OWASP Open Web Application Security Project | Standard

MASVS

Mobile Application Security Verification Standard

(Russian Translation)

Carlos Holguera, Bernhard Müller,
Sven Schleier and Jeroen Willemsen

Version 1.3

OWASP Mobile Application Security Verification Standard

Version 1.3 May 13, 2021

Резюме

Вступительное

Технологические революции могут происходить молниеносно: менее десятилетия назад смартфоны были громоздкими устройствами с клавиатурой, и являлись дорогими игрушками для некоторых компаний. Сегодня же смартфоны прочно вошли в нашу жизнь. Мы доверяем им информацию, навигацию, коммуникацию, они являются неотъемлемой составляющей как бизнеса, так и жизни в целом.

Каждая новая технология приносит новые риски безопасности, и попытка поспеть за этими изменениями и есть один из основных вызовов, которые стоят перед индустрией безопасности. Сторона защиты всегда на несколько шагов позади. Например, обычной реакцией многих была бы попытка применить старый подход: смартфоны - это маленькие компьютеры и мобильные приложения - обычное ПО, значит требования безопасности абсолютно такие же? Но так это не работает. Операционные системы смартфонов отличаются от ОС компьютеров и мобильные приложения отличаются от веб приложений. Например, классический метод поиска вирусов на основе сигнатурного анализа не имеет смысл в современных мобильных операционных системах: не только потому, что это не совместимо с моделью распространения мобильных приложений, но еще и потому, что это технически невозможно из-за ограничений среды выполнения приложений (sandbox). Кроме того, некоторые типы уязвимостей, такие как переполнение буфера и XSS, менее релевантны к мобильным приложениям, нежели к десктопным и веб-приложениям (есть исключения).

Со временем наша индустрия получила больше опыта в борьбе с мобильными угрозами. Как оказалось, мобильная безопасность в основном затрагивает хранение данных: приложения хранят нашу личную информацию, изображения, записи голоса и видео, заметки, учетные данные, информацию о бизнесе, местоположения и многое другое. Приложения играют роль клиентов, подключающих нас к сервисам, которыми мы используем ежедневно, и коммуникационных центров, обрабатывающих каждое сообщение, которым мы обмениваемся. Скомпрометировав телефон человека, вы получите неограниченный доступ к его личной жизни. Если учесть, что мобильные устройства легко теряются и похищаются, а мобильные вирусы сейчас активно развиваются, необходимость защиты данных становится ещё более очевидной.

Стандарты безопасности мобильных приложений должны сконцентрироваться на том, как они обрабатывают, хранят и защищают чувствительную информацию. Несмотря на то, что современные мобильные операционные системы, такие как iOS и Android, предоставляют API для безопасного хранения данных и сетевого взаимодействия, чтобы быть эффективным, оно должно быть корректно использовано. Хранение данных, межпроцессное взаимодействие, правильное использование криптографического API и безопасное сетевое взаимодействие - это только некоторые из аспектов, которые требуют внимательного рассмотрения.

Важный вопрос для нашей индустрии, в котором необходимо достичь соглашения:

как далеко должны заходить специалисты в вопросах защиты конфиденциальности и целостности данных. Например, многие из нас согласятся, что мобильное приложение должно проверять сертификат сервера во время соединения TLS. Но что насчёт SSL pinning? Невыполнение этого требования ведёт к уязвимости? Должно ли это быть требованием, если приложение обрабатывает чувствительную информацию или это может быть контрпродуктивно? Нужно ли шифровывать данные, хранящиеся в SQlite, несмотря на то, что ОС выполняет приложение в песочнице (sandboxing)? То, что подходит одному приложению, может не подходить для другого. MASVS - это попытка стандартизации требований на основании уровней проверок, подходящих для разных моделей угроз.

Появление вредоносных программ и инструментов удаленного управления заставляют осознать тот факт, что мобильные ОС имеют недостатки, которыми могут воспользоваться злоумышленники. Для дополнительной защиты чувствительных данных и предотвращения фальсификаций на стороне клиента всё шире используются стратегии контейнеризации. Это место, где всё усложняется. Аппаратные и программные решения, такие как Android for Work и Samsung Knox, существуют, но они доступны не на всех устройствах. В качестве решения можно реализовать дополнительные программные механизмы защиты, но, к сожалению, не существует стандартов или руководств по тестированию для верификации таких методов.

В результате при тестировании информационной безопасности мобильных приложений постоянно возникают разногласия. Например, некоторые тестировщики приложений Android считают, что недостаточная обфускация или отсутствие детектирования root-доступа серьезными уязвимостями. Другие считают, что такие меры, как шифрование строк, обнаружение отладчика или обфускация не являются обязательными. Однако, этот двоякий взгляд не имеет смысла, так как меры защиты зависят от конкретной модели угроз для клиентского приложения. Защита на программном уровне не является бесполезной, но в конечном итоге её всегда можно обойти, так что она не должна быть использована как замена основным требованиям безопасности.

Цель MASVS - предложить общий фундамент для безопасности мобильных приложений (MASVS-L1), усиленные меры защиты (MASVS-L2) и меры защиты против угроз на стороне клиента (MASVS-R). MASVS предназначен для достижения следующих целей:

- Обеспечить требования для архитекторов и разработчиков ПО, стремящихся создавать безопасные мобильные приложения.
- Предложить промышленный стандарт, по которому можно проводить аудит безопасности мобильных приложений.
- Прояснить роль механизмов защиты ПО в мобильной безопасности и предоставить требования для проверки их эффективности.
- Предоставить конкретные рекомендации, для разных уровней безопасности, которые зависят от конкретного варианта использования.

Мы пониманием что 100% согласия в отрасли невозможно достичь. Однако, мы надеемся, что MASVS будет полезен в качестве руководства на всех этапах разработки и тестирования мобильных приложений. MASVS, как открытый стандарт, будет развиваться со временем, и мы рады любым предложениям и вкладу в развитие проекта.

Слово от Bernhard Mueller

О стандарте

Добро пожаловать в стандарт проверки безопасности мобильных приложений (MASVS). MASVS - это результат совместных усилий в создании перечня требований информационной безопасности, необходимых для проектирования, разработки и тестирования мобильных приложений на iOS и Android.

MASVS - итог усилий сообщества и обратной связи от представителей индустрии. Мы надеемся на развитие стандарта в будущем и приветствуем обратную связь от сообщества. Лучший способ связаться с нами - через канал OWASP Mobile Project в Slack-е:

https://owasp.slack.com/messages/project-mobile_omtg/details/.

Аккаунты можно создать по этому адресу:

https://owasp.slack.com/join/shared_invite/zt-g398htpy-AZ40HOM1WUOZguJKbblqkw#/.

Авторское право и лицензия

Подтверждения

Руководитель проекта	Главные авторы	Авторы и рецензенты
Sven Schleier and Carlos Holguera	Bernhard Mueller, Sven Schleier, Jeroen Willem-sen and Carlos Holguera	Alexander Antukh, Mesheryakov Aleksey, Elderov Ali, Bachevsky Artem, Jeroen Beckers, Jon-Anthoney de Boer, Damien Clochard, Ben Cheney, Will Chilcutt, Stephen Corbiaux, Manuel Delgado, Ratchenko Denis, Ryan Dewhurst, @empty_jack, Ben Gardiner, Anton Glezman, Josh Grossman, Sjoerd Langkemper, Vinícius Henrique Marangoni, Martin Marsicano, Roberto Martelloni, @PierrickV, Julia Potapenko, Andrew Orobator, Mehrad Rafii, Javier Ruiz, Abhinav Sejpal, Stefaan Seys, Yogesh Sharma, Prabhant Singh, Nikhil Soni, Anant Shrivastava, Francesco Stillavato, Abdessamad Temmar, Pauchard Thomas, Lukasz Wierzbicki

Язык	Переводчики и рецензенты
традиционный китайский	Peter Chi, and Lex Chien, Henry Hu, Leo Wang
упрощенный китайский	Bob Peng, Harold Zang, Jack S
Французский	Romuald Szkudlarek, Abderrahmane Aftahi, Christian Dong (Review)
Немецкий	Rocco Gränitz, Sven Schleier (Review)
хинди	Mukesh Sharma, Ritesh Kumar, Atul Kunwar, Parag Dave, Devendra Kumar Sinha, Vikrant Shah
Испанский	Martin Marsicano, Carlos Holguera
Японский	Koki Takeyama, Riotaro Okada (Review)
Корейский	Youngjae Jeon, Jeongwon Cho, Jiyou Han, Jiyeon Sung
Русский	Gall Maxim, Eugen Martynov, Chelnokov Vladislav (Review), Oprya Egor (Review), Tereshin Dmitry (Review)

Язык	Переводчики и рецензенты
Персидский	Hamed Salimian, Ramin Atefinia, Dorna Azhirak, Bardiya Akbari, Mahsa Omidvar, Alireza Mazhari, Milad Khoshdel
португальский	Ana Filipa Mota, Fernando Nogueira, Filipa Gomes, Luis Fontes, Sónia Dias
бразильский португальский	Mateus Polastro, Humberto Junior, Rodrigo Araujo, Maurício Ariza, Fernando Galves

Работа над документом была начата как ответвление OWASP Application Security Verification Standard, написанного Jim Manico.

Спонсоры

Хотя MASVS и MSTG создаются и поддерживаются сообществом на добровольной основе, иногда требуется небольшая помощь извне. Поэтому мы благодарим наших спонсоров за предоставление средств для возможности нанять технических редакторов. Обратите внимание, что их спонсорство никоим образом не влияет на содержание MASVS или MSTG. Спонсорские пакеты описаны на OWASP Project Wiki.

Почетный благотворитель

Добрый самаритянин

Далее, мы хотели бы поблагодарить главу OWASP Bay Area за их спонсорскую поддержку. Наконец, мы хотели бы поблагодарить всех, кто купил книгу у Leanpub и спонсировал нас таким образом.

The Mobile Application Security Verification Standard

MASVS может быть использован для подтверждения определенного уровня уверенности в безопасности мобильных приложений. Данные требования были сформированы, ориентируясь на следующие цели:

- Использование в качестве метрики: для предоставления стандарта безопасности, по которому разработчики и владельцы мобильных приложений могут проверить свои продукты;
- Использование в качестве руководства: для предоставления рекомендаций во время всех этапов разработки и тестирования; *- Использование во время закупок: как основание для проверки безопасности мобильного приложения.

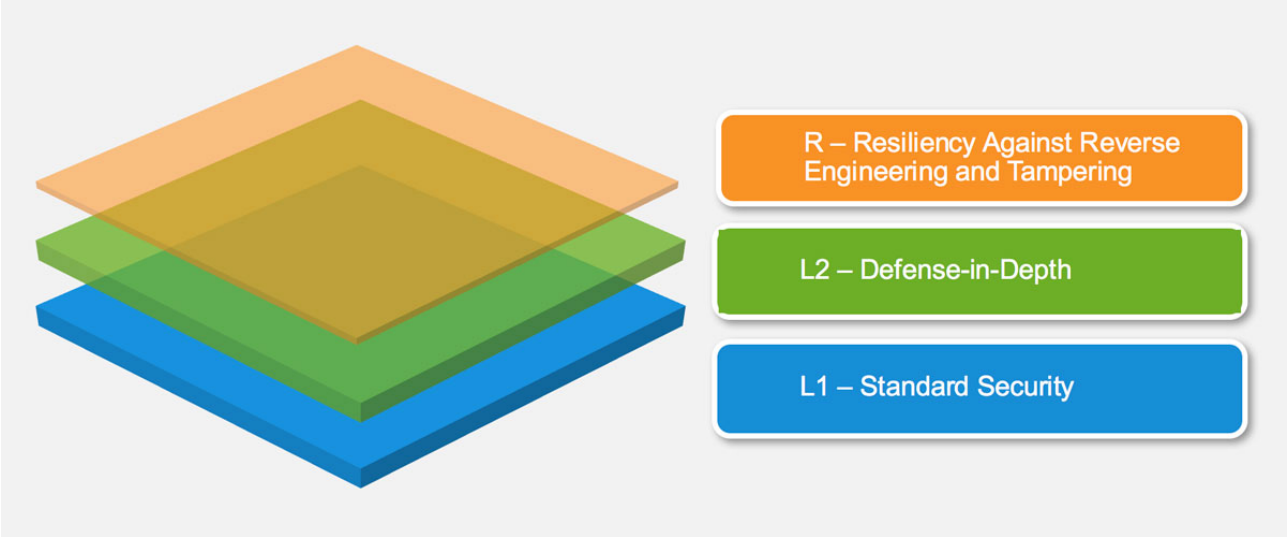
Модель безопасности мобильных приложений

MASVS определяет два уровня проверки безопасности (MASVS-L1 и MASVS-L2), а также набор гибких требований для обеспечения защиты от реверс инжиниринга (MASVS-R). MASVS-L1 содержит общие требования безопасности, которые рекомендованны для всех мобильных проложений, MASVS-L2 должен быть использован для приложений, оперирущих с наиболее уязвимыми кофиденциальными данными. MASVS-R охватывает дополнительные меры защиты, которые могут применяться в случае, если предотвращение атак на стороне клиента заложено в дизайн приложения.

Приложение, разработанное в соответствии с требованиями MASVS-L1, защищено лучшими практиками безопасности и не содержит часто встречающиеся уязвимости. MASVS-L2 предусматривает усиленные меры защиты, такие, как SSL pinning, защищающие приложение от более ухищренных атак, при условии, что безопасность операционной системы не скомпрометирована, а конечный пользователь не рассматривается как потенциальный злоумышленник. Реализация всех или хотя бы некоторых защитных техник из MASVS-R затрудняет атаки на стороне клиента, когда конечный пользователь является злоумышленником и/или ОС мобильного устройства скомпрометирована.

I: Хотя мы рекоммендуем использование MASVS-L1 мер защиты в каждом приложении, применение или отказ от конкретной меры в конечном счете должно быть основанным на оценке риска решением, которое принято/доведено до сведения с владельцами бизнеса.

II: Обратите внимание, что программные меры защиты, перечисленные в MASVS-R и OWASP Mobile Testing Guide, можно обойти, и они не должны использоваться в качестве замены основным требованиям безопасности. Вместо этого они должны быть реализованы как специализированное дополнение, направленное на локализацию конкретных угроз, в мобильном приложении, соответствующее требованиям MASVS-L1 или MASVS-L2.



Структура документа

Первая часть MASVS содержит описание модели безопасности и доступных уровней проверки, рекомендации о том, как использовать стандарт на практике. Подробные требования безопасности и их соответствие с уровнями проверки перечислены во второй части. Требования сгруппированы в восемь категорий (V1 - V8) по принадлежности к технической задаче/области. В MASVS и MSTG используется следующая номенклатура:

- *Категория требований:* MASVS-Vx, например, MASVS-V2: хранение данных и конфиденциальность
- *Требование:* MASVS-Vx.y, например, MASVS-V2.2: «Чувствительные данные не попадают в логи приложения».

Подробное описание уровней верификации

MASVS-L1: Стандартная безопасность

Приложение, удовлетворяющее MASVS-L1, соответствует лучшим практикам обеспечения безопасности мобильных приложений. Данный уровень проверки предоставляет основные требования с точки зрения качества кода, обработки чувствительных данных и взаимодействия с мобильной средой. Для подтверждения соответствия приложения данному уровню безопасности необходимо проведение тестирования. Этот уровень подходит для всех мобильных приложений.

MASVS-L2: Усиленная защита

MASVS-L2 предлагает расширенные средства проверки безопасности, выходящие за рамки стандартных. Для соответствия MASVS-L2, необходима сформированная модель угроз, и безопасность должна быть неотъемлемой частью архитектуры и дизайна приложения. Конкретные MASVS-L2 требования должны быть выбраны и успешно примененны базируясь на модели угроз. Этот уровень подходит для приложений, работающих с чувствительными данными, таких, как мобильный банк.

MASVS-R: Устойчивость к реверс инжинирингу и фальсификациям

Приложение имеет встроенные механизмы обеспечения безопасности, устойчиво к конкретным атакам на стороне клиента, таким, как фальсификация, модификация или реверс инжиниринг, направленным на извлечение чувствительных участков кода или данных. Такое приложение либо использует аппаратные средства безопасности, либо достаточно надёжные программные механизмы защиты. MASVS-R применим к приложениям, которые обрабатывают высокочувствительные данные и могут служить средством защиты интеллектуальной собственности.

Рекомендованное использование

Приложения могут быть проверены на соответствие MASVS L1 или L2, основываясь на предварительной оценке рисков и общем понимании требуемого уровня безопасности. L1 применим ко всем мобильным приложениям, в то время как L2 обычно рекомендуется для приложений, которые обрабатывают более чувствительные данные и/или функциональность. MASVS-R (или его части) может быть применен для проверки устойчивости к конкретным угрозам, таким, как переупаковка (repackaging) или извлечение конфиденциальных данных, *в дополнение* к основным проверкам безопасности.

Таким образом, доступны следующие типы проверки:

- MASVS-L1
- MASVS-L1+R
- MASVS-L2
- MASVS-L2+R

Различные комбинации отражают различные уровни безопасности и устойчивости к атакам. Цель состоит в том, чтобы обеспечить гибкость: например, игра для смартфона может не гарантировать соответствие таким мерам защиты MASVS-L2, как двухфакторная аутентификация, из-за неудобства использования, но имеет потребность в предотвращении фальсификаций.

Какой тип проверки выбрать

Соответствие требованиям MASVS L2 повышает безопасность, но в то же время увеличивает стоимость разработки и потенциально ухудшает опыт конечного пользователя (классический компромисс между удобством и безопасностью). В общем случае, L2 следует использовать для приложений, рассматриваемых с точки зрения риска и издержек (т.е. когда потенциальная потеря, вызванная нарушением конфиденциальности или целостности, выше, чем затраты, связанные с реализацией дополнительных проверок безопасности). Оценка рисков должна быть первым шагом перед применением MASVS.

Примеры

MASVS-L1

- Все мобильные приложения. В MASVS-L1 перечислены рекомендации по безопасности, которые могут быть выполнены с разумным воздействием на стоимость разработки и пользовательский опыт. Применяйте требования MASVS-L1 для любого приложения, которое не подходит ни под один из более высоких уровней.

MASVS-L2

- Индустрия здравоохранения: мобильные приложения, которые хранят персональные данные, которые могут использоваться для кражи личности, мошеннических платежей или других схем мошенничества. Для сектора здравоохранения США пункты проверок включают в себя Закон об охране и ответственности за информацию, полученную в результате медицинского страховани (HIPAA).
- Финансовая индустрия: приложения, которые обеспечивают доступ к высокочувс твительной информации, такой, как номера кредитных карт, персональным данным, или позволяют управлять финансовыми средствами. Эти приложения требуют дополнительных проверок безопасности для предотвращения мошенничества. Финансовым приложениям необходимо обеспечить соблюдение стандартов безопасности данных, таких, как Payment Card Industry Data Security Standard (PCI DSS), Gramm Leech Bliley Act и Sarbanes-Oxley Act (SOX).

MASVS L1+R

- Мобильные приложения, где защита IP является целью бизнеса. Меры защиты, перечисленные в MASVS-R, могут использоваться для увеличения усилий, необходимых для получения исходного кода, и для препятствия попыткам фальсификации или взлома приложения.
- Игровая индустрия: игры, для которых важное значение имеет предотвращение возможности модификации и использования читов, например, многопользоват ельские онлайн-игры. Читинг является важной проблемой в онлайн-играх, так как большое количество читеров вызывает недовольство у основной массы игроков

и в конечном итоге может привести к краху данного игрового продукта. MASVS-R содержит меры защиты, направленные на усложнение задачи читерам.

MASVS L2+R

- Финансовая индустрия: приложения для онлайн банкинга, которые позволяют пользователю управлять финансовыми средствами, для которых инъекции кода и использование специализированного инструментария для взлома на устройствах с jailbreak-ом/root-ом представляют риск. В этом случае, верификация MASVS-R может быть использована, чтобы препятствовать фальсификации, усложнить задачу авторам вредоносных программ.
- Все мобильные приложения хранят чувствительные данные на мобильном устройстве, и в то же время должны поддерживать широкий спектр устройств и версий операционной системы. В этом случае проверка устойчивости к фальсификациям может использоваться в качестве углублённой защиты, для максимального затруднения извлечения конфиденциальных данных злоумышленником.
- Приложения с платным контентом в идеале должны использовать серверные и MASVS-L2 элементы управления для защиты платного контента. Однако могут быть случаи, когда нет возможности использовать защиту на стороне сервера. В этих случаях, для увеличения усилия по обращению реверсирования и/или вмешательства следует дополнительно применять средства управления MASVS-R.

Оценка и сертификация

Позиция OWASP в отношении сертификатов MASVS

OWASP является некоммерческой организацией и не сертифицирует вендоров, аудиторов, или программное обеспечение.

OWASP не выдаёт официальные оценки, знаки доверия, или сертификаты, поэтому к организации, утверждающей, что она имеет сертификацию OWASP, следует относиться с осторожностью.

В то же время, отсутствие официальной сертификации OWASP не запрещает организациям предлагать услуги аудита по данному стандарту.

Руководство по сертификации мобильных приложений

Рекомендуемым способом проверки соответствия мобильного приложения стандарту MASVS является аудит методом «открытой книги», означающий, что проверяющие получают полный доступ к ключевым ресурсам, таким как: архитекторы и разработчики приложения, проектная документация, исходный код и авторизованный доступ к бэкенду (как минимум по одной учетной записи для каждой роли).

Важно отметить, что MASVS охватывает только безопасность мобильных приложений (на стороне клиента) и сетевое взаимодействие между приложением и его удалёнными сервисами, а также несколько базовых и общих требований, связанных с аутентификацией пользователя и управлением сессиями. Данный документ не содержит специфичных требований к удаленным сервисам (например, веб-сервисам), связанным с приложением, ограничиваясь набором базовых требований к безопасности аутентификации и управления сессиями. Однако MASVS V1 подчёркивает, что удалённые сервисы должны быть учтены в общей модели угроз и проверены по соответствующим стандартам, таким, как OWASP ASVS.

Проверяющая организация должна включать в отчёт область охвата проверки, резюме о результатах проверки, включая пройденные и непройденные тесты, с ясными указаниями о том, как исправить недостатки. Сохранение подробных документов, скриншотов или видео, сценариев для воспроизведения и эксплуатирования багов, электронных записей, таких как логи перехватывающего запросы прокси-сервера и прочих заметок являются стандартной практикой индустрии. Недостаточно просто запустить инструмент и сообщить об ошибках, это не дает достаточных доказательств того, что проверяющим были проведены все проверки должным образом. В случае возникновения спора должны быть достаточные доказательства для демонстрации того, что соответствие каждому требованию было проверено.

Использование OWASP Mobile Security Testing Guide (MSTG)

OWASP MSTG - это руководство по тестированию безопасности мобильных приложений. В нём описываются технические процессы для проверки требований, перечисленных в MASVS. MSTG включает список тест-кейсов, выстроенных в соответствии с требованиями в MASVS. Хотя требования MASVS являются высокоуровневыми и универсальными, MSTG предоставляет подробные рекомендации и процедуры тестирования для каждой целевой мобильной ОС.

Роль автоматических инструментов тестирования безопасности

Для повышения эффективности рекомендуется использовать статические анализаторы исходного кода и инструменты для blackbox тестирования. Однако невозможно выполнить проверку MASVS, используя только автоматизированные инструменты: каждое мобильное приложение уникально, и понимание общей архитектуры, бизнес-логики и технических проблем конкретных технологий и фреймворков является обязательным требованием для верификации безопасности приложения.

Другие применения

Как подробное руководство по архитектуре безопасности

Одно из наиболее распространенных применений MASVS - в качестве пособия для архитекторов безопасности. В двух основных методологиях по выстраиванию безопасной архитектуры SABSA и TOGAF отсутствует информация, необходимая для ревью безопасности архитектуры мобильных приложений. MASVS можно использовать для заполнения этих пробелов, позволяя архитекторам безопасности выбирать лучшие требования безопасности, адаптированные для мобильных приложений.

В качестве замены готовых чеклистов написания безопасного кода

Многие организации могут извлечь выгоду из соответствия MASVS, выбрав один из двух уровней проверки, или кастомизировав MASVS для собственных требований, предварительно оценив уровни риска для собственных приложений, беря во внимание область их применения. Мы приветствуем такие ответвления до тех пор, пока сохраняется преемственность, т.е. соответствие приложения требованию 4.1 оригинального стандарта должно означать то же самое в его кастомизированной копии.

В качестве основы для методологий тестирования безопасности

Хорошая методология тестирования безопасности мобильных приложений должна покрывать все требования, перечисленные в MASVS. В гайде OWASP по тестированию мобильных приложений (MSTG) описываются black-box и white-box тест-кейсы для каждого из требований данного стандарта.

Как руководство для автоматического модульного и интеграционного тестирований

MASVS, за исключением некоторых архитектурных требований, может быть использован как руководство для тестирования. Автоматические модульное, интеграционное и приёмочное тестирование на основе требований MASVS могут быть интегрированы в непрерывный жизненный цикл разработки. Это не только повысит уровень осведомлённости разработчиков в области безопасности, но также улучшит общее качество приложений и уменьшит количество находимых уязвимостей на этапе предрелиза.

Для курсов по обучению безопасной разработке

MASVS также может использоваться для определения характеристик безопасных мобильных приложений. Многие курсы «безопасного программирования» - это курсы этичного хакинга с лёгким намеком на подсказки по написанию кода, что, безусловно, не помогает разработчикам. Вместо этого курсы безопасной разработки могут использовать MASVS, уделяя особое внимание проактивным средствам контроля, задокументированным в MASVS, а не, например, списку наиболее часто встречающихся уязвимостей в мобильных приложениях (OWASP Mobile Top 10).

V1: Требования к архитектуре, дизайну и модели угроз

Цель верификации

В идеальном мире безопасность должна приниматься во внимание на всех этапах разработки. Однако на самом деле безопасность часто рассматривается только на поздней стадии SDLC. Помимо технических средств управления, MASVS требует наличия процессов, которые гарантируют, что безопасность была явно учтена при разработке архитектуры мобильного приложения и что функциональные и защитные роли всех компонентов известны. Поскольку большинство мобильных приложений выступают в качестве клиентов у веб-сервисов, необходимо обеспечить применение соответствующих стандартов безопасности: только тестирования изолированного мобильного приложения недостаточно.

В категории «V1» перечислены требования, касающиеся архитектуры и дизайна приложения. Таким образом, это единственная категория, которая не соответствует техническим тестам в OWASP MSTG. Чтобы охватить такие темы, как моделирование угроз, безопасный SDLC, управление ключами, пользователи MASVS должны проконсультироваться с соответствующими проектами OWASP и/или другими стандартами, такими как те, которые приведены ниже.

Требования безопасности

Ниже приведены требования к MASVS-L1 и MASVS-L2.

#	MSTG-ID	Описание	L1	L2
1.1	MSTG-ARCH-1	Все компоненты приложения идентифицированы и используются.	x	x
1.2	MSTG-ARCH-2	Проверки безопасности реализованы не только на клиенте, но и на бэкенде.	x	x
1.3	MSTG-ARCH-3	Архитектура мобильного приложения учитывает все удалённые сервисы. Безопасность заложена в архитектуре.	x	x
1.4	MSTG-ARCH-4	Определены данные, которые являются чувствительными в контексте мобильного приложения.	x	x

#	MSTG-ID	Описание	L1	L2
1.5	MSTG-ARCH-5	Все компоненты приложения определены с точки зрения бизнес логики и/или безопасности.		x
1.6	MSTG-ARCH-6	Сформирована модель угроз для мобильного приложения и связанных с ним удаленных сервисов, которая идентифицирует потенциальные угрозы и необходимые контрмеры.		x
1.7	MSTG-ARCH-7	Все проверки безопасности имеют централизованную реализацию.		x
1.8	MSTG-ARCH-8	Существует явная политика управления криптографическими ключами (если они есть) и их жизненным циклом. В идеале политика соответствует стандарту управления ключами, например, NIST SP 800-57.		x
1.9	MSTG-ARCH-9	Существует механизм принудительных обновлений мобильного приложения.		x
1.10	MSTG-ARCH-10	Безопасность заложена во все этапы жизненного цикла разработки программного обеспечения.		x
1.11	MSTG-ARCH-11	Существует и эффективно применяется ответственная политика раскрытия информации.		x
1.12	MSTG-ARCH-12	Приложение должно соответствовать законам о защите персональных данных.	x	x

Ссылки

Для дополнительной информации смотрите также:

- OWASP Mobile Top 10: M10 (Extraneous Functionality) - https://owasp.org/www-project-mobile-top-10/2016-risks/m10-extraneous-functionality
- OWASP Threat modelling - https://owasp.org/www-community/Application_Threat_Modeling

- OWASP Secure SDLC Cheat Sheet - https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets_excluded/Secure_SDLC_Cheat_Sheet.md
- Microsoft SDL - https://www.microsoft.com/en-us/sdl/
- NIST SP 800-57 (Recommendation for Key Management) - https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final
- security.txt - https://securitytxt.org/

V2: Требования к конфиденциальности и хранению данных

Цель проверки

Защита чувствительных данных, таких, как данные пользователя для авторизации (логин + пароль) и персональные данные, является ключевым аспектом в безопасности мобильных приложений. Во-первых, чувствительные данные могут быть непреднамеренно раскрыты другим приложениям, работающим на том же устройстве, если механизмы операционной системы, такие как межпроцессное взаимодействие (IPC), используются ненадлежащим образом. Данные также могут непреднамеренно попасть в облачное хранилище, резервную копию или кеш клавиатуры. Кроме того, мобильные устройства могут быть потеряны или украдены легче чем другие типы устройств, поэтому злоумышленник, получивший физический доступ к устройству, является наиболее вероятным сценарием. В этом случае могут быть реализованы дополнительные меры защиты для затруднения извлечения чувствительных данных с устройства.

Следует обратить внимание, что MASVS ориентирован на приложения, и потому не охватывает политики безопасности на уровне устройства (MDM - Mobile Device Management). Мы поощряем использование таких политик в контексте предприятия для повышения безопасности данных.

Определение чувствительных данных

К чувствительным данным в контексте MASVS относятся как данные пользователя для авторизации, так и любые другие данные, которые считаются чувствительными в конкретном контексте, например:

- Персональные данные, которые могут быть использованы для кражи личности: номера социального страхования, кредитных карт, банковских счетов, информация о здоровье.
- Конфиденциальная информация, которая может привести к репутационному ущербу и/или финансовым потерям, если она скомпрометирована: информация о договорах, информация, охватываемая соглашениями о неразглашении, управленческая информация;
- Любые данные, которые должны быть защищены по закону или внутренним требованиям компании.

Требования безопасности

Подавляющее большинство проблем с раскрытием информации можно предотвратить, следуя простым правилам. Большинство требований, перечисленных в этой главе, являются обязательными для всех уровней проверки.

#	MSTG-ID	Описание	L1	L2
2.1	MSTG-STORAGE-1	Хранилище учетных данных системы должно использоваться надлежащим образом для хранения чувствительных данных, таких как персональные данные, данные пользователя для авторизации и криптографические ключи.	x	x
2.2	MSTG-STORAGE-2	Чувствительные данные хранятся только во внутреннем хранилище приложения, либо в системном хранилище авторизационных данных.	x	x
2.3	MSTG-STORAGE-3	Чувствительные данные не попадают в логи приложения.	x	x
2.4	MSTG-STORAGE-4	Никакие чувствительные данные не передаются третьей стороне, если это не является необходимой частью архитектуры.	x	x
2.5	MSTG-STORAGE-5	Кэш клавиатуры выключен для полей ввода чувствительных данных.	x	x
2.6	MSTG-STORAGE-6	Чувствительные данные недоступны для механизмов межпроцессного взаимодействия (IPC).	x	x
2.7	MSTG-STORAGE-7	Никакие чувствительные данные, такие как пароли или пин-коды, не видны через пользовательский интерфейс.	x	x
2.8	MSTG-STORAGE-8	Никакие чувствительные данные не попадают в бэкапы, создаваемые операционной системой.		x
2.9	MSTG-STORAGE-9	Приложение скрывает чувствительные данные с экрана, когда находится в фоновом режиме.		x

#	MSTG-ID	Описание	L1	L2
2.10	MSTG-STORAGE-10	Приложение не хранит чувствительные данные в памяти дольше, чем необходимо, и полностью удаляет их из памяти после работы с ними.		x
2.11	MSTG-STORAGE-11	Приложение требует от пользователя минимальную настройку доступа к устройству, такую, как установку пин-кода на устройство.		x
2.12	MSTG-STORAGE-12	Приложение информирует пользователя о персональных данных, которые оно обрабатывает, а также о лучших практиках безопасности, которым должен следовать пользователь при использовании приложения.		x
2.13	MSTG-STORAGE-13	Конфиденциальные данные локально не должны храниться на мобильном устройстве. Вместо этого необходимые данные должны получаться с сервера и храниться только в памяти.		x
2.14	MSTG-STORAGE-14	Если конфиденциальные данные все же требуется хранить локально, они должны быть зашифрованы с помощью ключа, полученного из аппаратного хранилища, которое требует проверки подлинности.		x
2.15	MSTG-STORAGE-15	Локальное хранилище приложения должно быть стерто после превышения допустимого количества неудачных попыток.		x

Ссылки

OWASP MSTG содержит подробные инструкции по верификации требований, перечисленных в этом разделе.

- Android: Тестирование хранения данных - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05d-Testing-Data-Storage.md
- iOS: Тестирование хранения данных - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06d-Testing-Data-Storage.md

Для получения дополнительной информации смотрите также:

- OWASP Mobile Top 10: M1 (Improper Platform Usage) - https://owasp.org/www-project-mobile-top-10/2016-risks/m1-improper-platform-usage
- OWASP Mobile Top 10: M2 (Insecure Data Storage) - https://owasp.org/www-project-mobile-top-10/2016-risks/m2-insecure-data-storage
- CWE 117 (Improper Output Neutralization for Logs) - https://cwe.mitre.org/data/definitions/117.html
- CWE 200 (Information Exposure) - https://cwe.mitre.org/data/definitions/200.html
- CWE 276 (Incorrect Default Permissions) - https://cwe.mitre.org/data/definitions/276.html
- CWE 311 (Missing Encryption of Sensitive Data) - https://cwe.mitre.org/data/definitions/311.html
- CWE 312 (Cleartext Storage of Sensitive Information) - https://cwe.mitre.org/data/definitions/312.html
- CWE 316 (Cleartext Storage of Sensitive Information in Memory) - https://cwe.mitre.org/data/definitions/316.html
- CWE 359 (Exposure of Private Information ('Privacy Violation')) - https://cwe.mitre.org/data/definitions/359.html
- CWE 522 (Insufficiently Protected Credentials) - https://cwe.mitre.org/data/definitions/522.html
- CWE 524 (Information Exposure Through Caching) - https://cwe.mitre.org/data/definitions/524.html
- CWE 530 (Exposure of Backup File to an Unauthorized Control Sphere) - https://cwe.mitre.org/data/definitions/530.html
- CWE 532 (Information Exposure Through Log Files) - https://cwe.mitre.org/data/definitions/532.html
- CWE 534 (Information Exposure Through Debug Log Files) - https://cwe.mitre.org/data/definitions/534.html
- CWE 634 (Weaknesses that Affect System Processes) - https://cwe.mitre.org/data/definitions/634.html
- CWE 798 (Use of Hard-coded Credentials) - https://cwe.mitre.org/data/definitions/798.html
- CWE 921 (Storage of Sensitive Data in a Mechanism without Access Control) - https://cwe.mitre.org/data/definitions/921.html
- CWE 922 (Insecure Storage of Sensitive Information) - https://cwe.mitre.org/data/definitions/922.html

V3: Требования к криптографии

Цель верификации

Криптография является неотъемлимым компонентом защиты данных, хранящихся на мобильном устройстве. Но кроме того, это область, в которой все может пойти не так, особенно когда стандартные правила не соблюдаются. Цель верификационных требований в этой главе состоит в том, чтобы убедиться, что проверяемое приложение использует криптографию в соответствии с лучшими практиками индустрии, такими, как:

- Использование проверенных криптографических библиотек;
- Правильный выбор и настройка криптографических алгоритмов;
- Подходящий генератор случайных чисел там, где это необходимо.

Требования безопасности

#	MSTG-ID	Описание	L1	L2
3.1	MSTG-CRYPTO-1	Приложение не использует симметричное шифрование с захардкоженными ключами в качестве единственного метода шифрования.	x	x
3.2	MSTG-CRYPTO-2	Приложение использует проверенные реализации криптографических алгоритмов.	x	x
3.3	MSTG-CRYPTO-3	Приложение использует подходящие криптографические алгоритмы для каждого конкретного случая, с параметрами, которые соответствуют лучшим практикам индустрии.	x	x
3.4	MSTG-CRYPTO-4	Приложение не использует устаревшие и слабые криптографические протоколы и алгоритмы.	x	x
3.5	MSTG-CRYPTO-5	Приложение не использует один и тот же ключ несколько раз.	x	x
3.6	MSTG-CRYPTO-6	Все случайные значения генерируются с использованием безопасного генератора случайных чисел.	x	x

Ссылки

OWASP MSTG содержит подробные инструкции по верификации требований, перечисленных в этом разделе.

- Android: Тестирование криптографии - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05e-Testing-Cryptography.md
- iOS: Тестирование криптографии - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06e-Testing-Cryptography.md

Для получения дополнительной информации смотрите также:

- OWASP Mobile Top 10: M5 (Insufficient Cryptography) - https://owasp.org/www-project-mobile-top-10/2016-risks/m5-insufficient-cryptography
- CWE 310 (Cryptographic Issues) - https://cwe.mitre.org/data/definitions/310.html
- CWE 321 (Use of Hard-coded Cryptographic Key) - https://cwe.mitre.org/data/definitions/321.html
- CWE 326 (Inadequate Encryption Strength) - https://cwe.mitre.org/data/definitions/326.html
- CWE 327 (Use of a Broken or Risky Cryptographic Algorithm) - https://cwe.mitre.org/data/definitions/327.html
- CWE 329 (Not Using a Random IV with CBC Mode) - https://cwe.mitre.org/data/definitions/329.html
- CWE 330 (Use of Insufficiently Random Values) - https://cwe.mitre.org/data/definitions/330.html
- CWE 337 (Predictable Seed in PRNG) - https://cwe.mitre.org/data/definitions/337.html
- CWE 338 (Use of Cryptographically Weak Pseudo Random Number Generator (PRNG)) - https://cwe.mitre.org/data/definitions/338.html

V4: Требования к аутентификации и управлению сессиями

Цель верификации

В большинстве случаев авторизация в удаленных сервисах являются неотъемлемой частью общей архитектуры мобильного приложения. Несмотря на то, что большая часть логики происходит на бекэнде, MASVS определяет некоторые основные требования, касающиеся управления учетными записями пользователей и сессиями.

Требования безопасности

#	MSTG-ID	Описание	L1	L2
4.1	MSTG-AUTH-1	Если приложение предоставляет пользователям доступ к удалённым сервисам, на бэкенде должна быть реализована аутентификация, например, по логину и паролю.	x	x
4.2	MSTG-AUTH-2	Если используются сессии, бекэнд случайно генерирует идентификаторы сессии для аутентификации клиентских запросов без отправки данных учётной записи.	x	x
4.3	MSTG-AUTH-3	Если используется аутентификация на основе токена, сервер предоставляет токен, подписанный с использованием безопасного криптоалгоритма.	x	x
4.4	MSTG-AUTH-4	Бэкенд удаляет существующую сессию, когда пользователь выходит из системы.	x	x
4.5	MSTG-AUTH-5	На сервере реализована парольная политика.	x	x
4.6	MSTG-AUTH-6	На сервере реализован механизм защиты от перебора авторизационных данных.	x	x
4.7	MSTG-AUTH-7	Биометрическая аутентификация не является event-bound (т.е. использует только API, которое возвращает «true» или «false»). Вместо этого она основана на разблокировке keychain/keystore.		x

#	MSTG-ID	Описание	L1	L2
4.8	MSTG-AUTH-8	Сессии становятся невалидными на бэкенде после определенного периода бездействия, срок действия токена истекает.	x	x
4.9	MSTG-AUTH-9	Реализована и поддерживается двухфакторная аутентификация.		x
4.10	MSTG-AUTH-10	Для выполнения чувствительных транзакций требуется дополнительная или повторная аутентификацию.		x
4.11	MSTG-AUTH-11	Приложение информирует пользователя о всех важных действиях с их учетной записью. Пользователи могут просматривать список устройств, просматривать контекстную информацию (IP-адрес, местоположение и т.д.), и блокировать конкретные устройства.		x
4.12	MSTG-AUTH-12	Модели авторизации должны быть определены и проверенны на сервере.	x	x

Ссылки

OWASP MSTG содержит подробные инструкции по верификации требований, перечисленных в этом разделе.

- Общее: Аутентификация и управление сессиями - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x04e-Testing-Authentication-and-Session-Management.md
- Android: Тестирование локальной аутентификации - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05f-Testing-Local-Authentication.md
- iOS: Тестирование локальной аутентификации - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06f-Testing-Local-Authentication.md

Для получения дополнительной информации смотрите также:

- OWASP Mobile Top 10: M4 (Insecure Authentication) - https://owasp.org/www-project-mobile-top-10/2016-risks/m4-insecure-authentication
- OWASP Mobile Top 10: M6 (Insecure Authorization) - https://owasp.org/www-project-mobile-top-10/2016-risks/m6-insecure-authorization
- CWE 287 (Improper Authentication) - https://cwe.mitre.org/data/definitions/287.html

- CWE 307 (Improper Restriction of Excessive Authentication Attempts) - https://cwe.mitre.org/data/definitions/307.html
- CWE 308 (Use of Single-factor Authentication) - https://cwe.mitre.org/data/definitions/308.html
- CWE 521 (Weak Password Requirements) - https://cwe.mitre.org/data/definitions/521.html
- CWE 604 (Use of Client-Side Authentication) - https://cwe.mitre.org/data/definitions/604.html
- CWE 613 (Insufficient Session Expiration) - https://cwe.mitre.org/data/definitions/613.html

V5: Требования к сетевому взаимодействию

Цель верификации

Целью требований, перечисленных в этом разделе, является обеспечение конфиденциальности и целостности информации, передаваемой между мобильным приложением и сервером. Как минимум в мобильном приложении должен быть настроен безопасный шифрованный канал передачи данных с использованием протокола TLS с соответствующими настройками. L2 содержит меры усиленной защиты, такие, как SSL pinning.

Требования безопасности

#	MSTG-ID	Описание	L1	L2
5.1	MSTG-NETWORK-1	Данные, передаваемые по сети, шифруются с использованием TLS. Безопасный канал используется для всех сервисов приложения.	x	x
5.2	MSTG-NETWORK-2	Настройки TLS соответствуют современным лучшим практикам, или максимально приближены к ним, если операционная система не поддерживает рекомендуемые стандарты.	x	x
5.3	MSTG-NETWORK-3	Приложение верифицирует X.509 сертификаты сервера во время установления защищённого канала. Принимаются только сертификаты, подписанные доверенным удостоверяющим центром (CA).	x	x
5.4	MSTG-NETWORK-4	В приложении реализован SSL pinning и соединение с серверами, которые предлагают другой сертификат или ключ, даже если они подписаны доверенным центром сертификации (CA) не устанавливается.		x
5.5	MSTG-NETWORK-5	Приложение не полагается на единственный небезопасный канал связи (e-mail или SMS) для таких критических операций, как регистрация и восстановление аккаунта.		x

#	MSTG-ID	Описание	L1	L2
5.6	MSTG-NETWORK-6	Приложение использует только актуальные версии библиотек для подключения к сети и обеспечения безопасного соединения.		x

Ссылки

OWASP MSTG содержит подробные инструкции по верификации требований, перечисленных в этом разделе.

- Общее: Тестирование сетевого взаимодействия - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x04f-Testing-Network-Communication.md
- Android: Тестирование сетевого взаимодействия - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05g-Testing-Network-Communication.md
- iOS: Тестирование сетевого взаимодействия - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06g-Testing-Network-Communication.md

Для получения дополнительной информации смотрите также:

- OWASP Mobile Top 10: M3 (Insecure Communication) - https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication
- CWE 295 (Improper Certificate Validation) - https://cwe.mitre.org/data/definitions/295.html
- CWE 296 (Improper Following of a Certificate's Chain of Trust) - https://cwe.mitre.org/data/definitions/296.html
- CWE 297 (Improper Validation of Certificate with Host Mismatch) - https://cwe.mitre.org/data/definitions/297.html
- CWE 298 (Improper Validation of Certificate Expiration) - https://cwe.mitre.org/data/definitions/298.html
- CWE 308 (Use of Single-factor Authentication) - https://cwe.mitre.org/data/definitions/308.html
- CWE 319 (Cleartext Transmission of Sensitive Information) - https://cwe.mitre.org/data/definitions/319.html
- CWE 326 (Inadequate Encryption Strength) - https://cwe.mitre.org/data/definitions/326.html
- CWE 327 (Use of a Broken or Risky Cryptographic Algorithm) - https://cwe.mitre.org/data/definitions/327.html
- CWE 780 (Use of RSA Algorithm without OAEP) - https://cwe.mitre.org/data/definitions/780.html
- CWE 940 (Improper Verification of Source of a Communication Channel) - https://cwe.mitre.org/data/definitions/940.html

- CWE 941 (Incorrectly Specified Destination in a Communication Channel) - https://cwe.mitre.org/data/definitions/941.html

V6: Требования к взаимодействию с операционной системой

Цель верификации

Следование требованиям этого раздела обеспечивают безопасное использование API операционной системы. Дополнительно содержатся требования к межпроцессному взаимодействию (IPC).

Требования безопасности

#	MSTG-ID	Описание	L1	L2
6.1	MSTG-PLATFORM-1	Приложение запрашивает минимально необходимый набор разрешений.	x	x
6.2	MSTG-PLATFORM-2	Все данные, поступающие из внешних источников и от пользователя, валидируются и санитизируются. Сюда входят данные, полученные через пользовательский интерфейс, механизмы IPC (такие как intent-ы, кастомные URL-схемы) и из сети.	x	x
6.3	MSTG-PLATFORM-3	Приложение не экспортирует чувствительные данные через кастомные URL-схемы, если эти механизмы не защищены должным образом.	x	x
6.4	MSTG-PLATFORM-4	Приложение не экспортирует чувствительные данные через IPC механизмы без должной защиты.	x	x
6.5	MSTG-PLATFORM-5	JavaScript отключен в компонентах WebView, если в нём нет необходимости.	x	x
6.6	MSTG-PLATFORM-6	WebViews сконфигурирован с поддержкой минимального набора протоколов (в идеале только https). Поддержка потенциально опасных URL-схем (таких как: file, tel и app-id) отключена.	x	x

#	MSTG-ID	Описание	L1	L2
6.7	MSTG-PLATFORM-7	Если нативные методы приложения используются WebView, верифицировать, что исполняются только Javascript объекты данного приложения.	x	x
6.8	MSTG-PLATFORM-8	Десериализация объектов, если она есть, реализована с использованием безопасного API.	x	x
6.9	MSTG-PLATFORM-9	Приложение защищает себя от атак наложения экрана. (Только для Андроид)		x
6.10	MSTG-PLATFORM-10	Кэш веб-представление, хранилище и загруженные ресурсы (JavaScript и т. д.) должены быть очищены до того, как веб-представление будет уничтожено.		x
6.11	MSTG-PLATFORM-11	Убедитесь, что приложение предотвращает использование пользовательских клавиатур сторонних производителей при вводе конфиденциальных данных. (Только для iOS)		x

Ссылки

OWASP MSTG содержит подробные инструкции по верификации требований, перечисленных в этом разделе.

- Android: Тестирование взаимодействия с платформой - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05h-Testing-Platform-Interaction.md
- iOS: Тестирование взаимодействия с платформой - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06h-Testing-Platform-Interaction.md

Для получения дополнительной информации смотрите также:

- OWASP Mobile Top 10: M1 (Improper Platform Usage) - https://owasp.org/www-project-mobile-top-10/2016-risks/m1-improper-platform-usage
- OWASP Mobile Top 10: M7 (Poor Code Quality) - https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality
- CWE 20 (Improper Input Validation) - https://cwe.mitre.org/data/definitions/20.html
- CWE 79 (Improper Neutralization of Input During Web Page Generation) - https://cwe.mitre.org/data/definitions/79.html
- CWE 200 (Information Leak / Disclosure) - https://cwe.mitre.org/data/definitions/200.html

- CWE 250 (Execution with Unnecessary Privileges) - https://cwe.mitre.org/data/definitions/250.html
- CWE 672 (Operation on a Resource after Expiration or Release) - https://cwe.mitre.org/data/definitions/672.html
- CWE 749 (Exposed Dangerous Method or Function) - https://cwe.mitre.org/data/definitions/749.html
- CWE 772 (Missing Release of Resource after Effective Lifetime) - https://cwe.mitre.org/data/definitions/772.html
- CWE 920 (Improper Restriction of Power Consumption) - https://cwe.mitre.org/data/definitions/920.html
- CWE 925 (Improper Verification of Intent by Broadcast Receiver) - https://cwe.mitre.org/data/definitions/925.html
- CWE 926 (Improper Export of Android Application Components) - https://cwe.mitre.org/data/definitions/926.html
- CWE 927 (Use of Implicit Intent for Sensitive Communication) - https://cwe.mitre.org/data/definitions/927.html
- CWE 939 (Improper Authorization in Handler for Custom URL Scheme) - https://cwe.mitre.org/data/definitions/939.html

V7: Требования к качеству кода и настройкам сборки

Цель контроля

Следование требованиям данного раздела обеспечивает использование базовых практик безопасного написания кода при разработке приложения, а также стандартных средств безопасности, встроенных в компилятор.

Требования безопасности

#	MSTG-ID	Описание	L1	L2
7.1	MSTG-CODE-1	Приложение подписано валидным сертификатом.	x	x
7.2	MSTG-CODE-2	Приложение было собрано в release режиме с настройками, подходящими для релизной сборки (например, без атрибута debuggable).	x	x
7.3	MSTG-CODE-3	Отладочные символы удалены из нативных бинарных файлов.	x	x
7.4	MSTG-CODE-4	Код отладки и вспомогательный дла разработки код (например, тестовый код, бэкдоры, скрытые настройки) были удалены. Приложение не логирует подробные ошибки и отладочные сообщения.	x	x
7.5	MSTG-CODE-5	Все сторонние компоненты, используемые мобильным приложением (библиотеки и фреймворки), идентифицированы и проверены на наличие известных уязвимостей.	x	x
7.6	MSTG-CODE-6	Приложение обрабатывает возможные исключения.	x	x
7.7	MSTG-CODE-7	В логике обработки связанных с безопасностью ошибок по умолчанию запрещается доступ.	x	x
7.8	MSTG-CODE-8	В неконтролируемом коде память выделяется, освобождается и используется безопасно.	x	x

#	MSTG-ID	Описание	L1	L2
7.9	MSTG-CODE-9	Активированы все стандартные функции безопасности, предусмотренные инструментами разработчика (такие как минификация байт-кода, защита стека, поддержка PIE и ARC).	x	x

Ссылки

OWASP MSTG содержит подробные инструкции по проверке требований, перечисленных в этом разделе.

- Android: Тестирование качества кода и настроек сборки - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05i-Testing-Code-Quality-and-Build-Settings.md
- iOS: Тестирование качества кода и настроек сборки - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06i-Testing-Code-Quality-and-Build-Settings.md

Для получения дополнительной информации смотрите также:

- OWASP Mobile Top 10: M7 (Poor Code Quality) - https://owasp.org/www-project-mobile-top-10/2016-risks/m7-client-code-quality
- CWE 20 (Improper Input Validation) - https://cwe.mitre.org/data/definitions/20.html
- CWE 89 (Improper Neutralization of Special Elements used in an SQL Command) - https://cwe.mitre.org/data/definitions/89.html
- CWE 95 (Improper Neutralization of Directives in Dynamically Evaluated Code (‘Eval Injection’)) - https://cwe.mitre.org/data/definitions/95.html
- CWE 119 (Improper Restriction of Operations within the Bounds of a Memory Buffer) - https://cwe.mitre.org/data/definitions/119.html
- CWE 215 (Information Exposure through Debug Information) - https://cwe.mitre.org/data/definitions/215.html
- CWE 388 (7PK - Errors) - https://cwe.mitre.org/data/definitions/388.html
- CWE 489 (Leftover Debug Code) - https://cwe.mitre.org/data/definitions/489.html
- CWE 502 (Deserialization of Untrusted Data) - https://cwe.mitre.org/data/definitions/502.html
- CWE 511 (Logic/Time Bomb) - https://cwe.mitre.org/data/definitions/511.html
- CWE 656 (Reliance on Security through Obscurity) - https://cwe.mitre.org/data/definitions/656.html
- CWE 676 (Use of Potentially Dangerous Function) - https://cwe.mitre.org/data/definitions/676.html
- CWE 937 (OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities) - https://cwe.mitre.org/data/definitions/937.html

V8: Требования к устойчивости к атакам на стороне клиента

Цель проверки

В этом разделе рассматриваются меры усиленной защиты, рекомендуемые для приложений, которые обрабатывают или предоставляют доступ к чувствительным данным или функциональности. Отсутствие каких-либо из этих элементов защиты не означает наличие уязвимости - напротив, они призваны повысить устойчивость приложения к реверс инжинирингу и конкретным атакам на стороне клиента.

Требования в этом разделе должны применяться по мере необходимости, основываясь на оценке рисков, вызванных несанкционированным вмешательством в приложение и/или восстановлением исходного кода. Мы предлагаем обратиться к документу OWASP «Technical Risks of Reverse Engineering and Unauthorized Code Modification Reverse Engineering and Code Modification Prevention» (см. ссылки ниже) для составления списка бизнес рисков и связанных с ними технических угроз.

Чтобы любое из требований в приведенном ниже списке было эффективным, приложение должно выполнить, по меньшей мере, все MASVS-L1, а также все требования из V8, которые ему предшествуют. Например, если приложение соблюдает требование обфускации из раздела «Противодействие восстановлению логики работы приложения», оно должно также удовлетворять всем требованиям из разделов «Противодействие динамическому анализу и фальсификациям» и «Привязка к устройству».

Обратите внимание, что программные меры защиты из данного раздела не должны использоваться в качестве замены основным требованиям безопасности. Вместо этого они должны быть реализованы как специализированное дополнение, направленное на локализацию конкретных угроз, в мобильном приложении, соответствующем требования MASVS.

Следует рассмотреть следующие соображения:

1. Должна быть определена модель угроз, в которой прописаны конкретные атаки на стороне клиента, от которых необходимо защититься. Кроме того, должна быть указана степень защиты, которую следует обеспечить. Например, цель внедрения защитных мер может заключаться в том, чтобы заставить авторов вредоносного ПО, нацеленного на данное приложение, приложить значительные усилия для реверс инжиниринга.
2. Модель угроз должна отвечать здравому смыслу. Например, сокрытие криптографического ключа в whitebox реализации не имеет смысла, если злоумышленник может применить технику «code lifting».

3. Эффективность защиты всегда должна проверяться экспертом, имеющим опыт тестирования методов обфускации и защиты от фальсификации (см. также главы «Реверс инжиниринг» и «Оценка защиты ПО» в OWASP MSTG.

Противодействие динамическому анализу и фальсификациям

#	MSTG-ID	Описание	R
8.1	MSTG-RESILIENCE-1	Приложение обнаруживает и реагирует на наличие root или jailbreak, либо уведомляя пользователя, либо прекращая работу.	x
8.2	MSTG-RESILIENCE-2	Приложение не позволяет использовать отладчики и/или обнаруживает и реагирует на использование отладчика. Все доступные протоколы отладки должны быть учтены.	x
8.3	MSTG-RESILIENCE-3	Приложение обнаруживает и реагирует на внесения изменений в исполняемые файлы и критичные данные в своей песочнице.	x
8.4	MSTG-RESILIENCE-4	Приложение обнаруживает и реагирует на наличие на устройстве широко используемых инструментов и фреймворков для реверс инжиниринга.	x
8.5	MSTG-RESILIENCE-5	Приложение обнаруживает и реагирует на запуск на эмуляторе.	x
8.6	MSTG-RESILIENCE-6	Приложение обнаруживает и реагирует на изменение своего кода и данных в оперативной памяти.	x
8.7	MSTG-RESILIENCE-7	Приложение реализует несколько механизмов для каждой категории защиты (с 8.1 по 8.6). Обратите внимание, что на устойчивость к атакам влияет количество, разнообразие и оригинальность используемых механизмов.	x
8.8	MSTG-RESILIENCE-8	Механизмы обнаружения инициируют ответные меры разных типов, включая отложенные и скрытые.	x

#	MSTG-ID	Описание	R
8.9	MSTG-RESILIENCE-9	Обфускация применена в том числе и к тем программным механизмам, которые препятствуют деобфускации методами динамического анализа.	x

Привязка к устройству

#	MSTG-ID	Описание	R
8.10	MSTG-RESILIENCE-10	Приложение реализует функциональность привязки экземпляра приложения к устройству, формируя его отпечаток из нескольких свойств, уникальных для устройства.	x

Противодействие восстановлению логики работы приложения

#	MSTG-ID	Описание	R
8.11	MSTG-RESILIENCE-11	Все исполняемые файлы и библиотеки, принадлежащие приложению, зашифрованы на файловом уровне, либо важные участки кода и данных зашифрованы внутри исполняемых файлов. Простой статический анализ не позволяет обнаружить важный код или данные.	x
8.12	MSTG-RESILIENCE-12	Если задачей обфускации является защита конфиденциальных данных, то используется схема обфускации, которая подходит не только для этой задачи, но и защищает от ручной тестирования и автоматизированных деобфускаторов и учитывает последние исследования по данной теме. Эффективность схемы обфускации должна быть проверена с помощью ручного тестирования. Обратите внимание, что использование аппаратных средств защиты (если они поддерживаются устройством) предпочтительнее обфускации.	x

Противодействие Перехвату Сообщений

#	MSTG-ID	Description	R
8.13	MSTG-RESILIENCE-13	В качестве глубокой защиты, наряду с существенным усилением защиты взаимодействия, шифрование обмениваемых приложением сообщений может шифроваться для дальнейшего предотвращения перехвата.	x

Ссылки

OWASP MSTG содержит подробные инструкции по верификации соответствия требованиям, перечисленным в этом разделе.

- Android: Тестирование устойчивости к обратной разработке - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05j-Testing-Resiliency-Against-Reverse-Engineering.md
- iOS: Тестирование устойчивости к обратной разработке - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06j-Testing-Resiliency-Against-Reverse-Engineering.md

Для получения дополнительной информации смотрите также:

- OWASP Mobile Top 10: M8 (Фальсификация кода) - https://owasp.org/www-project-mobile-top-10/2016-risks/m8-code-tampering
- OWASP Mobile Top 10: M9 (Обратная разработка) - https://owasp.org/www-project-mobile-top-10/2016-risks/m9-reverse-engineering
- OWASP Reverse Engineering Threats - https://wiki.owasp.org/index.php/Technical_Risks_of_Reverse_Engineering_and_Unauthorized_Code_Modification
- OWASP Reverse Engineering and Code Modification Prevention - https://wiki.owasp.org/index.php/OWASP_Reverse_Engineering_and_Code_Modification_Prevention_Project

Приложение A: Список терминов

- **Address Space Layout Randomization (ASLR)** – Метод, затрудняющий использование ошибок повреждения памяти.
- **Application Security** – Безопасность на уровне приложений, сфокусированная на анализе компонентов, которые составляют прикладной уровень модели OSI (Open Systems Interconnection Reference), без рассмотрения безопасности, например, операционной системы или подключенных сетей.
- **Application Security Verification** – Оценка соответствия требованиям OWASP MASVS.
- **Application Security Verification Report** – Отчёт, включающий общие результаты проверки и анализа конкретного приложения, проведённые специалистом по безопасности.
- **Authentication** – Верификация соответствия пользователя приложения заявленной им личности.
- **Automated Verification** – Использование автоматических инструментов (для динамического и статического анализа), использующих сигнатуры уязвимостей для поиска проблемных участков приложения.
- **Black box testing** – Метод тестирования ПО, который анализирует функциональность приложения без знания о его внутреннем устройстве и принципах работы.
- **Component** – автономный блок кода, с соответствующими дисковыми и сетевыми интерфейсами, который взаимодействует с другими компонентами.
- **Cross-Site Scripting (XSS)** – Уязвимость, обычно обнаруживаемая в веб-приложениях, позволяющая внедрить в контент веб-страницы вредоносный код, исполняемый на стороне клиента.
- **Cryptographic module** – Аппаратное, программное, или программно-аппаратное обеспечение, реализующее криптографические алгоритмы и/или генерирует криптографические ключи.
- **CWE** – Общедоступный список часто встречающихся недостатков безопасности программного обеспечения.
- **DAST** – Динамический анализ безопасности (Dynamic application security testing) - поиск уязвимостей приложения во время его выполнения.
- **Design Verification** – Техническая оценка безопасности архитектуры приложения.
- **Dynamic Verification** – Использование автоматических инструментов для поиска уязвимостей во время выполнения приложения.
- **Globally Unique Identifier (GUID)** – уникальный номер, используемый в качестве идентификатора в программном обеспечении.
- **Hyper Text Transfer Protocol (HTTP)** – Протокол прикладного уровня для распределенных, совместных, гипермедийных информационных систем. Это основа передачи данных для Всемирной паутины.
- **Hardcoded keys** – захардкоженные ключи (хранятся непосредственно в коде приложения).

- **IPC** – межпроцессное взаимодействие (Inter Process Communications), в IPC процессы взаимодействуют друг с другом и ядром, чтобы координировать свою деятельность.
- **Input Validation** – Канонизация и проверка недоверенных данных, вводимых пользователем.
- **JAVA Bytecode** – Java байт-код - набор команд виртуальной машины Java (JVM). Каждый байт-код состоит из одного или, в некоторых случаях, двух байтов, которые представляют команду (код операции), а также ноль или более байтов для передачи параметров.
- **Malicious Code** – вредоносный код, добавленный в приложение во время его разработки без ведома владельца приложения, который обходит заложенную политику безопасности. Не то же самое, что вредоносное ПО, такое как вирус или червь!
- **Malware** – Исполняемый код, который вводится в приложение во время выполнения без ведома пользователя или администратора приложения.
- **Open Web Application Security Project (OWASP)** – Проект Open Web Application Security (OWASP) является всемирным бесплатным и открытым сообществом, направленным на повышение безопасности прикладного программного обеспечения. Наша миссия заключается в том, чтобы сделать безопасность приложений «видимой», чтобы люди и организации могли принимать обоснованные решения о рисках безопасности приложений. https://www.owasp.org/
- **Personally Identifiable Information (PII)** – Информация, которая может использоваться сама по себе или совместно с другой информацией для идентификации, получения контактов или поиска местонахождения человека.
- **PIE** – Независимый от положения исполняемый файл (PIE) представляет собой тело машинного кода, которое, будучи помещённым где-то в первичной памяти, выполняется должным образом независимо от его абсолютного адреса.
- **PKI** – PKI - это соглашение, которое связывает открытые ключи с соответствующими идентификаторами объектов. Связь устанавливается посредством процесса регистрации и выдачи сертификатов в удостоверяющем центре (CA).
- **SAST** – Статический анализ безопасности (SAST) представляет собой набор техник, предназначенных для анализа исходного кода приложения, байт-кода и бинарных файлов для обнаружения ошибок при написании кода и проектировании, которые приводят к уязвимостям. Решения SAST анализируют приложение «изнутри» в неработающем состоянии.
- **SDLC** – Жизненный цикл разработки программного обеспечения.
- **Security Architecture** – Абстракция проектирования приложения, которая идентифицирует и описывает, где и как используются требования безопасности, а также идентифицирует и описывает местоположение и чувствительность данных пользователя и приложения.
- **Security Configuration** – Конфигурация исполнения приложения, влияющая на то, как используются требования безопасности.

- **Security Control** – Функция или компонент, который выполняет проверку безопасности (например, проверку контроля доступа) или при вызове, влияет на безопасность (например, генерирует запись аудита).
- **SQL Injection (SQLi)** – Техника внедрения SQL кода в запрос к БД, используемая для атаки на мобильные и веб-приложения.
- **SSO Authentication** – Single Sign On (SSO) возникает, когда пользователь входит в аккаунт на одном клиенте, и происходит автоматический вход на других клиентах, независимо от платформы, технологии или домена, которые использует пользователь. Например, когда вы авторизуетесь в Google, вы автоматически авторизуетесь на YouTube, Google Docs и Gmail.
- **Threat Modeling** – Метод, состоящий в разработке все более совершенных архитектур безопасности для идентификации угроз, зон безопасности, средств контроля безопасности и важных технических и бизнес-активов.
- **Transport Layer Security** – Криптографические протоколы, обеспечивающие безопасность соединения по Интернету.
- **URI/URL/URL fragments** – Единый идентификатор ресурса - это строка символов, используемых для идентификации имени или веб-ресурса. URL часто используется в качестве ссылки на ресурс.
- **User acceptance testing (UAT)** – Тестовая среда, которая ведет себя как производственная среда, где все тестирование программного обеспечения выполняется до перехода в лайв.
- **Verifier** – Лицо или команда, которая проверяет приложение на соответствие требованиям ASVS OWASP.
- **Whitelist** – Список разрешённых данных или операций, например список символов, которые могут быть поданы на вход.
- **X.509 Certificate** – Сертификат X.509 это цифровой сертификат, использующий международную инфраструктуру открытых ключей (PKI) для проверки того, что открытый ключ принадлежит пользователю, компьютеру или сервису, указанному в сертификате.

Приложение B: Ссылки

Следующие проекты OWASP будут полезны для пользователей/последователей этого стандарта:

- OWASP Mobile Security Project - https://owasp.org/www-project-mobile-security/
- OWASP Mobile Security Testing Guide - https://owasp.org/www-project-mobile-security-testing-guide/
- OWASP Mobile Top 10 Risks - https://owasp.org/www-project-mobile-top-10/
- OWASP Reverse Engineering and Code Modification Prevention - https://wiki.owasp.org/index.php/OWASP_Reverse_Engineering_and_Code_Modification_Prevention_Project

Следующие веб-сайты также будут полезны для пользователей/последователей этого стандарта:

- MITRE Common Weakness Enumeration - http://cwe.mitre.org/
- PCI Security Standards Council - https://www.pcisecuritystandards.org
- PCI Data Security Standard (DSS) v3.0 Requirements and Security Assessment Procedures - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Список изменений

V1.3 - 13 May 2021

We are proud to announce the introduction of a new document build pipeline, which is a major milestone for our project. The build pipeline is based on Pandocker and Github Actions. This significantly reduces the time spent on creating new releases and will also be the foundation for the OWASP MSTG and will be made available for the OWASP ASVS project.

Changes

- 4 more translations are available, which are Hindi, Farsi, Portuguese and Brazilian Portuguese
- Added requirement MSTG-PLATFORM-11

Special Thanks

- Jeroen Willemsen for kick-starting this initiative last year!
- Damien Clochard and Dalibo for supporting and professionalizing the build pipeline.
- All our Hindi, Farsi, Portuguese and Brazilian Portuguese collaborators for the excellent translation work.

V1.2 - 7 марта 2020 - Международный релиз

Следующие изменения представлены в релизе 1.2:

- MASVS доступен на упрощенном китайском.
- Изменено название в обложке книги MASVS.
- Удалены Mobile Top 10 и CWE из MSTG и объединены с существующими ссылками в MASVS.

V1.2-RC - 5 октября 2019 - Предварительный релиз

Изменения в релизе 1.2:

- Повышен до статуса флагмана.
- Изменено трабование: MSTG-STORAGE-1 “нужно использовать”.
- Добавленны требования MSTG-STORAGE-13, MSTG-STORAGE-14, и MSTG-STORAGE-15 с акцентом на защиту данных.
- Изменено требование MSTG-AUTH-11 для сохранения контекстной информации.

- Изменено требование MSTG-CODE-4 чтобы охватить больше чем просто отладка.
- Добавлено трабование MSTG-PLATFORM-10 для более безопасного использования веб-представлений.
- Добавлено требование MSTG-AUTH-12 added чтобы напомнить разработчикам о внедренных разрешениях пользователей, особенно в случае многопользовательских приложений.
- Добавлено немного больше описания того, как следует использовать MASVS с учетом оценки риска.
- Добавлено еще немного описания платного контента.
- Добавлено требование MSTG-ARCH-11, чтобы включить политику раскрытия информации для приложений L2.
- Добавлено требоавние MSTG-ARCH-12, чтобы показать разработчикам, что соответствующие международные законы о конфиденциальности должны соблюдаться.
- Создан согласованный стиль для всех ссылок в английской версии.
- Добавлено требоавние MSTG-PLATFORM-11 для противодействия шпионажу с помощью сторонних клавиатур.
- Добавлено требоавние MSTG-MSTG-RESILIENCE-13 для предотвращения перехвата данных в приложении.

V1.1.4 - 4 Июля 2019 - Саммит версия

Изменения в релизе 1.1.4:

- Исправлены все ошибки markdown.
- Обновления во французском и испанском переводах.
- Список изменений переведен на китайский и японский языки.
- Автоматизирована проверка markdown синтаксиса и доступность ссылок в документах.
- Для облегчения поиска рекомендаций и тест-кейсов добавлены идентификационные номера требований, которые будут включены в следующих версиях MSTG.
- Уменьшен размер репозитория и папка Generated добавлена в .gitignore.
- Добавлен Кодекс Поведения и Рекомендации по внесению изменений.
- Добавлен шаблон для пул реквестов.
- Обновлена синхронизация с актуальным репозиторием для хостинга Gitbook сайта.
- Обновлены скрипты для генерации XML/JSON/CSV для всех переводов.
- Вступление переведено на китайский язык.

V1.1.3 - 9 Января 2019 - Мелкие Изменения

Изменения в релизе 1.1.3:

- Исправлена ошибка перевода требования 7.1 на испанский язык.

- Новый раздел переводчиков в списке благодарностей.
- Мелкие изменения в японском переводе.

V1.1.2 - 3 Января 2019 - Спонсорство и интернационализация

Изменения в релизе 1.1.2:

- Добавлены благодарности купившим электронную версию книгу.
- Добавлена отсутствующая ссылка для аутентификации и обновлена поломанная ссылка для аутентификации в V4.
- Исправлены поменянные местами требования 4.7 и 4.8 в английской версии.
- Первый интернациональный релиз!
  - Исправления в переводе на испанский язык. Перевод синхронизирован с английской версией (1.1.2).
  - Исправления в переводе на русский язык. Перевод синхронизирован с английской версией (1.1.2).
  - Добавлены первые версии переводов на китайский, французский, немецкий и японский языки!
- Для облегчения переводов документ был упрощен.
- Добавлены инструкции для автоматического релиза.

V1.1.0 - 14 Июля 2018

Изменения в релизе 1.1:

- Удалено требование 2.6 “Буфер обмена выключен для текстовых полей, которые могут содержать конфиденциальные данные.”
- Добавлено требование 2.2 “Конфиденциальные данные хранятся только во внутреннем хранилище приложения, либо в системном хранилище авторизационных данных.”
- Требование 2.1 перефразировано в “Хранилище учетных данных системы используется надлежащим образом для хранения конфиденциальных данных, таких как персональные данные, данные пользователя для авторизации и криптографические ключи.”

V1.0 - 12 Января 2018

Изменения в релизе 1.0:

- Удалена глава 8.9 как идентичная главе 8.12

- Обобщена глава 4.6
- Мелкие изменения (опечатки и др.)