**EMCS2020: Advanced Topics in Computer Security**

Physical Security Assessment

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

#### Executive Summary

Blush is a dating app that can be described as a “cross between eHarmony and Tinder.” We specialize in creating authentic connections between people without the hassle of long complicated assessments. The Blush App handles delivering and collecting assessments, storing profile information, matching users and facilitating communication between users. Each one of these steps carries an inherent risk which exponentially multiplied when considering all the physical parts of the application development ecosystem, hence the purpose of this assessment. Application security without security for the physical parts of the business, meaning its’ servers, people, real property and equipment, makes it easy for an attacker to use the physical parts of the business to launch software attacks. In other words, good physical facilitates higher levels of application and network security.

#### Overview

At Blush, physical security, meaning the security of our building, our equipment, and our people is paramount. Blush is a dating app, and even though we run a digital service, the type of information we collect about our users is extremely sensitive. Furthermore, the equipment we use to fuel the matching algorithm is very expensive. The MacOS machine running the main data regression algorithms cost $20,000 and the second Windows machine running the Deep Scalable Sparse Tensor Network Engine cost over $14,000. Physical access to these machines and the data they are processing should be highly restricted.

The physical space of the Sacramento Blush office is roughly 100 x 100 square feet with only one room, two door and three windows. The building resides in a high traffic area of Sacramento, better known as “Old Sacramento”, a well-known tourist attraction. While the office is fully out of sight from public view, an attacker with knowledge of where the office is and what the office has in terms of equipment may find easy access by following an employee or stumbling upon a hallway that leads to the office.

It may seem like “small potatoes”, but securing the Blush Sacramento office is an important task that we approach with a great sense of urgency and vigilance.

#### Assessment Goals

The goal of this assessment is threefold: Define, Evaluate and Test. The first goal, creating clear and actionable definitions will be seeded with guidelines from this RFP. The scope and deliverables will serve as a frame for the vulnerabilities, attack vectors, and areas requiring enhanced security. The second goal, a thorough and comprehensive evaluation, should see to give Blush a complete and detailed picture of the defenses. The last goal of the assessment, developing a battery of tests, will be used to measure the implementation of security after the implementation. Each of these goals depends on each other for quality and completeness. An incomplete definition will lead to an incomplete evaluation which will result in inadequate tests after security measures have been implemented.

Furthermore, the evaluation should include at least three types of possible threats: Traditional well-documented threats and vulnerabilities, Non Traditional attack vectors that may only be known among InfoSec researchers and finally attack vectors that are a result of forward-thinking. Each of these threat categories should carry an implied probability score based on the location of the Blush office, historical crime records and the level of difficulty or expertise required to execute the attack. For example, upgrading the doors on the office to protect against lock picking would be considered a traditional security vector, as opposed to fortify the doors against acid and silent explosives. The probability of an attacker having access to silent explosives, which are rare and very expensive, in Sacramento could be lower as opposed to a lock picking kit that can be purchased from Amazon. The implied score for the threat category should not completely override the probability of the specific threat vector, but instead, carry some overall weight when calculating the specific threat score.

In summary, the goals of the assessment should be to provide a complete, accurate and validated assessment of Blush’s security posture. The assessment should be well organized, based on historical data, account for threats from common and uncommon sources and include a test that will measure if the vulnerability or attack vector has been adequately dealt with.

#### Assessment Duration

The assessment will consist of four distinct phases, each with a boundary setting sub-phase: Gathering Core Requirements, Gathering Cultural Requirements, Penetration Testing and Delivery of the Final Assessment.

##### Gathering Core Requirements

The vendor will have 20 days to gather the core requirements. This should include interviews with all relevant stakeholders and time to conduct discovery for historical criminal records.

##### Gathering Cultural Requirements

The vendor will have 3 days to assess the cultural requirements at Blush, and more specifically

##### Penetration Testing

The vendor will have 7 days to conduct the physical penetration test. During this period Blush will not be given any advance notice of attempts to breach the physical defenses.

##### Delivery of the Final Assessment

The vendor will have 30 days to write and deliver a written assessment that addresses all the elements of the scope.

#### Assessment Scope

Before the assessment activities can be defined, the general targets of the assessment should be defined. Each target may be assessed from several perspectives depending on their value, the risk their compromise poses to the organization or the probability that their compromise will be used to compromise other targets. To make the perspectives consistent and measurable vendors should tag each asset in terms of their alignment to the commonly accepted Cyber Kill Chain[[1]](#footnote-0):

“***Reconnaissance****: Intruder selects a target, researches it, and attempts to identify vulnerabilities in the target network.*

***Weaponization****: Intruder creates remote access malware weapons, such as a virus or worm, tailored to one or more vulnerabilities.*

***Delivery****: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives)*

***Exploitation****: Malware weapon's program code triggers, which takes action on the target network to exploit a vulnerability.*

***Installation****: Malware weapon installs access point (e.g., "backdoor") usable by an intruder.*

***Command and Control****: Malware enables an intruder to have "hands on the keyboard" persistent access to the target network.*

***Actions on Objective****: Intruder takes action to achieve their goals, such as data exfiltration, data destruction, or encryption for ransom.*”

Each one of the elements below can be a target or a pivot point in the kill chain. The assessment should make an effort to identify when an element is one or both. Naturally, elements that are both targets and pivot points should be scored as being a higher risk for the organization.

##### Physical Entry Points

###### Doors

Every door in the property should be assessed by the following criteria:

* Resistance to lock picking attacks.
* Resistance to dismantling attacks, i.e. taking the door off the hinges
* Resistance to underbar or overbar attacks, i.e. sliding tools under the door to bypass the locks.

###### Windows

Every window in the property should be assessed for the following criteria:

* Resistance to dismantling attacks.
* Resistance to breakage and cutting attacks

##### Physical Barriers

Physical barriers are defined as anything that is not meant to be opened like a window or a door. Walls, for example, are designed to provide basic privacy and protection, however, an attacker may use the lack of soundproofing to overhear sensitive information.

###### Walls

* Resistance to dismantling attacks.
* Resistance to eavesdropping attacks

###### Vents

* Resistance to dismantling attacks.
* Resistance to probing attacks, i.e. the placement of a microphone in a vent

###### Gates

* Resistance to lock picking attacks
* Resistance to dismantling attacks.

##### Access Control

###### Authenticating Personnel and Visitors

Personel walking in an out of the office is one of the vectors with the highest risk, but also is the hardest to control. Personnel may be hard to identify, visitors may be hard to monitor and the devices that everyone brings into the office may be hard to detect or control. Authenticating personnel and vetting visitors should be evaluated on the following criteria :

* Identification / Authentication systems resistance to cloning attacks
* Resistance to unauthorized surveillance
* Identification / Authentication systems resistance to the usage of invalid credentials
* Secure storage of physical keys for doors among staff
* Identifying if any key systems have “key-alike” vulnerabilities
* Proper vetting of visitors and the devices they bring into the office, i.e. restricting dangerous items and items that could conduct unauthorized surveillance
* Proper vetting of the devices that personal bring into the office, i.e. restricting dangerous items and items that could conduct unauthorized surveillance

###### Access Change Management

* Resistance to usage of old credentials

##### Security of Utilities

###### Temperature Control

The office does not have built in temperature control and is dependent on an in the window AC system. While this system is permanently installed in the window it should be evaluated for the following criteria:

* Resistance to external tampering

###### Electricity

The office depends on electricity to run all the equipment. An attacker may seek to bring down the company’s defenses by tampering with the breaker box or other mechanisms that regulate or control the power to the office. The electricity for the office should be evaluated based on the following criteria:

* Resistance to external tampering

###### Waste Management

The trash can be a vector for attacks and breaches of privacy if confidential documents are not disposed of properly. Furthermore trash cans travel in and out of the office without much thought being given to who handled then. All trash and receptacle for holding trash must be evaluated for the following criteria:

* Resistance to external tampering
* Resistance to breach of privacy, i.e.

##### On-Site Equipment

###### Computers

The computer in the office are an obvious target for tampering and theft. Securing the computers in the office generally means ensuring that someone can’t just walk up and gain access, but it also means that an attacker can’t insert media into the ports or change the way the machine physical boots. The computers in the office should be evaluated on the following criteria:

* Resistance to external tampering and external media
* Resistance to electrical tampering
* Resistance to vandalism and theft
* Resistance to physical modifications that may affect configuration

###### Routers

Routers are another obvious target for an attacker. Physical access to a router can compromise the entire network and all the machines that are connected to it.

* Resistance to external tampering and external media
* Resistance to physical modifications that may affect configuration

##### Location Specific Threats

###### Local Foot Traffic

* Resistance to attacks that may confuse employees into allowing strangers access

###### Annual Public Events

* Resistance to group attacks that may confuse employees into allowing strangers access

###### Scheduled Private Events

* Resistance to strangers from nearby events wandering into the office

Vendors should take careful note to include all the elements mentioned in the scope but should feel free to include any elements not included in this scope. Each of the elements in scope should be evaluated on their ability to defend against the points in the kill chain[[2]](#footnote-1):

“*Detect: determine whether an attacker is poking around*

*Deny: prevent information disclosure and unauthorized access*

*Disrupt: stop or change outbound traffic (to attacker)*

*Degrade: counter-attack command and control*

*Deceive: interfere with command and control*

*Contain: network segmentation changes*”

#### Deliverables

##### Comprehensive Written Assessment

The comprehensive written assessment should include:

* Vulnerabilities Identified as it relates to the scope
* Recommendations for changes to policies, procedures, personnel or equipment
* Scoring Criteria as it relates to the risk factors mentioned in the goals section
* Historical Crime Records use to validate assumptions

#### Vendor Selection Criteria

Vendor submissions will be scored based on their completeness as it relates to the adherence to the guidelines in this document, thoroughness as it relates to the details of how the assessment will be conducted and accuracy as it relates to the references of historical crime data.

Furthermore, vendors should be present a response to the RFP that gives complete pricing details as it relates to their services and the pricing should be competitive, streamlined and reasonable.

1. "The Cyber Kill Chain or: how I learned to stop worrying and love data breaches". 2016-06-20. https://www.varonis.com/blog/cyber-kill-chain/ [↑](#footnote-ref-0)
2. “Kill Chain.” Wikipedia, Wikimedia Foundation, 30 Sept. 2019, https://en.wikipedia.org/wiki/Kill\_chain#Attack\_phases\_and\_countermeasures. [↑](#footnote-ref-1)