УДК 004.942

Г.Ю. Потерпеев

МЕТОД ПРОГНОЗИРОВАНИЯ ДЕЙСТВИЙ ЗЛОУМЫШЛЕННИКА ПРИ ВЫБОРЕ ОПТИМАЛЬНОГО СКРЫТНОГО ВОЗДЕЙСТВИЯ НА ОПЕРАЦИОННУЮ СИСТЕМУ МОБИЛЬНОГО ПЕРСОНАЛЬНОГО УСТРОЙСТВА

Потерпеев Г.Ю. **Метод прогнозирования действий злоумышленника при выборе оптимального скрытного воздействия на операционную систему мобильного персонального устройства.**

Аннотация. В статье реализован один из подходов количественной оценки скрытности вредоносных воздействий, приведён способ формирования множества потенциально реализуемых воздействий, раскрыто понятие демаскирующих признаков воздействий, проведено количественное сравнение отрицательного и положительного эффектов при выборе конкретного механизма воздействия.

Ключевые слова: операционная система, мобильное персональное устройство, ранжирование, расстановка коэффициентов.

Poterpeev G.Y. **Method of Forecasting Maleficent Actions when Choosing the Optimal Covert Action on the Operating System of Mobile Personal Device.**

Abstract. The article contains one of the approaches to quantitative maleficent actions secrecy evaluation. The paper shows a method to form a multitude of potentially implemented maleficent actions. The article also explains the term «sign of action» and includes measurement of positive and negative effects when choosing the specific action mechanism.

Keywords: operation system, mobile personal device, ranking, coefficients factoring.

1. Введение. Современные вирусы для мобильных платформ на сегодняшний день стали вполне осязаемой и реальной угрозой. Так же как и в случае атак на операционную систему персонального компьютера (ОС ПК), зачастую целью становится персональные данные пользователя – владельца МПУ, идентификационные данные устройства, сведения об особенностях работы операционной системы и т.д.

Можно выделить несколько основных направлений развития мобильных угроз:

– кража конфиденциальных и персональных данных;

– скрытная отправка платных SMS-сообщений или выполнение звонков на «партнерский номер» без ведома владельца;

– мошеннические транзакции с использованием систем интернет-банкинга;

– осуществление скрытного копирования пользовательских данных;

– нарушение работоспособности мобильного персонального устройства.

Среди особенностей мобильного устройства можно выделить следующие:

– возможность физическоо доступа к МПУ значительно выше, чем к ПК;

– для передачи данных в основном используется беспроводная среда;

– существует возможность получения доступа к ОС без её запуска;

– в конкретном устройстве содержатся персональные данные конкретного пользователя, что позволяет персонифицировать владельца МПУ

– практически отсутствует разграничение к ресурсам со стороны пользователя (принцип: «один пользователь – одно МПУ»).

2. Исходные данные. Будем считать, что злоумышленник располагает активной компьютерной системой S_A. «Активность» S_A заключается в том, что S_A может оказывать влияние на качество функционирования «пассивной» мобильной операционной системы S_P, которая активно не влияет на S_A.

Предполагается, что активные воздействия системой S_A производятся при наличии уязвимостей. К таковым относятся: открытые порты приёма у системы S_P, возможность прямого доступа приложений к памяти S_P, возможность запуска фоновых процессов, наличие «слабых» паролей или открытого административного доступа к операционной системе S_P, отсутствие шифрования персональной информации или хранение ключей шифрования в открытом виде, возможность не замечаемых системой S_P самопроизвольных запусков различных приложений и т.п. Перечень уязвимостей может быть получен из готовой базы данных уязвимостей (NVD, CVE и др.) либо сформирован самостоятельно.

Полагаем, что злоумышленник (далее система S_A) для каждой уязвимости системы S_P располагает некоторым множеством механизмов их реализации. В то же время считаем, что реализации уязвимостей могут обнаруживать себя множеством выявляемых (демаскирующих) признаков (например, изменение содержимого доступных для просмотра системных файлов, некорректная работа служб, невозможность авторизации легального пользователя и т.п.).

В этом случае для системы S_A множеством выявляемых (демаскирующих) признаков является множество отрицательных результатов воздействий на систему S_P. К множеству положительных результатов воздействий на S_P злоумышленник относит получение доступа к ОС, возможность считывания и/или

изменения системной информации, дестабилизацию функционирования системы S_P и т.п.

Требуется разработать инструментарий прогнозирования действий злоумышленника при выборе оптимального скрытного деструктивного воздействия на систему S_P, используя которое система S_A достигает наибольший результирующий эффект. Создание такого инструментария позволяет в дальнейшем определять необходимые меры (способы) и/или требования к разработке средств эффективной защиты системы S_P от подобного рода воздействий.

3. Модель угроз информационной безопасности системы. Для осуществления несанкционированного воздействия на систему необходимо изначально просканировать её на предмет наличия уязвимостей, включая сбор информации об ОС, используемых протоколах, сведениях о сетевом устройстве и т.д.

В результате получаем множество возможных уязвимостей объекта воздействия $R = \{r_1, r_2, ..., r_n\}$. Элементами данного множества являются открытые порты приема данных, прямой доступ приложений к памяти устройства, возможность запуска фоновых процессов, слабые пароли либо открытый административный доступ к ОС, отсутствие шифрования персональной информации либо хранение ключей шифрования в открытом виде, возможность скрытного самопроизвольного запуска приложений без ведома пользователя и т.п.

Для каждой уязвимости существует множество $M = \{m_1, m_2, ..., m_k\}$ – множество известных способов реализаций уязвимостей для каждого r в момент времени t. При этом время, затрачиваемое на реализацию, не должно превышать некоторого значения t_{max} .

Для объекта существует множество выявляемых признаков воздействий $P = \{p_1, p_2, ..., p_l\}$. К таковым относятся: изменение содержимого системных файлов, некорректная работа служб, невозможность авторизации легального пользователя и т.д.

Для каждого элемента множества M существует результат воздействия, принадлежащий множеству $I = \{i_1, i_2, ..., i_l\}$. Таковым результатом воздействия может быть, например, получение доступа к ОС, возможность считывания и/или изменения персональной и системной информации, дестабилизация работы системы.

Таким образом, при соответствии операционной системы мобильного персонального устройства (МПУ) некоторому состоянию r_i

и существующей возможности использования механизма реализации уязвимости, строится матрица возможных воздействий:

$R\backslash M$	m_1	m_2	...	...	m_k
r_1	$r_1 m_1$	$r_1 m_2$	...	...	$r_1 m_k$
r_2	$r_2 m_1$	$r_2 m_2$	...	...	$r_2 m_k$
...	...	...	...	...	...
...	...	...	...	...	...
r_n	$r_n m_1$	$r_n m_2$	...	...	$r_n m_k$

При этом если данный механизм реализации уязвимости m не может быть реализован по отношению к r в момент времени t то соответствующее поле принимает значение 0.

В процессе заполнения матрицы получаем набор возможных результатов реализаций имеющихся уязвимостей объекта. При этом ненулевой результат реализаций относится к множеству I, каждое i имеет фиксированное ненулевое значение, то есть предположительно приводит к определенному результату воздействия. К накладываемым ограничениям относятся:

1) Время, затрачиваемое на реализацию.

2) Обнаруживаемые признаки воздействия.

Таким образом, результатом будет являться множество:

$$I = R \times M$$

Математическая модель функционирования МПУ в условиях преднамеренного воздействия будет проиллюстрирована с помощью следующих выражений:

$$\Phi = \{\Phi_1 = \{\{\Phi_{11}\}, \{\Phi_{12}\}, ..., \{\Phi_{1n_1}\}\}, ..., \Phi_k = \{\{\Phi_{k1}\}, \{\Phi_{k2}\}, ..., \{\Phi_{kn_k}\}\}\},$$

$$W_1 = \begin{cases} \{w_{11}\} = <\{a_{11} * w_1'\}, \{C_{11} * w_1, C_{12} * w_2, ..., C_{1r} * w_r\}> \\ \{w_{1n_1}\} = <\{a_{1n_1} * w_{n_1}'\}, \{C_{1n_1} * w_1, C_{1n_1+1} * w_2, ..., C_{1n_1+r} * w_r\}> \end{cases},$$

$$W_k = \begin{cases} \{w_{k1}\} = <\{a_{k1} * w_{k1}'\}, \{C_{k1} * w_1, C_{k2} * w_2, ..., C_{kp} * w_r\}> \\ \{w_{kn_k}\} = <\{a_{kn_k} * w_{kn_k}'\}, \{C_{kn_k} * w_1, C_{kn_k+1} * w_2, ..., C_{kn_k+r} * w_r\}> \end{cases},$$

где: Ф – множество механизмов воздействий (при этом Φ_1 – множество механизмов воздействий на уязвимость U_1, а Φ_2 – множество механизмов воздействий на уязвимость U_2 и т.д.). Наборы демаскирующих признаков для каждого механизма воздействия формируются на

основании существующей базы знаний и проверяются экспериментально. При этом весовые коэффициенты расставляются на основании метода экспертной оценки, а при наличии временных ограничений - методом попарного сравнения.

В приведенном выше выражении: $W = \{W_1, \ldots, W_k\}$ – множество результатов воздействий на ОС, $\{w'_{11}, \ldots, w'_{k1}\}$ – множество целевых «положительных» результатов воздействий на U_1 уязвимость, $\{w_1, \ldots, w_r\}$ – множество «побочных» результатов воздействий, то есть так называемых демаскирующих факторов.

Таким образом, результат вредоносного воздействия можно представить в виде:

$$\Phi_i = \{\Phi_{i1}, \Phi_{i2}, ..., \Phi_{in_i}\} \to U_i \Rightarrow (F_i) \Rightarrow W_i \to \{w_{i1}, w_{i2}, ..., w_{in_i}\},$$

$$\{w_{i1}, w_{i2}, ..., w_{in_i}\} = \{a_i \otimes w_i^*\}\{C_{i1}^{(1)} * w_1, C_{i2}^{(2)} * w_2, ..., C_{ir}^{(*)} * w_r\}.$$

С практической точки зрения, к возможным уязвимостям следует относить:

- возможность НСД к персональной информации;
- утечка персональных данных;
- несанкционированная модификация персональных данных;
- угрозы дестабилизации работы устройства;
- воздействия на уровне ОС (к примеру, СМС сообщение с определенным текстом, приводящее к недекларированному поведению системы);
- воздействия на периферийные устройства (к примеру, вывод из строя GSM-модуля);
- угроза доступа к операционной системе мобильного передающего устройства с получением определенных прав.

Предложенная модель позволяет осуществить параметризацию имеющихся в целевой операционной системе уязвимостей и механизмов воздействия на них для последующей оценки полезности положительного эффекта и степени проявления демаскирующих признаков, проявляющихся в ходе применения того или иного механизма воздействия.

4. Метод выбора механизма воздействия на операционную систему. Сущность метода состоит в ранжировании выделенных уязвимостей и суммарной оценке механизмов реализации с учетом полезного эффекта и степени проявления демаскирующих признаков.

Структура метода представлена на рисунке 1.

Рис. 1. Структура метода выбора механизма воздействия

Метод состоит из следующей последовательности шагов:

1. Формирование множества уязвимостей системы S_P, где:

$$U = \{u_1, u_2, ..., u_k\}.$$

2. Для каждой уязвимости u_i из множества U определяется множество допустимых механизмов воздействий. Все допустимые механизмы воздействий на все уязвимости образуют множество Φ, где:

$$\Phi = \{\Phi_1, \Phi_2, ..., \Phi_n\}.$$

3. Для каждой пары $< U_i, \Phi_j >$, где U_i – i-я уязвимость u_i, Φ_j – j-й механизм воздействия, определяется при наличии положительного результата w^+_l ($l = 1(1)p$) и отрицательных результатов w^-_d ($d = 1(1)r$).

4. Для каждой вышеописанной пары $< U_i, \Phi_j >$ определяется весовой коэффициент положительного эффекта.

5. Для каждой вышеописанной пары $< U_i, \Phi_j >$ определяются весовые коэффициенты демаскирующих признаков.

6. Задаётся ограничение на суммарный эффект положительного результата (результативность) – не менее заданного положительного значения R^+:

$$c^+_{ijl} * w^+_l \geq R^+.$$

7. Задаётся ограничение на суммарный эффект отрицательных (демаскирующих) признаков (скрытность) – не более заданного положительного значения R^-:

$$\sum_{i=1}^{k} \sum_{j=1}^{n} \sum_{l=1}^{r} c^-_{ijl} * w^-_d \leq R^-.$$

8. Вычисляется результирующий эффект как разность положительного эффекта и суммы демаскирующих признаков с учетом весовых коэффициентов для каждого механизма воздействия:

$$(c^+_{ijl} * w^+_l - \sum_{i=1}^{k} \sum_{j=1}^{n} \sum_{l=1}^{r} c^-_{ijl} * w^-_d) \rightarrow \max.$$

9. Осуществляется выбор уязвимости и её механизма реализации, обладающих максимальным результирующим эффектом.

Заметим, что выше рассматривался подход, при котором значения w^+_l и w^-_d были заданы в абсолютной шкале измерений.

Однако, если величины w^+_l и w^-_d задаются в порядковой шкале,

алгоритм действий был бы другим. Изменяется данный алгоритм и в том случае, когда эти величины определяются не как числовые, а как лингвистические или нечёткие переменные.

Существенное влияние на изменение алгоритма оказывает учёт продолжительностей проявления отрицательных и положительных результатов воздействий на уязвимости, а также типы шкал, в которых изменяют упомянутые выше продолжительности проявлений.

5. Заключение. Таким образом, предложенный подход позволяет выявить наиболее результативные и наименее заметные возможные воздействия на МПУ, что позволяет прогнозировать наиболее вероятные вредоносные воздействия и пути их реализации.

Также результатом применения подхода является ранжирование угроз, на основании чего можно выработать рекомендации по предотвращению наиболее вредоносных воздействий на МПУ.

Литература

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных ФСТЭК // М. 2008. 231 с.
2. *Девянин П.Н.* Модели безопасности компьютерных систем // М.: 2011 128 с.
3. *Потерпеев Г.Ю.* Модель угроз информационной безопасности мобильных персональных устройств. Методы обеспечения информационной безопасности // 2013.
4. *Лукацкий А.В.* Обнаружение атак // Санкт-Петербург: БХВ. 2001. 624 с.
5. *Климов А.В.* Программирование для мобильных устройств // Санкт-Петербург: Питер. 2007. 321 с.
6. *Б. Харди, Б. Филлипс.* Программирование под Android:практическое руководство // Санкт-Петербург: Питер. 2014. 592 с.
7. *Еремеев М.А., Ломако А.Г., Новиков В.А.* Метод выявления дефектов и недокументированных возможностей программ // Информационное противодействие угрозам терроризма. 2010. №14. С. 46–49.
8. *Еремеев М.А., Пономарев Ю.А., Потерпеев Г.Ю.* Модель и методы дистанционного контроля мобильных персональных устройств: сборник трудов 23 научно-технической конференции СПБГПУ // Санкт-Петербург. 2014. 382 с.

References

1. [Basic model of personal data security during it's processing in personal data proceeding systems, FSTEC]. M. 2008. 231 p. (In Russ.).
2. Devianin P.N. *Modeli bezopasnosti komp'juternyh sistem* [Computer system security models]. M. 2011.128 p. (In Russ.).
3. Poterpeev G.Y. *Model' ugroz informacionnoj bezopasnosti mobil'nyh personal'nyh ustrojstv. Metody obespechenija informacionnoj bezopasnosti* [Model of information security vulnerabilities of mobile personal devices]. Spb. 2013. (In Russ.).
4. Lukatskiy A.V. *Obnaruzhenie atak* [Attack detection]. SPb. 2001. 624 p. (In Russ.).
5. Klimov A.V. *Programmirovanie dlja mobil'nyh ustrojstv* [Mobile device programming]. SPb. 2007. 321 p. (In Russ.).
6. B.Hardie, B. Fillips. *Programmirovanie pod Android:prakticheskoe rukovodstvo* [Android programming: a practical guide]. Spb. 2014. 592 p. (In Russ.).
7. Eremeeev M.A., Novikov V.A., Lomako A.G. [Method of program vulnerabilities detection]. *Informacionnoe protivodejstvie ugrozam terrorizma – Information*

counteraction to threats of terrorism. M. 2010. no. 14. pp. 46-79. (In Russ.).
8. Eremeev M.A., Ponomarev Y.A., Poterpeev G.Y. [Model and methods of personal mobile devices remote control] *Trydy 23-oi naychno-tehnicheskoi konferencii SPBGPU* [Proceedings of the 23-th Scientific and Technical Conference on SPbPU]. SPb. p. 382. (In Russ.).

Потерпеев Герман Юрьевич — старший научный сотрудник - начальник научно-исследовательской лаборатории экспериментального моделирования защищенного применения средств сбора, обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: защищенное представление и обработка данных, системы защиты информации, информационная безопасность, мобильные персональные устройства. Число научных публикаций — 14. gypo@mail.ru; ул. Ждановская 13, Санкт-Петербург, 197198; р.т.: +7(812)230-28-15.

Poterpeev German Yurievich — senior researcher - head of the experimental modeling of data proceeding system secure using laboratory, Mozhaisky Military Space Academy. Research interests: secure data proceeding, system of information protection, information security, mobile personal devices. The number of publications — 14. gypo@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812)230-28-15.

РЕФЕРАТ

Потерпеев Г.Ю. **Метод прогнозирования действий злоумышленника при выборе оптимального скрытного воздействия на операционную систему мобильного персонального устройства.**

Статья посвящена рассмотрению подхода к выявлению, классификации и ранжированию угроз защищенности мобильных персональных устройств. Реализован подход количественной оценки скрытности вредоносных воздействий, предполагающий расстановку коэффициентов для каждого потенциально возможного механизма воздействия.

В основе предлагаемого подхода лежит ранжирование альтернатив на основе метода анализа иерархий. Каждый элемент множества потенциально реализуемых механизмов воздействий оценивается с точки зрения скрытности и результативности, после чего проводится количественное сравнение положительного и отрицательных эффектов или демаскирующих признаков (ДП).

SUMMARY

Poterpeev G.Y. **Method of Forecasting Maleficent Actions when Choosing the Optimal Covert Action on the Operating System of Mobile Personal Device.**

The article considers the approach to the identification, classification and ranking of threats to the security of mobile personal devices. Implemented approach quantifies covert harmful interference, involving the alignment of coefficients for each possible mechanism of action.

The proposed approach is based on the ranking of alternatives based on the analytic hierarchy process. Each element of the set of potentially implemented action mechanisms is assessed in the view of its secrecy and efficiency, followed by a quantitative comparison of the positive and negative effects or telltale signs (TS).