Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management
Roger G. Johnston
Science and Global Security, 2001, Volume 9, pp. 93 - 112

ПЛОМБЫ С ИНДИКАЦИЕЙ ВМЕШАТЕЛЬСТВА ДЛЯ ЯДЕРНОГО РАЗОРУЖЕНИЯ И ОБРАЩЕНИЯ С ОПАСНЫМИ ОТХОДАМИ

Роджер Дж. Джонстон

Пломбы с индикацией вмешательства находят важное применение во многих областях, включая ядерное разоружение и обращение с опасными отходами. Однако, имеются многочисленные теоретические и практические проблемы с имеющимися пломбами и с использованием пломб, а также с обнаружением вмешательства в целом. Большая часть современных пломб представляется весьма уязвимой к простым и быстрым нарушениям, хотя это можно изменить как при помощи усовершенствования пломб, так и способа их использования. Проблемы ядерного разоружения и обращения с опасными отходами учитывались при разработке очень немногих пломб. Можно создать лучшие пломбы, в особенности при использовании новых подходов и технологий. Однако, пломбы, изготовленные по сложной технологии, не всегда обеспечивают большую безопасность.

Оригинальная версия данной статьи была получена редакцией журнала "Наука и всеобщая безопасность" 10 октября 1999 года.

Роджер Дж. Джонстон работает руководителем группы оценки уязвимости в Лос-Аламосской национальной лаборатории, Лос-Аламос, штат Нью-Мексико, США.

ВВЕДЕНИЕ

Пломбы с индикацией вмешательства, часто называемыми «секретными пломбами» или просто «пломбами», предназначены для регистрации несанкционированного доступа или входа. Пломбы широко используются во многих различных областях, которые включают контроль доступа, целостность записей, безопасность складов и грузов, предотвращение и обнаружение краж, учет опасных материалов, ядерное нераспространение, гарантии и безопасность, исполнение закона, таможни, борьба с терроризмом, контрразведка и целостная упаковка потребительских товаров.

Пломбы используются на протяжении тысячелетий. Однако, общая проблема обнаружения вмешательства остается относительно неразвитой и отягощенной проблемами. Не существует ни формальной теории обнаружения вмешательства, ни значимых и всеобъемлющих стандартов[1].

Немногие из тех, кто использует пломбы, обладают глубоким пониманием того, как выбирать пломбы, как лучше всего использовать их, и почему они уязвимы[2]. Многие из применяемых в настоящее время пломб (в том числе и в ядерной отрасли) не обладают главными свойствами, необходимыми для эффективной прозрачности, согласованности и безопасности для международных договоров по сокращению вооружений.

Возможности и технологии для новых, более эффективных, пломб используются не полностью. В случае обращения с опасными отходами часто игнорируются потенциальные преимущества применения пломб. Поэтому немногие из пломб приспособлены для обращения с опасными отходами.

Задачей этой статьи является обзор состояния пломб с индикацией вмешательства и предложение некоторых необходимых атрибутов для международного контроля над воору-

[1] Roger G. Johnston, “Effective Vulnerability Assessment of Tamper-Indicating Seals”, Journal of Testing and Evaluation, 25 (1997), pp. 451 – 455, адрес в Интернете http://lib-www.lanl.gov/la-pubs/00418792.pdf.

[2] Roger G. Johnston, “The Real Deal of Seals”, Security Management, 43 (1997), pp. 93 – 100, адрес в Интернете http://lib-www.lanl.gov/la-pubs/00418795.pdf; Ro-ger G. Johnston, “Tamper Detection Requires Dedication”, Metering International, issue 3, (1999), адрес http://lib-www.lanl.gov/la-pubs/00460170.pdf.

жениями и обращения с опасными отходами. Вторичная задача состоит в освещении текущих проблем с пломбами и обсуждении будущего развития.

Терминология

Одной из проблем, осложняющих применение пломб, является широко распространенная неоднозначность определений и отдельных функций замков, пломб и этикеток.

Для наших целей **пломба** (или **устройство с индикацией вмешательства**) определяется как устройство или материал, позволяющие сохранять не допускающее стирания свидетельство несанкционированного доступа. Пломба не обязана обеспечивать сопротивление вмешательству; она только регистрирует, что оно произошло. Некоторые пломбы изготовлены из бумаги или пластика и их легко сорвать пальцами. Это не обязательно означает, что они не эффективны.

Напротив, **замок** представляет собой устройство, предназначенное для задержки и затруднения несанкционированного доступа или входа. Замки не сильно останавливают нарушителя с достаточным опытом и/или мотивацией.

Преграждающая пломба является простым устройством, которое выполняет функции как замка, так и пломбы. Обычно она выдерживает достаточное усилие без открытия. Обычно преграждающая пломба является компромиссом – не совсем оптимальная пломба и не совсем оптимальный замок для любого конкретного применения.

Этикетка является внутренней или прилагаемой уникальной характеристикой («отпечатком пальцев»), используемой для однозначного отождествления объекта или контейнера.

Прочие представляющие интерес термины таковы:

Взлом пломбы: доступ или вход в то, что защищается пломбаю, без обнаружения этого события.

Попытка взлома пломбы: дословно.

Протоколы пломбы: официальные и неофициальные процедуры приобретения пломб, перевозки, хранения, проверки, ведения записей, установки, инспекции, снятия, утилизации и подготовки персонала. Эффективность пломбы во многом зависит от используемых для нее протоколов.

Последующий контроль: детальное исследование частей пломбы после того, как пломба была использована, снята и проверена на месте. Эта экспертиза может использовать сложные лабораторные методы для определения факта вмешательства, попытки взлома или фальсификации пломбы.

Оценка уязвимости: поиск (и, возможно, демонстрация) слабых мест в конструкции и эксплуатации охранного устройства или охранной программы, нередко сопровождаемое предполагаемыми контрмерами.

Ранние пломбы

Пломбы используются по крайней мере 7000 лет, задолго до появления письма[3]. Более того, некоторые исследователи считают, что пломбы способствовали развитию как письма, так и арифметики[4].

Типичная древняя пломба представляет собой небольшой цилиндр или штемпель, сделанный из глины, камня, или кости, на котором нанесен геометрический или сложный рисунок. Емкости (такие, как горшки или кувшины) защищались слоем глины, нанесенным на крышку, горлышко, отверстие или заглушку. Затем штемпельная или цилиндрическая плом-

[3] McGuire Gibson and R.D. Bridge (editors), Seals and Sealing (Malibu, California; Bibliotheca Mesopotamica, 1977); Dominique Collon, First Impressions: Cylinder Seals in the Ancient Near East (London, England; University of Chicago Press, 1987); Dominique Collon, Near Eastern Seals (Berkeley, California; University of California Press, 1990).

[4] Denise Schmandt-Besserat, Before Writing: Volume I: from Counting to Cuneiform (Austin, Texas; University of Texas Press, 1992), pp. 194 – 199; I.J. Gelb, A Study of Writing (Chicago, Illinois; University of Chicago Press, 1963).

ба использовались для выдавливания рисунка на глине нажатием на штемпель или катанием цилиндра по глине. Затем глину сушили, иногда на солнце. Любая попытка открытия емкости должна была привести к разрушению глины. Восстановление рисунка для повторной закупорки (и утаивания факта его открытия) требовало значительного времени и умения, если у нарушителя не было оригинальной пломбы. Можно было также завязать веревку на емкости, упаковке, связке или двери. После этого на веревку прилепляли комок глины (буллу) и прижимали к нему печать.

Пломбы в древности применяли и для документов. Глиняные таблички с надписями, начиная с 5000 года до нашей эры, нередко помечали рисунком со штемпеля или цилиндрической пломбы. Эта надпись утверждала документ и отождествляла автора. Глиняные таблички могли также быть запечатаны внутри глиняного конверта, опечатанного для обнаружения вмешательства.

Египтяне использовали буллы для опечатывания папирусных документов, начиная с 2500 года до нашей эры. Они применяли пломбы и в гробницах. Когда работы в погребальной камере заканчивались и в нее помещалась мумия, дверь замазывалась глиной и штукатуркой. Дверь могла быть открыта, но было видно, что пломба взломана. В наше время археологи могут определить, была ли ограблена гробница, проверяя целостность пломбы.

Начиная с 1100 года до нашей эры, и до средних веков, в Европе широко использовались восковые пломбы. На свиток капали расплавленным воском (впоследствии вместо воска стали применять шеллак). Кольцо-печатка с выгравированным рисунком прижималось к расплавленному воску, оставляя на нем сложный рисунок. С 4 века нашей эры до настоящего времени используются и свинцовые пломбы[5].

Очевидно, что пломбы древности, средневековья и эпохи Возрождения обеспечивали довольно низкую безопасность. Доказательством этого служат находки поддельных пломб[3,6] и проблемы с подделками живописи, когда фальсификаторы снимают пломбы с картин[7].

Современные пломбы

В настоящее время применяются около 5000 различных типов пломб. Их можно разделить на две больших категории: **пассивные** и **активные**. Пассивные пломбы работают без подвода электроэнергии. Они обычно предназначены для одноразового использования и обычно недороги. Активные (или динамические) пломбы используют электроэнергию от внутренних или внешних источников. Как правило, активные пломбы могут применяться повторно[8].

---

[5] Свинцовые пломбы, состоящие из небольшого кусочка свинца, в котором часто делаются отверстия для пропускания опечатывающей проволоки или струны. Проволока (или струна) пропускается через опечатывающий засов контейнера или двери, или даже (в старые времена) оборачивается вокруг скрученного документа. Затем проволока (или струна) пропускается через свинец или отверстия в свинце перед обжатием свинца для фиксации проволоки. Часто при обжатии свинца на него наносится логотип или порядковый номер. В последние годы популярность свинцовых пломб снизилась из-за низкой безопасности, высокой стоимости и связанных со свинцом проблем для здоровья и окружающей среды. Министерство обороны США сейчас запретило установку новых свинцовых пломб на своих объектах. Свинцовые пломбы, однако, все еще широко используются в США и России. Иногда вместо свинца используют мягкий сплав, не содержащий свинца. Такие пломбы могут называть (неверно) «свинцовыми пломбами» или «свинцово-проволочными пломбами».

[6] E. Porada, “Forged North Syrian Seals”, Archaelogy 10 (1957): 143; E. Porada, “True or False? Genuine and False Cylinder Seals at Andrews University, Andrews University Seminar Series 6”, Berrien Springs, Michigan; Andrews University, 1978.

[7] Ann Waldron, True or False?: Amazing Art Forgeries (Norwalk, Connecticut; Hastings House, 1983), 11.

[8] Охранную сигнализацию или противовзломную сигнализацию можно рассматривать как активную пломба, сообщающую о несанкционированном входе или доступе в реальном времени, а не записывающем результат для последующего времени.

Пассивные пломбы могут принимать различные формы[9,10]. Они могут быть хрупкими фольгами или пленками, пластиковыми обертками, чувствительными к давлению клейкими этикетками, «запирающими» болтами, завитыми проволоками или кабелями, или другими необратимыми (теоретически) механическими сборками, упаковками или секретными контейнерами с индикацией вмешательства, конвертами, носящими следы вскрытия, оптоволоконными пучками, меняющими пропускание света после перерезания, и другими устройствами или материалами, необратимо повреждающимися или изменяющимися при манипуляциях с ними.

На рис. 1 показан ассортимент коммерческих пассивных пломб; их выбор не имеет особого значения. Все показанные пломбы, за исключением пассивной оптоволоконной пломбы и двух пломб с клейкими этикетками, представляют собой необратимые механические сборки. Когда такая пломба закрывается, она «запирается» подобно соединительному кабелю. По крайней мере в теории такие пломбы не могут быть открыты без нанесения очевидного ущерба. Обычно все пломбы, кроме клейких этикеток, перед закрытием пропускаются через засов. Размер петли после закрытия пломбы может быть регулируемым или фиксированным, в зависимости от конструкции. Пломбы с клейкими этикетками делаются хрупкими для того, чтобы они повреждались при снятии с поверхности.

Активные пломбы обычно принадлежат к двум типам: электронные или активные оптоволоконные. Электронные пломбы непрерывно отслеживают некоторые изменения, характерные для вмешательства. Активные оптоволоконные пломбы периодически или случайно посылают световые сигналы по оптоволоконному пучку для проверки целостности.

Большинство современных пломб все еще проверяется вручную, хотя в некоторых пломбах для проверки вмешательства используются электронные или оптические считыватели.

Уязвимость пломб

Устройства с индикацией вмешательства, используемые правительством, или в коммерческих целях, представляются уязвимыми для быстрых, простых и низкотехнологичных попыток взлома. Наиболее полное исследование в поддержку этого вывода было проведено группой оценки уязвимости (ГОУ) Лос-Аламосской национальной лаборатории[1,2,11]. Однако, и другие опубликовали открытые отчеты и статьи с аналогичными выводами[9,12]. Кажется также, что имеется неформальный консенсус специалистов по уязвимости пломб, не входящих в ГОУ, что большинство или даже все пломбы уязвимы к простым попыткам взлома.

---

[9] David L. Poly, Security Seals Handbook, Report SAND78-0400 (Albuquerque, New Mexico, Sandia National Laboratories, 1983); Antipilferage Seal User's Guide, (Port Hueneme, California, Naval Facilities Engineering Services Center, 1997).

[10] DoD Training Course for Effective Seal Use, (Port Hueneme, California, Naval Facilities Engineering Services Center, 1999).

[11] Roger G. Johnson and Anthony R.E. Garcia, "Vulnerability Assessment of Security Seals", Journal of Security Administration 10 (1997): 15 – 23, доступно по адресу http://lib-www.lanl.gov/la-pubs/00418796.pdf; Ro-ger G. Johnson and Anthony R.E. Garcia, "Physical Security and Tamper-Indicating Devices", (Proceedings of the Information Privacy, Security and Data Integrity 1997 Mid-Year Meeting, Gregory B. Newby, ed., Scottsdale, Arizona, American Society for Information Science, 1997) 43 – 46, адрес http://lib-www.lanl.gov/la-pubs/00418796.pdf.

[12] Security Seals for the Protection and Control of Special Nuclear Material, AEC Regulatory Guide 5.15, (Washington, D.C.; Atomic Energy Commission, 1974); Cesar A. Sastre, The Use of Seals as a Safeguard Tool, Report BNL 13480, (Upton, New York; Brookhaven National Laboratory, 1969); James L. Jones, Improving Tag/Seal Technologies: The Vulnerability Assessment Component, Report 95/00599, (Idaho Falls, Idaho; Idaho National Engineering Laboratory, 1996); Ross J. Anderson and Markus G. Kuhn, "Low Cost Attacks on Tamper Resistant Devices", M. Lomas, et al., eds., (Proceedings of the 5th International Workshop on Security Protocols, Paris; Springer Verlag, 1997), 125 – 136.

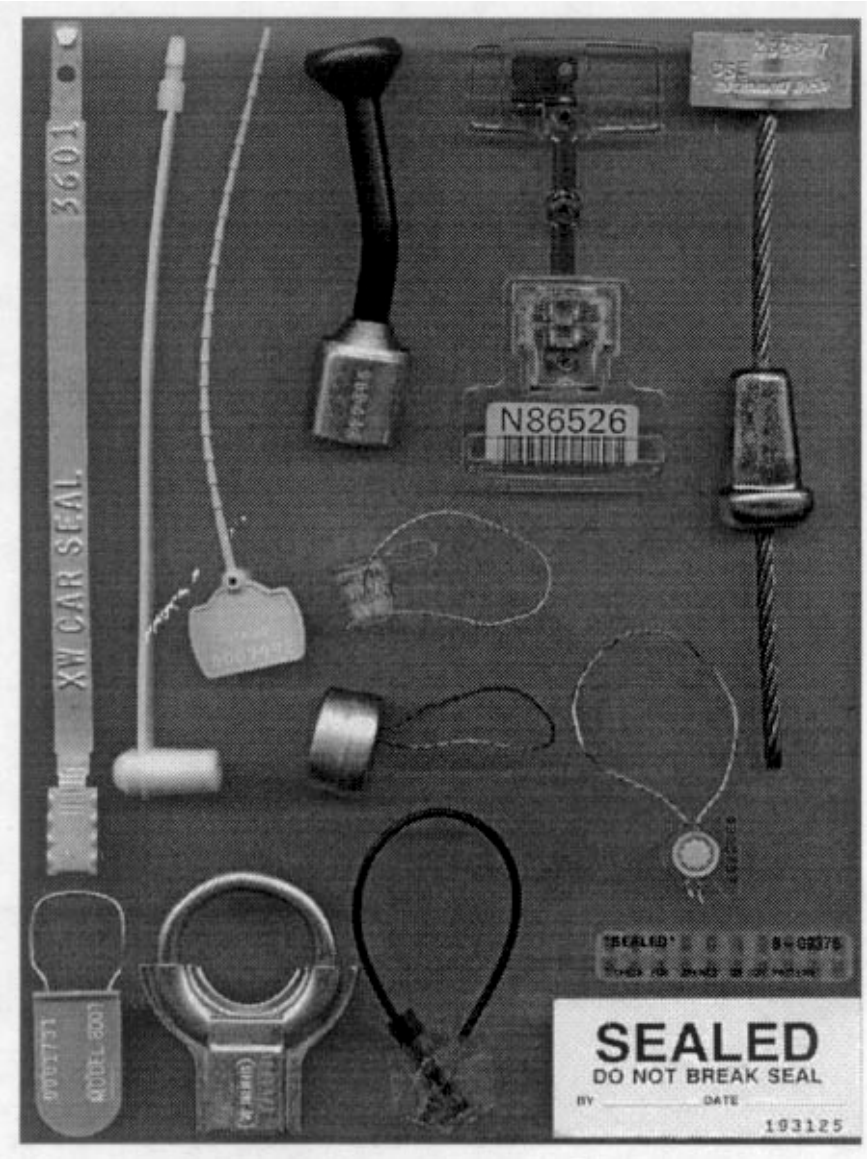

Рис. 1. Примеры некоторых коммерческих пломб. Верхний ряд, слева направо: пломба с металлической лентой, часто используемая в железнодорожных вагонах, две пломбы с пластиковыми лентами, пломба-болт (запирающая), пломба с пластмассовым болтом и кабельная пломба. Первые три пломбы открыты; для их закрытия надо один конец вставить в другой. В центре три пломбы-петли, включая “e-cup” (слева), традиционно используемую в ядерной отрасли. В нижнем ряду, слева направо: две пломбы «висячий замок» (которые, несмотря на название, являются пломбами, а не замками), пассивная оптоволоконная пломба и две пломбы с клейкими этикетками.

ГОУ изучило 120 различных широко применяемых пломб. В их число входили активные и пассивные устройства низкой и высокой технологии. ГОУ обнаружила, что все 120 пломб могут быть взломаны при помощи низкотехнологичных инструментов и простых методов, доступных широкой публике. Взломы не могут быть обнаружены при типичных протоколах инспекции, используемых для каждого типа пломбы. Времена взлома для одного опытного специалиста лежат в пределах от 3 секунд до 2 часов, при среднем времени менее 5 минут[13]. Если мы рассмотрим только те пломбы из 120, которые в настоящее время

[13] Мы определяем специалиста как «опытного» при конкретной атаке, если (1) он недавно провел тренировку по крайней мере с 8 полными попытками взлома; (2) он недавно провел тренировку по крайней мере с 12 наиболее трудными или критическими фазами попытки взлома; (3) работая с разумной поспешностью, он может провести 3 последовательных попытки взлома так, чтобы 2 или 3 из них было бы весьма маловероятно обнаружить при со-

используются в американской или зарубежных ядерных отраслях, то среднее время взлома (одним опытным специалистом) составит менее 8 минут.

Средняя стоимость взлома всех 120 пломб равна 55 долларам, хотя маргинальная стоимость намного меньше[1414]. Некоторые из высокотехнологичных пломб взламываются намного легче, чем пломбы низкой технологии. ГОУ пришла также к выводу, что стоимость пломбы не является надежным предсказателем уязвимости[11].

Важным обнаруженным результатом стало то, что простые изменения пломбы и/или протокола применения часто драматически улучшают обнаружение вмешательства. Однако, оптимальные протоколы критически зависят от конкретно используемой пломбы и от условий ее применения.

Правдоподобие уязвимости пломб

В этой статье нельзя представить полного доказательства уязвимости пломб. Для обсуждения конкретных уязвимостей не хватает места, и было бы безответственно распространять информацию о том, как можно победить устройства с индикацией вмешательства. Вместо этого мы рассмотрим 6 аргументов в пользу того, почему идея о том, что пломбы могут быть взломаны, является как разумной, так и неудивительной.

Первым аргументом является то, что все пломбы, по крайней мере теоретически, могут быть подделаны. Доказательство основано на атомной теории вещества. Все существующие пломбы состоят из комбинации абсолютно идентичных электронов, нейтронов и протонов. Эти основные строительные блоки доступны в больших количествах и по низкой цене. Для того, чтобы подделать пломба, достаточно «только» собрать эти базовые компоненты в приблизительно верной конфигурации[15]. Оригинальная пломба может быть разрезана и заменена получившейся подделкой без оставления каких-либо следов. На практике, разумеется, сборка правильной конфигурации элементарных частиц или атомов может потребовать огромного времени, мастерства и утонченной технологии. Однако, в нашем современном понимании физики нет ничего, фундаментально запрещающего репликацию любого изготовленного человеком предмета, в том числе и пломбы.

Второй аргумент в пользу правдоподобия уязвимости пломб основан на том факте, что оказывалось возможным подделывать широкий круг разнообразных объектов. В него входят произведения искусства, ископаемые останки, античные предметы, спортивные атрибуты, драгоценные камни, официальные и личные документы, драгоценные камни и деньги[16]. Нередко простые и низкотехнологичные методы работают очень эффективно[16].

ответствующем протоколе инспекции. Для наиболее трудных атак для выполнения условия (3) может потребоваться более 50 попыток. Отметим, что для проведения успешной попытки взлома не обязательно становиться «опытным», а только достичь времен поражения, обсуждающихся в этой статье. При некоторых попытках взлома помощник может существенно сократить рассматриваемые здесь времена атаки. Однако, в других случаях помощник только присутствует. Отметим также, что количество неиспользованных пломб, необходимое для приобретения «опыта», не обязательно велико. В зависимости от способа взлома и от типа пломбы, нередко можно повторно использовать пломба, или практиковаться на использованных частях пломбы.

[14] Маргинальной стоимостью считается стоимость взлома второй пломбы того же типа. Средняя маргинальная стоимость взлома намного меньше 55 долларов из-за того, что инструменты и средства, необходимые для попыток взлома конкретной пломбы, часто могут использоваться для дополнительных попыток взлома того же типа пломбы.

[15] На деле не требуется даже точной подделки оригинальной пломбы. Имеется огромное количество конфигураций электронов, протонов и нейтронов, которые достаточно близки к оригиналу, так что микроскопические отличия останутся незаметными. Фактически сама оригинальная пломба имеет непрерывно изменяющуюся конфигурацию из-за теплового движения, старения и поглощения света. Это допускает еще большую свободу в конструкции поддельной пломбы.

[16] См., например, сотни ссылок о подделках, приведенных в Roger G. Johnston, Physical Tampering and Counterfeiting: A Research Guide (Chicago, Illinois; American Library Association).

Третий аргумент основан на том, что подделка не является единственным способом атаки пломбы. Например, группа ГОУ составила подборку, включающую 105 общих методов попыток взлома пломб[17]. Эти 105 методов классифицированы по 11 категориям, перечисленным в Приложении А.

Четвертый аргумент в поддержку основан на хорошо известном факте, что замки (в том числе и электронные) могут быть скрытно и эффективно взломаны. Информация о том, как взламываются даже очень сложные замки, вполне доступна[18]. Верно, что замки выполняют несколько иную функцию обеспечения безопасности. Однако, они устанавливаются так же, как пломбы, и часто используются вперемешку с пломбами (не всегда разумно). Однако, в отличие от пломб, замки характеризуются простым двоичным состоянием. Они всегда либо заперты, либо отперты[19]. Если замки легко могут быть взломаны, то почему мы должны ожидать, что пломбы должны отличаться от них, учитывая, что они требуют значительно более тонкой человеческой или компьютерной интерпретации своего состояния, т.е. факта вмешательства? Человеческий фактор в особенности часто используется для целей взлома пломб[17].

Пятый аргумент фактически является предлагаемым экспериментом. Если вы приобрели пломба и научились ее использовать, то вы наверняка сможете представить себе многие способы ее взлома. Некоторые пользователи пломбы наверняка проделывали такой мысленный эксперимент.

Шестой аргумент за уязвимость пломб основан на трудности доказательства противного. Если попытка взлома любой конкретной пломбы не удалась, то это не обязательно означает, что пломба неуязвима. Это может просто означать, что для попытки были использованы неподходящие методы, исполнители или технологии. Даже предположение о том, что данная пломба эффективно неуязвима, может оказаться вредным, поскольку оно может привести к излишней самоуверенности – классическому недостатку любой программы безопасности или верификации.

Нередко думают, что взлом пломбы может оказаться трудным из-за того, что взломщик не будет знать конструкции пломбы или ее серийного номера вплоть до самого момента взлома. Однако на деле немногие из применяемых сейчас в ядерной отрасли пломб (если такие вообще есть) неизвестны или недоступны посторонним лицам в процессе подготовки взлома. Большинство пломб, используемых в ядерной отрасли, находятся в коммерческом секторе, или их конструкция доступна публике. Даже если это не так, возможно достать образцы таких пломб (использованных или целых), открыто или тайно. Конечно, в договорах по демонтажу обеим сторонам потребуется подробно знать конструкцию пломб с самого начала, так что предположение о том, что противник начнет попытку взлома, не зная устройства пломбы, неверно.

Точно так же, незнание противником серийного номера конкретной пломбы до начала попытки взлома не приводит обычно к предотвращению подделки. Пломба может быть подделана без знания серийного номера до начала попытки. Для большинства пломб нанести серийный номер на поддельную пломба можно быстро и на месте; это не является самой трудной или самой долгой фазой подделки пломбы.

---

[17] Roger G. Johnson and Anthony R.E. Garcia, An Annotated Taxonomy of Tag and Seal Vulnerabilities, Report LAUR 98-5158 (Los Alamos, New Mexico; Los Alamos National Laboratory, 1999). В этом отождествляется 27 различных групп персонала, которые могут участвовать в попытках взлома, как сотрудников, так и посторонних лиц.

[18] См., например, C.A. Roper, The Complete Book of Locks and Locksmithing (Blue Ridge Summit, Pennsylvania; Tab Books, 1983), в особенности, стр. 238 – 251, и видео B and E: A to Z (Boulder, Colorado; Paladin Press, 1990).

[19] Отсутствующий замок – это особый случай отпертого замка.

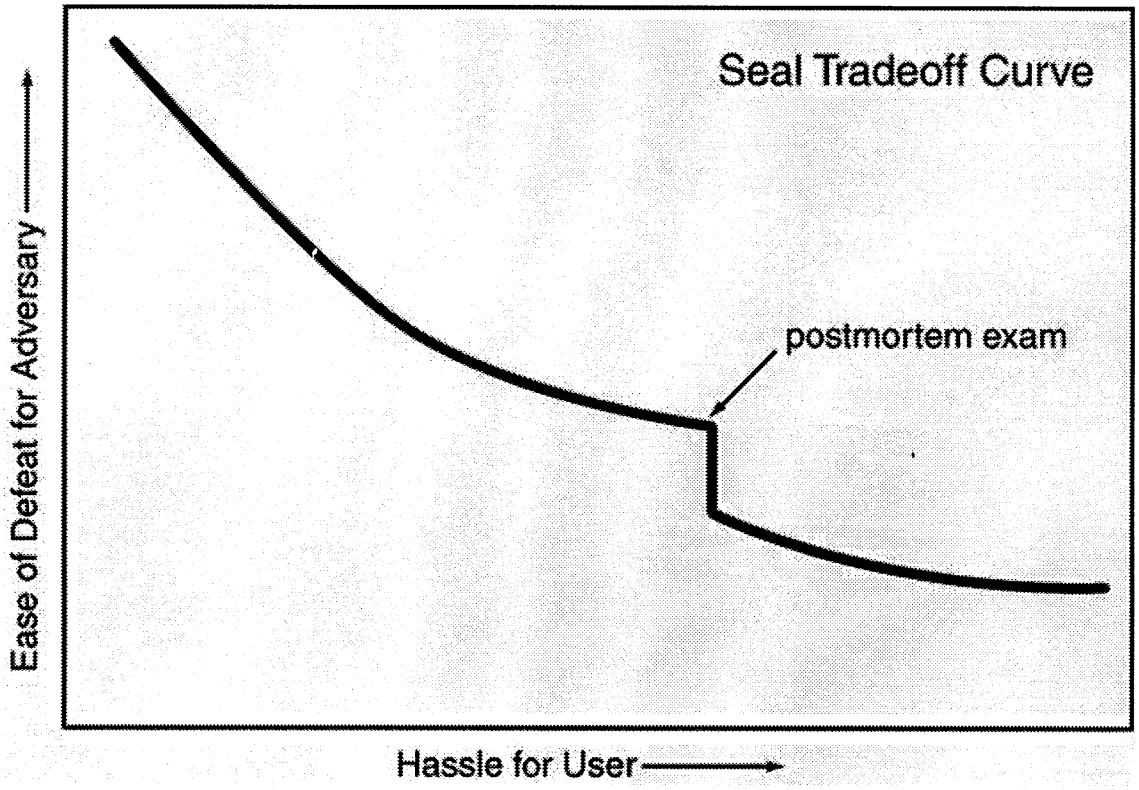

Рис. 2. Схематическая компромиссная кривая для типичной пломбы. Чем больше усилий вложит пользователь в применение пломбы (ось x), тем труднее будет противнику взломать ее (ось y). Резкий скачок кривой связан с проведением последующего контроля после удаления пломбы. Несмотря на то, что прочие участки кривой выглядят гладкими, ее увеличение показало бы, что она состоит из последовательности мелких скачков, каждый из которых соответствует введению новой процедуры в протокол пломбы.

Компромиссные решения для пломб

Типичная пломба с индикацией вмешательства характеризуется компромиссной кривой вида, показанного на рис. 2. Легкость взлома пломбы обычно показывается как функция от объема усилий, вкладываемого пользователем пломбы в ее применение. Эти усилия характеризуются качественным техническим параметром, обычно применяемым персоналом, который устанавливает и проверяет пломбы[20].

В целом, рис. 2 показывает, что чем больше усилий вложит пользователь в применение пломбы, тем труднее будет противнику взломать ее. Эти усилия могут потребовать тщательных процедур установки и инспекции пломбы, так же как и внимательного контроля качества, ведения записей и обучения. Если, с другой стороны, пользователь не желает вкладывать значительных усилий в применение пломб, то противнику будет проще взломать ее. Поэтому простая пломба, используемая с большим вниманием, может обеспечить лучшее обнаружение вмешательства, чем плохо применяемая сложная пломба.

Резкий скачок кривой на рис. 2 связан с проведением последующего контроля после удаления пломбы. Он включен лишь в немногие программы обнаружения вмешательства.

Согласно данным группы ГОУ, высокотехнологичные пломбы, или пломбы с провер-

[20] В коммерческих условиях усилия могут быть выражены в терминах экономических ресурсов (времени, персонала, материалов, оборудования), задействованных в выполнении выбранных протоколов пломбы. Однако, в условиях государственных организаций с их искусственной экономикой, термин «усилия» может оказаться более подходящим. Он может также более точно отражать психологические вопросы, связанные с использованием пломб, которые так сильно влияют на эффективность их применения.

кой считывателем характеризуются компромиссной кривой, подобной показанной на рис. 3. По сравнению с обычной низкотехнологичной пломбаю, высокотехнологичная или проверяемая считывателем пломба может обеспечить большую безопасность по сравнению с обычными пломбами, но только тогда, когда пользователь приложит дополнительные усилия при ее использовании. При малых прилагаемых усилиях обычные пломбы ведут себя лучше. К несчастью, многие пользователи пломб выбирают высокотехнологичные пломбы или считыватели в основном потому, что они хотят сократить рабочую нагрузку на инспекторов пломб.

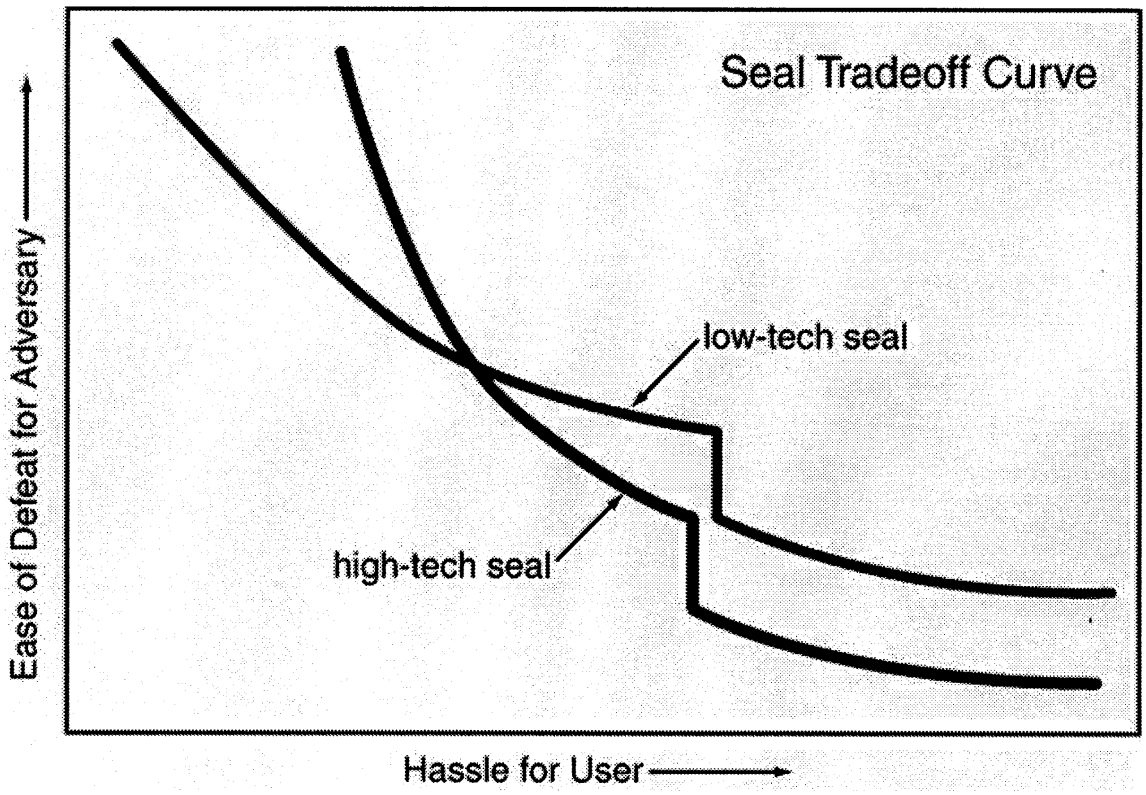

Рис. 3. Типичные компромиссные кривые для низкотехнологичных (надпись сверху) и высокотехнологичных пломб (надпись снизу); кривая относится и к пломбам со считывателем. Хотя высокотехнологичные пломбы способны обеспечить лучшее обнаружение вмешательства, вы зачастую должны затратить больше, а не меньше, усилий, чтобы добиться большей безопасности.

Одной из общих проблем с высокотехнологичными пломбами или считывателями является «эффект Титаника» – излишнее доверие к высокой технологии. При ручной проверке низкотехнологичных пломб инспекторы должны обращать пристальное внимание к деталям проверяемого ими места действия. Поэтому они получают хорошие шансы для обнаружения вмешательства или аномалий. Однако, при применении высокотехнологичных пломб и/или считывателей инспекторы нередко слепо доверяют показаниям пломбы или считывателя (в особенности, если они не очень понимают технологию) и обращают меньшее внимание на общее место действия. Взломщик может использовать это обстоятельство. Кроме того, высокотехнологичные пломбы или считыватели предоставляют взломщику значительно больший выбор возможностей атаки по сравнению с простыми пломбами.

Текущие проблемы пломб

С пломбами постоянно возникает много проблем, относящихся к представлению о них и методах их применения. Эти проблемы существуют в широком круге их приложений и

многих различных групп их пользователей. Некоторые из этих проблем уже обсуждались выше.

Фундаментальной проблемой современных пломб является то, что после обнаружения вмешательства пломба может не записать этого факта нестираемым образом. Если взломщик сумеет стереть или утаить свидетельство взлома, то пломба станет неэффективной. Улучшения в этом направлении очевидно необходимы, и они являются основной целью новых концепций пломб, разрабатываемых в Лос-Аламосской национальной лаборатории.

Особенно серьезной проблемой текущего использования пломб является распространенное отсутствие эффективной подготовки установщиков пломб и инспекторов. Наиболее эффективные меры противодействия попыткам взлома пломб требуют понимания конкретных слабых мест пломб и ознакомления с наиболее вероятными сценариями попыток взлома. Инструкции, которые получают инспекторы, обычно звучат так: «смотрите за следами вмешательства» (это справедливо даже для критических приложений). Информация о том, за чем в точности нужно следить, нередко отсутствует. С точки зрения группы ГОУ, инспекторам следует показывать примеры атакованных пломб. Еще лучше, если им будут показывать, как можно атаковать конкретно применяемые ими пломбы, поскольку это даст наиболее прямую и полезную информацию[21].

Также повсеместно и широко распространено непонимание испытаний пломб. Оценки уязвимости заметно отличаются от других типов испытаний, таких, как испытания пригодности, простоты применения, готовности к полевым условиям, прочности и устойчивости к окружающей среде. Многие пользователи пломб смешивают все типы испытаний в одну группу и обретают необоснованную уверенность в используемой ими пломбы, если она пройдет один или другой тип испытаний. Широко распространенное желание пользователей пломб получить какой-либо сертификат используемых ими пломб также не оказывается полезным[1]. Стандарты пломб и теория обнаружения вмешательства недостаточно хорошо развиты для того, чтобы сертификация имела какой-то смысл. Кроме того, сертификация неизбежно включает излишнее упрощение важных вопросов и поверхностное отношение к критическим деталям конкретно интересующего приложения.

Еще одной проблемой, препятствующей эффективному использованию пломб, является неоправданное отношение к оценкам уязвимости. Многие пользователи пломб думают, что оценка уязвимости должна определять нулевую уязвимость. На деле эффективная оценка уязвимости всегда должна найти таковую (поскольку она всегда существует); в противном случае такая оценка не имеет значения[1]. Обнаружение слабого места должно рассматриваться как хорошая новость – поскольку она означает, что безопасность пломбы можно улучшить – а не как плохую новость[22].

Некоторые пользователи пломб считают оптимизацию их безопасности ненужной, поскольку они в дополнение к пломбам используют другие уровни физической безопасности. Они могут включать ограды, замки, охранную сигнализацию, видеонаблюдение, охранников или сторожевых собак, правило доступа 2 или 3 лиц к особым объектам, или тщательную проверку критического персонала.

Очевидно верно, что эти меры при эффективном использовании могут значительно увеличить безопасность. Но другие уровни безопасности никогда не следует использовать

---

[21] Рекомендация указывать инспекторам на способы взлома пломб, которые они используют, противоречива. Некоторые руководители служб безопасности не хотят раскрывать конкретную информацию об уязвимости персоналу безопасности сравнительно низкого уровня. Однако, с точки зрения ГОУ, нелояльные или некомпетентные инспекторы пломб могут легко нанести вред программе обнаружения вмешательства даже в том случае, когда они не обладают такой информацией. В большинстве случаев потенциальные преимущества грамотности инспекторов значительно превосходят риск. Конечно, для проверки договоров каждая из сторон будет хотеть, чтобы ее инспекторы знали об уязвимости пломб, но может не хотеть поделиться этой информацией с другой стороной.

[22] Удивительно, что Ричард Фейнман поднял вопрос о «наказании вестника», который часто возникает при обнаружении нарушений безопасности: Ralph Leighton, Richard Philips Feynman, and Albert Hibbs, ‘Surely You are Joking, Mr. Feynman’: Adventures of a Curious Character. Edited by Edward Hutchings, New York; Batam, 1985, 119 – 137.

как оправдание избежать оптимизации эффективности пломб, в особенности, если (как обнаружила группа ГОУ) этого часто можно добиться довольно легко. В любом случае, полагаться на другие уровни безопасности для преодоления недостатков в одном конкретном уровне может оказаться опасным. Это может порождать мнение, что мы можем не относиться серьезно к тревоге или подозрительной ситуации на одном уровне, потому что другие уровни подстрахуют нас. Добавление новых уровней ненадежной защиты часто может понижать общую безопасность вместо того, чтобы повышать ее.

Многочисленные уровни безопасности могут также решить вопрос о природе противника. Сотрудники предприятия и инспекторы по договорам уже имеют право прохода через многие уровни безопасности в тот момент, когда они достигнут пломбы. Поэтому эти внешние уровни могут не иметь полного отношения к оценке безопасности пломбы.

Возможно также, что безопасность, обеспечиваемая видеонаблюдением или правилом доступа 2 или 3 лиц, часто переоценивается. Немногие работники службы безопасности получают подготовку в навыках наблюдения или в методике отвлечения внимания или указания ложного направления. При хорошем исполнении эти методы могут быть исключительно эффективными – это может показать любой хороший фокусник. Точно так же, члены команд из 2 или 3 человек могут зачастую вступать в дружеские отношения (даже при случайном назначении), что может помешать их объективности при слежении за другими членами команды. В случае мониторинга международных договоров инспекторы могут быть особенно подвержены отвлечению внимания, указанию ложного направления или ошибкам наблюдения из-за нарушения суточного ритма организма, усталости в полете, культурной дезориентации, робости и связанного с работой стресса.

Другая постоянная проблема с пломбами связана с тем, что рынок пломб в основном определяется коммерческими потребителями, внимание которых часто привлечено не к безопасности, а к стоимости[2]. Часть рынка, представленная государством и коммерческими потребителями, заинтересованными в высокой безопасности, остается относительно малой. В результате очень немногие разработчики и производители пломб серьезно занимаются оптимизацией безопасности пломб. Еще меньше тех, кто организует независимые оценки уязвимости. Разработчики и производители пломб, организующие независимую оценку уязвимости, стремятся подождать готовности конечного продукта, когда делать изменения будет уже поздно. В идеале оценка уязвимости должна быть итеративной и проводиться в течение всего процесса разработки прототипа[1].

Пломбы для разоружения

Пломбы, используемые для международных гарантий, верификации договоров, и разоружения, должны обладать определенными уникальными особенностями. В особенности, они будут сталкиваться с одной из классических проблем, связанных с верификацией договоров. Если инспектируемое предприятие предоставляет и контролирует пломбы, то инспекторы будут подозревать, что пломбы подделываются. Если, с другой стороны, инспекторы будут предоставлять и контролировать пломбы, то инспектируемое предприятие будет обеспокоено возможностью внедрения в пломбы миниатюрной шпионской аппаратуры, такой, как микрофоны, или миниатюрные детекторы излучений[23]. У инспектируемого предприятия могут возникнуть опасения по физической безопасности, связанные с размещением иностранной аппаратуры рядом со своим ядерным оружием.

Имеется много возможных решений этой проблемы, но их анализ будет выходить за рамки этой статьи[24]. Однако, здесь можно предположить, что высокотехнологичные электронные пломбы будут менее удобными как для инспектируемого предприятия, так и для инспекторов, чем качественные пассивные пломбы, из-за опасений по безопасности, подделкам и шпионажу. В любом случае, пломбы, используемые по международным договорам требуют прозрачности и возможности согласования, чего не требуют пломбы, применяемые

[23] Если одна из участвующих в договоре стран опасается, что другая страна обладает техническим превосходством, это беспокойство еще более усилится.

[24] Лос-Аламосская национальная лаборатория подготовила статью, в которой предлагаются некоторые новые удобные для переговоров подходы к протоколам СНВ-3, включающие нестандартное применение пломб и их дистанционный опрос.

для других целей. Кажется, ни одна из существующих пломб не была разработана с учетом выполнения требований по прозрачности и возможности согласования.

Отметим, что пломбы, используемые для договоров по ядерному разоружению, возможно, будут сосуществовать с пломбами, используемыми для внутренней безопасности и гарантий. Это может стать проблемой, поскольку на некоторых контейнерах для оружия не просто установить дополнительные пломбы. Как правило, имеющиеся контейнеры для оружия часто разрабатываются в основном для обеспечения ядерной физической безопасности и простоты использования, но не безопасности по отношению к вмешательству.

Одним из важных различий между обычными пломбами и пломбами, используемыми для верификации договоров, является значение обнаружения подозрительной пломбы. Если, например, подозрительная пломба будет обнаружена во внутренней программе ядерной безопасности, то это будет серьезной проблемой, поскольку это может предполагать хищение ядерных материалов. Однако, подозрительная пломба, обнаруженная по международному договору, может быть менее неприятной. Инспектируемая страна просто не получит доверия в разоружении конкретной единицы ядерного оружия. Оружие, по-видимому, будет возвращено на начальный этап и снова пройдет процесс разоружения.

И, наконец, пломбы, используемые в контролируемом договоре по разоружению, часто играют психологическую и церемониальную роль, в дополнение к обеспечению прозрачности и уверенности в процессе разоружения. Для внутренней безопасности и гарантий эта функция обычно не требуется[25].

Пломбы для обращения с опасными отходами

Удивительно, но пломбы редко используются в операциях обращения с отходами, включающими хранение, погрузку и перевозку ядерных и прочих опасных отходов. При эффективном использовании пломбы помогут обнаружить и предотвратить хищение опасных материалов для террористических или каких-либо других целей. Они помогут также в учете и контроле опасных материалов, и могут помочь в облегчении правовой ответственности, связанной с опасными материалами. Пломбы могут защитить от саботажа со стороны рассерженных сотрудников или посторонних активистов, защищающих окружающую среду с целью дискредитировать программу обращения с опасными отходами[26]. Пломбы могут также помочь обнаружить и предотвратить непреднамеренные ошибки в обработке и обращении с контейнерами с опасными отходами. Пломбы могут обнаружить злоумышленное или непреднамеренное вмешательство в данные об отходах, аналитические результаты, или калибровку или эксплуатацию аналитических приборов. Пломбы должны играть решающую роль в обнаружении недобросовестных попыток утилизации опасных отходов в контейнерах, уже сертифицированных для хранения неопасных или менее опасных отходов.

Очень немногие из существующих пломб (если такие вообще есть) специально разработаны или оптимизированы для применения в обращении с опасными отходами. Для использования в контейнерах с отходами пломбы должны обычно характеризоваться следующими свойствами: прочностью, хорошей стойкостью к воздействию окружающей среды, умеренной или высокой химической инертностью, физической безопасностью[27], простотой

---

[25] Учитывая слабую подготовку некоторых пользователей пломб даже в критических применениях, слово «церемониальный» может, тем не менее, оказаться подходящим описанием.

[26] См. R.G. Johnson and A.R.E. Garcia, “Tamper Detection for Waste Managers”, Proceedings of Waste Management ’99 (Tucson, Arizoina; WMI), CD-ROM, доступно по адресу http://lib-www.lanl.gov/la-pubs/00418763.pdf. Атаки со стороны недовольных сотрудников и посторонних лиц, желающих дискредитировать операции обращения с отходами, по-видимому, недостаточно полно рассматриваются при планировании безопасности в некоторых программах обращения с отходами.

[27] Физическая безопасность является важным фактором для некоторых применений пломб. Пломбы с проволочными или кабельными петлями на движущихся контейнерах могут поцарапать глаза или кожу, или захватить пальцы при перемещении около персонала предприятия. У металлических пломб иногда есть острые края или заусенцы, которые могут порезать кожу. Они могут стать очень горячими на солнце или очень холодными на морозе. Ус-

использования и малой стоимостью.

Одной из трудностей в многих применениях обращения с отходами является использование металлических 55-галлонных (двухсотлитровых) бочек. Крышка бочки обычно удерживается на месте кругообразной полосой, скрепляемой металлическим болтом. Это конфигурация неудобна для эффективной установки пломбы. Кроме того, такая конструкция плоха с точки зрения безопасности контейнера и обнаружения вмешательства.

Будущие пломбы

Представляется очевидным, что возможно создать гораздо лучшие пломбы. Во многих случаях существующие конструкции пломб могут быть улучшены относительно простыми модификациями, если их уязвимость полностью понята. Возможны также новые и улучшенные пломбы. Однако, разработка пломб правительством США в основном закончилась в 1993 году. Некоторые частные компании продолжают разрабатывать новые пломбы, но немногие из них (если таковые вообще имеются) разработаны с целями высокой безопасности, разоружения или обращения с отходами.

Очевидно, что имеются новые технологии, материалы и подходы для создания новых и улучшенных пломб. К ним относятся:

- тонкие пленки
- новые полимеры и композиционные материалы
- экзотическая органика и макромолекулы
- жидкие кристаллы и ферромагнитные жидкости
- микрочастицы
- биологические материалы
- новые стекла
- явления переноса и диффузии
- ультразвук
- экзотические оптические и электрооптические материалы
- нанотехнология
- тайные пломбы
- одноразовые клавишные панели
- пломбы, комбинированные с обнаружением присутствия человека
- пломбы, комбинированные с биометрикой

Возможно, что в будущем самыми эффективными пломбами станут простые и недорогие пассивные устройства, которые легко устанавливаются и проверяются, изготовленные из высокотехнологичных экзотических материалов, которые трудно мистифицировать или подделать. Вероятно, что электронные и электрооптические пломбы останутся уязвимыми к относительно простым попыткам взлома, хотя уровень изощренности, требуемый от взломщика, скорее всего, будет возрастать.

Серьезно необходимы также улучшенные контейнеры, разработанные с целью повышения безопасности и более эффективного применения пломб. Для разработки улучшенных контейнеров могут быть использованы многочисленные новые технологии и стратегии.

Существует значительный интерес к пломбам, которые могут опрашиваться на расстоянии для обнаружения факта вмешательства. Некоторые из коммерческих пломб сейчас могут опрашиваться на расстоянии до нескольких метров. Однако, для целей нераспространения и разоружения интересен дистанционный мониторинг на расстоянии в сотни и тысячи километров. Представляется вероятным, что даже весьма сложные и контролируемые на расстоянии пломбы должны время от времени проверяться вручную, чтобы достичь полной уверенности в отсутствии попыток взлома.

Обычный способ дистанционного мониторинга пломб обычно предусматривает при-

---

тойчивость к искрению может оказаться важной для применения в обращении с отходами, в которых имеются горючие или взрывоопасные вещества.

менение шифрования, методов идентификации и информационных барьеров. Однако, это представляет весьма серьезную проблему. Применение наиболее безопасной шифровки или схем отождествления вряд ли будет разрешено для международной верификации из-за ограничений по экспортному контролю и соображений безопасности. С другой стороны, менее сложные методы, вероятно, не смогут обеспечить высокой безопасности. Информационные барьеры, в некотором смысле, еще более проблематичны, поскольку они включают сложное взаимодействие физических и электронных систем, которые обладают множеством возможных слабых мест. Будет трудно также обеспечить совместимость информационных барьеров с соображениями контрразведки, переговоров и прозрачности. Мы надеемся обсудить некоторые возможные пути решения этой проблемы в будущей статье[24].

Приложение А
Систематизация попыток взлома пломб

Группа оценки уязвимости Лос-Аламосской национальной лаборатории разработала классификацию различных общих видов попыток взлома пломб. Эти 105 различных общих видов были разделены на 11 широких категорий:

Попытки взлома на базе режима отказа (тип F): вмешательство в программу безопасности пломб непосредственно, или с помощью неправильных указаний, для того, чтобы обнаружить, имеются ли ошибки в обнаружении вмешательства; или ожидание сделанной ошибки и ее последующее использование.

Попытки взлома с отмычками (тип P): использовать отмычку так, чтобы открыть пломба без повреждений или любых следов ее открытия. Отмычки хорошо работают с удивительно большим количеством пломб.

Попытки взлома с распечатыванием (тип U): распечатать (открыть) пломба, и после этого починить или скрыть любое повреждение или свидетельство ее открытия. Это делается до или после повторной установки пломбы. Эти виды попыток взлома могут быть весьма эффективными, в особенности, если пользователь пломбы не производит детального последующего исследования пломбы.

Попытки взлома с вмешательством в данные о пломбы (тип D): вмешательство в данные (такие, как серийный номер) пломбы, или в отчеты и объяснения результатов инспекции.

Попытки взлома с вмешательством в считыватель или верификатор пломбы (тип V): вмешательство в считыватель или верификатор пломб, который основан на электронном или оптическом считывании для проверки наличия вмешательства.

Попытки взлома с саботажем процесса опечатывания (тип S): использование сотрудников или посторонних лиц для нарушения процесса опечатывания.

Попытки взлома «с черного хода» (тип B): установка дефекта в пломбы до ее применения, который может быть использован в дальнейшем. Этот «дефект с черного хода» может быть введен во время конструирования пломбы, или процесса производства, или перевозки и хранения, или непосредственно перед использованием.

Попытки взлома с репликацией (тип R): использование завода для изготовления дубликата пломбы, используя многочисленные возможные методы, включающие взлом и проход, тайные методы, подкуп, насилие, или методы социотехники.

Попытки взлома с подделкой (тип C): взломщик изготавливает дубликат пломбы вне завода, возможно, начиная с новых пломб или деталей использованных пломб.

Электронные попытки взлома (тип E): для электронных пломб используется вмешательство в различные компоненты, такие, как датчики, микропроцессор, сигнальные цепи, источники

питания, сигнализатор, или запоминаемое условие тревоги.

Альтернативные попытки взлома (тип А): эти попытки используют разнообразные прочие методы.

Благодарности и заявления

Эта работа проводилась под покровительством Министерства энергетики США. Представленные в ней мнения принадлежат автору и не обязательно отражают любую официальную позицию Лос-Аламосской национальной лаборатории. Энтони Гарсиа, Эрик Гердес, Джени Энтер, Эрик Бака, Рон Мартинец, Джим Дойл, и Джефф Миллер внесли полезный вклад.