Энтропия как мера конфиденциальности

А. Н. Петухов
Национальный исследовательский университет,
«Московский институт электронной техники» (МИЭТ)
anpetukhov@yandex.ru

П. Л. Пилюгин
Институт проблем информационной безопасности,
Московский государственный университет
им. М.В. Ломоносова.
ppl@mail.ru

С. Ю. Гуснин
Московский авиационный институт (национальный исследовательский университет)
gusnin@testing.ru

Аннотация. **В работе рассматриваются возможности количественной оценки одного из критериев информационной безопасности – конфиденциальности. В основу предлагаемой модели положены формализмы, отражающие традиционную концепцию конфиденциальности с бинарной формой оценки критерия. Такая концепция расширяется в результате анализа изменений, которые претерпевает критерий в случае не одномоментной, а протяженной во времени реализации информационной атаки, использующей многоэтапный сценарий, каждый этап которого предполагает разрушение конфиденциальности различных объектов. Уточняется понятие критерия конфиденциальности для различных ситуаций несанкционированного доступа, рассматривается возможность одновременной деградации других критериев информационной безопасности. Делается вывод о целесообразности привлечения энтропийных форм оценки конфиденциальности, предлагается мера такой оценки, обсуждается использование этой меры на примере конкретной атаки.**

Ключевые слова: мера; энтропия; конфиденциальность

Одной из «застарелых» и фундаментальных проблем информационной безопасности в части защиты от несанкционированного доступа является явный дефицит оснований для измерения основных ее критериев, например конфиденциальности. Привлечение для таких критериев меры, даже не претендующей на полностью естественное происхождение, но хотя бы лишенной экспертной субъективности, дает возможность более адекватной и непосредственной оценки реального уровня защищенности. Тем самым создаются предпосылки для эффективного управления информационной безопасностью.

Единственное направление, систематически разрабатывающее тему измерения эффективности – это криптография, где для таких измерений широко привлекается мера криптостойкости, основанная, например, на результатах исследования моделей сложности алгоритмов криптоанализа. Все остальные направления, модели и методы борьбы с несанкционированным доступом (методы технической защиты информации в настоящей работе не рассматриваются) вынуждены иметь дело с бинарной оценкой критериев безопасности, предполагающей, что безопасность в смысле соответствующего критерия либо есть, либо ее нет.

Введем некоторые формализмы для описания такого подхода (т.н. «примитивная» схема) в отношение, например, конфиденциальности.

Пусть заданы множества информационных ресурсов (объектов доступа **O** и субъектов доступа **S**). Также задано всюду определенное неинъективное и несюръективное отображение множества **O** на множество подмножеств **S**:

$$\mathbf{p: O \rightarrow 2^S}$$

Это отображение назовем «политикой» (неинъективность нужна для учета групповых политик), оно ставит в соответствие каждому информационному ресурсу $\mathbf{o_i \in O}$ некоторое множество $\mathbf{S_i \in 2^S}$. Элементы $\mathbf{S_i}$ - это субъекты, осуществляющие легитимный доступ к $\mathbf{o_i}$.

Реальное состояние доступности $\mathbf{o_i}$ характеризуется множеством $\mathbf{S^*_i}$, которое включает всех субъектов, фактически имеющих доступ (без разделения на легитимные и нелегитимные способы) к $\mathbf{o_i}$. Очевидно, что множества $\mathbf{S_i}$ и $\mathbf{S^*_i}$ могут не совпадать (например, из-за уязвимостей в управлении доступом).

В этих обозначениях конфиденциальность относительно объекта $\mathbf{o_i}$ эквивалентна справедливости утверждения, что разность множеств $\mathbf{S^*_i}$ и $\mathbf{S_i}$ пуста:

$$\mathbf{S^*_i \backslash S_i = \emptyset} \qquad (1)$$

Конфиденциальности относительно всего множества объектов **O** соответствует одновременное выполнение условия (1) для всех $\mathbf{o_i \in O}$.

Из этого следует, по крайней мере, одно полезное соображение, касающееся того, что в рамках

«примитивной» схемы конфиденциальность не является ни свойством самой информации, ни свойством обрабатывающей ее технологии, а есть свойство структуры множества субъектов, которое, разумеется, зависит от системы защитных мер.

Внешняя незамысловатость «примитивной» схемы, тем не менее, оставляет место для целого ряда вопросов касательно ее применимости в условиях конкретных информационных технологий. Прежде всего, эти вопросы относятся к множествам $\mathbf{S^*_i}$, поскольку в отличие от множеств $\mathbf{S_i}$, исчерпывающе определяемых множеством **S** и отображением «политики» **p**, перечисление субъектов, фактически обладающих доступом к $\mathbf{o_i}$, представляется смутным. Если в качестве **S** имеются в виду все зарегистрированные субъекты (а, как правило, именно так и обстоит дело, так как в «примитивной» схеме множество **S** «задано»), то вне рассмотрения аспектов конфиденциальности оказываются все внешние угрозы и атаки. Априорно перечислить всевозможных внешних нарушителей и злоумышленников не представляется возможным, но можно объединить их в одном дополнительно введенном абстрактном субъекте $\mathbf{s'} \in \mathbf{S}$, про который известно, что он не входит ни в одно множество $\mathbf{S_i}$ (несюръективность отображения **p** позволяет нам это сделать). Тогда множество **S** будет состоять из зарегистрированных субъектов $\mathbf{s_j}$, доступ которых к объектам $\mathbf{o_i}$ регулируется отображением политики **p,** и, кроме того, одного абстрактного субъекта $\mathbf{s'}$, «олицетворяющего» всех внешних претендентов получить доступ к $\mathbf{o_i}$.

Это дополнение ничего в схеме не меняет, так как, легко видеть, что если условие (1) выполняется для более «сильного» случая с учетом такого дополнения, то оно выполняется и для любого «ослабления», в том числе, и для случая только зарегистрированных субъектов. С другой стороны, «концентрация» всех внешних субъектов (по определению считающихся нарушителями) в рамках одного элемента $\mathbf{s'}$, также не нарушает схему, поскольку они неразличимы в том смысле, что получение любым из них фактического доступа к любому $\mathbf{o_i}$, приводит к невыполнению условия (1), т.е. к утрате конфиденциальности.

Следующая группа вопросов требует уточнения понятия «фактический доступ», прежде всего для субъектов, не входящих в $\mathbf{S_i}$, т.е. там, где речь идет о нелегитимном доступе. В частности, следует ли включать в $\mathbf{S^*_i}$ субъекты, которые объективно обладают возможностью доступа к $\mathbf{o_i}$, но никогда такой возможностью не пользовались, например, ничего не зная о ней? Влияют ли на конфиденциальность еще не обнаруженные уязвимости? Такие вопросы реально встают при анализе безопасности программного кода или при создании методов высоконадежного проектирования и тестирования, например, критических информационных инфраструктур.

Другим уточнением понятия доступа является отношение конфиденциальности к результатам этого доступа. В ранних версиях беспроводной связи WiFi (WEP-комплекс решений по безопасности [1]) конфиденциальность связи обеспечивалась потоковым шифрованием, на последнем этапе которого использовалась XOR-функция для наложения гаммы. Целостность сообщений поддерживалась процедурой формирования контрольной суммы на базе циклического избыточного кода. Сочетание этих решений образовало уязвимость, которая позволяла корректно с точки зрения контрольной суммы вносить изменения в зашифрованное сообщение. Поскольку прочитать сообщение все равно было невозможно, конфиденциальность не нарушалась, однако корректный (целостность не нарушена) и, в то же время, нелегитимный доступ для внесения изменений осуществлялся. В связи с этим возникает вопрос: включает ли конфиденциальность оценку ограничений только на получение «знания» об объекте (узкий смысл) или она является критерием корректности управления любым доступом, в том числе и с целью «влияния» на объект (широкий смысл). Применительно к классическим моделям управления доступом (например, матрица доступа для дискреционного доступа или модель Белла-Лападула для мандатного доступа [2]) это вопрос включения в $\mathbf{S_i}$ и $\mathbf{S^*_i}$ субъектов с правами доступа к $\mathbf{o_i}$ только на чтение или с любыми другими правами тоже.

Вполне определенный ответ на этот вопрос дает гексада Паркера [3], которая является набором критериев информационной безопасности, включающим наряду с критерием собственно конфиденциальности (в узком смысле, т.е. ограничивающим получение «знания» об объекте), еще отдельный критерий управляемости или владения, предназначенный для ограничения «влияния» на объект. Таким образом, гексада Паркера как бы расщепляет общее понятие доступа, соотнося каждой его части свой специфический критерий.

Ограничив рассмотрение только реализованной конфиденциальностью, и понимая ее в узком смысле (наиболее традиционный вариант), можно предложить вполне конструктивный способ отбора субъектов в $\mathbf{S^*_i}$. Ими будут те субъекты, которые имеют принципиальную возможность воспроизведения (или предъявления) объекта $\mathbf{o_i}$, причем принципиальность заключается в том, что не важно, какие действия предпримет субъект для такого воспроизведения. Единственные два требования, которые могут быть предъявлены к воспроизведению субъектом $\mathbf{s_j}$ объекта $\mathbf{o_i}$ в рамках «примитивной» схемы, это верность воспроизведения – результат воспроизведения $\mathbf{d(s_j, o_i)}$ должен полностью совпадать самим объектом $\mathbf{o_i}$:

$$\forall\, \mathbf{s_j \in S^*_i} \rightarrow \mathbf{d(s_j, o_i)=o_i} \qquad (2)$$

и детерминированность (воспроизводимость) – гарантия неизменности результата при повторениях воспроизведения:

$$\forall\, \mathbf{s_j \in S^*_i} \rightarrow \mathbf{P_{rob}\{\, d(s_j, o_i)=o_i\}=1} \qquad (3)$$

Отметим, что требования (2) и (3) распространяются и на абстрактного субъекта s', и что эти требования актуальны только в пределах «примитивной» схемы, которая, несмотря на все уточнения, продолжает оставаться бинарной, т.е. предполагает, что конфиденциальность либо полностью есть, т.е. условие (1) выполнено для всех o_i, либо ее совсем нет, если хотя бы для одного o_i оно не выполняется. Тем не менее, эту схему можно использовать в качестве основы для создания меры оценки конфиденциальности, особенно если записать требование (3) в несколько измененном виде:

$$\forall s_j \in S^*_i \rightarrow H(d(s_j, o_i))=0 \quad (4)$$

где $H(d(s_j, o_i))$ – энтропия воспроизведения субъектом s_j объекта o_i. Будем строить меру $K(s_j, o_i)$ на отрезке [0,1], полагая, что единица соответствует наличию конфиденциальности (в смысле «примитивной» схемы), а ноль ее отсутствию. Другими словами, если $K(s_j, o_i)$ равна нулю, то s_j принадлежит S^*_i, а если $K(s_j, o_i)$ равна единице, то s_j не принадлежит S^*_i, других значений $K(s_j, o_i)$ «примитивная» схема не поддерживает:

$$K(s_j, o_i) =0 \rightarrow s_j \in S^*_i$$

$$K(s_j, o_i) =1 \rightarrow s_j \notin S^*_i$$

Можно рассмотреть ситуацию, когда объект содержит очевидную, общеизвестную информацию, например, результат вычисления однозначной функции известного аргумента (возведение в квадрат двойки) или мировую физическую константу. Какими бы ни были ухищрения по управлению доступом, вряд ли имеет смысл говорить о какой-либо конфиденциальности. Любой субъект, в том числе и не принадлежащий к S_i (в частности s') воспроизведет этот объект, тем самым обеспечив заведомое невыполнение условия (1). Поскольку никакой неопределенности в содержании самого объекта o_i, нет, или, говоря теоретико-информационным языком [4], энтропия объекта o_i равна нулю, любой субъект может воспроизвести его с соблюдением требований (2) и (4). Поэтому мера конфиденциальности в этом случае равна нулю. Это обстоятельство заставляет задуматься о возможной зависимости меры конфиденциальности от информационного содержания объекта, по крайней мере, от его энтропии.

Другим примером разрушения конфиденциальности является неправомерная замена значения объекта на известное нарушителю. В этом случае нарушитель может не читать и не знать старое значение, важно, что он может воспроизвести и использовать текущее значение. Разумеется при этом нарушается целостность, но и конфиденциальность становится нулевой, поскольку энтропия объекта o_i для нарушителя предельно снижается. Особенно разрушительны такие действия, когда атакуются управляющие структуры самих средств безопасности, например, происходит несанкционированная замена паролей в месте их хранения или детерминированная подмена гаммы в схеме потокового шифрования. В этих случаях наряду со снижением конфиденциальности атакованного объекта утрачивается безопасность более широкого круга информационных активов.

Во всех приведенных примерах обращает на себя внимание общая черта – снижение в том или ином виде энтропии информационного объекта. Приобретение субъектом «знания» об объекте можно ассоциировать с некоторым информационным потоком, например, как это делается в моделях мандатного доступа, или (что то же самое) с каналом передачи информации (неважно в пределах системы или вовне ее, как в случае с общеизвестными знаниями). «Примитивная» схема трактует эту передачу, как одномоментную и неделимую транзакцию доступа. Однако современные угрозы разрушают конфиденциальность, используя сложные сценарии длительных, многоэтапных и итеративных процедур, последовательно преодолевая эшелоны защиты. Поэтому предметом исследования становятся состояния безопасности в процессе самой передачи, в частности, эволюция меры конфиденциальности.

До начала такой передачи претендующий на доступ субъект, стремясь выполнить верное воспроизведение в соответствии с требованием (2), но, не обладая никакими знаниями об объекте (кроме, возможно, форматных сведений, таких как длина, алфавит, структура и т.п.), представляет себе вероятностную схему, события которой соответствуют тому или иному возможному значению объекта. Реальные вероятности этих событий субъект может и не знать, например, полагая их равновероятными, как это делается в криптографии при оценке энтропии информационных агрегатов. Такая вероятностная схема характеризуется соответствующей энтропией, которую назовем собственной энтропией объекта. Мера конфиденциальности $K(s_j, o_i)$ до начала передачи равна единице.

По завершении передачи (транзакции доступа) субъект обладает полным знанием об объекте, и соответствующая вероятностная схема вырождается в вид, где ставшему известным значению соответствует единичная вероятность (достоверное событие), а всем остальным – нулевые (невозможные события). Энтропия такой схемы равна нулю, и мера конфиденциальности $K(s_j, o_i)$ тоже нулевая. Таким образом, конфиденциальность падает в процессе получения сведений об объекте. Учитывая, что получаемая об объекте информация $I(o_i)$ не может превышать его собственную энтропию $H_{соб}(o_i)$ [5], предположим, что уменьшение уровня конфиденциальности в процессе доступа к объекту происходит пропорционально той доли, которую составляет уже полученная информация об объекте $I_{тек}(o_i)$ от его собственной энтропии:

$$K_{тек}(s_j, o_i) = 1 - (I_{тек}(o_i) / H_{соб}(o_i)) = 1 - (H_{соб}(o_i) - H_{ост}(o_i)) / H_{соб}(o_i) = H_{ост}(o_i) / H_{соб}(o_i)$$

где $\mathbf{H_{ост}(o_i)}$ – остаточная энтропия, характеризующая состояние вероятностной схемы значений объекта в момент времени или на том этапе доступа, когда оценивается текущий уровень конфиденциальности $\mathbf{K_{тек}(s_j, o_i)}$.

Проиллюстрируем полученный результат на примере атаки, используемой против WEP-комплекса решений безопасности, и известной как «побитовое выращивание гаммы» [2]. Суть ее состоит в поэтапном подборе разрядов гаммы – псевдослучайной битовой последовательности, накладываемой с использованием XOR-функции на открытый текст в процессе потокового шифрования. При проведении атаки провоцируется передача шифртекстов, соответствующих известным открытым текстам, и на каждой такой передаче делается попытка «угадать» очередной бит гаммы, присоединяя его к уже сформированной части. Если период гаммы равен **N**, то для ее полного выращивания нужно в среднем 2**N** попыток, поскольку при каждой попытке бит гаммы «угадывается» с вероятностью 0,5, а математическое ожидание числа попыток для определения одного разряда (геометрическое распределение) определяется как:

$$\lim_{k\to\infty} \sum_{i=1}^{i=k} (i \times 0,5^i) = 2$$

Максимальная собственная энтропия идеальной гаммы $\mathbf{H_{соб}(гамма)}$ как конфиденциального объекта составляет **N** бит. На каждом шаге с вероятностью 0,5 атакующий получает 1 бит информации о гамме, т.е. в среднем остаточная энтропия $\mathbf{H_{ост}(гамма)}$ сокращается за одну попытку на 0,5 бита и после **m** попыток выращивания составит в среднем:

$$\mathbf{H_{ост}^{m}(гамма) = H_{соб}(гамма) - 0.5 \times m = N - 0.5 \times m \text{ бит}}$$

а средняя конфиденциальность будет равна:

$$\mathbf{K_{тек}^{m}(нарушитель, гамма,) = H_{ост}^{m}(гамма) / H_{соб}(гамма) = (N - 0.5 \times m) / N = 1 - [0.5 \times m / N]}$$

Поскольку на каждом шаге конфиденциальность уменьшается по схеме испытаний Бернулли с накоплением результата [5], ее распределение как дискретной случайной величины после **m** шагов имеет биномиальный вид:

$$\mathbf{P_{rob}\{ K_{тек}^{m} = x\} = 0.5m \times m! / \{[N \times (1-x)]! \times [m - (N \times (1-x)]!\}}$$

где **x** – дискретная величина кратная **1/N**, поскольку именно такими квантами происходит уменьшение конфиденциальности.

На каждом шаге атакующий обладает некоторыми знаниями, которые позволяют ему частично осуществлять доступ к объекту (в нашем примере – вскрывать некоторые фрагменты шифртекста), такому состоянию соответствует промежуточное (между нулем и единицей) значение конфиденциальности. В общем случае это значение определяется двумя факторами: эффективностью управления доступом и исходной энтропией объекта.

Таким образом, если рассматривать конфиденциальность как свойство множества субъектов доступа относительно объекта и политики доступа, то в ряде случаев (скрытые каналы, многоэтапные и/или протяженные во времени атаки и др.) удобной мерой конфиденциальности может служить изменение энтропии объекта в процессе или результате доступа.

СПИСОК ЛИТЕРАТУРЫ)

[1] Щербаков В.Б., Ермаков С.А. Безопасность беспроводных сетей: стандарт IEEE 802.11, РадиоСофт, 2010, 255 стр.

[2] Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М.: Издательство Агентства «Яхтсмен», 1996.

[3] Parker, Donn B. (1998). Fighting Computer Crime. New York, NY: John Wiley & Sons. ISBN 0-471-16378-3

Яглом А.М., Яглом И.М. Вероятность и информация. М. Наука, 1973, 512 стр.