Bring Your Own Disclosure: Analysing BYOD Threats to Corporate Information

Denys A. Flores *†, Farrukh Qazi*, Arshad Jhumka*
*University of Warwick. Department of Computer Science. Coventry, United Kingdom
d.flores-armas@warwick.ac.uk, f.a.qazi@warwick.ac.uk, h.a.jhumka@warwick.ac.uk
†Escuela Politécnica Nacional. Departmento de Informática y Ciencias de la Computación (DICC). Quito, Ecuador
denys.flores@epn.edu.ec

***Abstract*—Mobile device consumerisation has introduced the Bring-Your-Own-Device (BYOD) trend to the organisational context, allowing employees to work using their personal devices. However, as personal mobile devices are perceived as less secure than those provided by the organisation, BYOD has risen security concerns about corporate information being accessed by mobile devices from inside and outside the corporate perimeter. Moreover, this uncontrolled mobile device activity makes it difficult to differentiate external (outsider) malicious activity from reckless/naive employee (insider) behaviour, preventing effective correlation of unauthorised actions with the perpetrators. In this paper, a *STRIDE-based BYOD Threat Model* is proposed to analyse *BYOD Threat Interactions* from inside and outside the corporate perimeter. Our research contributes to a better understanding and awareness about the influence of BYOD Threats on disclosure and contamination of corporate information, encouraging future work in the field of BYOD security and digital forensics in order to protect information and manage an increasing number of evidence sources.**

***Index Terms*—BYOD, threat model, STRIDE, disclosure, contamination, insider, outsider, attack, forensics.**

I. Introduction

Bring-Your-Own-Device (BYOD), or Dual-Use Devices [1] is a growing trend inside organisations [2] due to the ever increasing mobile device consumerisation phenomenon [3][4]. Actually, BYOD is now a common practice which has increased employee access to new mobile technology [5], and has improved their productivity and satisfaction [1]. As a consequence, organisations allow and even encourage employees to use their preferred personal mobile device [3][6] for accessing corporate information assets [7][8][9].

On the contrary, as corporate technology adoption is currently being driven by employees [5][10], organisations have very little (or no) control over mobile device activity [4][11][12] as well as the security conditions that employees are accessing corporate information with [13]. A case in point is the traditional corporate scenario, where employees were provided with desktops and laptops [14], giving organisations complete security control over these devices, and expecting security threats to be mainly perpetrated by cybercriminals (outsiders). However, as BYOD takes over, organisations struggle to determine whether threats to corporate information are posed by cybercriminals (outsiders), or by a trusted employee (insider) who may compromise corporate information, either maliciously or mistakenly [15].

Then, adopting BYOD not only gives benefits [1][7][13][16], but also introduces potential security threats due to uncontrolled mobile device access to information assets [8] which, if not handled correctly [5][14], may lead to corporate information disclosure [17] or contamination [16]. Also, challenges for security professionals and digital forensic investigators [18] are posed, as BYOD brings on a vast number of evidence sources (information, operating systems and formats) [19], hindering any future effort to correlate unauthorised actions with the perpetrators.

Hence, this article begins discussing BYOD Threats in order to define general *External and Internal BYOD Threat Contexts* (Sections II and III, respectively) in which BYOD practices may compromise corporate information, leading to digital forensic investigations [20]. Next, potential threats to corporate information are determined by applying the *STRIDE Threat Modelling* approach to a common corporate BYOD scenario (Section IV). Here, the identified *External and Internal BYOD Threat Contexts* are considered to define *Trust Boundaries* so that *BYOD Threat Interactions* from inside and outside the corporate perimeter can be analysed.

Subsequently, by analysing these interactions (Section V), possible attack vectors, leading to information disclosure and contamination can be defined. For this analysis, relevant research literature and security reports have been considered so that the proposed *Threat Model* can be used for a better understanding of real world BYOD cases in which corporate information may be either disclosed or contaminated, requiring further digital forensic investigations.

Finally, in Section VI, an explanation of related and future work in the field of BYOD security and digital forensics is given, followed by conclusions of our current research (Section VII).

II. External Threat Context: Still the BYOD Criminal Playground

Cybercriminals (outsiders) are currently targeting unprepared organisations to access information assets by using emerging technologies and communication channels [21]. Since the inception of BYOD in the enterprise and employee's access to more sophisticated and convenient technology [3], it is easier than ever for an outsider to steal information or obtain financial gain [22]. Actually, because of the lack of

security awareness, outsiders have an advantage point to access corporate information by turning employees' normal leisure activities into attack vectors [11], making it difficult to investigate illegal actions. Thus, downloading mobile applications or sharing content on social networks may be backdoors for disclosing or contaminating sensitive corporate information through a range of different external threats, the contexts of which are explained as follows.

A. Malware

Since 2011, the number of mobile malware families have increased 58 per cent [11] and malware samples increased more than 10 times between July 2012 and January 2014 [22]. This suggest that malware is still the most dangerous and persistent threat to corporate information. In the BYOD context, existent security vulnerabilities in employees' mobile devices [13] are exploited by malware to steal confidential information [11], sabotage networks or deviate financial transactions [23]. Moreover, since the BYOD inception, IT departments have lost control on mobile devices, which means that accidental malware infections may be undetected [14], and therefore very difficult to investigate.

B. Phishing

Attackers are becoming more creative, not only with malware, but also phishing scam which is getting more space in the cyber threat stage [10]. For instance, a well-constructed phishing email (spear phishing) or fraudulent SMSs [22] may even evade traditional network security devices (firewall, IDSs and antivirus) [23] in order to steal personal information, or obtain financial gain. Also, since this threat spreads with ease in unacknowledged employee collaboration environments, social networks and cloud services become the perfect "bait" to catch naive users [15]. Thus, very little readiness to timely investigate and respond to security incidents is revealed since majority of organisations with poor security awareness fully entrust BYOD protection strategies to the employee's security common sense [11].

C. Social Engineering

The lack of security awareness and broad adoption of mobile devices [10][12], makes social engineering another persistent threat in the BYOD context. As people are still the weakest security link inside organisations [15], attackers send spam on emails and social networks to spread malware [11][12][15], taking advantage of human emotions [10]. Hence, naive users who check emails and use social networks during leisure breaks, increase infection opportunities to the corporate network [14] because the activities performed in their personal mobile devices are harder to monitor and control [12], making it difficult to acquire first-hand evidence.

D. Malicious Mobile Applications

Regardless of the device ownership (company or employee owned), employees install non-corporate and unauthorised applications either to aid their daily work activities [3][11], or for personal leisure and socialisation [9]. As a consequence, these applications may introduce serious threats to corporate information as some of them may be used by attackers to collect and disclose sensitive information, once installed on the device [10]. Additionally, "rooted" mobile devices (Section III-B) may give more privilege to malicious applications to disseminate spam and send anonymous device information [2] to an unknown outsider whose actions are not under corporate supervision, and may not be investigated properly.

E. Insecure Wireless Networks

The BYOD trend has also been encouraged by the employee's accessibility to more advanced technology outside the office [3]. This includes faster home and public wireless networks with unknown security configuration [16], which are far from the forensics and security organisational scope, but closer to sensitive information assets that employees access through them [4]. As a result, interception attacks can be easily launched through insecure communication channels [9][13] where they can go undetected, as long as the attacker and the victim are in the same wireless signal range [4].

F. Fake Certificate Authorities

Digital Certificates are still a trusted means for authenticating computers over the Internet, as long as they have been issued by a trusted Certificate Authority (CA) [24]. Actually, mobile devices not only come with preloaded CA credentials from factory, but also enable users to either add their own, or remove existing ones [2], if convenient. Considering this, corporate information can be compromised if a naive employee has been persuaded to add a fake CA to a mobile device, or if a trusted corporate digital certificate has been impersonated [9]. In either case, employees may be deceived to access "bogus" digital-signed services where attackers may steal credentials or sensitive corporate information without leaving any evidence of their actions.

G. Denial of Service

Denial of Service (DoS) is sometimes an overlooked threat because recent advances in high-availability computing prevent service disruption by using redundancy and backup strategies [1]. Although these attacks are currently being used as a diversion to launch more sophisticated and complex ones [21][23], the emerging BYOD paradigm facilitates them because of the uncontrolled number of mobile devices that join corporate networks. In fact, the more connected devices the more resource consumption [12] and without proper network infrastructure planning [14], attacks against important evidence sources, such as databases and log repositories may be undetected.

III. Internal Threat Context: Malicious or Naive Employee Actions?

Currently, BYOD adoption has promoted a mobile device acceptance wave [3][5][10] fully driven and promoted by the employee's device appropriation and initiative [5]. As a result,

organisations are left with almost no control over these devices [14][16], and much less over the actions performed through them which are important to know in order to investigate security breaches. For instance, a naive employee, ignoring company security policies becomes an internal threat [13], if installing an unauthorised application in his mobile device introduces malware that was not specifically targeting the organisation, but may create the perfect opportunity for an undetected and unknown outsider to access corporate information assets [22][25]. Meanwhile, databases may be tampered with by a reckless highly-trusted employee who is trying to deceive the organisation[26] by misusing his access credentials [27]. Hence, although these illegal actions may be investigated if proper auditing is enabled, in the BYOD context, it is more difficult to audit and control trusted insiders' actions [12] because digital investigations might be challenged by the following internal threat contexts.

A. Uncontrolled Inception of Heterogeneous Devices

Heterogeneous mobile devices that connect to corporate networks significantly increase threats to sensitive information [9]. Depending on the internal support level that IT departments give to the increasing and uncontrolled range of mobile devices available [5], these may not be compatible [3] with the organization security measures, configurations [2] or applications [4]. Consequently, mobile hardware and operating system fragmentation [22], may prevent that minimum security requirements can be met [7] to protect corporate information that these devices access to, making it very difficult to define digital forensics and incident response practices that encompass BYOD emerging technologies [28].

B. Mobile Device Misconfiguration

Misconfiguration in mobile devices can happen by giving elevated privileges either to mobile applications, or to the device user himself (root privilege). The former occurs when a user is required to give access authority to privileged information, applications [29] and configurations [10]. The latter happens when users choose to unlock (aka root or jailbreak) their mobile devices [3] for using the operating system with administrator permission [2], or when IT departments are required to "jailbreak" mobile devices in order to control and monitor them [3]. Hence, mobile device misconfiguration poses an evident dilemma regarding giving elevated privileges to applications and "rooted devices" because security issues may be faced even if rooting devices is required for monitoring and control. Also, since malicious applications may obtain potential access to collect sensitive corporate information [10], or perform network-related attacks [2], certain misconfigured device functionality, such as automatic data streaming, backup and content sharing [8] may pose serious threats to corporate information as well as disseminating evidence in different repositories which may be out of the organisation's control.

C. Information Sharing on Personal Cloud Services

Employees use mobile devices in different contexts [3] not only for personal reasons, but also for continuing working outside the workplace [13]. Thus, personal cloud services, in particular cloud storage [12], are used to increase employee productivity [7] as well as availability and flexibility [12] for accessing corporate and personal information on the same device [10]. However, as mobile devices and cloud storage sites are exposed to hacking activities and malware infection [16], sharing information on cloud services may expose sensitive information to unauthorised disclosure [3][12], or corruption [23]. Also, employees can share and modify information on their devices[16], affecting information security and intellectual property compliance [12][22], making it more difficult to ensure information integrity and confidentiality, and requiring organisations to get more control over evidence traces that may be left on cloud repositories [19].

D. Mixture of Personal and Corporate Information

Employees prefer using their own mobile device [2] in order to keep contact with family and friends [6] whilst working. In addition, organisations allow employees to use their devices to connect and access corporate networks, databases, and servers [7] to facilitate their work and increase their productivity. Nonetheless, accessing and storing both personal and corporate information in the same device [7] is a threat that may compromise corporate information integrity due to the complexity to differentiate and separate personal from corporate information [13], along with the uncertainty of corporate resource usage on the employees' mobile devices [3], which may prevent effective monitoring of unauthorised actions for further investigation.

E. Lost, Stolen and Unlinked Mobile Devices

Employees may have enabled the "remember password" feature on web browsers and applications, or may have chosen to remain logged into their on-line accounts [11]. Then, if lost or stolen, the device will put in hands of an outsider, login credentials [16] to be used to access multiple services [11][17]. On the contrary, some employees keep corporate information on their mobile devices [16], even after they have been "unlinked" from the corporate network in case of termination of employment [3]. This last scenario is particularly dangerous because it can expose corporate information and services [4] to intellectual property violations, or disruption of critical business obligations [12] if a vengeful employee wants to attack corporate information assets as retaliation for having lost his job. If the mobile device is not controlled, even after termination of employment, the risk of identity forgery increases [10], reducing the possibility of finding the real culprit in case of security incidents.

F. Information Ownership

In the past, organisations provided laptops and mobile phones for professional purposes only [14]. Currently, employees' preference to work with their own device [2] has shifted the balance of device control from the organisation to the employee [4], opening a gap related to information ownership. For example, if employees own their devices,

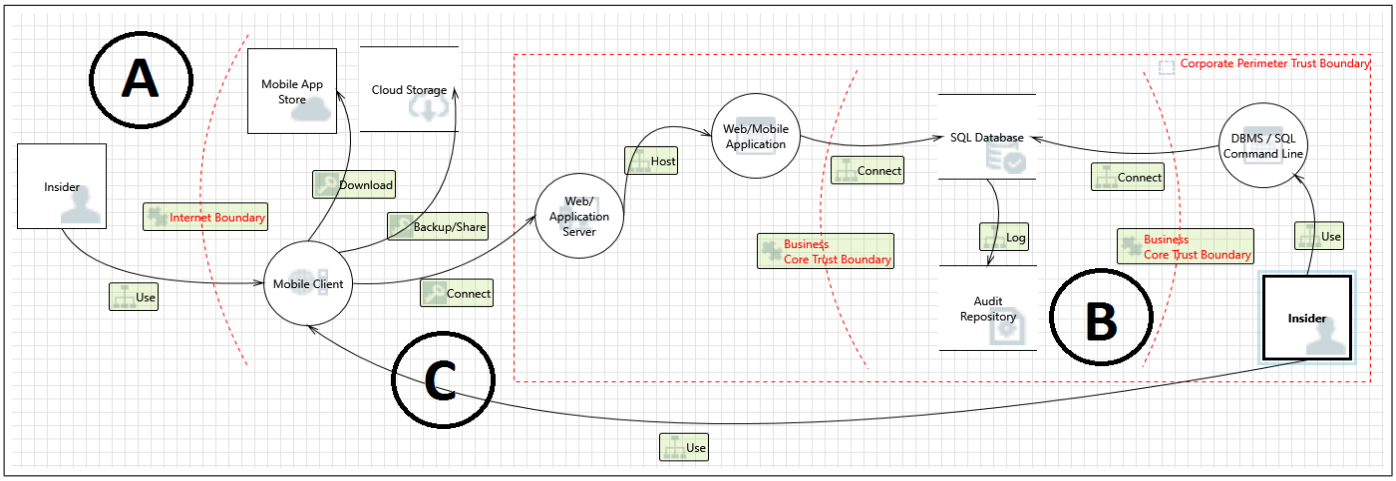

Fig. 1. BYOD Threat Model representing insider activity from inside and outside the CPTB

the company may not have much control over them [7], including over the information that is generated and stored in them. Conversely, if technologies already being used in the organisation are used by the employee on the device [4], the information generated by them and stored in the mobile device belongs to the company [2][6], granting property rights over it. However, in case the organisation, by exercising its lawful right to protect its information, decides to remotely wipe the mobile device if stolen, lost, or if the employee leaves the organisation [6], all the information, including the employee's may be lost forever. Also, if the company wants to investigate an employee-owned device, legal procedures must be placed to avoid raising privacy and ownership violations [18].

IV. Modelling BYOD Threats to Corporate Information

After having identified the *BYOD Internal and External Threat Contexts*, it is evident that corporate information is an important asset that must be protected [3] as in the BYOD paradigm corporate information (and digital evidence) may reside in a variety of electronic media repositories, from file systems and databases (owned by the company) to laptops, tablets and phablets (owned by the employee). Thus, information security concerns increase when dealing with BYOD [16] because personal and corporate data becomes more disperse, mixed and uncontrolled. Moreover, uncontrolled BYOD activity may expose corporate information to outsider and insider threats, leading to potential data disclosure [4][16] and contamination. [2][16][23]. Hence, our research analyses the *BYOD Threat Interactions*, applying the *STRIDE Threat Modelling* approach [30] to a common BYOD scenario (Figure 1). This *STRIDE-based BYOD Threat Model* represents the *interactions in between a trusted employee (insider) and corporate information assets, from inside and outside the corporate perimeter*, providing a better understanding of the *BYOD Threat Environment* that organisations need to consider in order to define their security and forensics readiness policies [28] to prevent disclosure or contamination of corporate information. This *BYOD Threat Model* considers the previously analysed *BYOD External and Internal Threat Contexts* to define the following *Trust Boundaries*:

A. Internet Trust Boundary (ITB): It is placed outside the *Corporate Perimeter Trust Boundary (CPTB)* to represent *lower-trust insider activity*. This trust boundary represents a scenario in which *External BYOD Threats* can compromise corporate information assets due to *uncontrolled insider activity* through mobile clients. Whilst these clients interact with Internet-located personal cloud storage services and mobile application stores, they may be simultaneously accessing corporate-owned web applications/servers, as shown in **Figure 1-A**. Here, it is assumed that connections, downloads, and sharing activities are performed using secure communication channels in between the mobile clients and the services.

B. Business Core Trust Boundaries (BCTB): These are represented inside the CPTB to depict *higher-trust insider activity* from within the corporate perimeter. In **Figure 1-B**, a *CPTB-located insider* interacts with a relational database and an audit repository using a DBMS/SQL Command Line Client, which represents not only sensitive information repositories, but also important evidence sources for audit and forensic purposes.

C. Corporate Perimeter Trust Boundary (CPTB): In this *BYOD Threat Model*, *Internal/External Insider Interactions* are delimited inside and outside the CPTB. As shown in **Figure 1-C**, these interactions are represented by a *CPTB-located insider* who uses an *ITB-located Mobile Client*, not only for interacting with corporate Web/Mobile Applications, but also for accessing Mobile App Stores and Cloud Storage Services for external mobile application downloading and file sharing activities, respectively.

A. Threat Modelling Results

After modelling the proposed BYOD scenario using STRIDE (Figure 1), 76 threats were identified; the most relevant threats are shown in Table I.

TABLE I
IDENTIFIED BYOD THREATS APPLYING STRIDE

ID	Threat	Attack Vector	Insider	Outsider
I01	Data Flow Interception	Attacker sniffs data flow to capture info.	x	x
I02	DB Credential Interception	S01; S02; I01; T03; DB credential stolen	x	x
I04	Disclose info. in Cloud Storage	Share info in cloud storage.	x	
I05	Mobile Device Lost/Stolen	Info/Credentials stored in the mobile device		x
D01	Excessive Resource Consumption	Unhandled resource consumption in DB or Web/Mob. App.		x
D02	Data Flow Interruption in Web Server/DB	D01; E01; An attacker forces data flow to stop/change.	x	x
D03	DB Unavailable	D02; Data reception is interrupted	x	x
D04	Log Repository Unavailable	D02; Logs not enough/unavailable	x	x
E01	Buffer Overflow	E03; change data flow/app. execution		x
E02	Social Engineering	Deceive user to disclose info.		x
E03	Malware/Botnet	Remote Code Exec. through Mobile Client		x
E05	DBMS/SQL Command Line Misuse	Unauth./Misused DB Access	x	
S01	DB Forgery	Change destination of SQL DB	x	x
S02	Web Server/Mobile App.Forgery	Change destination of web serv/mobapp		x
S03	Cloud Storage Forgery	Change destination of Cloud Storage		x
S04	Unauth. Access to SQL DB	DBMS/SQL Comm. Line Spoofed	x	x
T01	SQL Injection	Bad select statem. from web/mobileapp. to DB	x	x
T02	DB Corruption	R03; T01; T03; Data flow modified before reaching DB.	x	x
T03	XSS in Web/Mob. App.	User input is not sanitised.	x	x
R01	Data no Received	D03; Repudiate activity in DB.	x	
R02	Untraceable Cloud Activity	Repudiate activity in cloud storage.	x	
R03	Insufficient Web Server / DB Auditing	R01; R02; Not enough audit logs	x	x

Each threat ID begins with the initial of the six threat categories considered by this threat modelling approach [30]: *(S) Spoofing, (T) Tampering, (R) Repudiation, (I) Information Disclosure, (D) Denial of Service and (E) Elevation of Privilege*. The likelihood of being performed by Insiders and Outsiders has also been considered to provide a better understanding of insider/outsider threat interaction in the BYOD context.

V. CHALLENGES OF BYOD THREATS TO SECURITY AND FORENSICS

The results in Table I are not enough to understand the interactions and influence that each one of them may have over corporate information. Therefore, based on the most relevant identified threats in Table I, further analysis was performed to determine the interactions amongst them, considering relevant research literature and security reports so that the proposed BYOD Threat Model can be used to understand real threat scenarios that may challenge security and forensics strategies to prevent disclosure or contamination of corporate information.

A. BYOD Threats leading to Information Contamination or Corruption

In BYOD, *keeping information integrity is more challenging* [3] due to threats related to employee habits towards access and usage of corporate information assets [2], which can expose information to data contamination [23]. For instance, as shown in Figure 2, Tampering threats may be used by insiders and outsiders as attack vectors to corrupt corporate databases through SQL injection or Cross Site Scripting (XSS) attacks. Similarly, an outsider or a malicious insider may use DoS attacks to interrupt the data flow to the database, or to the audit log repository, bringing on *Repudiation issues* due to insufficient or inexistent audit trail generation which challenges forensic investigations.

Actually, insider and outsider malicious activity against

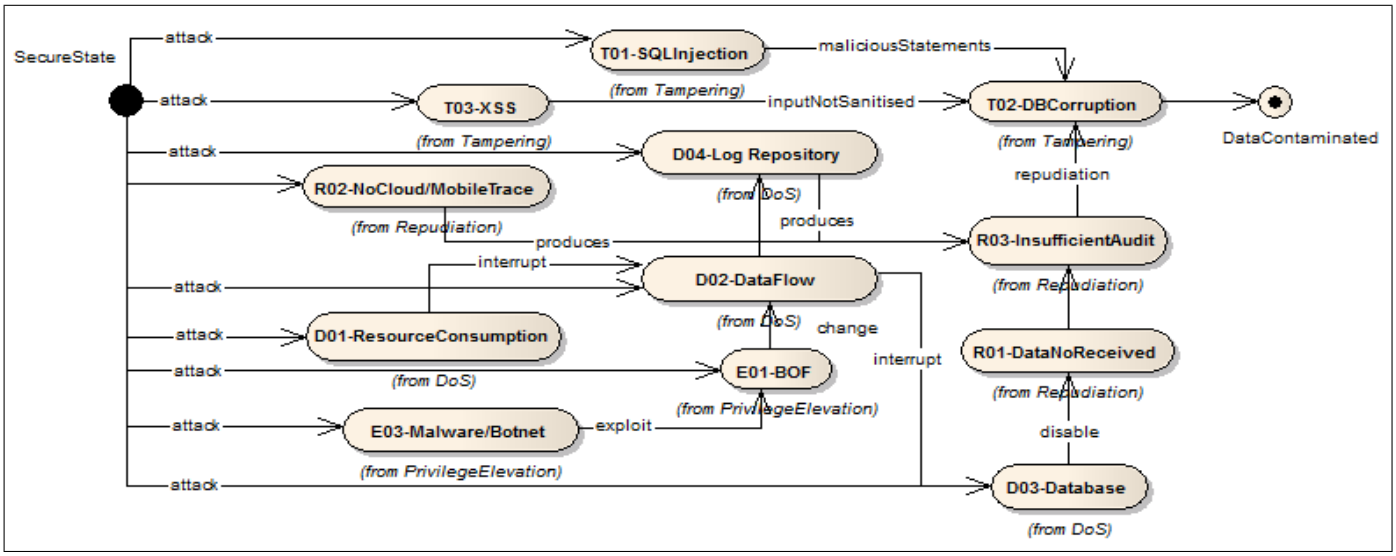

Fig. 2. Interactions amongst BYOD Threats that may lead to information contamination

corporate data was already reported back in 1975 [31], where computer systems vulnerabilities were known as means for gaining operative system control in order to, firstly, disable accounting and auditing programs (log and audit repositories), and then read or modify programs and data without being detected. This scenario has not changed much in recent years as these actions are still being carried out by malicious database administrators (DBAs), urging database vendors and security professionals to issue security bulletins to mitigate malicious insider risks [32] along with advice on insider activity detection and prevention [33], which is vital for forensic readiness purposes [28].

Conversely, malware was always related to malicious outsider activity to contaminate data, and has been associated with DoS attacks and data flow interruption, which urged U.S. Courts to incorporate changes to their Computer Crime Laws, early during the '90s [34]. Nonetheless, it has been reported [35] that malware is used by insiders as "retaliation" for employment termination in order to damage information, or infecting corporate networks using USB devices as when the Stuxnet worm infected Iran's uranium facilities [36].

Thus, before BYOD, organisations had control over the information assets used by employees to access corporate information, making it easier to detect and investigate malicious insider activity. Now, it would be almost impossible to determine if certain attacks are linked to malicious outsiders, or in the worst scenario, to naive or reckless insider behaviour [37], such as accidental malware infections [14], or risky file sharing in Cloud Storage Services [23], respectively. As shown in Figure 2, the proposed BYOD Threat Model may be considered accurate and simple enough to depict not only BYOD threats to corporate information integrity, but also their interactions, providing better understanding of possible attack vectors that can be used to investigate information contamination by either malicious employees (insiders), or cybercriminals (outsiders).

B. BYOD Threats leading to Information Disclosure or Leakage

As previously discussed, in BYOD contexts, mixture of personal and corporate information (section III-D), exposes the latter to attacks [2] that may lead to *unauthorised disclosure, compromising information confidentiality*. Since organisations are usually prepared to defend the corporate perimeter [12] against outsider attacks in the Internet Trust Boundary (ITB) (Figure 1-A), they overlook security measures in the Business Core Trust Boundary (BCTB) (Figure 1-B), allowing insiders to become dangerous threats to information assets, and preventing effective investigations to find the perpetrators. This is an evident effect of the lack of insider activity control, either being illegitimate (privilege misuse, financial gain) or naive (victims of social engineering or malware) [38].

On the other hand, although some companies are reluctant to give employees more freedom over corporate information [5], employees keep using cloud services to share information (section III-C), which may lead to security implications and regulatory compliance issues [9]. However, file sharing in Cloud Storage Services is not the only problem to consider. In fact, data leakage can also happen when mobile devices are lost [11][12][23], stolen[4][2], or unlinked from the organisation in case of termination of employment [3][4]. This scenario has been depicted in the proposed BYOD Threat Model (Figure 3) as lost, stolen or unlinked mobile devices are usually ignored evidence sources and information repositories that can be lost forever when an employee leaves the organisation [39]. Additionally, disclosing information nowadays is not just about stealing data in transit, but also data at rest (stored in databases) that could be threatened by any vulnerability, as reported by TrustWave in 2014 [40]. This has been represented in Figure 3, where the proposed BYOD Threat Model also depicts classic *Spoofing and Tampering*

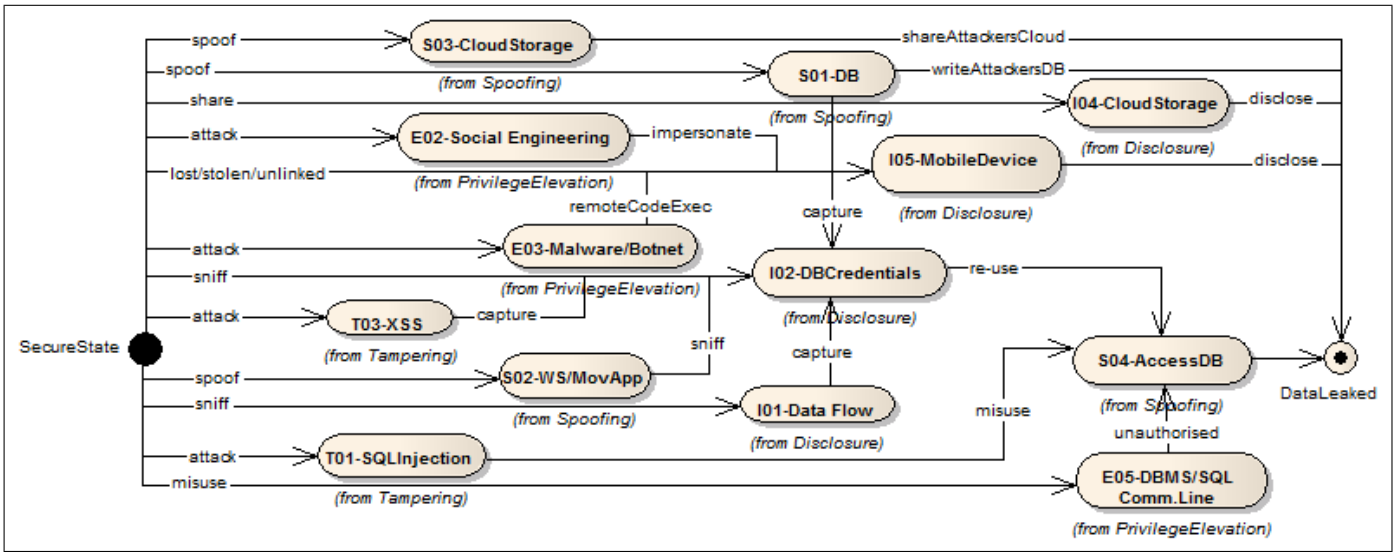

Fig. 3. Interactions amongst BYOD Threats that may lead to information disclosure

threats as attack vectors, leading to information leakage. For instance, by spoofing Web/Mobile Applications, Cloud Storage Services or Databases, corporate information can be diverted and stored in the attacker's repository leaving no evidence of the leakage for later investigation. Similarly, by using Tampering attacks like XSS, database access credentials can be captured, and subsequently re-used to get unauthorised access to databases, actions that may give an slight chance of generating digital evidence unless database audit and logging mechanisms are disabled [41].

Finally, in Figure 3, Interception (Sniffing) attacks can be used by insiders and outsiders to steal credentials and data that is travelling through an insecure, but not necessarily, unencrypted channel. For example, by the end of 2015, 84 per cent of Australian companies were still vulnerable to the OpenSSL Heartbleed vulnerability which was being used by outsiders to steal user names and passwords [42]. In the proposed BYOD Threat Model, encrypted communication channels in between clients and services have been considered (Figure 1-A) to analyse the threats of Data Interception, even through encrypted channels. For example, attackers can 'spoof' Cloud Storage locations and encrypt the communication channel using a fake or replicated Digital Certificate to deceive the victims, having their credentials and information written in the "spoofed" attacker's service, avoiding any evidence generation in the corporate systems.

VI. Related Work

Previous work to analyse BYOD Threats has been done, but neither considering both security and digital forensics issues. First, Mobile Device Management (MDM) solutions [2][4][16] have been proposed to help organisations securing mobile device access to the corporate network [16] rather than preventing and monitoring information access and misuse (i.e. disclosure and contamination). On the contrary, although *STRIDE-based Threat Models* have already been applied for supporting digital forensic readiness initiatives [43], *BYOD Threat Interactions* have not been considered to identify security and forensics requirements that need to be fulfilled. Hence, our research not only provides a baseline for understanding the environment in which such proactive initiatives may be deployed [28], but also encourages future work towards protecting corporate information from unauthorised disclosure and contamination, considering different evidence sources in the BYOD context.

VII. Conclusions

Internal and External BYOD Threat Interactions to corporate information have been analysed, using a *STRIDE-based Threat Model* (Fig. 1) so that security and forensic challenges of BYOD threats to corporate information can be understood. Thus, it has been found that adopting BYOD introduces potential threats which may lead to corporate information contamination (Fig. 2) and disclosure (Fig. 3).

Regarding information contamination (Section V-A), the analysis showed that uncontrolled mobile device access to information assets [8] brings challenges for security professionals and digital forensic investigators [18] due to the ever increasing number of heterogeneous evidence sources (Section III-A) that may hinder any future effort to investigate security incidents in the BYOD environment. Also, even though insiders are not seen as potential threats, their naive or malicious actions become attack vectors that can compromise not only information integrity (see section III-D), but also introducing repudiation issues when disabling logging and auditing repositories (Figure 2).

With regard to information disclosure (Section V-B), information confidentiality issues are introduced, either unintentionally when outsiders deceive naive insiders to disclose sensitive information, or intentionally when malicious insiders misuse their high-privilege credentials to access sensitive information (Figure 3). In either case, unless insider actions are

properly monitored and controlled, unintentional or malicious mobile activity to disclose information cannot be timely determined, affecting chain of custody provenance requirements during forensic investigations.

ACKNOWLEDGEMENTS

The current research has been sponsored by the Secretariat of Higher Education, Science, Technology and Innovation (SENESCYT) of the Republic of Ecuador.

REFERENCES

[1] S. Gimenez Ocano, B. Ramamurthy, and Y. Wang, "Remote mobile screen (RMS): An approach for secure BYOD environments," in *Computing, Networking and Communications (ICNC), 2015 International Conference on*. IEEE, 2015, pp. 52–56.

[2] U. Vignesh and S. Asha, "Modifying Security Policies Towards BYOD," in *Procedia Computer Science*. Elsevier, 2015, vol. 50, pp. 511–516.

[3] R. Bamforth and C. Longbottom, "Byod - who carries the can?" in *Computer Weekly*, 2013. [Online]. Available: http://bit.ly/1TAmzXj

[4] A. Sobers, "BYOD and the Mobile Enterprise - Organisational challenges and solutions to adopt BYOD." 2015. [Online]. Available: http://bit.ly/1Z8ZkG2

[5] A. Leclercq-Vandelannoitte, "Managing BYOD: How do organizations incorporate user-driven IT innovations?" in *Information Technology & People*. Emerald Group, 2015, vol. 28, no. 1, p. 2.

[6] B. M. Gaff, "Byod? omg!" in *IEEE Computer*. IEEE, 2015, vol. 48, no. 2, pp. 10–11.

[7] T. A. Yang, R. Vlas, A. Yang, and C. Vlas, "Risk Management in the Era of BYOD: The Quintet of Technology Adoption, Controls, Liabilities, User Perception, and User Behavior," in *Social Computing (SocialCom), 2013 International Conference on*. IEEE, 2013, pp. 411–416.

[8] M. Faulds, K. Bauchmuller, D. Miller, J. Rosser, K. Shuker, I. Wrench, P. Wilson, and G. Mills, "The feasibility of using 'bring your own device'(BYOD) technology for electronic data capture in multicentre medical audit and research," in *Anaesthesia*, 2016, vol. 71, no. 1, pp. 58–66.

[9] B. Morrow, "Byod security challenges: control and protect your most sensitive data," in *Network Security*. Elsevier, 2012, vol. 2012, no. 12, pp. 5–8.

[10] S. Earley, R. Harmon, M. Lee, and S. Mithas, "From BYOD to BYOA, phishing, and botnets." in *IT Professional*. IEEE Computer Society, 2014, vol. 16, no. 5, pp. 16–18.

[11] D. Dang-Pham and S. Pittayachawan, "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach," in *Computers & Security*. Elsevier, 2015, vol. 48, pp. 281–297.

[12] P. Beckett, "BYOD-popular and problematic," in *Network Security*. Elsevier, 2014, vol. 2014, no. 9, pp. 7–9.

[13] P. De Las Cuevas, A. Mora, J. Merelo, P. Castillo, P. García-Sánchez, and A. Fernández-Ares, "Corporate security solutions for BYOD: A novel user-centric and self-adaptive system." in *Computer Communications*, vol. 68. Elsevier, 2015, pp. 83–95. [Online]. Available: http://bit.ly/24p95CR

[14] C. Tzoumas, "The BYOD World." in *BusinessWest*, 2013, vol. 30, no. 2, p. 45. [Online]. Available: http://bit.ly/1SD6pd9

[15] B. Densham, "Three cyber-security strategies to mitigate the impact of a data breach." in *Network Security*, vol. 2015, 2015, pp. 5–8. [Online]. Available: http://bit.ly/1Wv9CQJ

[16] K. Downer and M. Bhattacharya, "BYOD security: A new business challenge." 2016. [Online]. Available: http://bit.ly/1O08xJY

[17] N. Pohlmann, M. Hertlein, and P. Manaras, "Bring your own device for authentication (BYOD4A)–the Xign–System," in *Information Security Solutions Europe (ISSE) 2015 Conference*. Springer, 2015, pp. 240–250.

[18] CG, "The BYOD Trend: What It Means For Corporate Internal Investigations." Capsicum Group, 2016. [Online]. Available: http://bit.ly/1NFMEVr

[19] K. Francis and M. Larson, "Digital Forensics in the Mobile, BYOD, and Cloud Era." Deloitte, 2015. [Online]. Available: http://bit.ly/1T9TxdY

[20] T. Olavsrud, "How IT Can Prepare for Mobile Forensic Investigations." CIO, 2016. [Online]. Available: http://bit.ly/1rEYiGT

[21] W. Ashford, "Security models often ill-prepared for a modern, sophisticated attack." in *Computer Weekly*, 2012, pp. 7–8. [Online]. Available: http://bit.ly/1TAmzXj

[22] J. Chang, P.-C. Ho, and T.-C. Chang, "Securing BYOD." in *IT Professional*, vol. 16, no. 5, 2014, pp. 9–11. [Online]. Available: http://bit.ly/1SD6k9i

[23] H. Romer, "Best practices for BYOD security," in *Computer Fraud & Security*. Elsevier, 2014, vol. 2014, no. 1, pp. 13–15.

[24] U. Raj and M. S. Catherine, "Certificate based hybrid authentication for Bring Your Own Device (BYOD) in Wi-Fi enabled Environment," in *International Journal of Computer Science and Information Security*. LJS Publishing, December 2015, vol. 13, no. 12, pp. 41–47. [Online]. Available: http://bit.ly/1T9VarW

[25] P. Newswire, "Experian data breach resolution and the Ponemon Institute release Second Annual Study on Corporate Data Breach Preparedness." in *PR Newswire US*, 2014. [Online]. Available: http://bit.ly/1VEAIX0

[26] K. E. Pavlou and R. T. Snodgrass, "Achieving database information accountability in the cloud," in *Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on*. IEEE, 2012, pp. 147–150.

[27] Y. A. Rathod, M. Chaudhari, and G. Jethava, "Database intrusion detection by transaction signature," in *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on*. IEEE, 2012, pp. 1–5.

[28] P. Henry, J. Williams, and B. Wright, "The SANS Survey of Digital Forensics and Incident Response." SANS, 2013. [Online]. Available: http://bit.ly/1SDdomv

[29] Y. Dong, H. Guan, J. Li, J. Mao, and Y. Chen, "A virtualization solution for BYOD with dynamic platform context switching." in *IEEE Micro*, vol. 35, no. 1, 2015, pp. 34–43. [Online]. Available: http://bit.ly/1N6J9rf

[30] Microsoft, "The STRIDE Threat Model," in *Microsoft MSDN*, 2016. [Online]. Available: http://bit.ly/1qUPcFp

[31] W. H. W. Rein Turn, "Privacy and security in computer systems: The vulnerability of computerized information has prompted measures to protect both the rights of individual subjects and the confidentiality of research data bases," in *American Scientist*. Sigma Xi, The Scientific Research Society, 1975, vol. 63, no. 2, pp. 196–203. [Online]. Available: http://0-www.jstor.org.pugwash.lib.warwick.ac.uk/stable/27845364

[32] D. Petri, "Mitigate the risk of malicious dbas." ObserveIT, 2015. [Online]. Available: http://bit.ly/1O08Vbx

[33] L. Musthaler, "13 best practices for preventing and detecting insider threats." Networld, 2008. [Online]. Available: http://bit.ly/24p9sx5

[34] K. C. DeGroot, "Overview of Recent Changes in California Computer Crime Laws: The Criminalization of Computer Contamination and Strengthened Penalty Provisions, California Penal Code Sections, 502, 502.01, 1203.047, 1203.048," in *Santa Clara Computer and High-Technology Law Journal*. HeinOnLine, 1990–1991, vol. 6, no. 1, pp. 135–142.

[35] S. Northcutt, "Logic bombs, trojan horses, and trap doors." SANS, 2005-2016. [Online]. Available: http://bit.ly/1WXiwae

[36] D. M. Upton and S. Creese, "The danger from within." Harvard Business Review, 2014. [Online]. Available: http://bit.ly/1N3x43S

[37] N. Lewis, "Can internal threats be distinguished from outside malware coders?" SearchSecurity, 2015. [Online]. Available: http://bit.ly/1pOzDgZ

[38] N. Bradley, "The threat is coming from inside the network: Insider threats outrank external attacks." IBM Security Intelligence, 2015. [Online]. Available: http://ibm.co/1QAAIiu

[39] E. Schindler, "Protecting corporate data... when an employee leaves." Druva, 2014. [Online]. Available: http://bit.ly/1SyINtH

[40] TrustWave, "Global Security Report," in *TrustWave Document Library*, 2014. [Online]. Available: http://bit.ly/1HF34ad

[41] M. Aphale, U. Borikar, B. Kardile, V. Vasekar, and J. Shital, "Forensic investigation for database tampering using audit logs," in *International Journal of Engineering Research and Technology*, E. Publication, Ed., 2015, vol. 4, no. 3. [Online]. Available: http://bit.ly/1N7yBYY

[42] ACSC, "Threat Report," in *Australian Cyber Security Centre*, 2015. [Online]. Available: http://bit.ly/1DadAb0

[43] K. Lourida, A. Mouhtaropoulos, and A. Vakaloudis, "Assessing database and network threats in traditional and cloud computing," in *International Journal of Cyber-Security and Digital Forensics*, T. S. of Digital Information and W. Communications, Eds., 2013, vol. 2, no. 3. [Online]. Available: http://wrap.warwick.ac.uk/65197/