scheme for enumerating taxonomy contents. We name the contents from top to bottom as ‘class’, ‘subclasses’, ‘elements’, ‘subelements’ (or ‘examples’), ‘attributes’, ‘subattributes’, ‘features’, and ‘subfeatures’ in order to define the formal levels. We refer all of them as ‘nodes’ in total eight levels like eight ranks in biology. We have also adopted a new notation for enumerating taxonomic units in verbal style that is described in Table 1.

We found that this leveling scheme and notation quite useful to specify and understand taxonomy contents and their levels quickly in a compact verbal form as applied in the Summary. This formal notation, which is both human and machine readable, could also be used to parse, import and export taxonomy contents.

2.2. Security Taxonomies

The first part in the Summary denotes the specific security domain on which the surveyed taxonomy classifies. It also summarizes basic metrics related to size and high-level structure of the taxonomy (number of classes, subclasses, or total size). The remaining part lists the content of the taxonomy by using our new notation and shows its sub metrics (size of the low-level structure).

As seen in the Summary, the taxonomies are mainly related to attacks [7], [8], [9], [10], incidents [11], [12], [13], [14], malware [15],

threats [16], vulnerabilities [17], [18], [19], [20], and security in broader scope [21], [22], [23], [24]. Lough surveys even the earlier taxonomic studies date back to 1975s on attacks or misuses [19].

SUMMARY:
Security Related Taxonomies (1993–2015)
Security Domain (Metrics) [Reference]
Class(es), Sub Nodes (SC, E, SE, A, SA, F, SF) # Sub Metrics

- **Security Flaws on Computer Programs** (3 C, total 50 N) [18]
  Genesis (Intentional; Inadvertent); **Time of Introduction** (Development; Maintenance; Operation); **Location** (Software, Hardware)
- **UNIX and Network Vulnerabilities** (6 C) [17]
  Vulnerability (Nature of the flaw based on protection analysis [25]); **Time of Introduction** # based on [18]; **Exploitation Domain**; **Effect Domain**; **Minimum Number of Components for Exploitation**; **Source** # reference to information on identification of vulnerability
- **Misuse techniques for intrusion** (9 C and 26 SC) [7]
  External Misuse; **Hardware Misuse**; **Masquerading**; **Setting Up Subsequent Misuse**; **Bypassing Intended Controls**; **Active Misuse of Resources**; **Passive Misuse of Resources**; **Misuse Resulting From Inaction**; **Use as an Indirect Aid in Committing Other Misuse**
- **Incidents on CERT** CERT: Computer Emergency Response Teams (5 C, total 28 SC) [11]
  Attacker Type # 6 SC; **Tools Used** # 6 SC; **Access Information** # 8 SC; **Results** # impact of attacks, 4 SC; **Attack Objective** # 4 SC
- **Cyber Threats to Critical Infrastructure** (7 C, total 45 SC) [21]
  Attackers (Hackers; Spies; Terrorists; Corporate raiders; Professional criminals; Vandals; voyeurs); **Tool** (Physical attack; Information exchange; User command; Script or program; Autonomous agent; Toolkit; Distributed tool; Data tap); **Vulnerability** (Design; Implementation; Configuration); **(Malicious) Action** (Probe; Scan; Flood; Authenticate; Bypass; Spoof; Read; Copy; Steal; Modify; Delete); **Target** (Account; Process; Data; Component; Computer; Network; Internetwork); **Unauthorized Result** (Increased access; Disclosure of information; Corruption of information; Denial of service; Theft of resources); **Objectives** (Challenge, Status, Thrills; Political gain; Financial gain; Damage)
- **Attacks on UNIX hosts** (4 C, total 32 N) [8]
  Denial of Service, DoS; **Remote to Local, R2L**; **User to Root, U2R**; **Surveillance/Probing**
- **Threat Profiles' Properties** (5 C, total 22 SC) [16]
  Asset (Critical) # >1; **Actor** (Inside; Outside) || (Non-malicious employees; Disgruntled employees; Attackers; Spies; Terrorists; Competitors; Criminals; Vandals) || (Human actors using network access; Human actors using physical access; System problems; Other problems) || (Software defects; Malicious code; System crashes; Hardware defects) || (Power supply problems; Telecommunications problems; 3rd-party problems; Natural disasters; Physical arrangement of buildings, equipment, etc.) # >11; **Motive** (Accidental; Deliberate) Access (Network access; Physical access; System problems; Other problems); **Outcome or Effect**: (Disclosure; Modification; Destruction or loss; Interruption of access)
- **Vulnerabilities of computer attacks** (4 C) [19]
  Improper Validation; **Improper Exposure**; **Improper Randomness**; **Improper Deallocation**
- **DDoS attacks / DDoS defense** (8 C / 3 C) [9]
  Attacks (Degree of automation; Exploited weakness; Source address validity; Attack rate dynamics; Possibility of characterization; Persistent agent set; Victim type; Impact on victim); **Defense** (Activity level; Cooperation degree; Deployment location)
- **Dependable and Secure Computing** (3 C, total 75 N) [26]
  Attributes (Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability); **Threat** (Faults [development faults; physical faults; interaction faults; elements {phase of creation or occurrence <development vs. operational>; system boundaries <internal vs. external>; phenomenological cause <natural vs. human-made>; dimension <hardware vs. software>; objective <malicious vs. non-malicious>; intent <deliberate vs. non-deliberate>; capability <accidental vs. incompetence>; persistence <permanent vs. transient>}; examples {software flaws; logic bombs; hardware errata; production defects; physical deterioration; physical interference; intrusion attempts; viruses and worms; input mistakes}]; Errors; Failures [service failures; development failures; dependability failures]); **Means** (Fault prevention; Fault tolerance [error detection {concurrent vs. preemptive}; recovery {error handling vs. fault handling}]; Fault removal [verification {static vs. dynamic}; diagnosis; correction; non-regression verification}]; Fault forecasting [ordinal evaluation, probabilistic evaluation: {modeling vs. operational testing}])
- **Attack dimensions** (5 C, total 77 N) [22]
  Attack Characteristics (Viruses; Worms; Buffer overflows; DoS; Network; Physical; Password; Information gathering) # 8 SC, total 20 E, total 17 SE; **Target Characteristics** (hardware; software) # 2 SC, 4 E, >9 SE; **Vulnerabilities and Exploits** (In implementation; In design; In configuration) # 3 SC; **Payloads and effects** (Attack payloads; Corruption of information; Disclosure of information; Theft of service; Subversion) # 5 SC; **Others** (Damage; Cost; Propagation; Defense) # 4 SC
- **Computer security incidents** (4 C, 22 SC) [12]
  Source Sectors # 6 SC; **Method of Operation** # 9 SC; **Impact** # 5 SC; **Target Sectors** # 2 SC
- **Computer attacks** (4 C, 15 SC, 13 E) [27] **Motivation** (Just for

fun; To be the best defacer; Not available; Patriotism; Political reasons; Revenge; As a challenge); **Characteristics** (Interruptions; Intercept; Modification; Fabrication); **Meta properties** (Attacker # 2 E; Target # 3 E; Course # 2 E; Goal # 4 E; Location # 2 E); **Types** (Code exploit; Eavesdropping; DoS; Indirect attacks; Backdoor; Direct access; Social engineering; Cryptographic)

- **(Desktop) malware and spyware** (11 C, total 49 N) [28]
  Main Types of Malware (Virus; Worm; Trojan horse; Backdoor; Spam; Rootkit; Dialer; Exploit; Keylogger; Browser hijacking; Spyware); **Up-to-Date Malware**: (Adware; Parasiteware; Thiefware; Pestware; Browser helper object, BHO; Remote administration tool, RAT; Commercial RAT; Botnet; Flooder; Hostile ActiveX; Hostile Java; Hostile script; IRC takeover war; Nuker; Packer; Binder; Password capture - password hijacker; Password cracker; Key generator; Mail bomber; Mass mailer; E-mail harvester; Web bugs; Hoax; Phishing; Web scam and fraud; Phreaking - phone breaking; Port scanner; Probe tool; Search hijacker; Sniffer; Spoofer; Spyware cookie; Tracking cookie; PIE; Trickler; War dialer; Wabbit)
- **Nature of attacks** (5 C, total 32 N) [23]
  Attack Vector # 10 N, actually most of them are vulnerabilities; **Operational Impact** # 6 N; **Defense** # for network administrators, 2 N; **Informational Impact** # 5 N; **Target** # 6 N
- **Cyber security vulnerabilities** (4 C, 13 SC, 57 E, total 74 N) [20]
  Actions of People # 3 SC; **Systems and technology failures** # 3 SC; **Failed Internal Processes** # 3 SC; **External Events** # 4 SC
- **Social engineering attacks** (2 C, 16 SC, total 26 N) [29]
  Person-Person (Real person impersonation; Fake person impersonation; Pretexting; Reverse social # quid pro quo, something for something; Tail gating); **Person-Person via Media** (Text; Phishing; SMSishing; Malware # 4 N; E-mail; Popups; Search engine poisoning, SEP; Social networks; Cross-site request forgery, CSRF; Voice [vishing]; video)
- **Social engineering attacks** (2 C, 21 SC) [30]
  Human-Based (Impersonation and important user; 3rd-party authorization; In person; Dumpster diving and shoulder; Creating a sense of urgency; Simple persuasion; Reverse social engineering); **Technical-based** (Trojan horse; Pop-up windows; E-mail; Software; Web sites; Signal hijacking; Network monitoring; Phishing; Spam/scam; Instant messages; DoS; Digital dumpster diving; Vishing; Theft on mobile)
- **Networks attacks** (5 C, total 62 N) [24]
  Networks (Wireless personal area network, WPAN; Wireless local area network, WLAN; Broadband; 3G mobile; Internet service provider, ISP infra-structure; Ad hoc and VANETs, vehicular ad hoc networks; Supervisory control and data acquisition, SCADA; Cloud; Voice over Internet protocol, VoIP; Messaging networks); **Systems** (Web browser; Web server; WPAN handheld device; GPS device; 3G mobile phone; Hub-switch-router-firewall; Industrial devices and control system; Cloud client; OS; Application); **Attacks** (Social engineering; Exponential attacks; Hacking and cracking; Trojans; Spyware; Zero day; Botnets; Spam; Beaconing; Spoofing and hijacking; (D)DoS; Web server; Data leakage; Authentication failures; Blended); **Attack Techniques** (Drive-by-download; Traffic analysis; MAC and IP address manipulation; TCP segment falsification; ARP and cookie poisoning; Buffer overflow; Command injection; Man-in-the-middle, MITM; Re-play; Flooding and backscatter; Auto blocking; Privilege escalation; XSS/XSRF; Input manipulation); **Protection Systems** (Physical security; Encryption; Authentication; Backup and disaster management; Sandboxing; Traceback; Honeypots/honeynets; Digital certificates)
- **Mobile malware detection** (2 C, 4 SC, 4 E, total 10 N) [31]
  Reference Behavior (Malicious vs. Normal); **Method** (Signature vs. Anomaly); **Analysis Approach** (Static vs. Dynamic); **Malware Behavior Representation**
- **Cyber conflict** (4 C, 4 SC, 28 E, total 36 N) [13]
  Action # 2 N: Defense # 4 N; Intrusion # 18 N in 4 SC; Actor (Non-state; State); Entity (Dynamic metadata per case); Event (Dynamic metadata per case)
- **Phishing attacks with detection techniques** (2 C, total 11 N) [32]
  Attacks (Bluetooth; SMS; Vishing; Mobile web application); **Detection Techniques** (Content based; Blacklist; Whitelist; Hotspot; Gaussian mixture model)
- **Cyber attacks** (3 C, total 19 SC, total 38 E) [10]
  Characteristics (Harmonized; Organized; Enormous; Regimented; Scrupulously designed; Not spontaneous or ad hoc; Demanding time and re-source); **Purpose and Motivations** (Obstruction of information; Counter international cyber security measures; Retardation of decision making process; Denial in providing public services; Abatement of public confidence; Reputation of the country will be denigrated; Smashing up legal interest); **Categorizations** (Purpose: Reconnaissance attack # >4 N; Access attack # >6 N; DoS attack # >4 N)
- **Social engineering in social networking sites** (4C, 11 SC, 11 N) [33]
  Social Networking Sites (Privacy settings; Friendship and connection; Content); **Plan and Technique** (Suitability to targeted victim; Quality of the plan and technique); **Social Engineer** (Ability to perform the plan; Ability to understand the victim; Ability to develop a plan); **Victim** (Risk belief [perceiving threat; perceiving severity; perceiving susceptibility]; Socio-psychology [personality type; motivation and drive {need-based; emotion-based}]; User demographics; Countermeasures [education and training; auditing and testing; policy and management])
- **Malware characterization** (5 C, 21 SC, 5 E) [15]
  Attack Goals and Behavior # 5 SC; **Distribution and Infection** # 6 SC; **Privilege Acquisition** # 2 SC; **Type of Incentives** # 4 SC; **Behavior Related to Incentives** # 4 SC
- **Web Threats with controls / Smartphone Threats with C-I-A impact** (11C / 4 C,

24 SC) [34]
Annoyance; **Browser Fingerprinting**; **Exploits/Malware**; **Identity Theft**; **Data Interception**; **Phishing**; **Privacy Breach**; **Resource Abuse**; **Rogue Certificates**; **Spam Advertisements**; **Technical Failure**; **Network Connectivity** (Spoofing; Scanning; DoS, Network congestion; Spam, Advertisement; Eavesdropping; Jamming); Device (Loss; Theft; Disposal or damage; Cloning SIM, subscriber identity module card; Technical failure of device; Unauthorized device -physical access); **Operating System** (Unauthorized access; Offline tampering; Crashing); **Applications** (Misuse of phone identifiers; Electronic tracking-surveillance-exposure of physical location; Resource abuse; Sensitive information disclosure, Spyware; Corrupting or modifying private content; Disabling applications or the device; Client side injection-malware; Direct billing; Phishing)

- **Attributing cyber attacks** (9 C, 24 SC, 24 E, 122 SE, total 179 N) [14]
  Levels (Strategic; Operational; Tactical, Technical); **Staff** (Leaders; Analysts; Forensic experts); **Goals** (Response; Understanding; Technical analysis); **Responsibility** (Government; Agency, Group; Individual); **Target** (Government; Organizations, Individual; Data, Documents, Processes); **Certainty** (Lower; Medium; Higher; Detail [concise; synthesis; detailed]); **Questions** (Why? # 15 strategic questions; Who? [skills; scope; stages; evolution; claims; insider; intelligence; cost; significance; context-aperture] # 34 operational questions); What? How? [indicators of compromise; entry; targeting; infrastructure; modularity; language; personas; pattern-of-life; stealth; cluster; functionality; approval; mistakes; unknown] # 65 tactical and technical questions); **Communication** ([questions to politicians, executives, the public] # 8 N; Estimates; Hypothesis; Description)
- **(Semantic) social engineering attacks** (3 C, 16 SC, 1 E, 2 SE, total 22 N) [35]
  Orchestration (Target description [explicit vs. promiscuous]; Method of automation [manual vs. automatic]; Method of distribution [software {execution <local vs. remote>}; hardware without software interaction; hardware with software interaction]); **Exploitation** (Deception vector [cosmetic, behavior; hybrid]; Interface manipulation [user interface; programming interface]); **Execution** (Execution steps [single vs. multiple]; Attack persistence [one-off vs. continual])

Most of the reviewed studies are in a narrow perspective; their terminologies are intermingled, scopes are shallow, and elements are open-ended. In a quantitative comparison, total numbers of nodes are low apart from: taxonomy [14] in 122 nodes related to incidents, taxonomy [22] in 77 nodes related to security, taxonomy [20] in 74 nodes related to vulnerabilities, and taxonomy [24] in 62 nodes related to security.

Hansman and Hunt admitted that implementing such a universal taxonomy is unrealistic and unmanageable and tried to section it into a specific topic such as cloud and malware in 3G networks [22]. As the latter relates to our study, the total nodes are even smaller comparing their whole taxonomy (21 nodes).

Avizienis et al. provided a taxonomy of dependable and secure computing in a well-defined manner with total 75 nodes [26]. Although their taxonomy comprises secure computing, they focused mainly on dependability (mostly non-malicious faults with integrity and availability aspects, e.g. maintainability) and partly studies the security related subjects (ignoring the confidentiality aspects of security; e.g. malicious objective, deliberate intent, software flaws, logic bombs, intrusion attempts, viruses and worms). Their work is worth mentioning because it provides two useful representations of the taxonomy namely matrix and tree.

Among the 28 studies reviewed, the following three studies are only directly related to mobile security: Amamra et al. focused on mobile malware detection with a very basic four subclasses [31]; Foozy et al. focused on security in scope of mobile phishing only [32]; and Mylonas examined mobile security in 24 subclasses in addition to server side attacks [34].

Amamra et al. presented an introductory level taxonomy for mobile malware analysis, and discussed the advantages and disadvantages of signature-based methods (static vs. dynamic/static behavior), and anomaly-based methods (dynamic vs. static) [31]. Foozy et al. presented the propagation channels of mobile phishing and touched on a few detec-

tion methods that mostly contain whitelisting and blacklisting approach [32]. Mylonas was one of the researchers examined mobile security relatively broader scope in his Ph.D. thesis [34]. He compared the security controls in web browsers in desktop/mobile operation systems, collected, and analyzed the adoption of on-device security controls via interviews. Because mobile computing replaces desktop computing, the taxonomies in other fields such as malware and cyber security for desktop computers can give inspiration for mobile security taxonomic studies. Although Rid and Buchanan's study was about attributing cyber attacks, it is a well-established example for a visualized taxonomy [14]. They modeled the attribution in the context of computer network intrusions as titled 'Q Model' for explaining, guiding and improving the attribution making in tactical, technical, operational, and strategic level in scope of concept, practice and communication. The study is a well and distinct example of taxonomy in cyber security with a neat visual representation of the model for attributing cyber attacks.

2.3. Quality Criteria of (Security) Taxonomies

The literature includes studies related to quality of taxonomies. Alberts and Dorofee presented 18 criteria for qualifying taxonomies based on five related studies from 1994 to 1998 [16]. The criteria are 'accepted', 'appropriateness', 'based on the code, environment, or other technical details', 'comprehensible', 'completeness', 'determinism', 'exhaustive', 'internal vs. external threats', 'mutually exclusive', 'objectivity', 'primitive', 'repeatable', 'similar vulnerabilities classified similarly', 'specific', 'terminology complying with established security terminology', 'terms well defined', 'unambiguous', and 'useful' in alphabetical order.

Considering those quality criteria, the reviewed taxonomies above successfully meet only a few criteria. As seen in the Summary, their classes are mostly broad and unclear. They contain incomplete subclasses or sub contents that could not provide a sufficient depth. The taxonomies tend to present the primitives and provide some metadata for the phenomena. We have founded that even most of the basic terminology is confused in those taxonomies. For example, actual propagation channels, attack surfaces, and vectors are mixed with attacks in [30].

With respect to the taxonomies related to mobile security, which is already a new, broad, sophisticated and interpretive domain, we are of the opinion that the limited works could not meet most of the criteria. Beyond, they fail to cover offensive and defensive aspects developing day-by-day along with continuous technology improvements.

Summarizing our review, previous security taxonomies have failed to address mobile security and even cyber or information security aspects in an acceptable level. The taxonomies are generally oversimplistic, not instructive and could not give the big picture from both defensive and offensive views.

The aim of our work at this point is to propose comprehensive high quality taxonomies on mobile security and mobile malware analysis in order to expand both breadth and depth of current knowledge; present the known or new offensive perspectives as well as the defensive ones; revisit and establish the fundamental concepts to provide a common terminology; and support the education and research activities.

2.4. Major Obstacles in Achieving Efficient Mobile Security Taxonomy

Having a mobile security taxonomy should be a necessary step, implicitly or explicitly, for anyone either researches or practitioners working on this

domain. However, as our literature review implies, presenting the big picture and entire perspective on mobile security is not an easy work.

Considering the reviewed works along with our own experience, the followings are our findings about obstacles to achieving an efficient taxonomy in mobile security:

- The domain is new, fast developing, versatile, and multidisciplinary,
- The researches tend to focus on a specific subject and ignore other related subjects,
- Establishing better and comprehensive taxonomies require deep knowledge, practical experience, and expertise,
- The literature has a natural tendency to focus and solve the tangible and specific problems,
- Implementing, updating or even maintaining a taxonomy requires continuous, painstaking and sometimes tedious efforts,
- Reference sources are limited, and
- Terminology in available sources are usually ambiguous or incorrect.

3. Proposed Method for Building Security Taxonomy

The reviewed studies listed in the Summary generally do not follow a specific formal methodology for taxonomy building. Most of them are based on expert opinions. They try to present a narrow subject into a number of classes in common 'denominators', 'axes', 'dimensions', and 'characteristics'. Taxonomies reflects the authors' own intuitions or observations dominantly. The existing classes are coarse, they usually represent the prominent properties of the subject and they are not canonical (inclusive and incomplete).

As an example, Landwehr et al. organized available information about software security flaws according to simple questions: how, when, and where [18]. Bishop [17] tried to make use of the earlier works [25], [18]. He mentions about 'flaw hypothesis methodology', which is actually a natural way of elaborating the founded flaws with hypothesized flaws compiled from the specifications and documentation of the evaluated system. A few of the taxonomies were established based on the security data. Lindqvist and Jonsson's taxonomy was the categorization of 3,000 computer abuse cases [7]. While [11] investigates 4,299 reported security related incidents on the Internet. Naturally, different perceptions lead to different taxonomies even for the same domain (e.g. see four different taxonomies on social engineering in the Summary: [29], [30], [33], [35]).

In this study, we have proposed and successfully used a novel method that is definite and complete from general security perspective. This method depicted in Figure 1 accurately determines the main classes, which is a first and fundamental step in order to establish a well-organized taxonomy structure. Figure 1 provides the high-level interpretation of security in general based on a UML (Unified Modelling Language) use case diagram (should be called as 'use and misuse case' diagram).

The proposed diagram actually provides the big picture on security or a compact design plan. It enlightens on security concept as a whole and presents the fundamental components including actors, attacks, and controls (i.e. countermeasures) with their essential dependencies. The diagram was used as a guide to construct the taxonomy structure. Although security is a well-known and studied field, to the best of our knowledge, a diagram specifying offensive and defensive security in this scope and manner, has not been encountered.

The diagram presented in Figure 1 is valuable in terms of providing all the ingredients of secu-

rity with their associations in both offensive and defensive point of views in a comprehensive manner and reducing the complexity. We adopted the coloring scheme of the diagram from 'red/black' concept in cryptographic systems. The red depicts the vulnerable side that is susceptible to attacks; the black depicts the offensive side. Extending the concept, the green represents the defensive side and the orange depicts security side surrounded by cyberspace such as security violations (see Figure 7) and other domain specific (e.g. mobile security) aspects (such as protection by-pass).

The diagram provides the general framework to identify the taxonomic structures in a correct context and can be summarized as follows: 'end users have tangible and intangible assets on mobile devices. These devices and underlying mobile technologies have vulnerabilities by design or in use and present several attack surfaces to attackers in cyberspace where the virtual and physical domains are combined. While the users have their own goals to make use of mobile technologies without safety, privacy and security risks, the attackers with malicious goals and different motivations seek feasible threats to harm the users. There are several threats including malware that first propagate in cyberspace and conduct attacks that use some vectors and include some malicious payloads. The players in mobile technology industry and the defenders work together in defense to protect the users against the attackers. They design and implement effective controls including malware detection and analysis to avoid exposures, to decrease breaches and to mitigate the risks'.

From quality perspective as described in Section 2.3, devising such a diagram is crucial to make the proposed taxonomy built on this diagram 'appropriate', 'complete', 'deterministic', 'mutually exclusive', 'primitive', and 'specific'.

Regarding to taxonomy development process, the taxonomies proposed in this study are the result of more than two years' study. We have reviewed many articles, reports, whitepapers, blog and social media entries to compile various taxonomic units and classified them accordingly with the help of the proposed method under the established classes.

The followings are our distinct goals for establishing a comprehensive taxonomy: being specific to mobile computing; determining proper classes and subclasses; providing correct usage of terminology and concepts; separating defensive and offensive concepts; presenting rich and up-to-date content; identifying niche as well as fundamental subjects; and adding visual aids to enhance understanding and to ease educational usage. The next section summarizes the high level structure of the proposed taxonomy and its classes.

4. Proposed Mobile Security Taxonomy and Its High Level Structure

Our mobile security taxonomy comprises two types of classes and two separate subtaxonomies:

- Mobile security taxonomy: conceptual classes
- Mobile security taxonomy: core classes
- Mobile malware analysis subtaxonomy
- Machine learning subtaxonomy (for malware analysis)

Conceptual classes express the fundamental aspects of security that are mostly static and partially well known, while core classes reflect the dynamic security aspects. One exception is the 'Payloads' class, which is represented in both groups as explained in Section 4.1.9. Other exceptions are the 'Concepts', 'Characteristics', 'OSs', 'Protection By-Pass' classes that are fundamental but evolving and very specific to mobile computing. Although mobile malware analysis is a critical part of mobile

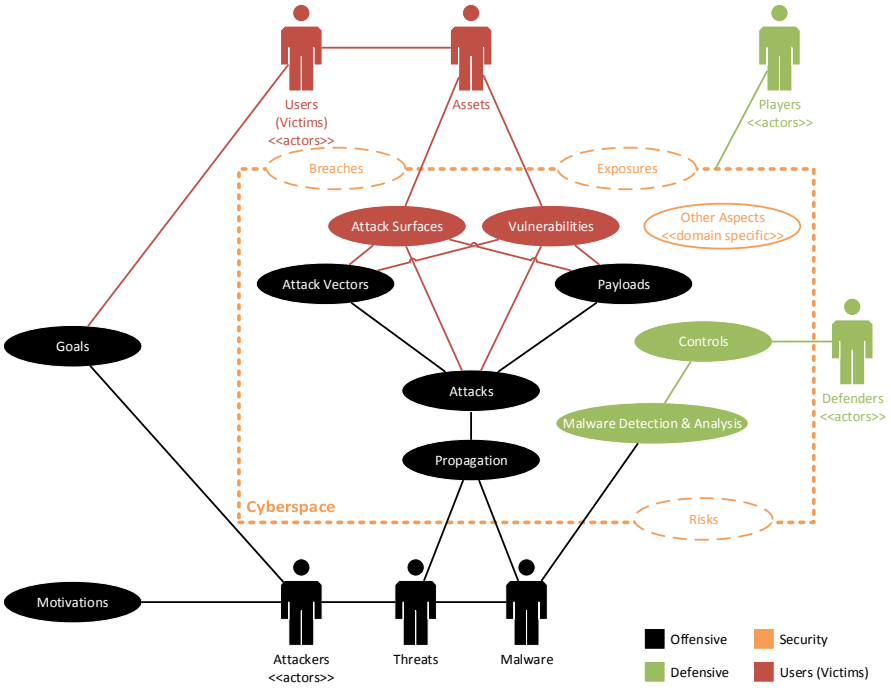

Fig. 1. A new approach to develop security taxonomy: (mobile) security taxonomy's main classes and taxonomic relations depicted as a 'use and misuse case' diagram

security, we have separated its details from our mobile security taxonomy as a subtaxonomy.

Figure 2 and Figure 11 shows final forms of the proposed taxonomies on mobile security and mobile malware analysis, respectively. We employed a mind map style to visualize broad range of nodes and branches of the taxonomies. Nevertheless, the taxonomies are actually databases populated from hierarchically linked nodes in a tree structure. We have shared both taxonomies online in a simple tree representation at http://bit.ly/securitytaxo and http://bit.ly/mobilemalwaretaxo. Note that these two taxonomies were never published in any other journal.

One of the distinctive properties of our proposed mobile security taxonomy is the visualization approach employed. We believe this visualization will aid readers to easily explore the content and will be user-friendly and extremely useful for not only in researches but in mobile security practices and education. The angular position of the main class branches (the branches around the central 'mobile security' topic) along with their colors is determined according to defensive, offensive or neutral/common characteristics of the classes. Text colors are also set according to the same characteristics. We enhanced visualization by adding a representative icon beside the nodes properly.

4.1. Mobile Security Taxonomy Conceptual Classes

Although information or cyber security, as lately called, has progressed in a long period, the fundamental core concepts have not been described sufficiently in a holistic perspective. This should be as important as the critical practical issues such as

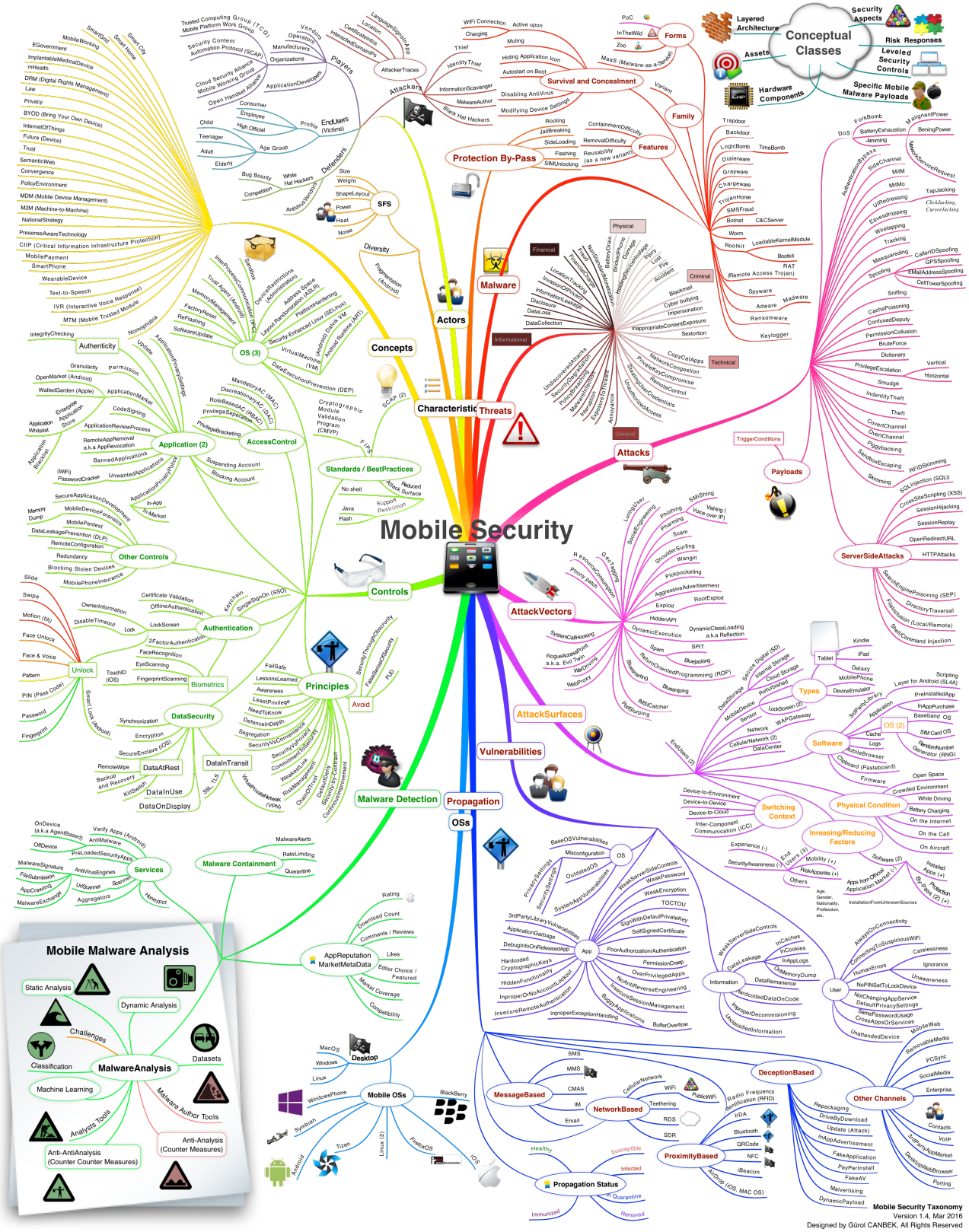

Fig. 2. Mobile security taxonomy having total 816 nodes (online access to nonvisualized taxonomy: http://bit.ly/securitytaxo) (mobile malware analysis is presented in another subtaxonomy in Figure 11)

emerging technologies' security. Information security becomes an "all or nothing" phenomenon in the presence of adversaries seeking a tiny hole that is practical to exploit in cyberspace where the barriers are not materialized easily or effectively as in the physical world. Thus, we have revisited, reanalyzed and reorganized the fundamental security concepts and adapted them into mobile security domain.

The followings are the nine mobile security conceptual classes: layered architecture, security aspects, actors, assets, hardware components, attack anatomy, levelled security controls, risks and responses, and mobile malware specific payloads. Following subheadings describe each of the conceptual classes.

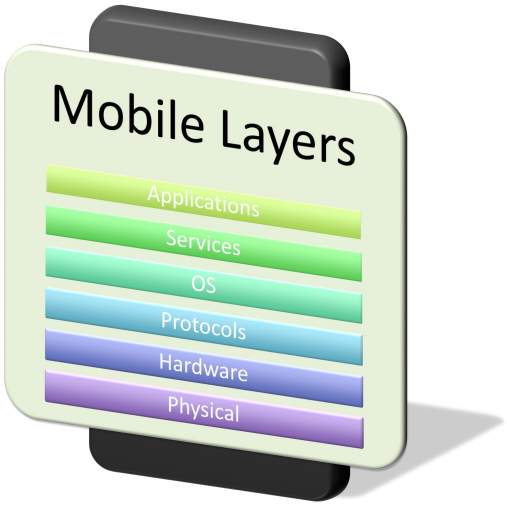

Fig. 3. The layered architecture for mobile computing

4.1.1 Layered Architecture on Mobile Computing

It is more understandable to see mobile security in an architecture composed of stacked layers resembling the Open Systems Interconnection (OSI)'s 7 layers of networking. The proposed layered approach as illustrated in Figure 3 helps to understand mobile threats, vulnerabilities, risks, countermeasures and security at different level without causing exclusion and losing the dependency so that the defense-in-depth principle could be achieved.

4.1.2 Mobile Security Aspects (going beyond C-I-A)

In a conventional manner, 'confidentiality, integrity and availability', also known as C-I-A triad, are considered as the main aspects of information security in the literature. However, there are other security aspects as listed in Figure 4. These aspects are different from the ones in other domains such as desktop computing and should be examined from mobile computing perspective. 'Privacy', 'Identification', and 'Anonymity' are the comparatively new aspects that should be more focused in modern mobile computing. For example, owing to the benefits of mobile computing, the end users could be so addicted to their mobile device and mobile services that when they lose the device, forget to bring it, or the device doesn't work they may feel emptiness, isolation or insecure (i.e. no-mobile-phone phobia 'nomophobia' as shown in related Concepts class in the taxonomy). This dependency and sometimes addiction to a very personal mobile device can be considered as the root cause of necessity of high availability comparing the other security aspects such as confidentiality. In a more social mobile Internet, users may sacrifice confidentiality over the availability and ignore threat signals.

In essence, these aspects should be taken into account in every study of mobile computing from designing mobile operating systems to implementing secure mobile applications.

Fig. 4. The 18 aspects of mobile security

4.1.3 Actors (who are playing their roles)

One of the most important concepts in mobile security is the actors (i.e. stakeholders) involved in mobile computing ecosystem. Without such an approach, it is difficult to see the motivations and responsibilities behind any risk and under any security measures as well as establish an effective coordination and information exchange between security industry and academia. Players and defenders together try to relief end users' burden while attackers seeking holes to overcome the resist and downgrade end user's benefits.

The end users, owners of the mobile device or clients of a mobile service, wish to make use of the mobile technology for their own benefits without any obligation and risks. The players normally are the researchers and builders of both mobile technologies and environments supporting mobile computing in industry and academia. They are concentrated on making mobile technologies and platform useful but faced with dilemma to make them both usable and secure at the same time. These conflicting concerns and stress of short time-to-market may cause flaws in security posture of mobile devices. The attackers are malicious people or organizations to disrupt the protection mechanism by exploiting the vulnerabilities in mobile technology that are not adequately handled by the players and the weaknesses in the attitudes of the end users. They are not called as 'the hackers' since not all hackers are malicious. Some of them, white hat hackers as they called, see the vulnerabilities quickly, inform the players and even suggest a method to fix them. The defenders are entities whose concerns are only securing mobile devices, mobile applications and mobile platforms.

4.1.4 Mobile Assets

Anything that has a value to an individual or organization in mobile platforms is classified in mobile assets. Figure 5 depicts our novel mobile asset classification. As mobile devices are all-in-one device, mobile assets are inherently intense and critical/sensitive. The identifiers such as IMEI (International Mobile Station Equipment Identity) numbers are one of the targets of malware authors. Following static or dynamic information can be gathered about a mobile device by capturing its IMEI: device model, brand, type, design, release date, dimensions, weight, display type, touch screen existence, SIM card size, GSM (Global System for Mobile Communications) talk and standby time, battery information, built-in memory, operating systems, keyboard support, and etc.

IMSI (International Mobile Subscriber Identity), ICCID (Integrated Circuit Card Identifier, SIM card identifier), device serial number, Transaction Authentication Number (TAN) are other identifiers that possess critical tracking information about mobile devices and consequently their owners. Vibrate state, remaining battery, installed applications, running applications, light status, device orientation,

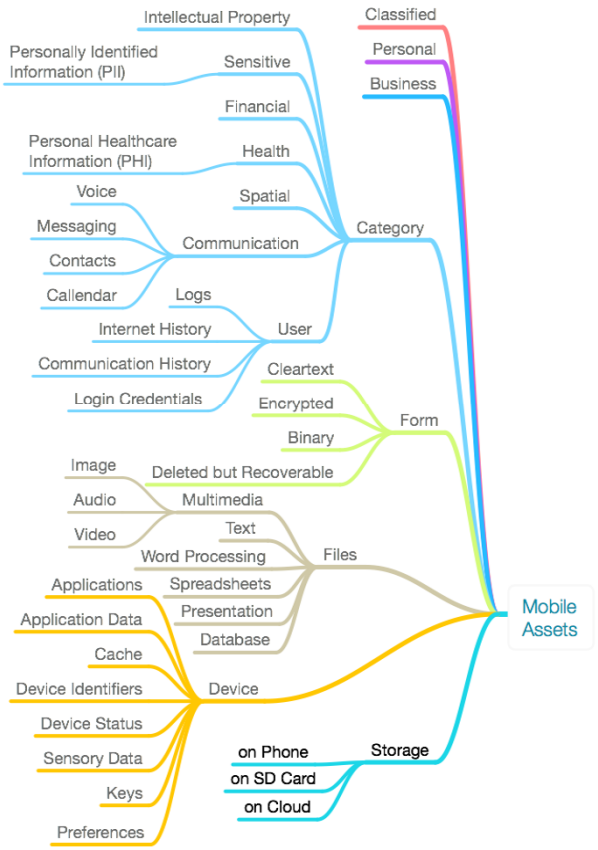

Fig. 5. Mobile assets

lightness, connected cellular networks, connected Wi-Fi networks are the examples of 'Device Status' type of information.

4.1.5 Hardware Components

The rich capability of the mobile computing (as summarized in Introduction) is the result of several special purpose hardware integrated into mobile devices. Keeping track of the hardware as new components have been manufactured and integrated into mobile devices leads to control the attack surface on devices. A new component means a weakness both for the attackers to seek vulnerabilities and for

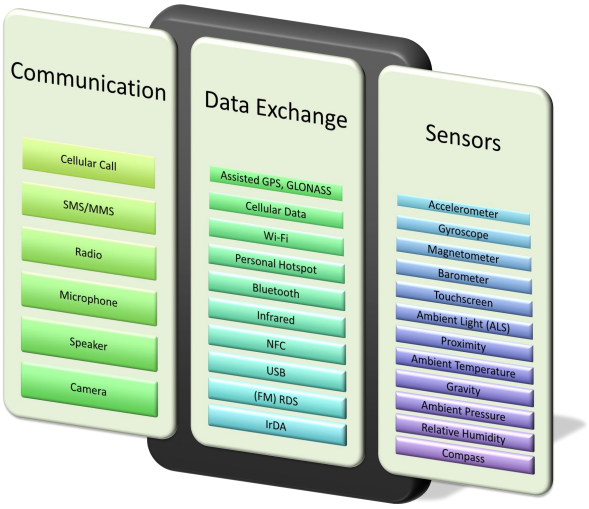

Fig. 6. Mobile device hardware components

the defenders to mitigate risks. Figure 6 lists 28 categorized hardware components of mobile devices currently available on mobile platforms.

4.1.6 Anatomy of (Mobile) Attacks

Although the terminology used in communications among security community has its own specific terms, the confusion and misnomers can be seen in wide variety of sources such as blogs, reports (e.g. attack announcements and proof-of-concepts), newspapers, and even academic papers. Thus, the very basic terminology related to anatomy of attack is included and presented visually to understand the related classes in our taxonomy as illustrated in Figure 7 and Figure 8.

Although our original figurative visualization for the terminology is in scope of mobile security, it can be adapted in other security areas. For lack of space, definitions of threat, threat agent, and risk are only briefly provided in this study. Threat is defined as "the capabilities, intentions and attack methods of adversaries, or any circumstance or event, whether originating externally or internally, that has the

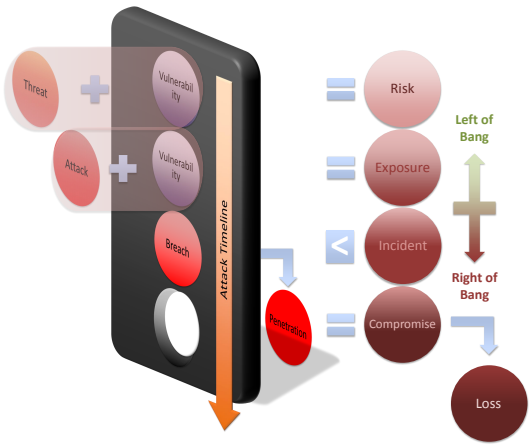

Fig. 7. Levels of security violations (severity increases from top to bottom, adapted from [ISO/IEC 2382-8])

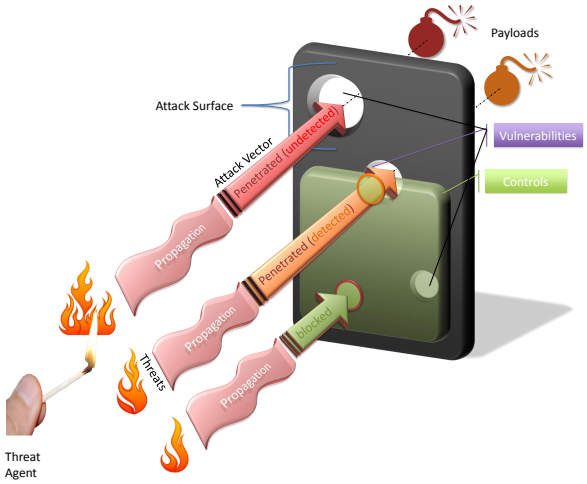

Fig. 8. Anatomy of attacks, the main classes of the mobile security taxonomy: threat agent, threat, propagation, attack vector, attack surface, vulnerabilities, controls, and payloads. Some controls block the attacks while others could not (some is only able to detect though)

potential to cause harm to information or a program or system or cause those to harm others [ISO/IEC 21827:2002].” Threat agent is “the originator and/or the initiator of deliberate or accidental man-made threats [ISO/IEC 21827:2002].” Risk is “the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets [ISO 13335-1:1996].” Impact or hazard could be defined the loss or damage in assets caused by malicious payload.

Figure 7 and Figure 8 are significant to show the time line of attacks. Figure 7 depicts the attacks occurred in a relatively long term while the latter is focused on the internal dynamics of attacks which may be detected or worst of all undetected. Attacks detected by applied controls could be blocked via further controls or could not be blocked. Figure 8 should be considered as a 3-dimensional representation of the use and misuse case diagram in Figure 1.

4.1.7 Mobile Security Controls in Levels

Control (also known as safeguard or countermeasure) is defined as “measure that is modifying risk [ISO Guide 73:2009].” Figure 9 illustrates controls, which are leveled by us according to effect degree (e.g. 2nd level controls are effective for the attacks that could not be resisted by 1st level controls). Controls could also be grouped into physical, logical (technical), administrative, management, and legal controls.

4.1.8 Risks and Responses

Our taxonomy presents the distinctive threats and vulnerabilities on mobile platforms. For the sake of completeness, ‘risks’ conceptual class is also included. Risks could be defined and -if possible- measured the likelihood of threat, the severity of

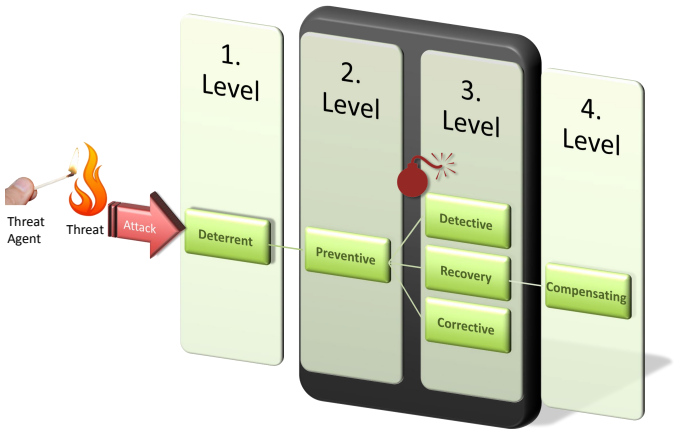

Fig. 9. Mobile security controls in levels

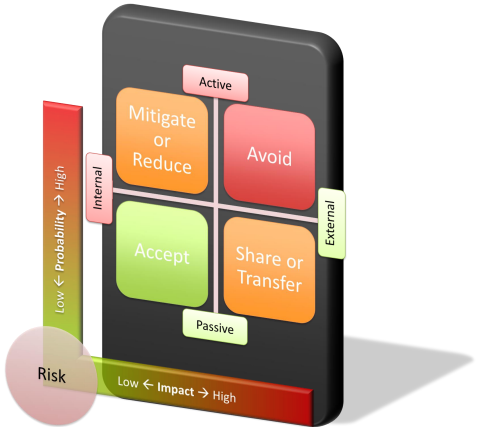

Fig. 10. Risk, risk response choices (accept, share or transfer, avoid, mitigate or reduce) and their types (active vs. passive) and scopes (internal vs. external)

impact caused, and the value of asset. Figure 10 depicts the risk concept and the choices of responses to risks. Note that Figure 10 is our original representation of risk methodology from a leveled standpoint; the contents are about the conventional risk management approach and are not specific to mobile security.

4.1.9 Mobile Malware Specific Payloads

Mobile malware could have several payloads to achieve its malicious purpose. Security professionals such as mobile malware analysts and even ordinary end users should know currently realized payloads in order to find the countermeasures or at least to be aware of possible damages.

When we review the academic or industrial literature, we have seen that a few payloads are mentioned such as sending SMSs (Short Message Service) to premium numbers. In this study, complementing our taxonomy, we have compiled and characterized the broad range of payloads specific to mobile malware and listed them in Table 2. For lack of space, we could not provide the type and calculated C-I-A impact of the payloads in Table 2. The distribution of the mobile payloads is PII (16%), Call (13%), Financial (10%), Device (9%), DoS (7%), Annoyance (7%), Infection (7%), SMS (7%), Application (7%), File (7%), Internet (6%), and Network (4%) in decreasing order.

The impact distribution of the payloads that 71% of them have impact on integrity, 56% have impact on availability, and 43% have impact on confidentiality. This could be a significant indicator of generic impact order of mobile threats and should be monitored up on the addition of new payloads to see the tendency. Some of the provided payloads have diverse impact. For example, up on ‘deleting contacts (Nr. 65)’ from a mobile phone’s address book, the data loss will propagate in cloud on the next synchronization. This may be recovered if the cloud has multiple backup copies for the contacts. In addition, the payloads that are stated in generic form and thus may seem innocent, could actually serve to make a critical damage. For instance, by ‘changing the appearance of icons (Nr. 1)’; a shortcut to a common application (e.g. web browser) can be

removed from the screen and the same (or similar) shortcut icon of malware is replaced. Again, after employing 'call forwarding of outgoing calls (Nr. 12)', the victim believes that he is calling to an insurance company as an example but she/he is actually calling to an attacker.

4.2. Mobile Security Taxonomy Core Classes

The core classes are the most important part of the proposed mobile taxonomy. As explained above they are dynamic and complicated. As the new attack surfaces and threats are introduced, they change and expand. For lack of space, explaining the taxonomy node by node is beyond the scope of this study. Most of the classes and the child nodes also relate to other fields of information security. For example, 'Principles' for 'Controls' are fundamental for any security approach. These principles can guide to design and develop mobile architectures, applications and to establish security controls.

Most of the mobile threats, payloads, malware, and vulnerabilities are also valid in other scope (e.g. desktop computing). As a comparison to desktop malware, there were 11 classes and 38 subclasses of desktop malware in [28] (see the Summary). As seen in Figure 2, there are 16 classes and 5 subclasses of mobile malware in our mobile security taxonomy.

Although some of the nodes in our taxonomies may look like very basic or well known, occurring attacks proves that, security professionals or researches in fact ignore or forgot them. For this reason, we have included the basic but necessary issues in the taxonomies. During our taxonomy building process, we came up with various studies that successfully present some of the exceptional or overlooked aspects of mobile security. We have reviewed and appropriately incorporated them into our taxonomy. Although we have kept the representative references to such resources, it is impossible to list them here due to the space limitation. In this respect, although this study provides some new approaches or nuances, it includes acquiring, collecting, synthesizing, grouping and classifying of the common body of knowledge on mobile security.

5. Mobile Malware Analysis Subtaxonomy

Mobile malware analysis is a separate subtaxonomy of the proposed Mobile Security Taxonomy. Figure 11 shows the subtaxonomy that provides malware analysts with the concepts related to malware analysis such as classification methods, static/dynamic analysis and feature selection approaches, tools, and challenges.

Mobile malware analysis subtaxonomy also sets light to the subject by providing the offensive point of view: malware authors' view such as their counter measures to avoid or complicate malware analysis and their tools. The subtaxonomy goes a step further and provides some counter measures to malware authors' counter measures.

As specified in Section 2, we have encountered only one study focusing on mobile malware detection with a very basic four subclasses (see the Summary for details) [31]. However, malware analysis in general and mobile malware analysis in specific are actually one of the most advanced emerging security fields focusing on analyzing applications on top of complex software and hardware platforms of modern operating systems and devices.

The proposed mobile malware analysis subtaxonomy brings different concepts, methodologies and tools together for the first time and includes 308 nodes in total in following classes:

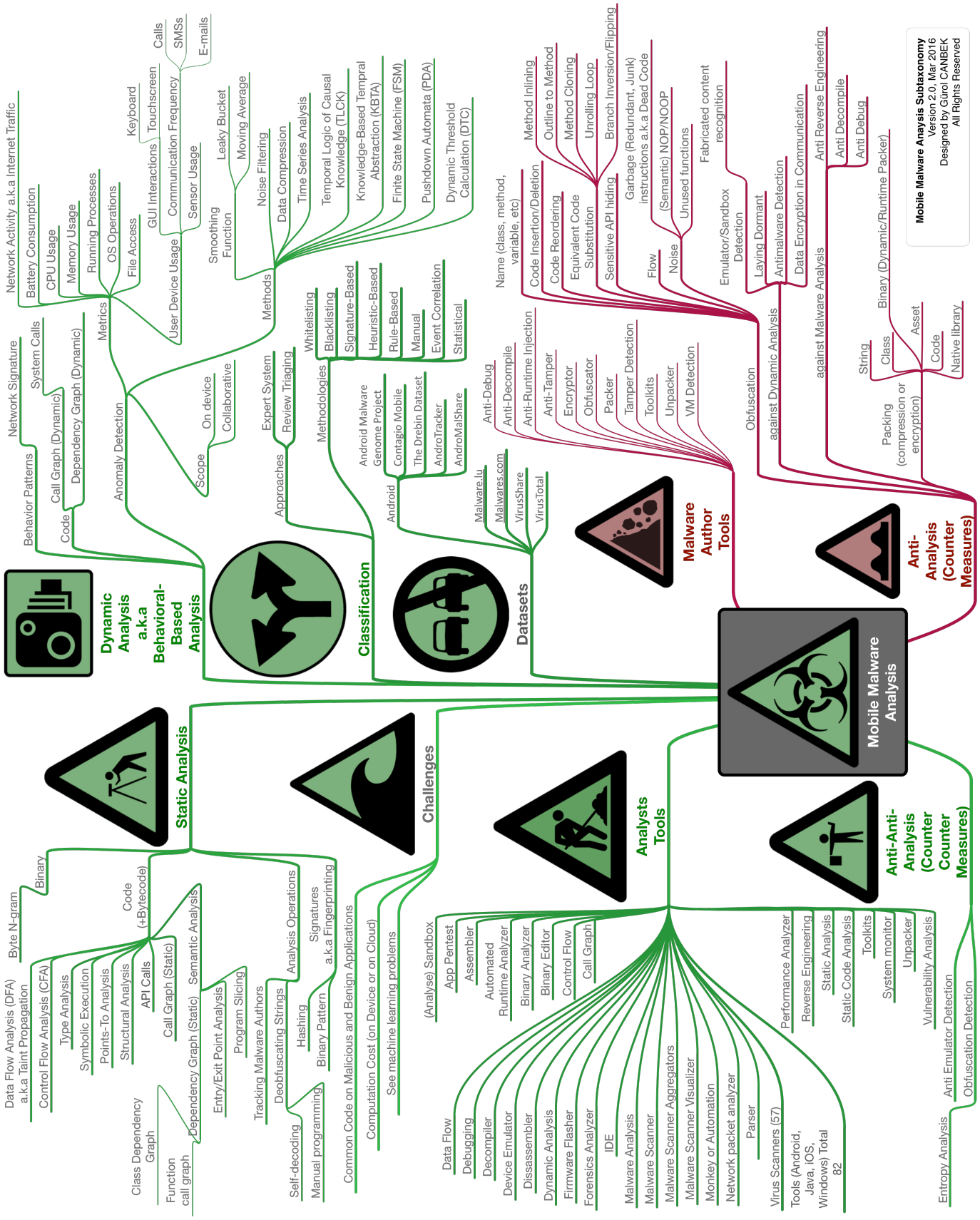

Fig. 11. Mobile malware analysis subtaxonomy having 308 nodes (online access to nonvisualized taxonomy: http://bit.ly/mobilemalwaretaxo)

- Feature selection or clustering methods to find the better characteristics to distinguish malware from benign applications,
- Classification with available approaches and machine learning algorithms,
- Static and dynamic analysis methodologies,
- Tools used by experts and malware authors
- Outstanding challenges in malware analysis, and
- Measures and counter-measures employed by the opponents.

The subtaxonomy is established after a comprehensive literature review on mobile malware analysis especially on Android malware. Because those studies are ongoing to search better methods for classifying malware from benign mobile applications, the subtaxonomy also guides researches and malware analysts to recognize other potential areas. In our view, representing the comprehensive knowledge about mobile malware analysis as a taxonomy directly contributes related researches and practices. In order to improve mobile malware analysis process, the alternatives in all their aspects should be provided in a definitive manner. For instance, 'feature selection' (or reduction) is a critical but possibly overlooked step in the first stages of malware analysis. For achieving a measurable efficiency in this step, none of the applicable methods specified in the subtaxonomy can be disregarded in trials or assessments. Otherwise, the results based on a limited scope could be highly misleading.

This incomplete approach could also be observed in studies in the literature that research on mobile malware classification via machine learning algorithms. Most of those studies on detecting mobile malware on Android platforms for example employ limited number of familiar algorithms such as Support Vector Machines (SVM), Naïve Bayes, and Random Forest (RF).

We have proposed and employed 'traffic sign' metaphor in our visualization for enhancing the understanding of the mobile malware analysis subtaxonomy. The subtaxonomy could also be represented as exclusive (non-overlapping) dendograms.

Please note that the comprehensive machine learning subtaxonomy as one of the crucial parts of mobile malware analysis subtaxonomy is not included in this study due to the space limitation and the integrity of the subject.

6. Taxonomy Usage Examples

Providing the possible uses of a taxonomy on especially real case scenarios could help to validate it that it meets the needs of its users such as security researchers, industry experts, and even end users. Following examples are provided to describe the possible uses of our mobile security and malware analysis taxonomies. The first example is for mobile security taxonomy and mostly conceptual classes while the second one is for mobile security, malware analysis taxonomies and mostly core classes.

6.1. Example 1: Risk around the Small Form Factor of Mobile Phone Used in Cars

Small Form Factor (SFS) is one of the most distinguishable characteristics of mobile devices [36]. As experienced in PCs, SFS has been a competitive advantage for mobile devices. SFS consists of the following categories: size, weight, shape and layout, power, heat, noise or other unwanted outputs such as SAR (Specific Absorption Rate) value. The followings are the shape and layout types that are presented to customers by different vendors: brick, bar, flip (or clamshell), slider, QWERTY, touchscreen, swivel, watch, mixed, and flexible. SFS should be considered from not only aesthetics or usability but also safety and security point of view since design

flaws and implementation mistakes in some factors may expose some attacks or vulnerabilities at least against the availability of mobile devices.

Comparing the desktop computers, mobile devices have limited computing capabilities due to the power and size constraints. Hence, either mobile malware could not perform complex algorithms to attack or mobile antimalware and security tools could not perform complex algorithms to detect, prevent or recover against security threats. For the sake of simplicity, we explain our taxonomy from physical security perspective and consider the following scenario.

EXAMPLE 1. A **risk** of accident due to answering a mobile phone call while driving.

Risks (Impact [high]) *for* **Actors** (End users [age group {-child}])
in **Layers** (Physical; Hardware)
by **Threats** (Accident; Damage; Injury)@Physical
upon **Attack Surfaces** (Physical condition [while driving])
exploiting **Vulnerabilities** (User [human errors {carelessness}])
degrading **Security Aspects** (Safety) # see Figure 4
Risks (Response [Mitigate]) *by*

Controls (Preventive) # Control 1: The suitability of possible design approaches on **Characteristics** (SFS [shape and layout {to minimize the need of attention to accept/reject the call}]) should be tested and compared by **Actors** (Players [manufacturer]) according to **Controls** (Principles [security vs. convenience]).

Controls (Deterrent) # Control 2 and 3: Although the mobile phones with keys are easy to use, they have gone out of use recently and touchscreen phones have been preferred for the maximum screen [Size]. Thus, accepting current **Characteristics** (SFS: [size; shape and layout]) trend, the other applicable **Controls** may be Control 2: using an auxiliary car kit that allows hands free use or Control 3: configuring the phone to auto accept incoming calls and turn on the speaker. These deterrent controls should be provided in the design of mobile device or the auxiliary kit. However, in scope of **Controls** (Principle [awareness]); **Actors** (End users) should be conscious so that they apply one of the suggested **Controls** to "prevent" accidents or at least not to attempt to accept the call at all in order to "avoid" accidents (the related concepts are shown in Figure 9 and Figure 10).

Controls (Deterrent) # Control 4: Today, some countries employ Legal Controls to "deter" related **Risks** by prohibiting the use of mobile phones while driving even via hands free methods.

This example shows that even a scenario-based risk (a car accident, see a related video picturing this critical risk at [37]) around a single characteristics of mobile computing (SFS) in scope of a single aspect of security (safety) presents many security concerns (e.g. risk responses, controls, and attack surfaces).

As seen in above example, even verbose usage of the taxonomy elements as distinguished and common keywords would make such security analyses structural, procedural, and standardized. This example consists of 12 classes, 16 subclasses, 10 elements, and 4 elements, total 42 nodes with 1 label except the mentioned controls. Our taxonomies can help analyzing, defining and stating the concerns in a systematic and easy way by providing the whole ingredients related to mobile security.

6.2. Example 2: Malware Analysis Based On Mobile Security Taxonomy

This example is more technical and practical in which we refer to a malware analysis report on a malware sample that causes several annoyances and provides revenue for its attackers [38]. The followings are the mobile security and malware analysis taxonomy units that are excerpted from the report structurally. Security researches and companies publish several reports like this example report. However, each of reports has its own style, order, outline, and terminology.

EXAMPLE 2. An Android **malware** taking control of the mobile device and gaining revenue through advertisement and malware installation without user consent.

Threats (Malware Infection; Remote Control; Information Leakage; Non Standard Monetization; Security Degradation; Annoyance; Inappropriate Content Exposure)

in **Layers** (Applications; Services; OS) where **OSs** (Mobile OS [Android])

by **Actors** (Attackers [malware author; thief; Attacker Traces {language signs in app; location; certification infos; interacted domains & IPs # the report provides the obtained values of each element for example, language := Chinese, interacted domains & IPs := # see the real entries in the report}])

to **Actors** (End users [profile {consumer}; Age Group {adult}]) *against* Mobile Assets (Personal; form [encrypted]; device [device identifiers {IMEI}]) via Malware (Trojan Horse; Botnet; Rootkit; Backdoor; Adware)@ Transformation ||(Forms [in the wild])

conducting **Attacks** (Privilege Escalation; Click Jacking; Theft)

by using **Propagation** (Other Channels [social media; 3rd party app market]; Deception Based [repackaging; dynamic payload])

by means of **Attack Vectors** (Dynamic Execution; Exploit; Aggressive Advertisement; Luring Users)

upon **Attack Surfaces** (Increasing-Reducing Factors [software {installation from unknown sources}])

exploiting

Vulnerabilities (OS [outdated OS # the malware cannot root devices with Android OS 5.0 and above))

Vulnerabilities (OS [misconfiguration # changing accessibility settings to automatically clicking the certain prompts such as install or yes for attacks a.k.a Click Jacking)

delivering

Payloads (46, downloading other potentially malicious files into the device)@Infection

Payloads (43, gaining highest privilege on the device's OS)@Infection

Payloads (35, modifying and deleting card contents)@File

Payloads (47, modifying the device's settings and system files)@Infection

Payloads (1, changing appearance -fonts, icons, logos)@Annoyance

Payloads (36, display ads in SMS messages)@Financial

MOBILE MALWARE ANALYSIS

Anti-Analysis (Obfuscation [packing string])

Anti-Analysis (Against dynamic analysis [data encryption in communications])

Like the first example, our taxonomy could also make such verbose reports structural and convenient. This example consists of 21 classes, 41 subclasses, 18 elements, and 9 elements, total 89 nodes with 7 labels that is more than the first example. As seen in both examples, we have also introduced specific conjunction keywords, which are shown in italic, to combine various taxonomic nodes to produce meaningful text. We will define such templates to enhance the usability and standardization. This approach supports ontological connections in the taxonomy.

7. Results

Although there has been a considerable amount of research on mobile malware detection and analysis [15], taxonomical studies that lay the background foundations have been a neglected area in the literature. Possible reason for this gap along with the major obstacles mentioned in Section 2.4 may be the earlier belief that there could not be a scientific basis for the classification of security, malware and malware analysis [39]. This study could be a very useful endeavor and a significant leap to fill such a gap.

Our mobile security taxonomy gives the entire perspective while our mobile malware analysis taxonomy provides advanced view in a separate taxonomy. The former is for any professionals in mobile computing industry and the latter is mainly for mobile malware analyst but they are meant to be interdependent.

The conceptual classes lay the fundamental background in a mobile specific context. The representation of the classes is enhanced via visualization methods. Especially, malware payloads and assets provide broad range of elements to the interested parties. For a quantitative perspective, Table 3 summarizes our taxonomies according to number of classes, subclasses, elements, subelements, attributes, and the total nodes. It also includes the

size metrics of three academic general knowledge taxonomies published by ACM, IEEE, and Thomson Reuters.

As seen in Table 3, our taxonomies have considerable amount of contents in vertical hierarch or depth (i.e. class, subclass, elements, subelements, and attributes). Figure 12 depicts the relative taxonomy sizes of different taxonomies namely academic general knowledge and reviewed security taxonomies. The followings are our main deductions of such a quantitative comparative analysis:

- Actual security related topics constitutes the very small portion of the three academic general knowledge taxonomies (ACM [4%], ScholarOne [1%], and IEEE [0.5%]; orange circles named 'Security' or 'Sec.' for short)
- Our mobile security taxonomy size is closer to those deeply rooted general knowledge taxonomies.
- The size of security related taxonomies in the literature is less than our mobile security taxonomy (maximum 16% and average 3%)

For a qualitative perspective, we have examined the security related taxonomies and matched to the content into our main classes that are explained in Section 3 in order to infer how they cover the whole security domain. Table 4 depicts the distribution of main classes per taxonomy and shows whether it is related to mobile security and defensive.

The order arrangement of the main classes (i.e. single dimensional) in Table 4 is the logical order that is transformed from the arrangement of those in Figure 1 (i.e. two-dimensional). Ignoring the domains, which can be a small subset of security, Table 4 makes clear that most of the taxonomies focus on narrow part of security such as on 'Attacks', 'Vulnerabilities', and 'Attack vectors'. Whereas some classes such as 'Payloads' and 'Assets', which are deeply analyzed and uniquely classified in our taxonomy, are not addressed sufficiently. Most of the taxonomies are also lack of defensive point of view. Only eight taxonomies (29% of all taxonomies) cover the defensive concepts.

In Table 4, the taxonomies are sorted according to the coverage column showing the percent of covered main classes. As an interesting finding, the taxonomy having the maximum number of nodes (total 179 nodes) does not necessarily have the maximum coverage (28%). Therefore, coverage should be a complementary factor of overall quality of taxonomies along with the size. Those factors could be the objective indicators of satisfying the 'completeness' and 'exhaustive' quality criteria of security taxonomies mentioned in Section 2.3.

Regarding to evaluation of our taxonomy's quality criteria; since the main classes of the taxonomy has been established by a well-defined method as depicted in Figure 1, it suffices the 'comprehensible', 'determinism', 'mutually exclusive', 'objectivity', 'primitive', 'repeatable', 'specific', and 'unambiguous' criteria.

Employing visualization techniques supports 'accepted', 'comprehensible', 'terms well defined', 'unambiguous', and 'useful' criteria. The compiled representative references and resources attached to the taxonomy enhances 'based on the code, environment, or other technical details', 'comprehensible', and 'terminology complying with established security terminology'. Since the nine conceptual classes provide a solid ground, they contribute to 'comprehensible', 'primitive', 'terminology complying with established security terminology', and 'terms well defined' criteria. 'Actors' class partially contributes to 'internal vs. external threats' criterion. Mobile specific 'Payloads', 'Assets', 'Propagation', and other classes covers 'Similar things classified similarly' criterion in high level. Another contribution of this study is the additional quality criterion

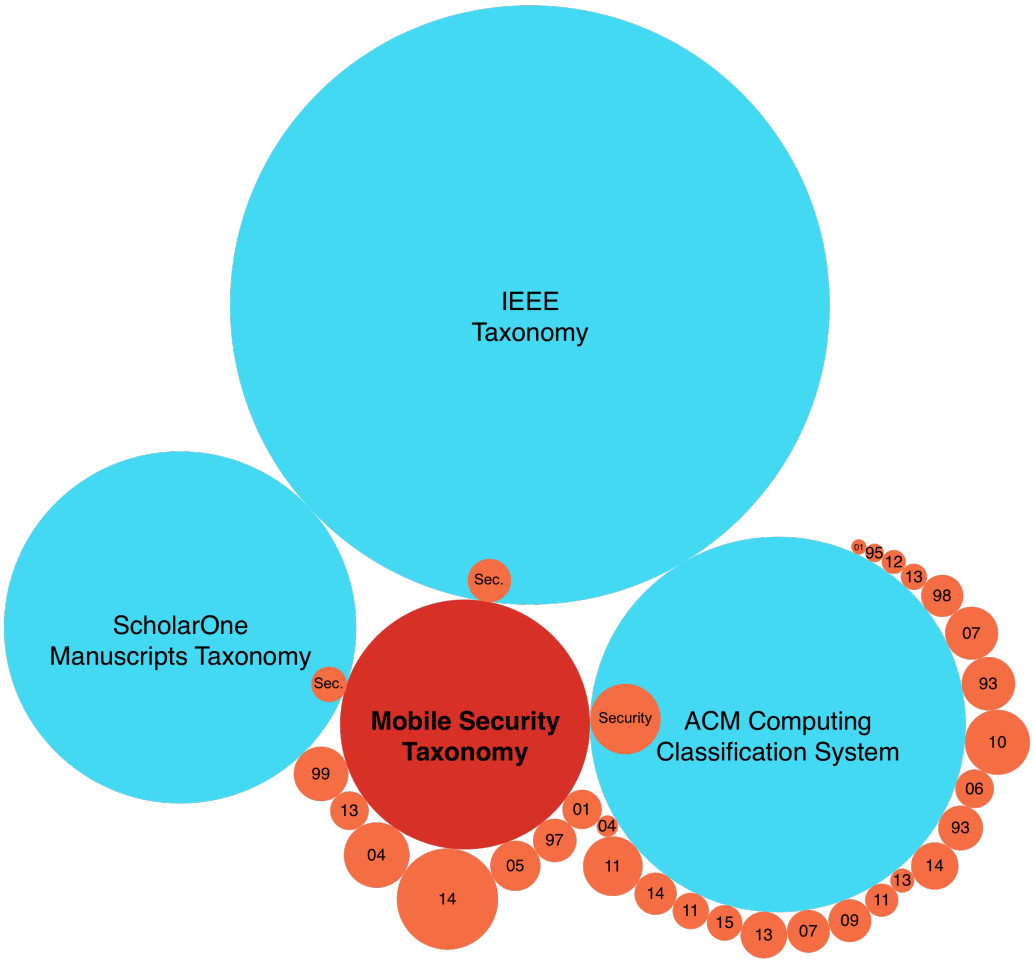

Fig. 12. Quantitative comparative analysis of taxonomy sizes (our mobile security taxonomy vs. other security taxonomies [orange, numbers are the last two digits of year] vs. academic general knowledge taxonomies [blue]))

that we have named as 'defensive vs. offensive separation'.

Indeed, as specified in Section 2.3 this separation should be the essential quality criterion. Although separating threats as internal vs. external is a recommended quality criterion, mobile threats are mostly external. However, we have categorized the treats into six types namely physical, criminal, technical, general, informational, and financial. Finally, our taxonomy complies with the quality criterion 'similar vulnerabilities classified similarly'. The vulnerabilities are organized in the following subclasses: operating system, application, information, and user. Therefore, the proposed taxonomies satisfy all the quality criteria. Only 'completeness' and 'exhaustive' criteria partly satisfied in the leaf nodes because of the dynamic and continuously developing characteristics of mobile security domain.

We have gained the following experiences as the results of completing the taxonomy building process. First, the established taxonomies have changed our view on mobile security and malware analysis. It has become obvious that both fields of study are extensive and intricate. Nevertheless, after laying the

foundations of taxonomy by determining the main classes in a consistent manner, the classifications became straightforward. Second, although the root of mobile security is similar to desktop computing security, we have seen that it has many distinctive aspects. Finally, from a psychological perspective, having such a handy map has encouraged us to delve further into specific details and made us highly motivated to add new concepts quickly.

8. Discussions

Some could perhaps argue that why we would need such a broad and detailed taxonomy. Beside such a global view in an especially sophisticated and holistic domain guides researches to define problems precisely, completely and very quickly, having all the defensive and offensive matters in a well-structured knowledge base allows accelerating and facilitating the related important processes on mobile security such as eliciting security requirements, analyzing threats, assessing risks, correcting vulnerabilities, establishing effective controls, improving security posture, analyzing malware, and establishing optimal malware detection.

As was mentioned in the Introduction, asymmetric characteristics and holistic requirements of mobile security requires a broad coverage. This also forces or at least facilitates the one of the crucial principle of effective security, 'lessons learnt'. Having a detailed taxonomy has help us to record the tangible concepts and findings such as controls against threats so that others can be aware of them later for similar purposes.

Our taxonomies provide a common language to convey information among interested parties. As described in Example 2, the results of unstructured and verbose security analysis could be codified by using taxonomic structures. The security approaches around desktop computing should set a good example for assessing the value of an established mobile security taxonomy. As seen in insufficient previous taxonomies reviewed, a major obstacle to establishing a comprehensive taxonomy on desktop computing is being too late to classify the developing and existing knowledge due to the extensive backlog. Our taxonomies could make a massive advance on time for addressing the lack of taxonomies on mobile security.

8.1. Benefits

The taxonomies presented in this article on mobile security and mobile malware analysis provide subjects that are mostly confused in academic literature and public resources or even not addressed 'in place' such as attack vectors, attack surfaces, payloads, and machine learning methods. Therefore, they could be used or give inspiration in other information and cyber security fields.

It may seem paradoxical that one of the most practical benefits of our taxonomies proposed in this study is to ease the researchers to spot the missing items by providing them the similar examples. Since the gaps can be only filled, after the known items are provided around the well-established backbone within the big picture. Otherwise, the missing parts could be forgotten or ignored. This might cause not to develop plausible solutions for the research areas.

By definition, well-structured taxonomies permit expansion and even reorganization. Therefore, the newly recognized and emerging elements could be easily added into a proper node. Eventually, continuously updating and improving the taxonomies that are outputs of our extensive literature survey could help to distinguish, understand, classify, measure, evaluate, and develop new techniques that could be synthesized by combining or relating the different taxonomic elements.

Another possible usage of our taxonomies is to give the ability to spot the areas where the attacks are occurred or which vulnerabilities are exploited at most, when the historical incident data is attached to the taxonomy. Versioning the taxonomy could allow seeing the chronology and evolution of newly developed defensive and offensive approaches.

8.2. Limitations

Although our taxonomies are not intended to be in a specific mobile product, it is inevitable to include some highlighted ones of leading platforms such as Android or iOS platforms. While we had done our best not to make a mistake or bare omissions in the taxonomy, it is likely that there may be some. Since this published study may give us the opportunity of receiving readers' feedback, the taxonomies would be more correct.

It should be noted that many of the contents of the classes in taxonomies such as attacks and malware could not be definitive for especially offensive point of view. Even with a more collaborated approach, it is not possible to circumscribe the attacker's options. Depending on their creativity and skills, attackers could revisit existing attacks, form hybrid attacks, and even arrange a completely new attack [40].

As the examples could be seen in the literature review in Section 2, some of the side elements and some types of labeling are not included in the taxonomy in the first stage. These elements such as impact, attacker motivation, threat source and scenario could be included to the mobile security taxonomy later.

8.3. Future Work and Challenges

For the present, the most of the elements in our taxonomies are grouped in a single level. Further to our research, we are planning to level them in further subnodes. This approach would especially beneficial for vulnerabilities, malware and malware analysis methodologies.

Future work will look into coding the taxonomical nodes in a systematic approach. Recognizing this coding as a common language to share information would be helpful especially while analyzing malware or defining the risks in academic and security community.

As anticipated, the ultimate success of such taxonomy depends on being its up-to-datedness. We hope that our taxonomies become living documents by collaborating the researches on updating them according to changes in threats, vulnerabilities, attacks, and malware methods as well as the technological improvements and solutions.

Security communities may have been working on the specific security taxonomies in strict manner. Any such a taxonomy could be referred from our umbrella mobile security taxonomy as a self-governing subtaxonomy. As we see in desktop computing security, the incident details and vulnerability databases on mobile computing could be bound into our taxonomy as metadata or historical data.

One possible suggested technique for complementing the freshness of our taxonomies would be adding a newly developed technology into the taxonomy and declaring it as a new attack surface. Subsequently, the possible threats, exploitable vulnerabilities, potential attack vectors, and the applicable controls around it can be figured out. Actually, every new development is a tempting challenge for attackers. Even white hat hackers want to reveal and announce proof-of-concept attacks while vendors invoke bug bounty programs.

The taxonomy could be a first step toward automatic information extraction from unstructured

sources such as a malware analysis reports and automatic interpretation of the available taxonomic information such as the tendency of a specific malware family. Our taxonomy can also guide the certification of mobile products according to the Common Criteria (ISO/IEC 15408) or information security management systems (ISMS) having mobile security concerns according to ISO/IEC 27001 information security management system standard.

We believe that our taxonomies could potentially lead to mobile security ontology by defining the relationship between the classes and nodes as explained in the given two examples above.

9. Conclusions

In this study, we have surveyed 28 security taxonomies since 1999, summarized their contents by using our notation and found that the majority of them insufficient to systematically classify even the small part of security from quantitative and qualitative perspective. Unfortunately, we haven't seen a significant security taxonomy on mobile computing which becomes the critical component of information or cyber security. Most of the taxonomies did not cover the defensive aspects and even follow a specific methodology.

We have developed a new levelling scheme to structure the taxonomy hierarchy and adopted a new notation to express the taxonomy contents in a compact form for the first time. These new approaches could be used efficiently for not only mobile security, as we did in this study, but also in other areas including cyber security as seen in our security survey.

This paper has also successfully introduced a novel method based on use and misuse case to establish the base of security taxonomy clearly and completely. Having a clear-cut distinction between the high level taxonomic structures (i.e. classes) makes the taxonomy building process straightforward, avoids misclassification and facilitates the reader's understanding. Again, the method is not specific to mobile security. It can be used in other security domains such as desktop security or cyber security successfully.

Using this method, we have provided the entire perspective of the two advanced fields on mobile computing namely 'mobile security' as a taxonomy and 'mobile malware analysis' as a subtaxonomy. The visualized taxonomies consist of total 1,322 nodes (14 classes, 177 subclasses, 528 elements, 382 subelements, 72 attributes, and 149 subattributes). According to our survey, these metrics are far from the 25 years' security literature. Especially the taxonomies in mobile scope provide less than 25 nodes.

Beyond the unmatched size of the proposed taxonomies, we have verified their efficiencies by examining the quality criteria for security taxonomies and giving some practical usage examples. Moreover, the taxonomies in nonvisualized form have been published online since April 2016 at http://bit.ly/securitytaxo and http://bit.ly/mobilemalwaretaxo to understand the merit of this work clearly.

Considering the unending asymmetric struggle between the defenders who must master the entire area to spot and avoid vulnerabilities and the attackers who seek for a tiny hole to bypass that security. Such a systematic big picture from both offensive and defensive view should always be provided to the defenders as well as the users for situational awareness.

As the mobile technologies become "all the time everywhere" and the purport of securing them effectively is to staying one-step ahead of attackers or at least following them closely and gaining the

overall visibility, the two proposed taxonomies are the first step towards enhancing our understanding of how to secure mobile environments in breadth and depth. The taxonomies also contribute to the continuous improvement that is one ultimate goal of security.

As a conclusion, our study provides taxonomies for a new platform to research, teach, learn, and state the subjects related to new developing fields on mobile computing: mobile security and mobile malware analysis for securing mobile platforms. The results of this study in generally support the idea that assuring the information, cyber, or mobile security is a comprehensive and stringent process and requires the explicit contribution of multi-disciplined approach. In this regard, we believe that our method could probably be employed in educational studies as well as the other advanced research and development studies in mobile security, mobile malware analysis and cyber security generally.

In our opinion, the manufacturers and professionals in mobile and security industry as well as the researchers, instructors and students in the academia could make use of the proposed visualized taxonomies in this study.

Acknowledgments

The authors would like to thank HAVELSAN for supporting this study.

References

[1] L. Howell, Ed., *Global Risks 2013*, 8th ed. Cologny/Geneva: World Economic Forum, 2013.

[2] *Global Risks 2015*, 10th ed., Cologny/Geneva, 2015.

[3] *The Global Risks Report 2016*, 11th ed. Cologny/Geneva: World Economic Forum, 2016.

[4] V. Melvin, M. Cousin, S. Thorne, L. Liu, and A. Cheeseman, "Threat Horizon 2016: On the edge of trust Review," Information Security Forum Limited, Tech. Rep., 2014.

[5] D. McMorrow, "Science of Cyber-Security," The MITRE Corporation, McLean, Virginia, Tech. Rep. November, 2010.

[6] C. von Linn, *Systema naturae per regna tria naturae: secundum classes, ordines, genera, species, cum characteribus, differentiis, synonymis, locis (System of nature through the three kingdoms of nature, according to classes, orders, genera and species, with characters)*, 10th ed. Stockholm: Impensis Direct. Laurentii Salvii,, 1758, vol. v.1.

[7] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," in *IEEE Symposium on Security and Privacy*. Oakland, CA: IEEE, 1997, pp. 154–163.

[8] R. P. Lippmann, D. J. Fried, I. Graf, J. Haines, K. R. Kendall, D. McClung, D. Weber, S. E. Webster, D. Wyschogrod, R. K. Cunningham, and M. A. Zissman, "Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation," in *Proceedings DARPA Information Survivability Conference and Exposition DISCEX'00*, vol. 2. Hilton Head, SC: IEEE, 2000, pp. 12–26.

[9] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, p. 39, 2004.

[10] M. Uma and G. Padmavathi, "A survey on various cyber attacks and their classification," *International Journal of Network Security*, vol. 15, no. 5, pp. 390–396, 2013.

[11] J. D. Howard, "An Analysis of Security Incidents on the Internet 1989 - 1995," Ph.D. Dis-

sertation, Carnegie Mellon University, 1997.

[12] M. Kjaerland, "A taxonomy and comparison of computer security incidents from the commercial and government sectors," *Computers and Security*, vol. 25, no. 7, pp. 522–538, 2006.

[13] S. D. Applegate and A. Stavrou, "Towards a cyber conflict taxonomy," in *The Fifth International Conference on Cyber Conflict*. Tallinn: NATO CCD COE, 2013, pp. 1–18.

[14] T. Rid and B. Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, vol. 38, no. 1-2, pp. 4–37, 2014.

[15] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 961–987, 2014.

[16] C. Alberts and A. Dorofee, "OCTAVE Threat Profiles," Software Engineering Institute, Pittsburgh, Tech. Rep., 2001.

[17] M. Bishop, "A Taxonomy of UNIX System and Network Vulnerabilities," University of California, Davis, Tech. Rep., 1995.

[18] C. E. Landwehr, A. R. Bull, J. P. McDermott, and W. S. Choi, "A Taxonomy of Computer Program Security Flaws, with Examples," Naval Research Laboratory, Washington, DC, Tech. Rep., 1993.

[19] D. L. Lough, "A Taxonomy of Computer Attacks with Applications to Wireless Networks," Ph.D. Dissertation, Faculty of the Virginia Polytechnic Institute and State University, 2001.

[20] J. J. Cebula and L. R. Young, "A Taxonomy of Operational Cyber Security Risks," Carnegie Mellon Software Engineering Institute, Hanscom AFB, Tech. Rep. December, 2010.

[21] J. Christy, "Cyber threat to critical infrastructure," in *The NEbraskaCERT Conference*, Omaha, NE, 1999.

[22] S. Hansman and R. Hunt, "A Taxonomy of Network and Computer Attacks," *Computers and Security*, vol. 24, no. 1, pp. 31–43, 2005.

[23] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, "AVOIDIT: A cyber attack taxonomy," University of Memphis, Tech. Rep., 2009.

[24] R. Hunt and J. Slay, "A new approach to developing attack taxonomies for network security - Including case studies," in *17th IEEE International Conference on Networks (ICON)*. Singapore: IEEE, 2011, pp. 281–286.

[25] P. G. Neumann, "Computer system security evaluation," in *1978 National Computer Conference Proceedings (AFIPS Conference Proceedings)*, S. P. Ghosh and L. Y. Liu, Eds. Anaheim, California: AFIPS Press, 1978, pp. 1087–1095.

[26] A. Algirdas, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[27] G. Canbek and S. Sagiroglu, "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme {Attacks against Computer Systems and Their Types: A Review Study}," *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, vol. 23, no. 1-2, pp. 1–12, 2007.

[28] ——, "Kötücül ve Casus Yazılımlar: Kapsamlı bir Araştırma {Malware and Spyware: A Comprehensive Review}," *Journal of the Faculty of Engineering and Architecture of Gazi University*, vol. 22, no. 1, pp. 121–136, 2007.

[29] K. Ivaturi and L. Janczewski, "A taxonomy for social engineering attacks," in *International Conference on Information Resources Management (CONF-IRM)*. AIS Electronic Library (AISeL) CONF-IRM, 2011.

[30] C. F. M. Foozy, R. Ahmad, M. F. Abdollah, R. Yusof, and M. Z. Mas'ud, "Generic taxonomy of social engineering attack," in *Malaysian Technical Universities International Conference on Engineering Technology MUiCET 2011 (2011)*, 2011, pp. 527–533.

[31] A. Amamra, C. Talhi, and J.-M. Robert, "Smartphone malware detection: From a survey towards taxonomy," in *7th International Conference on Malicious and Unwanted Software (MALWARE)*. Fajardo, PR: IEEE, oct 2012, pp. 79–86.

[32] C. F. M. Foozy, R. Ahmad, and M. F. Abdollah, "Phishing Detection Taxonomy for Mobile Device," *International Journal of Computer Science Issues (ISSN)*, vol. 10, no. 1, pp. 338–344, 2013.

[33] A. Algarni, Y. Xu, Taizan Chan, and Yu-Chu Tian, "Social engineering in social networking sites: Affect-based model," in *Proceedings of the 8th IEEE International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, 2013, pp. 508–515.

[34] A. Mylonas, "Explo(r—it)ing the User's Exposure to Security and Privacy Threats in the Smartphone Ecosystem," Ph.D. Dissertation, Athens University of Economics & Business, 2014.

[35] R. Heartfield and G. Loukas, "A Taxonomy of Attacks and a Survey of Defence Mechanisms for Semantic Social Engineering Attacks," *ACM Computing Surveys*, vol. 48, no. 3, p. 39, 2015.

[36] C. W. Hanson, "Mobile devices in 2011," in *Library Technology Reports*, 2011, ch. 2, pp. 11–23.

[37] "Eyes on the road," 2014. [Online]. Available: https://youtube.com/watch?v=R22WNkYKeo8

[38] Y. Zhang, Z. Chen, and Y. Kang, "Guaranteed Clicks: Mobile App Company Takes Control of Android Phones," FireEye, Tech. Rep., 2015. [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/09/guaranteed_clicksm.html

[39] J. D. Aycock, *Computer viruses and malware*. Springer, 2006.

[40] M. Bailey, S.-P. Oriyano, and R. Shimonski, "Dissection of a Client-side attack," in *Client-side attacks and Defense*. Waltham,MA: Syngress, 2012, ch. 2, p. 26.

TABLE 1
Proposed Notation for Leveled Taxonomic Enumeration

Level	**Taxonomic Type**	**Abbreviation**	**Format**	**Boundary or Delimitation**
1	Classes	C	Title Case, **bold**	
2	Subclasses	SC	Sentence case	between ‘(’ and ‘)’
3	Elements	E	lowercase	between ‘[’ and ‘]’
4	Subelements (or examples)	SE	lowercase	between ‘{’ and ‘}’
5	Attributes	A	lowercase	between ‘<’ and ‘>’
6	Subattributes	SA	lowercase	between ‘/’ and ‘/’
7	Features	F	lowercase	between ‘|’ and ‘|’
8	Subfeatures	SF	lowercase	between ‘\’ and ‘\’
Any	Nodes	N		delimited by ‘;’
Any	Nodes (Common Parent)	N		delimited by ‘||’
Any	Attached label or tag	N		@label or @tag after N or Ns
Any	Attached label or tag	N		# after N or Ns

TABLE 2
Mobile Malware Payloads

Nr	Payload	Nr	Payload
1	Changing appearance (fonts, icons, logos)	36	Display ads in SMS messages
2	Changing browser home page	37	Displaying premium ads
3	Fake antivirus	38	Installing other (Premium) applications
4	Playing audio ads upon dialing a number	39	Making changes in user bills or balance
5	Churning out notifications	40	Making paid service (Premium) calls
6	Running an application	41	Receiving commissions per malware installation
7	Sending list of permissions requested by host application	42	Sending SMS messages (to Premium number)
8	Crashing applications	43	Gaining highest privilege on the device's OS
9	Disabling applications	44	Adding bookmark to browser
10	Hiding/redirecting application	45	Downloading malicious files via NFC-tags, bar or QR codes
11	Unconditional/conditional call forwarding	46	Downloading potentially malicious files into device
12	Call forwarding of outgoing calls	47	Modifying the device's settings and system files
13	Generating fake Call	48	Reverse Shell over Cellular Network or Wi-Fi
14	Listening calls (eavesdropping)	49	Intercepting browser session
15	Monitoring calls	50	Accessing the Internet
16	Delete call logs	51	Gathering browser history
17	Mute phone ring	52	Concealed Bluetooth connection
18	Modifying ring settings	53	Toggling the Cellular network on and off
19	Ending out-going call	54	Toggling the Wi-Fi on and off
20	Unblocking stolen mobile devices	55	Collecting online accounts and passwords
21	Blocking operating system functions	56	Monitoring E-mails
22	Controlling camera	57	Capturing contact information
23	Circumventing audio/visual sensor in use notification	58	Keystroke logging
24	Blocking after reboot	59	Recording voice through Bluetooth
25	Freezing operating system	60	Recording voice through microphone
26	Avoid auto-locking	61	Screen capturing
27	HTTP flooding on a victim URL	62	Sending camera pictures/videos
28	Darkening screen	63	Tracking phone's location
29	Lock screen	64	Changing contacts
30	Locking SD/MMC cards	65	Deleting contacts
31	Accessing the device's SD/MMC card	66	Generating fake SMS
32	Transferring files (data exfiltration)	67	Monitoring SMSs
33	Encrypting disk	68	Coming SMS spam (operator channel)
34	Encrypting files	69	Changing SMS content
35	Modifying and deleting card contents	70	Removing SMS notification

TABLE 3
Size Metrics of Our Taxonomy Contents

Our Taxonomies	**C**	**SC**	**E**	**SE**	**A**	**SA**	**Total N**
Mobile Security Taxonomy (Conceptual Classes)		6	43	145	12	3	209
Mobile Security Taxonomy (Core Classes)	14	150	328	96	19		607
Mobile Security Taxonomy Totals:	14	156	371	241	31	3	816
Subtaxonomies	**C**	**SC**	**E**	**SE**	**A**	**SA**	**Total N**
Mobile Malware Analysis		9	63	54	36	146	308
Machine Learning		12	94	87	5		198
GLOBAL TOTALS:	14	177	528	382	72	149	1322
Other General Knowledge Taxonomies[1]	**C**	**SC**	**E**	**SE**	**A**	**SA**	**Total N**
ACM Computing Classification System[2]	1/14	11/88	51/926	24/1079	0/333		87/2465
IEEE Taxonomy[3]	0/49	1/677	12/2502	20/3053			33/6281
ScholarOne Manuscripts Taxonomy[4]	0/15	0/115	2/594	20/1438	0/5		22/2167

1. Size metrics are given as a fraction: security related nodes/total nodes **2.** ACM Computing Classification System, 2012: Class: Security and privacy (total 79 N); Elements: Network security (total 6 N); Subelements: Theory of database privacy and security; Cyberwarfare (total 2 N) **3.** IEEE Taxonomy, 2014 Subclass: Security (11 E, 18 SE); Elements: Communication system security; Subelements: Radio communication countermeasures; Information security **4.** ScholarOne Manuscripts Taxonomy, Retrieved January 2016 Elements: Security and privacy protection (7 SE); Security and protection (5 SE); Subelements: Support for security; Network-level security and protection; 2 x Security, integrity, and protection; 2 x Security; Internet security polices; Mobile code security

TABLE 4

Qualitative comparative analysis of taxonomy contents according to security main classes