УДК 004.056

ФОРМАЛЬНАЯ ПОСТАНОВКА ЗАДАЧИ РАЗРАБОТКИ ПОДСИСТЕМЫ УПРАВЛЕНИЯ ПОКАЗАТЕЛЯМИ ЗАЩИЩЕННОСТИ ФАЙЛООБМЕННОГО СЕРВИСА

Медведев Н.В.

Московский государственный технический университет имени Н.Э. Баумана
Москва, Российская Федерация

Задача проектирования и разработки информационной системы управления показателями защищенности сервиса для обмена сообщениями на платформе Android заключается не только в самом управлении доступом, с которой справляются формальные модели доступа, описанные ранее, но и в обеспечении безопасности файлов от возможных угроз нарушения конфиденциальности или целостности. То есть защита на более высоком уровне.

Сама концепция открытости мобильной платформы Android несёт как преимущества, так и недостатки. Преимуществами являются большой выбор устройств и доступность средств разработки. Недостатком же – большое количество всевозможных угроз безопасности системы [1].

Таковым предполагается назначить критерий, задаваемый через средний предотвращенный ущерб системе при использовании мер и средств защиты, направленных на противодействие угрозам безопасности. Под системой в данной работе понимается объединение пользовательского приложения и его среды функционирования.

Обеспечивать безопасность системы планируется использованием совокупности программных и организационных мер защиты. Предусмотреть защиту от всех угроз безопасности невозможно, потому что это нивелировало бы экономическую целесообразность использования приложения.

Поэтому дополнительным критерием оптимальности будет являться стоимость использования соответствующих мер и средств защиты. Данная стоимость не должна превышать некий порог, устанавливаемый заказчиком разработки .

Соответственно возникает необходимость выделения критических угроз, предотвращение которых является обязательной процедурой, несмотря на их стоимость, потому что иначе теряется смысл использования всего приложения – оно будет скомпрометированным по умолчанию.

Возможные угрозы делятся на два типа: угрозы среде функционирования и угрозы при работе из-под приложения. Первый тип угроз направлен на вмешательство в нормальное функционирование приложения со среды операционной системы, второй – на эксплуатацию уязвимостей самого приложения при его нормальном режиме работы. Для предотвращения угроз будут использоваться как программные меры, так и организационные, которые могут быть выделены в отдельную методику [2].

Соответствующая математическая постановка задачи оперирует следующими исходными данными:

$A_1 = \{a_{11}, a_{12}, \dots, a_{1n_1}\}$ – множество возможных угроз среде функционирования приложения со стороны операционной системы с соответствующими индексами $N_1 = \{1,2, \dots, n_1\}$.

$A_2 = \{a_{21}, a_{22}, \dots, a_{2n_2}\}$ – множество возможных угроз, возникающих при эксплуатации уязвимостей приложения в процессе работы с ним, с соответствующими индексами $N_2 = \{1,2, \dots, n_2\}$.

$A = A_1 \cup A_2 = \{a_1, a_2, \dots, a_n\}$ – множество всех возможных угроз безопасности системы в целом от всех источников с соответствующими индексами $N = N_1 \cup N_2 = \{1,2, \dots, n\}$, $n = n_1 + n_2$.

$A_0 = \{a_{01}, a_{02}, \dots, a_{0n_0}\}$ – множество угроз, которые обязательно должны быть предотвращены любым способом, несмотря на стоимость, для нормального функционирования приложения, с соответствующими индексами $N_0 = \{1,2, \dots, n_0\}$, $A_0 \subseteq A, N_0 \subseteq N, n_0 \leq n$. Таковыми на данном этапе являются угрозы наличия Root-доступа, декомпиляции приложения, несанкционированного доступа к защищенным пользовательским данным.

$B_1 = \{b_{11}, b_{12}, \dots, b_{1m_1}\}$ – множество мер и средств защиты от угроз среде функционирования приложения со стороны операционной системы с соответствующими индексами $M_1 = \{1,2, \dots, m_1\}$. Данные меры будут в основном являться организационными.

$B_2 = \{b_{21}, b_{22}, \dots, b_{2m_2}\}$ – множество мер и средств защиты от угроз, возникающих при эксплуатации уязвимостей приложения в процессе работы с ним, с соответствующими индексами $M_2 = \{1,2, \dots, m_2\}$. Данные меры будут в основном являться программными.

$B = B_1 \cup B_2 = \{b_1, b_2, \dots, b_m\}$ – множество всех возможных мер и средств защиты от угроз безопасности системы в целом от всех источников с соответствующими индексами $M = M_1 \cup M_2 = \{1,2, \dots, m\}$, $m = m_1 + m_2$.

$B_0 = \{b_{01}, b_{02}, \dots, b_{0m_0}\}$ – множество мер и средств защиты от угроз, которые обязательно должны быть предотвращены любым способом, несмотря на стоимость, для нормального функционирования приложения, с соответствующими индексами $M_0 = \{1,2, \dots, m_0\}$, $B_0 \subseteq B, M_0 \subseteq M$, $m_0 \leq m$, $m_0 \leq n_0$. Таковыми на данном этапе являются меры и средства по предотвращению соответствующих угроз из A_0: проверка на нали-

чие Root-доступа, обфускация приложения при сборке.

$C = \{c_1, c_2, \dots, c_m\}$ – множество стоимостей исполнения j-го средства или меры защиты от угроз безопасности системы в целом, $j \in M$.

$C_0 = \{c_{01}, c_{02}, \dots, c_{0m_0}\}$ – множество стоимостей мер и средств защиты от угроз, которые обязательно следует предотвратить любым способом для нормального функционирования приложения. Соответствует мерам из B_0. $C_0 \subseteq C$. Предполагаемая длительность эксплуатирования системы обозначается периодом времени $T = [t_0, t_{max}]$. На соответствующем интервале времени T вероятность проявления i-й угрозы обозначается как p_i, где $p_i \in [0,1]\ \forall i \in N$ (определяется по данным статистики или с использованием экспертных оценок). При этом ожидается обязательное проявление угроз из множества A_0: $p_k = 1\ \forall k \in N_o$.

Предотвращенный ущерб от возможной реализации i-й угрозы безопасности системы обозначается u_i, где $u_i \geq 0\ \forall i \in N$.

$v_{ij}, \forall i \in N, \forall j \in M$, $v_{ij} \in [0,1]$ – вероятность предотвращения реализации i-й угрозы безопасности системы при использовании j-го средства или меры защиты (определяется по данным статистики или с использованием экспертных оценок). При этом $v_{ij} \to 1, \forall i \in N_0, \forall j \in M_0$. Вероятность предотвращения реализации обязательных угроз должна стремиться к единице.

Затраты на обеспечение защиты не должны превышать некий установленный, например, заказчиком порог: C_{max}. При этом стоит учитывать, что затраты на предотвращение обязательных угроз также составляют это значение [3].

На этапе разработки можно предусмотреть большое количество различных мер и средств обеспечения безопасности. Но не все из этих средств надлежит использовать при эксплуатации приложения: некоторые из-за высокой стоимости исполнения, некоторые из-за недостаточной эффективности предотвращения соответствующей угрозы. В итоге возникает ситуация, когда мера описана, но не используется. Для оценки показателя эффективности выбора используемых средств и мер защиты системы от угроз безопасности используется множество $X = \{x_1, x_2, \dots, x_m\}\ \forall j \in M\ x_j \in \{0,1\}$, где $x_j = 1$, если j-е средство или мера защиты будет применяться в системе для защиты от реализации некоторой угрозы безопасности; $x_j = 0$, если не применяется. Очевидно, что $x_k = 1\ \forall k \in M_o$

Подытоживая вышеописанные ограничения, можно сформулировать итоговую математическую постановку задачи проектирования и разработки информационной системы управления показателями защищенности сервиса для обмена сообщениями, которая описывает эффективность выбора средств и мер защиты от угроз безопасности системы в целом и демонстрирует средний возможный предотвращенный ущерб:

$$\begin{cases} R(X) = \sum_{i=1}^{n} p_i u_i \max_{j \in M} (v_{ij} x_j) \to \max\limits_{X} \\ \sum_{j=1}^{m} c_j x_j \leq C_{max}. \end{cases}$$

где $R(X)$ – суммарный предотвращенный ущерб от реализации угроз при использовании соответствующих мер или средств защиты. Этот показатель полагается максимизировать [4].

Поскольку множество X можно интерпретировать как вектор булевых переменных, то поставленная задача является задачей булева программирования. Ее решением будет являться нахождение всех неизвестных компонент этого вектора и выбор тех средств и мер защиты $b_j \in B$, для которых j-я компонента $x_j, \forall j \in M$ равна 1. Для решения поставленной задачи необходимо рассмотреть основные угрозы безопасности приложения и пользовательских данных, включая обязательные для предотвращения угрозы из множества A_0, а также соответствующие им меры и средства защиты для обеспечения противодействия.

Литература

1. Цирлов В.Л. Теоретические основы информационной безопасности автоматизированных систем / В.Л. Цирлов. – М.: Феникс, 2008. – 173с.

2. Android for developers. – Режим доступа: https://developer.android.com. – Дата доступа 25.09.2020.

3. Android security for developers – Режим доступа: https://source.android.com/security. – Дата доступа: 23.09.2020.

4. Android vulnerabilities – Режим доступа:. https://www.androidvulnerabilities.com. – Дата доступа: 27.09.2020.