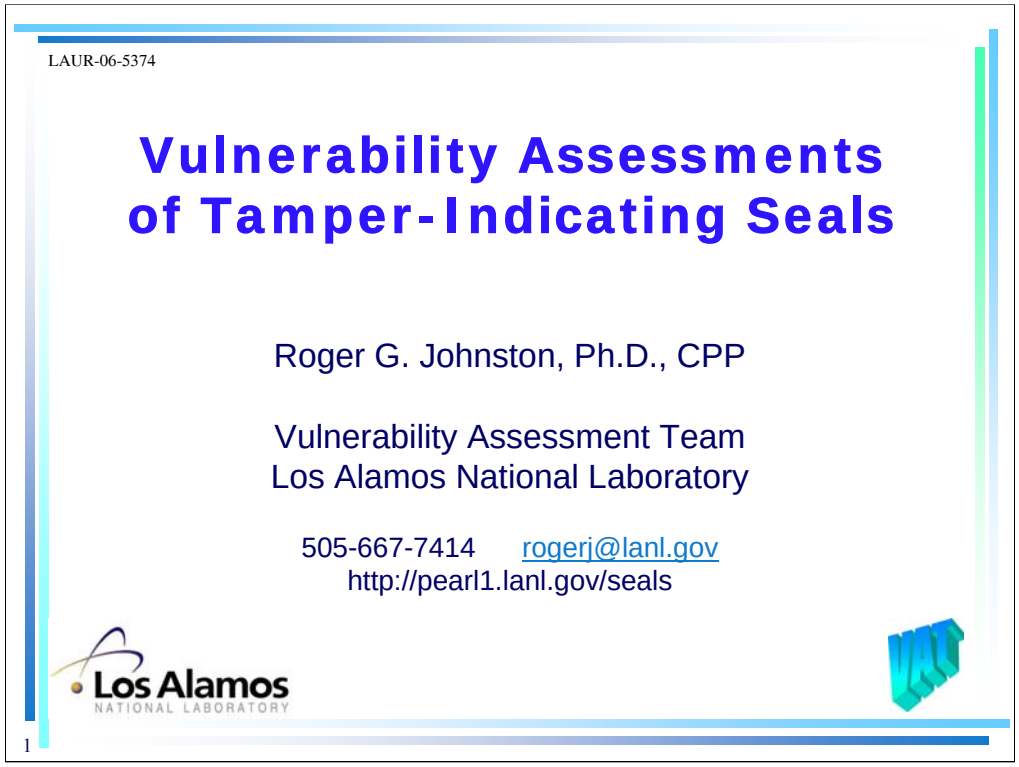
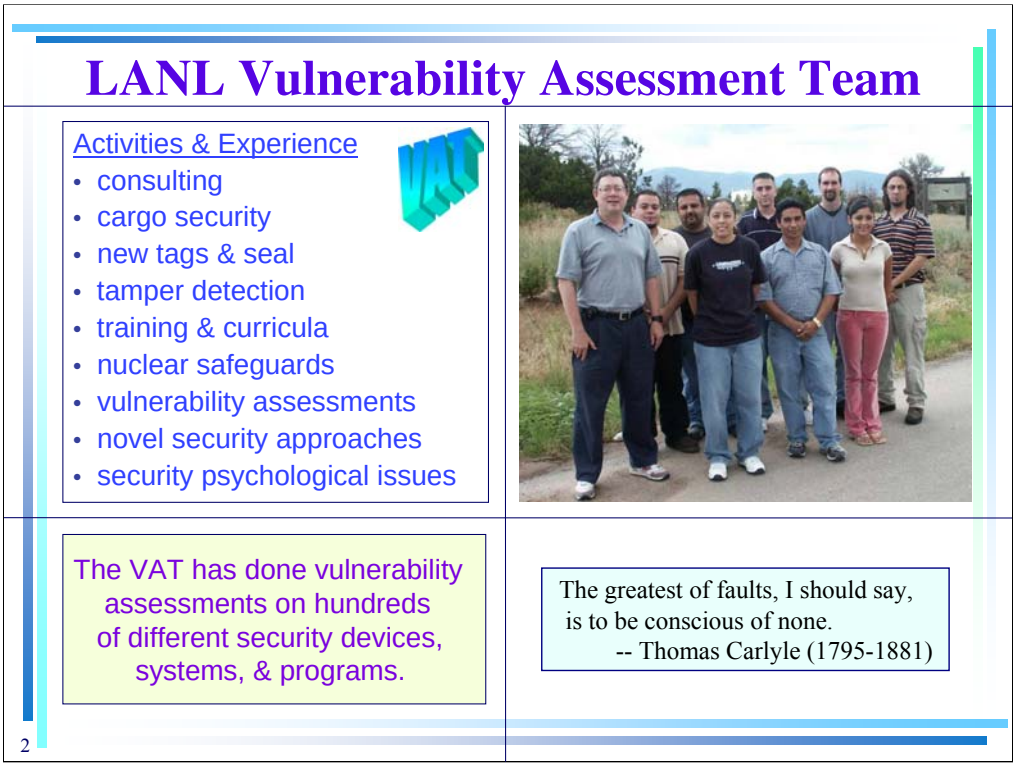
Invited Talk for the TID Working Group Meeting,
Moscow, Russia, September 11-16, 2006



ОЦЕНКА УЯЗВИМОСТИ УСТРОЙСТВ ИНДИКАЦИИ ВМЕШАТЕЛЬСТВА

Роджер Джонстон, доктор наук, CPP
Группа по оценке уязвимости (ГОУ)
Лос-Аламосская Национальная Лаборатория
505-667-7414 rogerj@lanl.gov
http://pearl1.lanl.gov/seals



ГРУППА ЛЛНЛ ПО ОЦЕНКЕ УЯЗВИМОСТИ

Деятельность и опыт

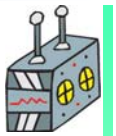
- консультирование
- обеспечение безопасности грузов при транспортировке
- новые пломбы и печати
- обнаружение вмешательства
- обучение и учебные программы
- обеспечение сохранности ядерных материалов
- оценки уязвимости
- новейшие подходы к обеспечению безопасности
- психологические аспекты деятельности по обеспечению безопасности

ГОУ выполнила оценку уязвимости для сотен различных устройств, систем и программ обеспечения безопасности.

Должен сказать, что величайшей из ошибок является уверенность в их отсутствии.

-- Томас Карлайл (1795-1881)

Security Maxims



1. **Infinity Maxim**: There are an unlimited number of vulnerabilities, most of which will never be discovered (by the good guys or bad guys).

2. **Arrogance Maxim**: The ease of defeating a security device is inversely proportional to how confident the designer, manufacturer, or user is about it, and to how often they use words like “impossible” or “tamper-proof”.

3. **High-Tech Maxim**: The amount of careful thinking that has gone into a given security device is inversely proportional to the amount of high-technology it uses.

Confidence is that feeling you sometimes have before you fully understand the situation. -- Anonymous

3

ПРАВИЛА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

1. **Правило бесконечности**: Существует неограниченное количество уязвимых точек, большая часть из которых никогда не будет обнаружена (как "хорошими" людьми, так и злоумышленниками).
2. **Правило самонадеянности**: Легкость, с которой можно взломать защитное устройство, обратно пропорциональна степени уверенности проектировщика, производителя или пользователя в этом устройстве, а также тому, насколько часто они используют слова вроде "невозможно взломать" или "несанкционированный доступ исключен".
3. **Правило высоких технологий**: Объем знаний, вложенных в реализацию данного защитного устройства, обратно пропорционален объему используемых им высоких технологий.

Уверенность — это то чувство, которое посещает вас перед тем, как вы полностью уяснили ситуацию.

-- Анонимный автор

Security Maxims

4. **Low-Tech Maxim**: Low-tech attacks work (even against high-tech devices).

5. **Yes! Maxim**: There are effective, simple, & low-cost countermeasures to most vulnerabilities.

6. **Oh No! Maxim**: But users, manufacturers, and bureaucrats will be reluctant to implement them.

If you think that technology can solve your security problems, then you don't understand the problems and you don't understand the technology. -- Bruce Schneier

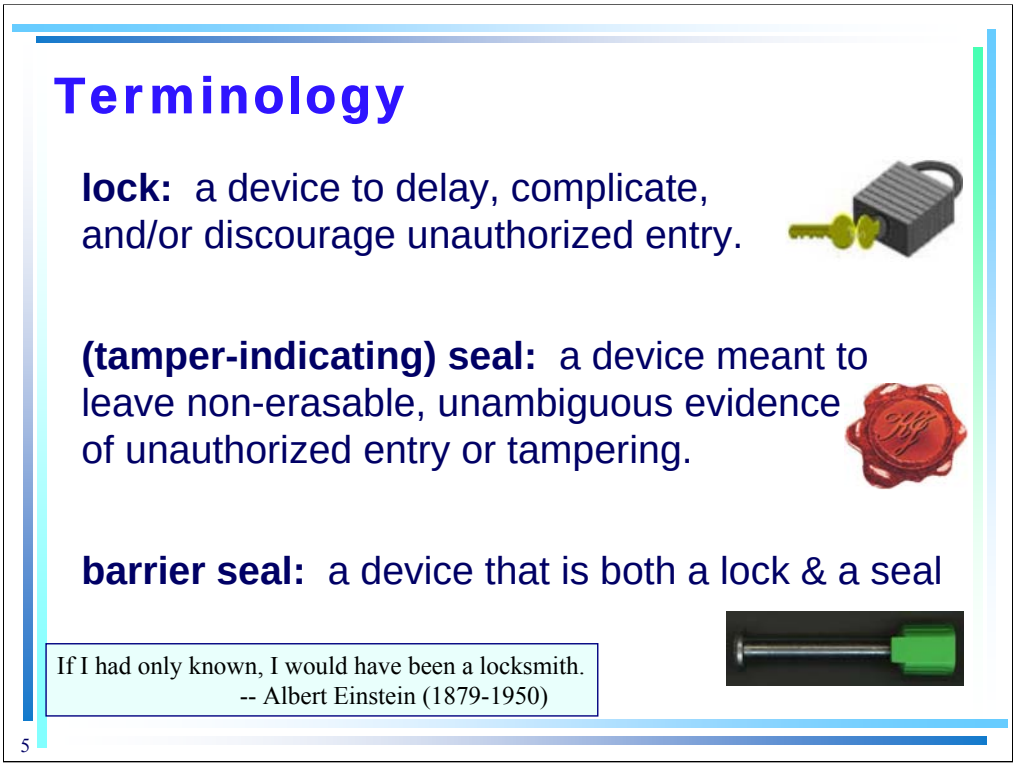
4

ПРАВИЛА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

1. **Правило устаревших технологий**: Атаками с применением устаревших технологий нельзя пренебрегать (даже против высокотехнологичных устройств).
2. **Правило "Да!":** Практически для любых уязвимых мест можно подобрать эффективные, простые и недорогие меры противодействия.
3. **Правило "О нет!":** Однако, пользователи, производители и бюрократы внедряют их с неохотой.

Если вы полагаете, что технология может решить ваши проблемы с безопасностью, значит, вы не понимаете в этих проблемах и не понимаете в технологии.

-- Брюс Шнайер



ТЕРМИНОЛОГИЯ

замок: устройство, предназначенное для задержки, усложнения и/или препятствования несанкционированному вторжению.

устройство индикации вмешательства (пломба/печать): устройство, предназначенное для оставления неустранимого, явного свидетельства несанкционированного вторжения или вмешательства.

защитная пломба: устройство, являющееся одновременно замком и пломбой.

Если бы я все знал заранее, то стал бы слесарем.
-- Альберт Эйнштейн (1879-1950)

Terminology

defeating a seal: opening a seal, then resealing (using the original seal or a counterfeit) without being detected.

attacking a seal: undertaking a sequence of actions designed to defeat it.

Defeating seals is mostly about fooling people, not beating hardware (unlike defeating locks, safes, or vaults)!

6

ТЕРМИНОЛОГИЯ

нарушение целостности УИВ: невыявленное вскрытие УИВ с его повторным опломбированием (с помощью оригинального или поддельного УИВ).

попытка нарушить целостность пломбы: ряд предпринятых действий с целью взломать УИВ.

Взлом УИВ обычно подразумевает введение в заблуждение людей, а не взлом технических средств (например, взлом замков, вскрытие сейфов или хранилищ)!

ТЕРМИНОЛОГИЯ

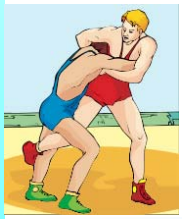
протокол применения (УИВ): официальные и отступающие от правил способы применения УИВ. Включает закупку, отправку, хранение, установку, проверку, снятие, уничтожение, предоставление отчетов, расшифровку и обучение.

УИВ ничем не лучше чем протокол о его применении!

меры противодействия УИВ: способы улучшить УИВ за счет изменения его конструкции и/или протокола применения УИВ.

Terminology

vulnerability assessment (VA): discovering and demonstrating ways to defeat a seal or tamper-detection program. Should include suggesting countermeasures.



He that wrestles with us strengthens our skill. Our antagonist is our helper.
-- Edmund Burke (1729-1797)

8

ТЕРМИНОЛОГИЯ

оценка уязвимости (ОУ): обнаружение и демонстрация способов нарушения целостности УИВ или нарушения программы применения УИВ. Должна включать в себя предполагаемые меры противодействия.

Тот, кто борется с нами, оттачивает наше мастерство.
Наш противник — это наш помощник.

-- Эдмунд Бурк (1729-1797)

Vulnerability Assessments

The purpose is to improve tamper detection, not to:

- Pass a test
- Generate metrics
- Justify the status quo
- Check against some standard
- Claim there are no vulnerabilities
- Rationalize the research & development
- Certify a seal as “good” or “ready for use”
- Perform material, environmental, or quality tests
- Apply a mindless, bureaucratic stamp of approval
- Praise or accuse the developer, manufacturer, or user

Nothing is easier than self-deceit. For what each man wishes, that he also believes to be true.
-- Demosthenes (382-322 BC)

9

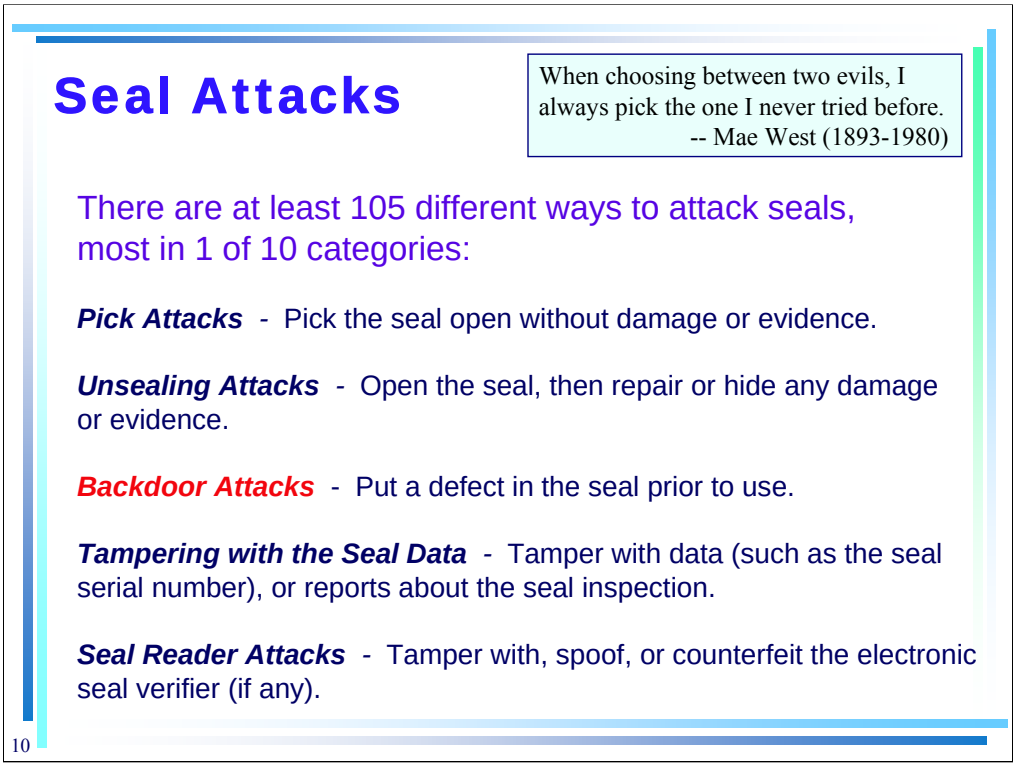
ОЦЕНКИ УЯЗВИМОСТИ

Цель – улучшить качество индикации вмешательства, а не:

- Сдать экзамен
- Создать показатели
- Обосновать существующее положение
- Проверить на соответствие определенному стандарту
- Заявить отсутствие уязвимых мест
- Рационализировать научно-исследовательские и опытно-конструкторские разработки
- Сертифицировать УИВ как "хорошее" или "готовое к применению"
- Провести испытания материалов, климатические испытания или контроль качества
- Поставить бессмысленное бюрократическое приемочное клеймо
- Похвалить или осудить разработчика, производителя или пользователя

Нет ничего проще самообмана.
Желаемое человеком является для него истинным.

-- Демосфен (382-322 до н. э.)



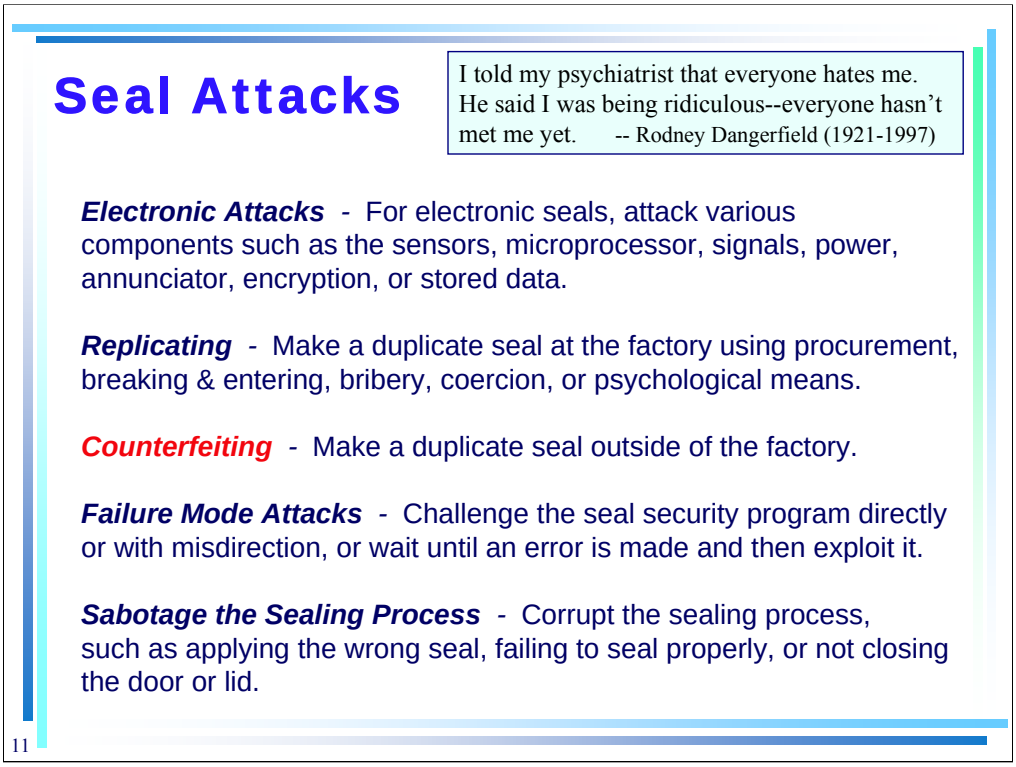
ПОПЫТКИ НАРУШИТЬ ЦЕЛОСТНОСТЬ УИВ

Существует не менее 105 различных способов нарушить целостность УИВ, большая часть из которых попадает в 1 из 10 следующих категорий:

- **Срыв УИВ** – УИВ срывается так, чтобы не оставить следов повреждения.
- **Вскрытие УИВ** – УИВ вскрывается, затем следы повреждения маскируются или уничтожаются.
- **Скрытые атаки** - в УИВ вносится дефект еще до применения этого УИВ.
- **Подделка данных об УИВ** – подделка данных УИВ (например, серийного номера) или протоколов с результатами проверки УИВ.
- **Вмешательство в устройства считывания УИВ** – подделка результатов проверки или вмешательство в работу электронных устройств считывания УИВ (если таковые используются).

Выбирая из двух зол, я всегда предпочитаю то, которое еще не испробовал.

-- Маэ Вест (1893-1980)



ПОПЫТКИ НАРУШИТЬ ЦЕЛОСТНОСТЬ УИВ

Электронные атаки – вмешательство в работу электронных элементов – датчиков, микропроцессора, в сигналы, электропитание, сигнализатор, устройство кодирования сигналов или хранящиеся данные.

Дублирование – производство дубликата УИВ на заводе посредством закупки, взламывания и вторжения, подкупа, насилия или психологического воздействия.

Подделка – производство дубликата УИВ не на заводе.

Режим отказа – непосредственное испытание программы применения УИВ, либо испытание посредством неправильных указаний, либо ожидание до тех пор, пока не появится ошибка с целью воспользоваться ею.

Вредительство во время нанесения УИВ – например, нанесение неправильного УИВ, неправильное нанесение либо неправильные условия нанесения (не закрыта дверь или крышка и т.п.).

Я пожаловался своему психоаналитику, что все меня ненавидят. Он ответил, что я смешон — ведь еще не все со мной знакомы.

-- Родни Дэнджерфильд (1921-1997)

Fake Counterfeits

Often overlooked: an adversary often needs only to mimic the superficial appearance and perhaps simulate the apparent performance of a seal or reader. This is much easier than true counterfeiting.

Sincerity is everything. If you can fake that, you've got it made.
-- George Burns (1896-1996)

12

ЛОЖНЫЕ ПОДДЕЛКИ

Часто игнорируется: злоумышленнику часто необходимо только сымитировать внешний вид и, возможно, фиктивную работу УИВ или устройства считывания УИВ. Это намного проще чем действительно подделать настоящее УИВ.

Искренность — это самое главное. Если вы можете притвориться искренним, то у вас все получится.

-- Джордж Бернс (1896-1996)

Seals Vulnerability Assessment

We studied 244 different seals in detail:

- government & commercial
- mechanical & electronic
- low-tech through high-tech
- cost varies by a factor of 10,000

Over half are in use for critical applications, and ~19% play a role in nuclear safeguards.

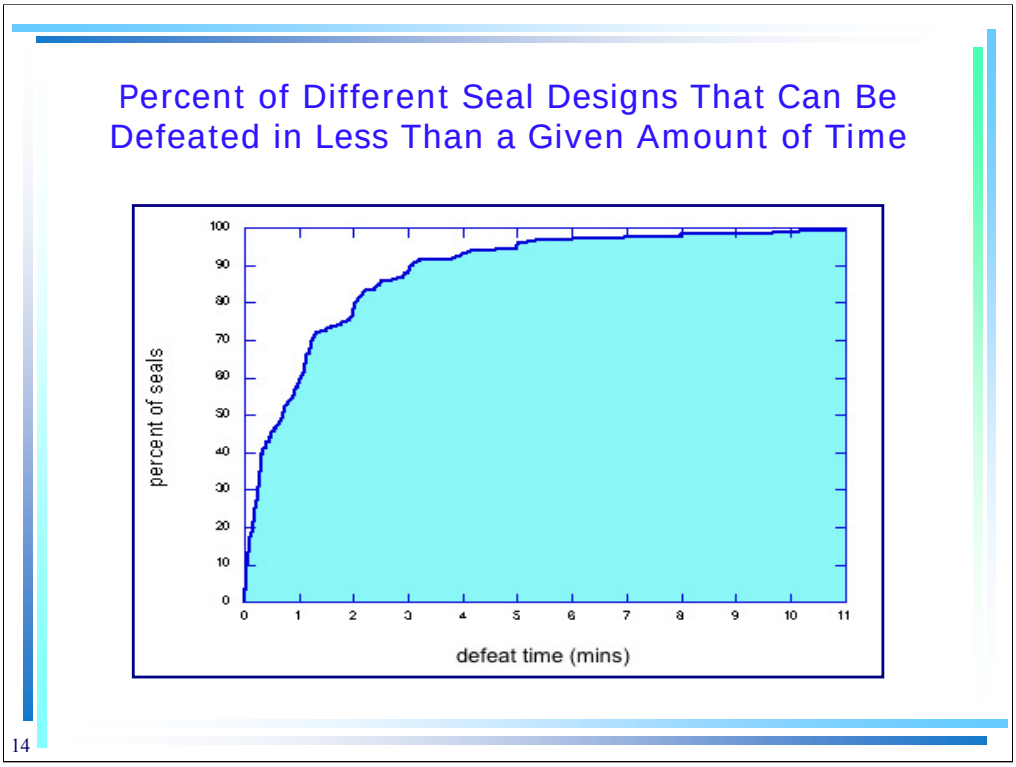
13

ОЦЕНКИ УЯЗВИМОСТИ УИВ

Мы тщательно изучили 244 различных УИВ:

- государственные и промышленные
- механические и электронные
- от устаревших до новейших технологий
- различной цены – перепад цен составлял до 10.000 раз.

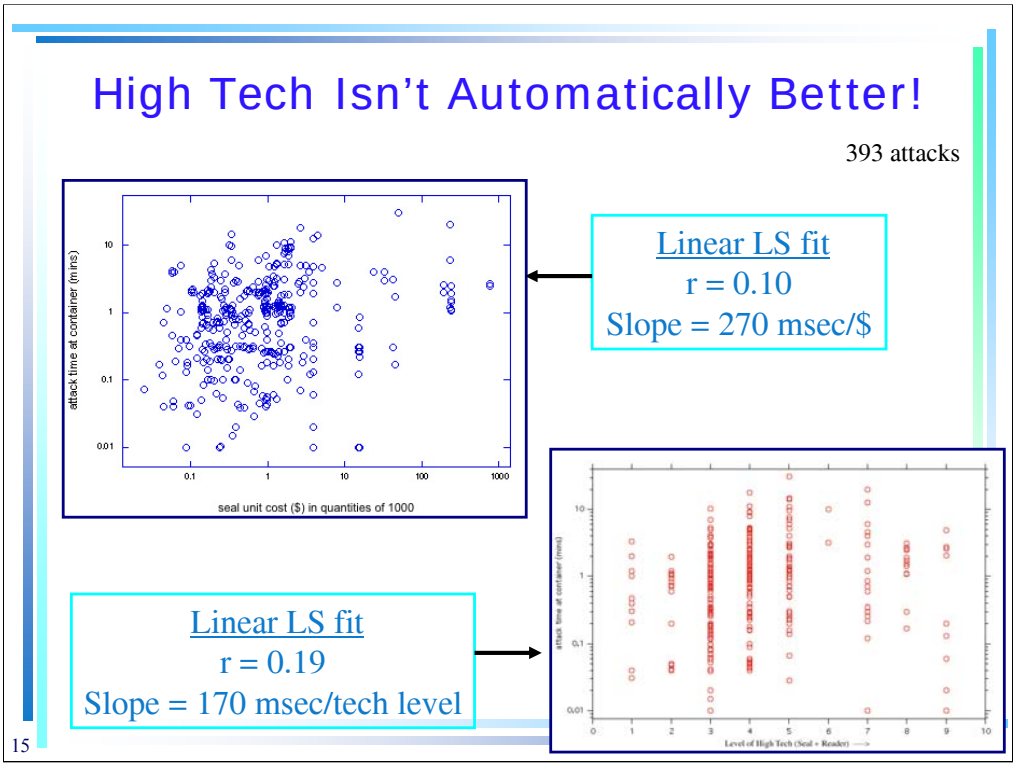
Более половины используются в критических приложениях, примерно 19% - в сфере обеспечения сохранности ЯМ.



ПРОЦЕНТ РАЗЛИЧНЫХ КОНСТРУКЦИЙ УИВ, КОТОРЫЕ МОЖНО ВЗЛОМАТЬ ЗА МЕНЬШЕЕ ВРЕМЯ

Процент УИВ

Время взламывания

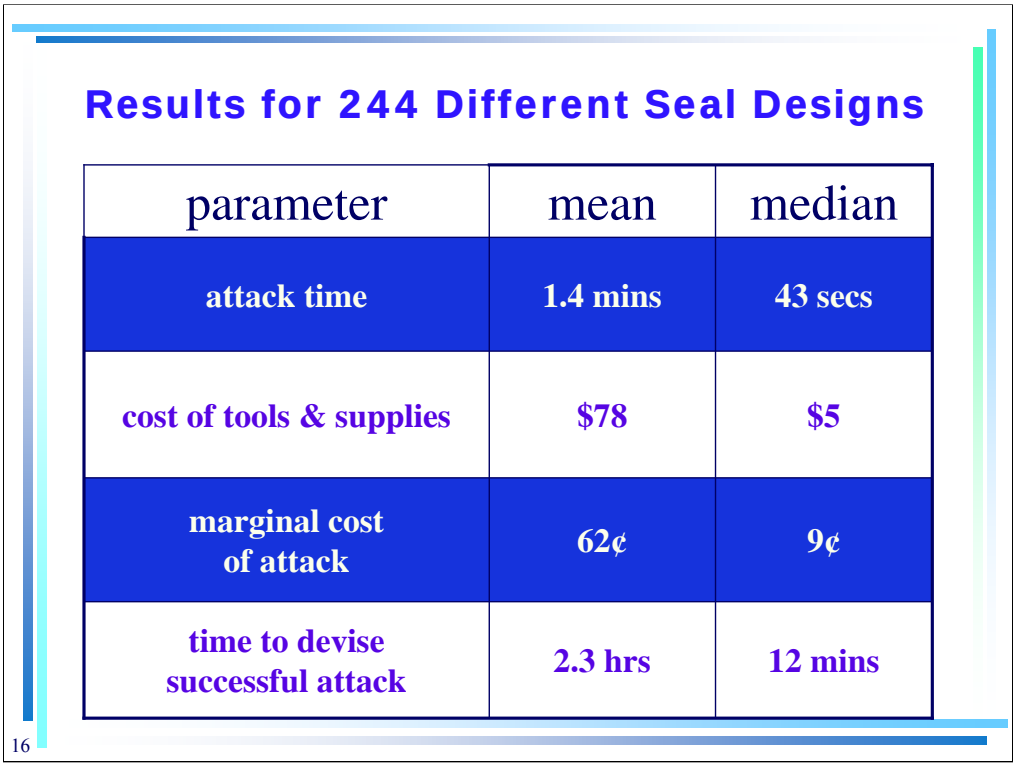


ВЫСОКИЕ ТЕХНОЛОГИИ НЕ ОБЯЗАТЕЛЬНО АВТОМАТИЧЕСКИ ОЗНАЧАЮТ БОЛЕЕ ВЫСОКОЕ КАЧЕСТВО!

393 атаки

Время атаки УИВ, нанесенного на контейнер
Стоимость одного УИВ ($/тыс.шт.)
Линейное приближение
r = 0.10
Наклон = 270 мсек/$

Линейное приближение
r = 0.19
Наклон = 170 мсек/тех.уровень

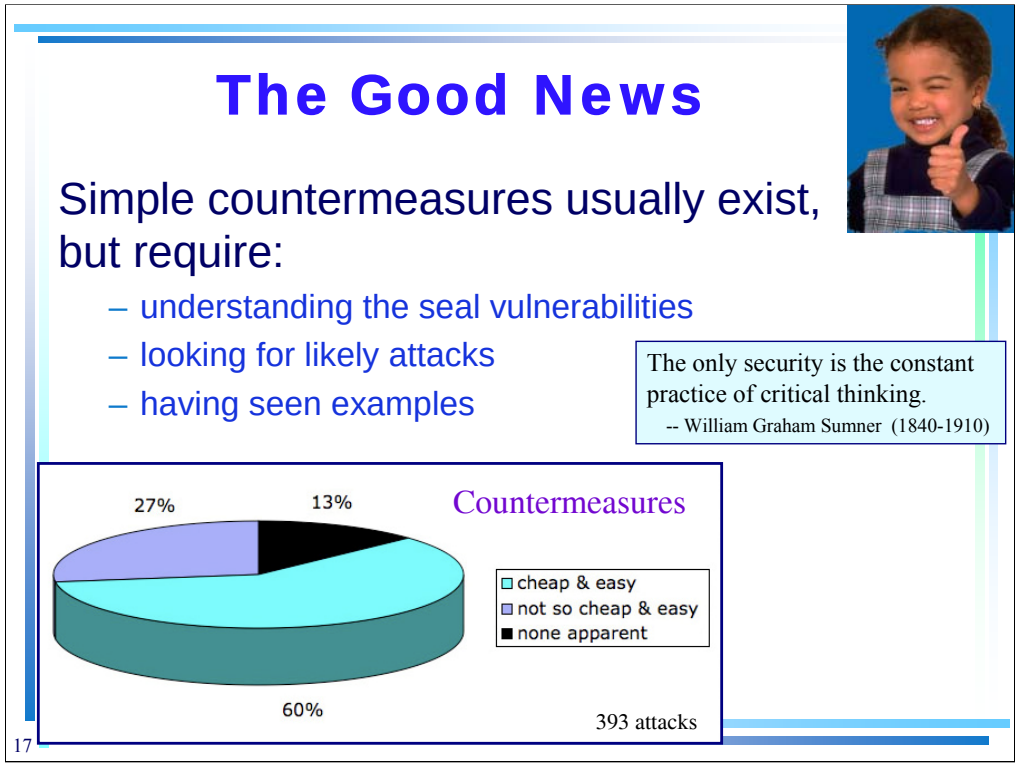


Результаты для 244 различных конструкций УИВ

параметр	**среднее значение**	**медиана**
время атаки	1,4 мин	43 сек
стоимость инструментов и вспомогательных материалов	$78	$5
предельная себестоимость атаки	62 цента	9 центов
время на разработку успешной атаки	2,3 ч	12 мин

“attack time” = time actually spent at the container

“время атаки” = время, фактическое поведенное у контейнера



ХОРОШИЕ НОВОСТИ

Обычно существуют простые меры противодействия, но для них требуется следующее:

- понимание уязвимых мест УИВ
- слежение за вероятными атаками
- знакомство с примерами

Единственный способ обезопасить себя — это постоянно мыслить критически.

-- Уильям Грэм Самнер (1840-1910)

Меры противодействия
- Дешево и просто
- Не так дешево и просто
- Неочевидно

393 атаки

The Good News (con't)

But better seals are also possible!

conventional seals:

They must store the fact that tampering has been detected until the seal can be inspected. But this "alarm condition" can be easily hidden or erased, or eliminated by making a fresh counterfeit seal.

anti-evidence seals:

At the start, when the seal is first installed, store information that tampering hasn't yet been detected. Erase this "anti-evidence" when tampering is detected. This leaves nothing for an adversary to hide, erase, or counterfeit!

18

ХОРОШИЕ НОВОСТИ (продолжение)

Но также возможно применение и более надежных УИВ!

обычные УИВ:

Они должны сохранять факт обнаружения вмешательства до тех пор, пока УИВ не будет проверено. Однако, это "тревожное состояние" можно легко скрыть или уничтожить, либо подменить это УИВ новым поддельным УИВ.

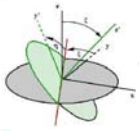
УИВ, не служащие доказательством:

При первом нанесении УИВ сохраните информацию о том, что вмешательство еще не было обнаружено. Удалите эту информацию при обнаружении вмешательства. После этого злоумышленнику будет нечего скрывать, удалять или подделывать!

Более 20 УИВ ЛЛНЛ, не служащих доказательством

- более надежное обеспечение безопасности
- не требуется засов
- не требуется инструмент для нанесения или снятия УИВ
- полностью пригодные для повторного применения, даже для механического типа
- УИВ можно помещать внутрь контейнера
- можно контролировать объемы или площади пространства, а не только двери
- можно автоматически узнать, проверил ли инспектор УИВ

Effective Vulnerability Assessments



- Perform a mental coordinate transformation and pretend to be the bad guys. (This is much harder than you might think.)

- Gleefully look for trouble, rather than seeking to reassure yourself that everything is fine.

- Be much more creative than your adversaries. They need only stumble upon 1 vulnerability, you have to worry about all of them.

It is sometimes expedient to forget who we are.
-- Publilius Syrus (~42 BC)

20

ЭФФЕКТИВНАЯ ОЦЕНКА УЯЗВИМОСТИ

- Представьте, что вы - злоумышленник. (Это намного сложнее, чем вы думаете).
- Постарайтесь найти нужное вам уязвимое место, вместо того, чтобы убедить себя, что все в порядке.
- Будьте намного более изобретательны, чем ваш противник. Им достаточно найти хотя бы одно уязвимое место – вам необходимо беспокоиться обо всех.

Иногда выгодно и вести себя недостойно.
Публий Сирус (~42 до н. э.)

VA Steps

1. Fully understand the device and how it is REALLY used. Talk to the low-level users.
2. Play with it.
3. **Brainstorm--anything goes!**
4. Play with it some more.

Nothing is like is seems, but everything is exactly like it is.
-- Yogi Berra (baseball player & coach)

21

ЭТАПЫ ОУ

1. Полностью изучить конструкцию устройства, принцип работы и то, как оно ФАКТИЧЕСКИ используется. Поговорить с конечными пользователями.
2. "Поиграть" с УИВ.
3. **Мозговой штурм – годятся любые версии!**
4. Еще "поиграть" с УИВ.

Ничто не таково, каково кажется,
но все в точности таково, каково оно есть.
-- Йоги Бера (бейсболист и тренер)

VA Steps

5. Edit & prioritize potential attacks.
6. Partially develop some attacks.
7. Determine feasibility of the attacks.
8. Devise countermeasures--more brainstorming!

You have to be careful if you don't know where you are going because you might not get there. -- Yogi Berra

22

ЭТАПЫ ОУ

5. Изучить и назначить приоритеты вероятным атакам.
6. Частично разработать некоторые атаки.
7. Определить выполнимость атак.
8. Придумать меры противодействия – провести дополнительный мозговой штурм!

Будьте внимательны, если не знаете,
куда идете, потому что можете туда и не придти.
-- Йоги Бера

VA Steps

9. Perfect attacks.
10. Demonstrate attacks.
11. Rigorously test attacks.
12. Rigorously test countermeasures.

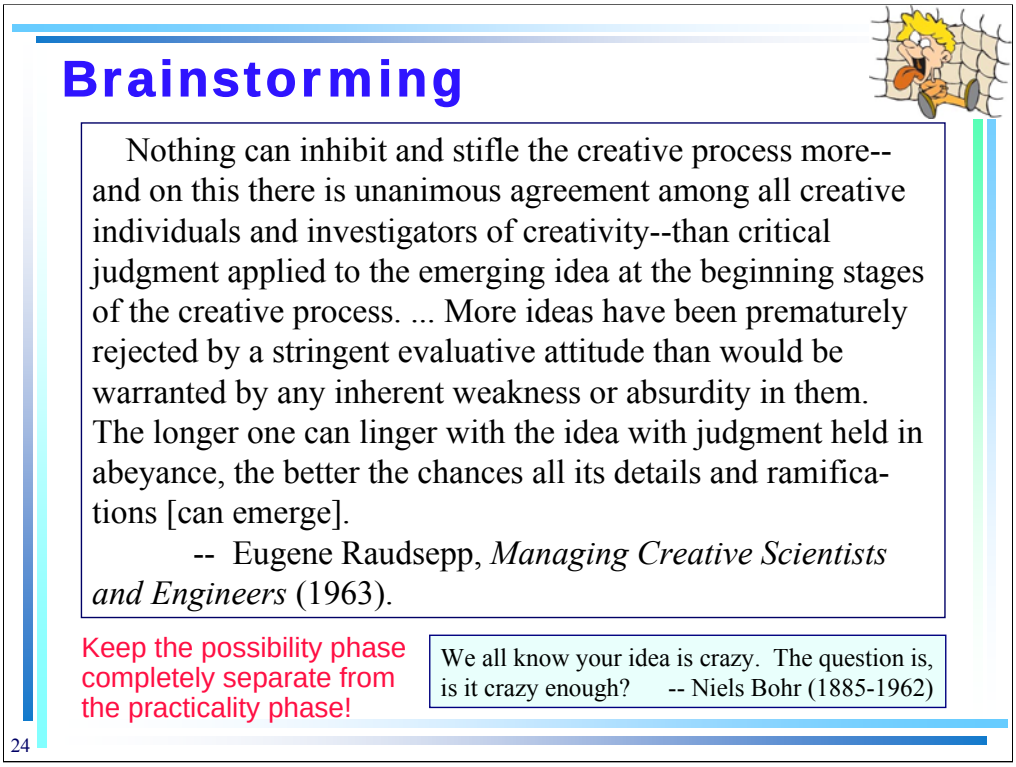
In theory there is no difference between theory and practice. In practice there is.
-- Yogi Berra

23

ЭТАПЫ ОУ

9. Отточить атаки.
10. Продемонстрировать атаки.
11. Тщательно испытать атаки.
12. Тщательно испытать меры противодействия.

В теории нет разницы между теорией и практикой.
На практике эта разница есть.
-- Йоги Бера



МОЗГОВОЙ ШТУРМ

Ничто не может в большей степени подавить и задушить творческий процесс, — и в этом единодушны все творческие личности и исследователи творчества, — чем критика, высказанная на начальных этапах процесса творчества в адрес рождающейся на свет идеи… Многие идеи были скоропалительно отвергнуты скорее по причине жесткой предварительной оценки, нежели по причине объективных внутренних слабостей или нелепостей, в них содержащихся. Чем дольше критик воздерживается от вынесения своего суждения, тем больше шансов на то, что станут ясны все подробности и детали идеи.

-- Юджин Родсепп, Руководство творческими учеными и инженерами (1963)

Не путайте "возможные действия" с "реально осуществимыми".

Все мы знаем, что ваша идея безумна.
Вопрос в том, достаточно ли она безумна?

-- Нильс Бор (1885-1962)

Realities of Creativity

Individuals are creative, not groups…

but the right group dynamics can energize & encourage individuals…

and a group is usually necessary to fully explore attacks & countermeasures.

A new idea is delicate. It can be killed by a sneer or a yawn; it can be stabbed to death by a joke or worried to death by a frown on the right person's brow.
-- Charles Brower

25

ПОДЛИННАЯ СУЩНОСТЬ ТВОРЧЕСКИХ СПОСОБНОСТЕЙ

Творчески созидательными являются отдельные люди, но не группы...

но правильная динамика группы может зарядить энергией и поддержать отдельных людей...

а для полного исследования всех аспектов атак и мер противодействия обычно требуется группа специалистов.

Новая идея — это тонкая вещь. Ее можно убить усмешкой или зевком; зарезать насмерть шуткой, или свести с ума нахмуренными бровями нужной персоны.

-- Чарльз Брауэр

VA Brainstorming Tips

Pay close attention to explicit or unstated assumptions, and to security or design features that are widely praised or admired. These are often the source of serious vulnerabilities.

Concentrate on the 2nd and 3rd best attacks or countermeasures. You are likely overlooking something that would make them the best solutions.

If there is widespread agreement about an attack or countermeasure, re-examine.

No authority figures!

If everybody is thinking alike,
then nobody is thinking.
-- George S. Patton (1885-1945)

26

РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ МОЗГОВОГО ШТУРМА ДЛЯ ОУ

Уделяйте особое внимание явно выраженным или несформулированным предположениям, а также элементам защиты или конструктивным особенностям, которые широко расхваливают или которыми восхищаются. Обычно эти элементы являются источниками серьезных уязвимых мест.

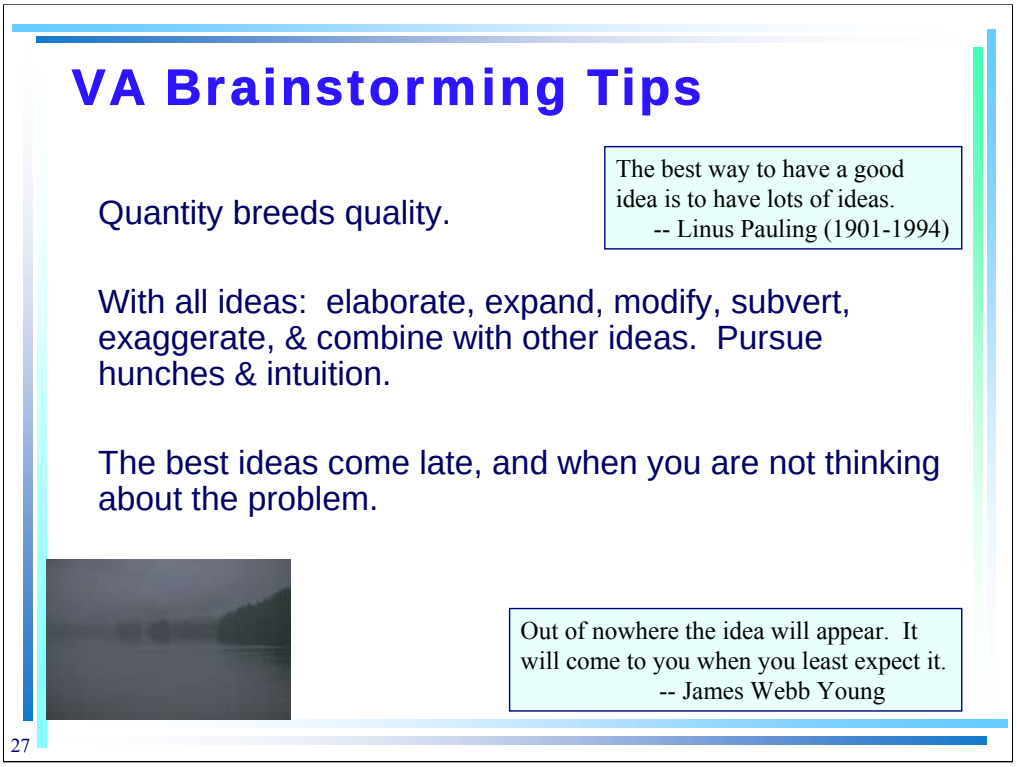
Сконцентрируйтесь на второй и третьей наилучшей атаке или мерах противодействия. Вы наверняка пропустили что-то, что могло бы сделать их наилучшими решениями.

Если по какой-либо атаке или мере противодействия имеется широко распространенное соглашение, повторно изучите эту атаку (меру противодействия).

Авторитетов нет!

Если все думают одинаково, значит, все вообще не думают.

-- Джордж С. Паттон (1885-1945)



Лучший способ получить хорошую идею —
получить множество идей.

-- Линус Паулинг (1901-1994)

РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ МОЗГОВОГО ШТУРМА ДЛЯ ОУ

Количество порождает качество.

Со всеми идеями: тщательно разрабатывать, подробно излагать, изменять, ниспровергать, преувеличивать и комбинировать с другими идеями. Пользуйтесь догадками и интуицией.

Лучшие идеи приходят последними, когда вы не думаете о проблеме.

Идея появится ниоткуда.
Она придет тогда, когда вы ее менее всего ждете.

-- Джеймс Уэбб Янг

VA Brainstorming Tips

Pursue what is interesting, controversial, contrarian, exciting, or silly.

Mentally remove some design features, or pretend the seal was made of different materials. Then consider the implications.

Develop and explore models, metaphors, & analogies.

Terminology constrains our thinking. Rename everything and re-examine.

There's a fine line between fishing and just standing on the shore like an idiot.
-- Steven Wright

28

РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ МОЗГОВОГО ШТУРМА ДЛЯ ОУ

Используйте все, что интересно, неоднозначно, противоречиво, увлекательно или глупо.

Удалите мысленно некоторые конструкционные характеристики, либо представьте, будто УИВ изготовлено из различных материалов. Затем рассмотрите последствия.

Разработайте и исследуйте модели, метафоры и аналогии. Терминология ограничивает наше мышление. Переименуйте все и заново изучите.

Лишь тонкая грань отделяет рыбную ловлю
от просто стояния на берегу как идиот.
-- Стивен Райт

Attributes of Effective VAs

1. No conflicts of interest or wishful thinking.
2. No “Shoot the Messenger” Syndrome. No retaliation or punishment against assessors, security personnel, or managers when vulnerabilities are inevitably found.

3. Rejection of a finding of zero vulnerabilities, or of VAs as some kind of “certification” or test to be passed.

4. No binary views of security. 0 1

I don’t want any yes-men around me. I want everyone to tell me the truth, even if it costs him his job. -- Samuel Goldwyn (1879-1974)

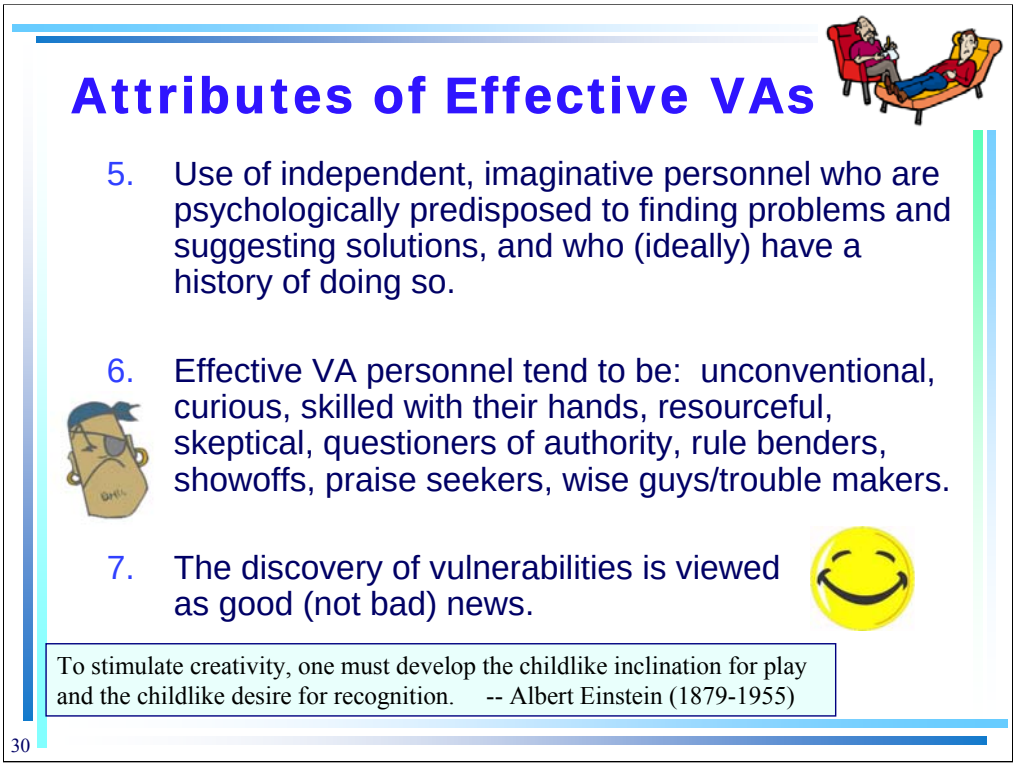
29

АТРИБУТЫ ЭФФЕКТИВНОЙ ОУ

1. Никаких конфликтов интересов или попыток выдать желаемое за действительное.
2. Никакого синдрома "убить гонца, принесшего плохие вести". Никакого возмездия или наказания для экспертов-консультантов, сотрудников охраны или руководителей при неизбежном обнаружении уязвимых мест.
3. Непринятие необнаружения уязвимых мест или ОУ некоторого рода "сертификации" или испытания, которое должно быть пройдено.
4. Никаких двойных точек зрения относительно безопасности.

Мне не нужны поддакивающие. Я хочу, чтобы каждый говорил мне правду, даже если это будет стоить ему работы.

-- Самюэль Голдуин (1879-1974)



АТРИБУТЫ ЭФФЕКТИВНОЙ ОУ

5. Использование независимого, одарённого творческим воображением персонала, психологически предрасположенного находить проблемы и предлагать их решения, который (в идеале) имеет опыт в таких вопросах.
6. Эффективные специалисты по ОУ обычно таковы: чуждые условностям, любопытные, с практическим опытом работы, изобретательные, скептически настроенные, не признающие авторитетов и правил, хвастуны, искатели похвал, критиканы/источники проблем.
7. Обнаружение уязвимых мест рассматривается как хорошие (не плохие) новости.

Для стимулирования творческих способностей следует развивать в себе детское влечение к играм и детское желание познания.

-- Альберт Эйнштейн (1879-1955)

Attributes of Effective VAs

8. Done early, iteratively, and periodically.
9. Done holistically, not by component, sub-system, function, or layer. (Attacks often occur at interfaces.)
10. No unrealistic time or budget constraints, or on what attacks or adversaries can be considered.
11. Done in context.

Honest criticism is hard to take, particularly from a relative, a friend, an acquaintance, or a stranger.
-- Franklin B. Jones

31

АТРИБУТЫ ЭФФЕКТИВНОЙ ОУ

8. Осуществляется на ранних этапах, несколько раз и на периодической основе.
9. Осуществляется целостно, не по элементам, подсистемам, функциям или слоям. (Атаки обычно происходят на границах между компонентами).
10. Никаких нереалистичных сроков или бюджетных ограничений, либо ограничений касательно того, какие атаки или каких противников можно рассматривать.
11. Осуществляется в контексте происходящего.

Трудно воспринимать честную критику, особенно от родственников, от друзей, от знакомых и от чужих людей.

-- Франклин Б. Джонс

Attributes of Effective VAs

12. No underestimation of the cleverness, knowledge, skills, dedication, or resources of adversaries.

13. The good guys don't get to define the problem, the bad guys do.

14. Simple, low-tech attacks are examined first.

I don't know a greater advantage than to appreciate the worth of an enemy.
-- Johann Wolfgang von Goethe (1749-1832)

32

АТРИБУТЫ ЭФФЕКТИВНОЙ ОУ

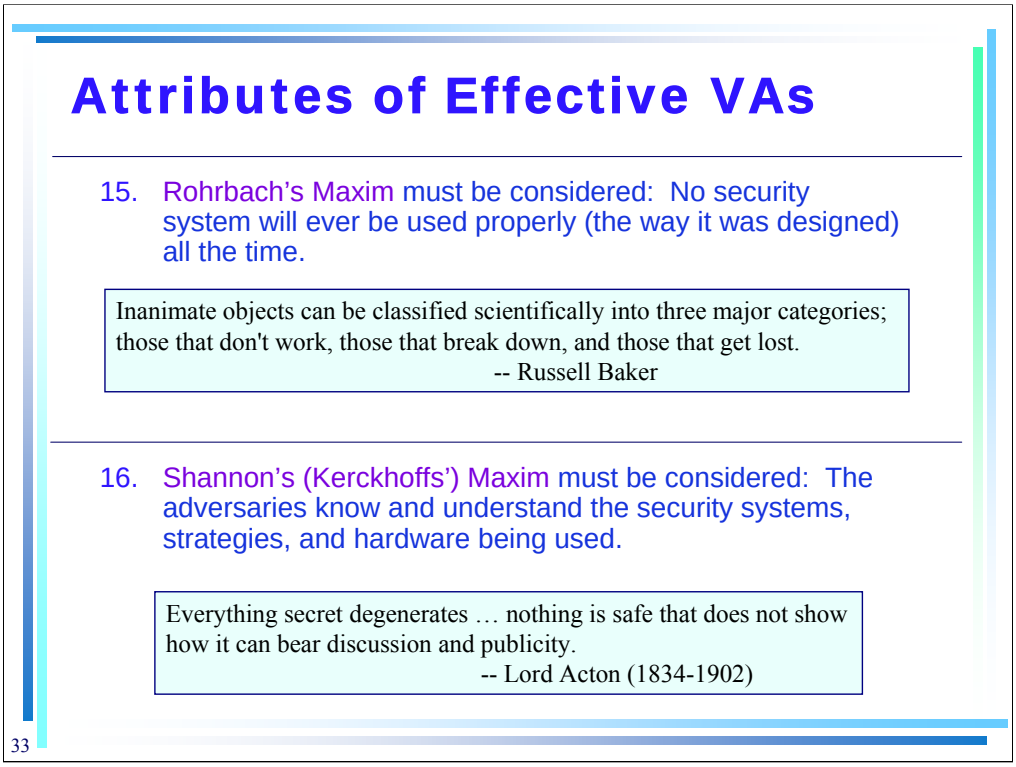
12. Никакой недооценки умения, знаний, навыков, самоотверженности или ресурсов противника.

13. Хорошие люди не принимаются за определение проблемы; злоумышленники – принимаются.

14. Сначала изучаются простые атаки с применением устаревших технологий.

Ничто так не способствует пользе дела,
как признание достоинств врага.

-- Иоганн Вольфганг Гете (1749-1832)



АТРИБУТЫ ЭФФЕКТИВНОЙ ОУ

15. Необходимо учитывать правило Рорбаха: Ни одну систему не используют правильно (т.е. именно так, для чего она предназначена) в течение всего времени.

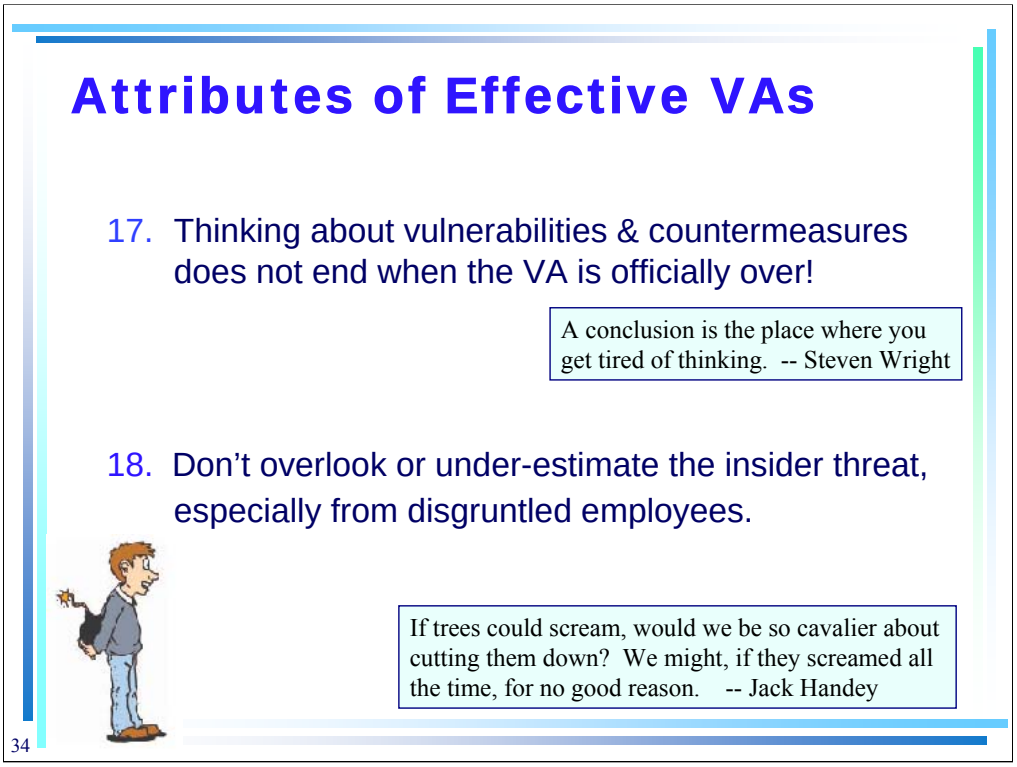
С научной точки зрения неодушевленные предметы могут быть классифицированы по трем категориям: неработающие, сломанные и потерянные.

-- Рассел Бейкер

16. Необходимо учитывать правило Шэннона (Керкхоффа): Противник знает и понимает используемые системы безопасности, стратегии и технические средства.

Все тайное становится явным… Все, что невозможно обсудить открыто, является небезопасным.

-- лорд Эктон (1934-1902)



АТРИБУТЫ ЭФФЕКТИВНОЙ ОУ

17. Об уязвимых местах и мерах противодействия нельзя забывать сразу как только ОУ официально будет завершена!

Выводы — это то место в тексте, где вы устали думать.

-- Стивен Райт

18. Не забывайте и не недооценивайте внутреннюю угрозу, особенно исходящую от недовольных сотрудников.

Если бы деревья умели кричать, то хватило бы у нас жестокости их рубить? Возможно, хватило бы, если бы они кричали все время и без особых на то причин.

-- Джек Хэнди

The VA Report

1. The VA Report should contain more countermeasures than are likely to be implemented.
2. The good features need to be praised.
3. Findings should be reported to the highest appropriate level without editing, interpretation, or censorship by middle managers.

The problem is not that there are problems. The problem is expecting otherwise and thinking that having problems is a problem. -- Theodore Rubin

35

ОТЧЁТ ПО РЕЗУЛЬТАТАМ ОУ

1. Отчет по результатам ОУ должен содержать большее число мер противодействия, чем предположительно будет внедрено.
2. Необходимо похвалить хорошие стороны.
3. Обнаруженные уязвимые места необходимо докладывать на самый высокий уровень руководства без редактирования, интерпретации или цензуры руководителями среднего звена.

Проблема не в том, что проблем нет. Проблема — это думать обратное и думать, что наличие проблем представляет проблему.

-- Теодор Рубин

The VA Report

4. The report should include:

+ identity & experience of the assessors
+ any conflict of interest
+ any *a priori* constraints
+ time & resources used
+ samples of attacked seals
+ details, videos, or demonstrations of the attacks
+ time, expertise, & resources required by an adversary to execute the attacks
+ possible countermeasures
+ a non-sensitive, statistical summary of the findings if the sponsor wishes to take public credit for the VA

I don't care what is written about me as long as it isn't true.
-- actress Katherine Hepburn (1907-2003)

36

ОТЧЁТ ПО РЕЗУЛЬТАТАМ ОУ

4. Отчет должен включать:
+ информацию об экспертах-консультантах с указанием опыта
+ наличие каких-либо конфликтов интересов
+ любые заранее заданные ограничения
+ требуемое время и ресурсы
+ образцы УИВ, подверженных атаке
+ подробное описание, видеозаписи или демонстрации атак
+ время, опыт и ресурсы, которыми должен обладать противник для осуществления атаки
+ возможные меры противодействия
+ несекретные статистические выводы по результатам ОУ, если заказчик хочет получить общественное доверие для ОУ

Мне нет дела до того, что обо мне пишут до тех пор, пока это не является правдой.

-- актриса Катерина Хепберн (1907-2003)