ОСОБЕННОСТИ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В АСУ ТП

Семен Корт

Senior Security Analyst, Critical Defense Infrastructure, Future Technologies

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ПРОБЛЕМАТИКА

Краткий обзор

ПРИЧИНЫ ИСПОЛЬЗОВАНИЯ СОВ

- Многие существующие системы содержат уязвимости, которые трудно обнаружить и устранить по техническим и экономическим причинам.
- Существующие системы, содержащие уязвимости, непросто заменить на «безопасные» системы
- Разработка «абсолютно безопасной системы» скорее всего невозможна
- Даже безопасные системы являются уязвимыми для некорректного использования со стороны авторизованных пользователей.

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Сетевые и хостовые системы

Сигнатурные системы и системы выявления аномалий

Системы с машинным обучением

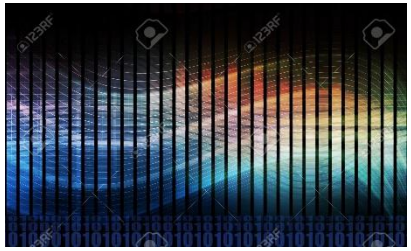
Системы предотвращения и обнаружения

ТРЕБОВАНИЯ К СОВ

- Эффективность работы в смысле точности обнаружения вторжений за приемлемое время.
- Минимальное вмешательство пользователя в работу системы.
- Учет характеристик защищаемой системы в виде параметров.
- Непрерывность работы. Непрерывность работы системы подразумевает ее возможности по переобучению без прекращения выполнения алгоритмов обнаружения.

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ. ПРОБЛЕМЫ

Ложные срабатывания



Противоречие между интеллектуальностью алгоритма обнаружения и производительностью системы

Противоречие между удобством администрирования и точностью обнаружения

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ ДЛЯ АСУ ТП С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

ПРИМЕР. СИСТЕМА УПРАВЛЕНИЯ ВОДОСНАБЖЕНИЕМ

Модель - трехуровневая нейронная сеть с обратным распространением.

Признаки, получаемые от протокола Modbus.

Оценки точности:

- ✓ атаки повтора (42.7% p_{fn}, 45.1% p_{fp});
- ✓ атаки Man-In-The-Middle (MITM) (0 − 8.9% p_{fn}, 0 − 6.2% p_{fp})
- ✓ атаки DoS (0 − 2.0% p_{fn}, 0 − 8.2% p_{fp})

Синтезированные кибератаки

- ✓ Отрицательный уровень воды
- ✓ Уровень воды выше максимально возможного
- ✓ Уровень воды выше максимально разрешенного
- ✓ Уровень воды ниже минимально возможного
- ✓ Уровень воды ниже минимально разрешенного
- ✓ Случайный уровень воды

Wei Gao, Thomas Morris, Bradley Reaves, Drew Richey «On SCADA control system command and response injection and intrusion detection», Proceedings of the 5th Annual Anti-Phishing Working Group eCrime Researchers Summit (eCrime). Dallas, TX, USA, 1–9., 2010

ПРИМЕР. СИСТЕМА УПРАВЛЕНИЯ ЭЛЕКТРОЭНЕРГИЕЙ

Модель - иммунные алгоритмы:

- CLONALG (без учителя)
- AIRS2Parallel (с учителем).

Оценки точности ($1 - p_{fp} - p_{fn}$):

- ✓ CLONALG: 80.1% - 99.7%
- ✓ AIRS2Parallel –82.1% - 98.7%

Yichi Zhang, LingfengWang,Weiqing Sun, R. C. Green, M. Alam «Distributed intrusion detection system in a multi-layer network architecture of smart grids», IEEE Transactions on Smart Grid 2, 4 (December 2011), 796–808, 2011

ПРИМЕР. СИСТЕМА УПРАВЛЕНИЯ ЭЛЕКТРОЭНЕРГИЕЙ

Модель - метод n-грамм:

Данные: системная нагрузка (мощность) для 6 энергетических сетевых шин.

Для внесения анормальностей в данные вносились редкие ошибки включая изменение знака, степени, цифры наблюдаемого значения

Оценки точности: ROC-кривые, демонстрирующие хороший процент обнаружения.

John Bigham, David Gamez, Ning Lu «Safeguarding SCADA systems with anomaly detection», Computer Network Security, Vladimir Gorodetsky, Leonard Popyack, and Victor Skormin (Eds.). Lecture Notes in Computer Science, Vol. 2776. 171–182, 2003

ПРИМЕР. СИСТЕМА УПРАВЛЕНИЯ ЭЛЕКТРОЭНЕРГИЕЙ

Модель - оценка предсказания состояний системы с помощью методов:

- Locally Optimum Unknown Direction (LOUD),
- Locally Optimum Estimated Direction (LOED)
- LOUD-Generalized Likelihood Ratio (LOUDGLR)
- LOED-Generalized Likelihood Ratio (LOED-GLR)

Данные: напряжение и фаза, измеряемая сенсорами

Оценки точности: наилучшими характеристиками обладает LOUDGLR: максимальное значение $(1- p_{fn}) = 95\%$

Qian He, Rick S. Blum «Smart grid monitoring for intrusion and fault detection with new locally optimum testing procedures», Proceedings of the International Conference on Acoustics, Speech and Signal Processing. Prague, Czech Republic, 3852–3855, 2011

ПРИМЕР. СИСТЕМА УПРАВЛЕНИЯ ЭЛЕКТРОЭНЕРГИЕЙ

Модель - нейросети (алгоритм обратного распространения и алгоритм Levenberg-Marquardt - метод затухающих наименьших квадратов для решения нелинейных проблем)

Признаки: количество IP адресов, средний интервал между пакетами, количество протоколов, количество флагов, количество пакетов нулевого размера, средний размер окна, средний размер пакета

Данные: окно, 5 наборов данных, каждый из 20000 пакетов, 100000 вторжений

искусственно сгенерировано 100000 вторжений (Metasploit, Nessus, Nmap)

Ondrej Linda, Todd Vollmer, Milos Manic «Neural network based intrusion detection system for critical infrastructures» Proceedings of the International Joint Conference on Neural Networks. Atlanta, GA, USA, 1827–1834, 2009.

ПРИМЕР. СИСТЕМА ДОСТУПА К МЕДИЦИНСКОЙ ИНФОРМАЦИИ

Модель: алгоритм классификации, основанной на ассоциации (Classification Based on Association, CBA):

- генератор правил (Rule Generator, CBA-RG)
- построитель классификации (Classifier Builder, CBA-CB).

Данные с мобильных устройств о доступе: местоположение и субъект доступа.

Оценка точности работы системы не в работе не приводилась.

B. Asfaw, D. Bekele, B. Eshete, A. Villafiorita, K. Weldemariam «Host-based anomaly detection for pervasive medical systems», Proceedings of the 5th International Conference on Risks and Security of Internet and Systems. Montreal, QC, Canada, 1–8, 2010

ПРИМЕР. СИСТЕМА ДОСТУПА К МЕДИЦИНСКОЙ ИНФОРМАЦИИ

Модель - частичное обучение для анализа серии событий.

Данные: ID сенсора, начало серии, длительность.

Признаки:

- наименьшей общей последовательности (LCS),
- количестве общих событий, не принадлежащих LCS,
- начало серии,
- длительность серии.

Kyungseo Park, Yong Lin, Vangelis Metsis, Zhengyi Le, Fillia Makedon «Abnormal human behavioral pattern detection in assisted living environments», Proceedings of the 3rd International Conference on Pervasive Technologies Related to Assistive Environments. 9:1–9:8, 2010

ТРЕБОВАНИЯ ФСТЭК К СОВ

2012 год. Профили защиты

- 6 классов защиты (Самый низкий класс - 6, самый высокий – 1)
- 3, 2 и 1 класс защиты, ИС, в которых обрабатывается информация, содержащая государственную тайну. Профили защиты для уровней 1 – 3 в открытом доступе отсутствуют
- В документах очень хорошо и подробно описаны гарантии разработки, механизмы безопасности и механизмы собственной защиты СОВ, а также права пользователей системы. Отдельно рассматриваются вопросы безопасного обновления базы знаний СОВ.

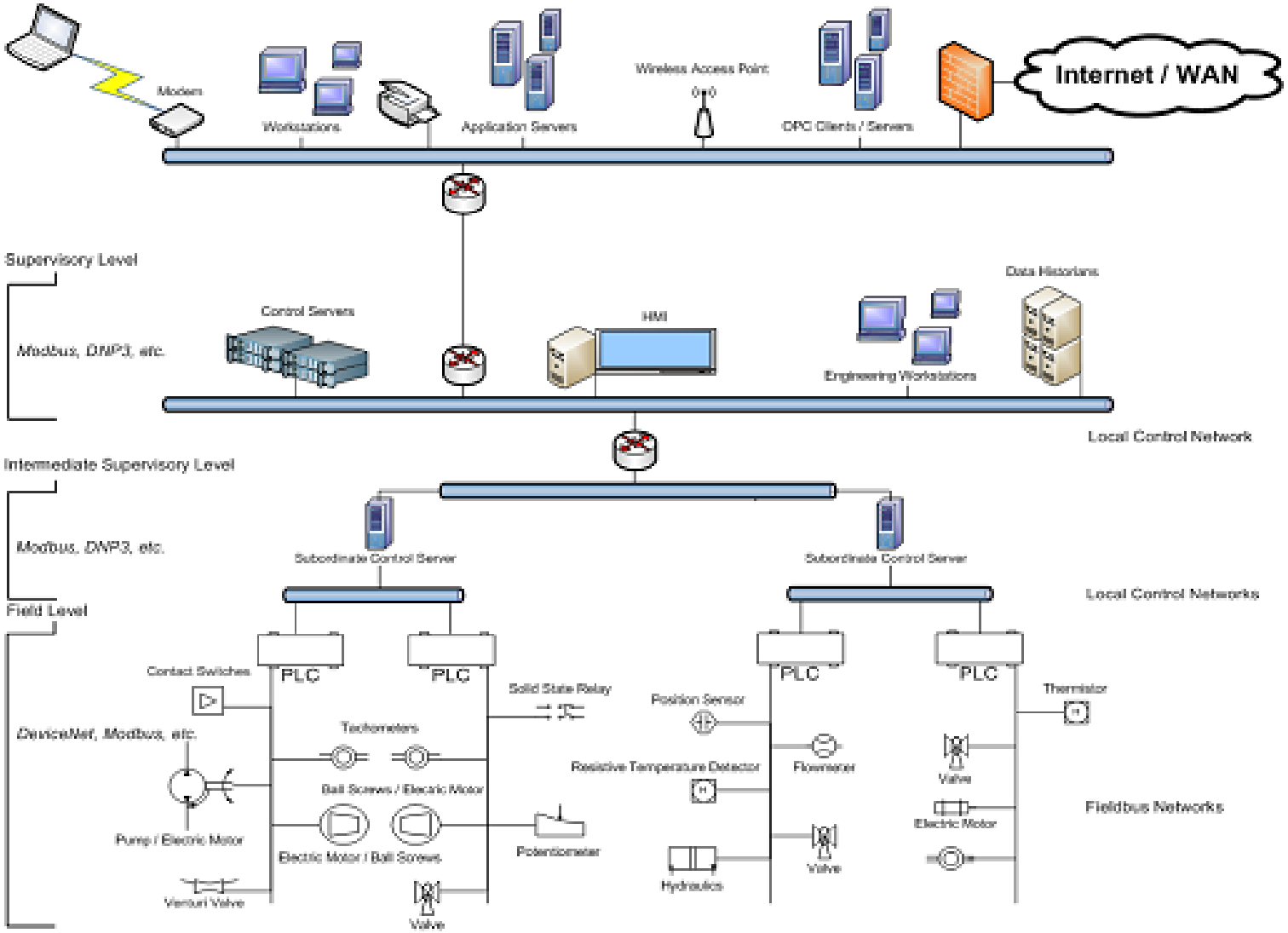
ОСОБЕННОСТИ АСУ ТП С ТОЧКИ ЗРЕНИЯ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

31 ПРИКАЗ ФСТЭК

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в автоматизированной системе управления, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на автоматизированную систему управления и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

- ✓ АСУ ТП класса защищенности 1 СОВ не ниже 3 класса
- ✓ АСУ ТП класса защищенности 2 СОВ не ниже 4 класса
- ✓ АСУ класса защищенности ТП 3 СОВ не ниже 5 класса

СХЕМА ВКЛЮЧЕНИЯ СИСТЕМЫ АСУ ТП



ОБЪЕКТЫ, КОТОРЫЕ МОГУТ ЯВЛЯТЬСЯ ЦЕЛЬЮ АТАКИ:

1) Канал связи между сенсорами, контроллером и HMI, определяющий, что видит оператор (View);

2) Канал связи между приводом, контроллером и HMI, определяющий, что посылается на привод (Control);

3) Модификация настроек (граничных значений) сенсоров с использованием атаки на модуль хранения настроек оборудования

4) Модификация настроек приводов (граничных значений) приводов с использованием атаки на модуль хранения настроек оборудования;

5) Модификация технологического процесса

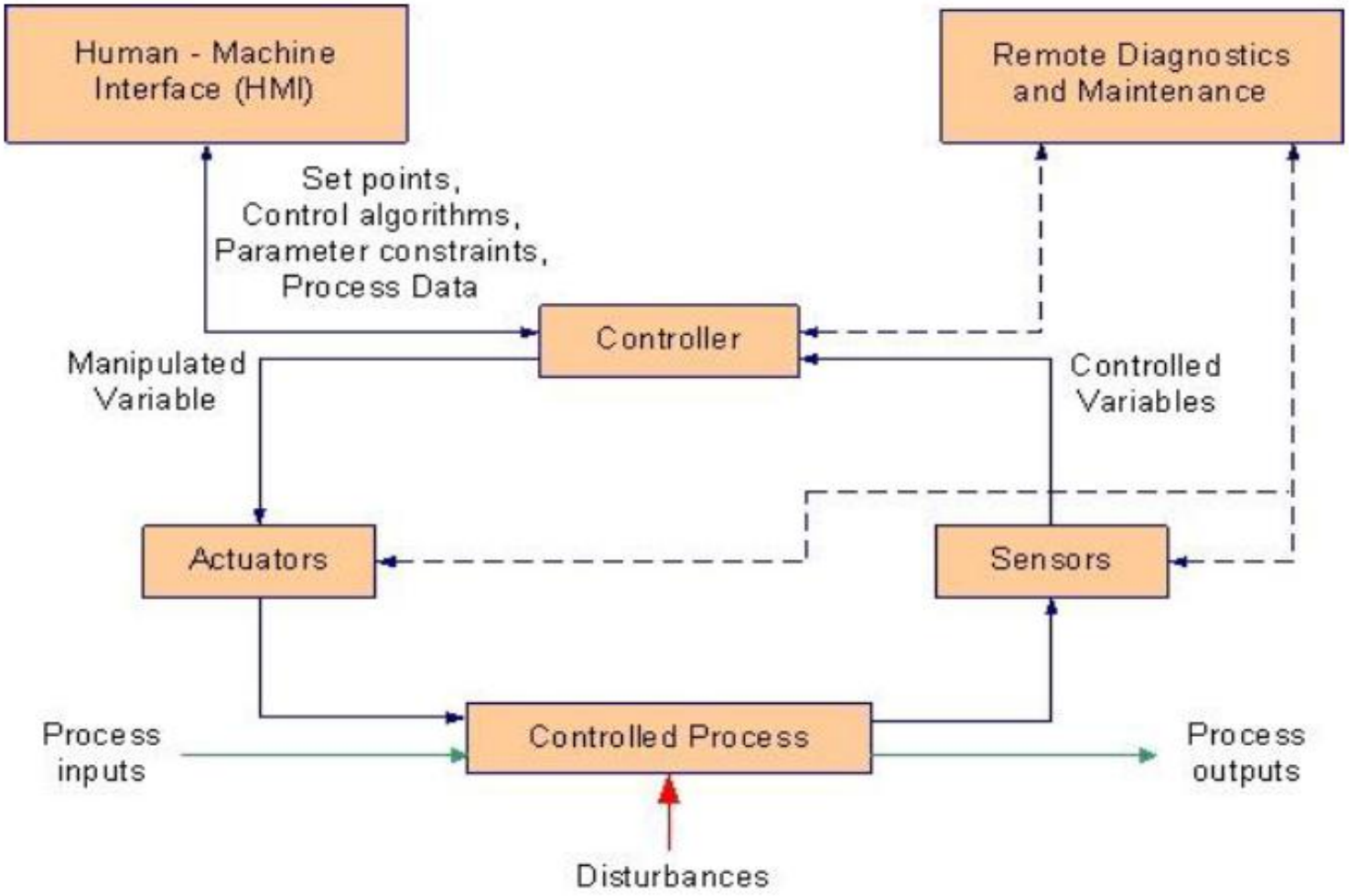
УГРОЗЫ АСУ ТП

	Потеря доступности (временная)	Потеря ресурса (постоянная)	Манипуляция
Контроль	DoC	LoC	MoC
Просмотр	DoV	LoV	MoV

D – deny, L – lost, M – modify, C – control, V - view

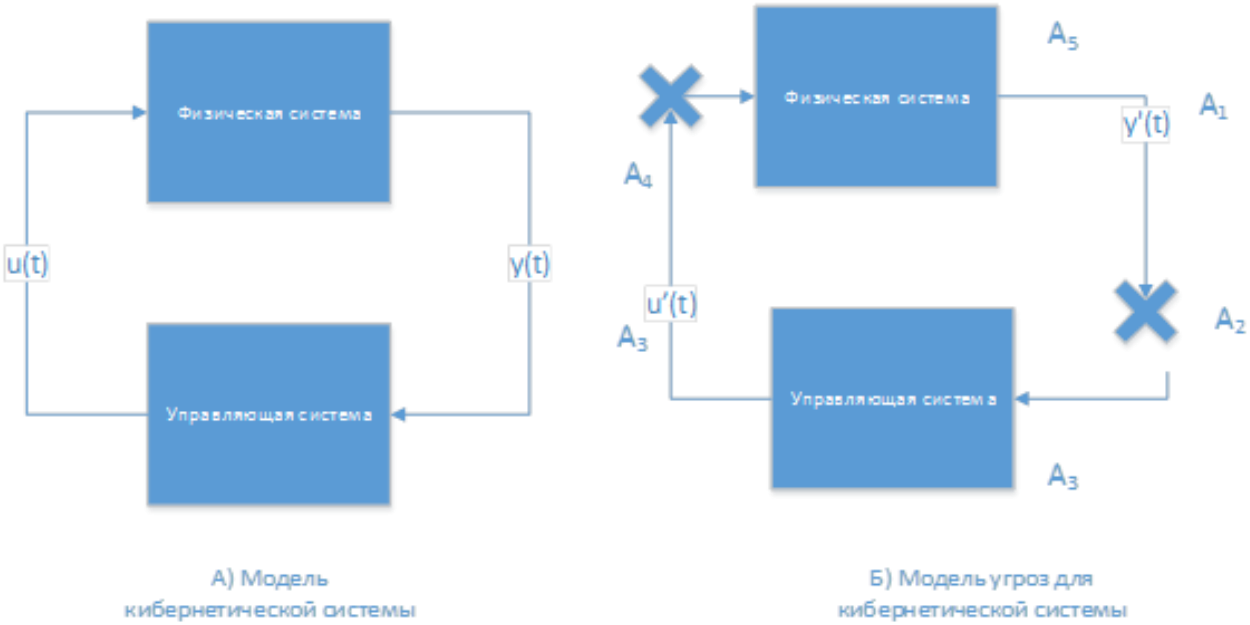
KASPERSKY lab

ОПЕРАЦИИ В АСУ ТП



KASPERSKY lab

МОДЕЛЬ УПРАВЛЯЮЩЕЙ СИСТЕМЫ



u(t) - управляющий сигнал

y(t) - состояние контролируемого объекта

A_1, A_3 – нарушитель искажает информацию отправляемую на (от) привод (сенсор).

A_2, A_4 - DoS атаки на передачу информации на (от) привода (сенсора).

A_5 – атака непосредственно на привод (сенсор).

ТИПОВЫЕ СЕТЕВЫЕ АТАКИ НА СИСТЕМЫ АСУ ТП

DoS

Атаки на уязвимости протоколов

сетевого, транспортного и прикладного уровня

Man in the Middle

Сканирование системы

Атаки на устройства

ТИПОВЫЕ АТАКИ В СИСТЕМАХ АСУ ТП

Атака	Предусловия	Этап вторжения	Угроза
DoS	Сетевое взаимодействие с атакуемым устройством	2, 3	DoC, DoV, LoC, LoV
Атаки уязвимости протоколов	Сетевое взаимодействие с атакуемым устройством	2, 3	DoC, DoV, LoC, LoV, MoC, MoV
Man in the Middle	физический доступ к сетевой инфраструктуре успех атаки на оконечное устройство	3	MoC, MoV
Сканирование	Сетевое взаимодействие с атакуемым устройством	1	
Атаки на устройства	Сетевое взаимодействие с атакуемым устройством	2	MoC, MoV

Этапы вторжения

1 Сканирование

2 Атака

3 Использование

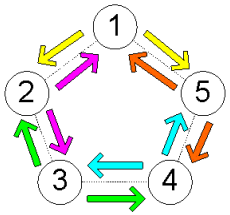
KASPERSKY lab

ОСОБЕННОСТИ АСУ ТП

- доступность является важным свойством
- вычислительные процессы имеют влияние на процессы физического мира
- оконечные устройства имеют ограниченные вычислительные ресурсы
- часто используемые сетевые протоколы являются пропреитарными.
- физическая безопасность системы обычно обеспечена

ОСОБЕННОСТИ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В АСУ ТП

Замкнутые цепи управления



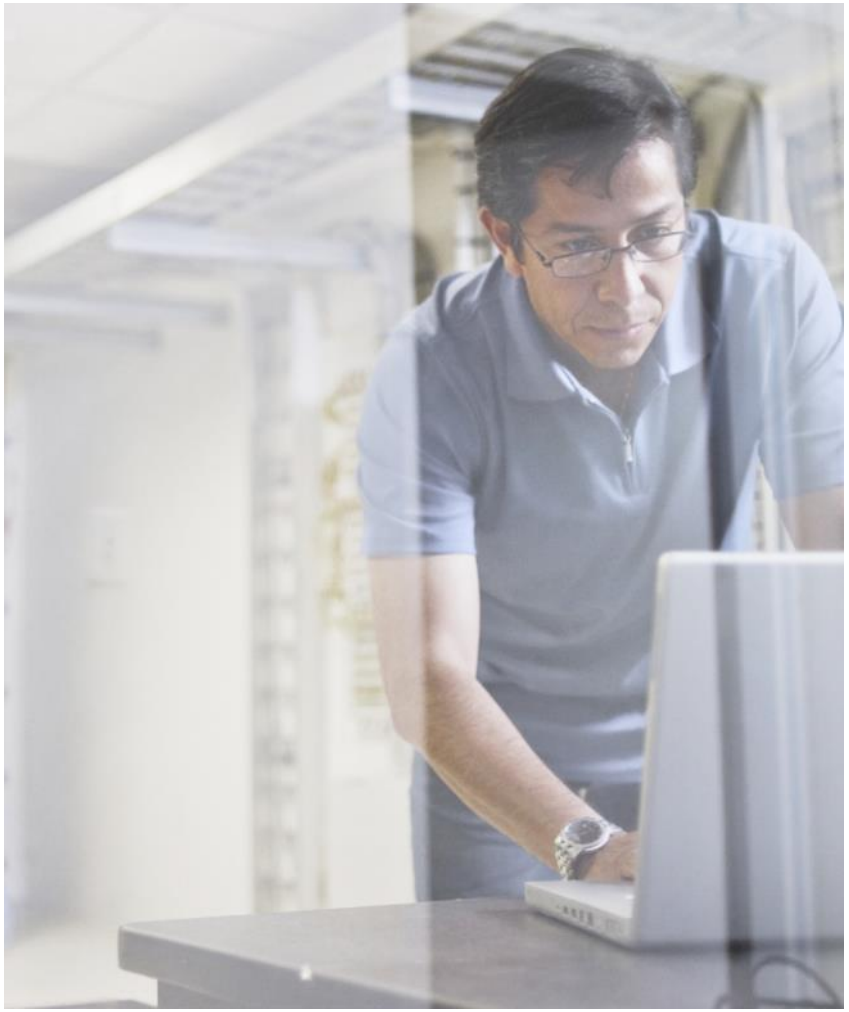
Статичная топология

Простые сетевые протоколы

Мониторинг физических процессов.

Высокие риски

ОСОБЕННОСТИ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В АСУ ТП



Общие положения

- ✓ Учет предметной области систем АСУ ТП помогает упростить задачу обнаружения вторжений за счет введения ограничений на поведение системы
- ✓ Упрощение задачи обнаружения вторжений позволяет избавится от недостатков соответствующих методов обнаружения
- ✓ Оконечные устройства теоретически имеют ограниченные вычислительные ресурсы. Эта особенность приводит к тому, что целесообразным решением является использование сетевых устройств.

ПОДХОД К РЕАЛИЗАЦИИ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В АСУ ТП

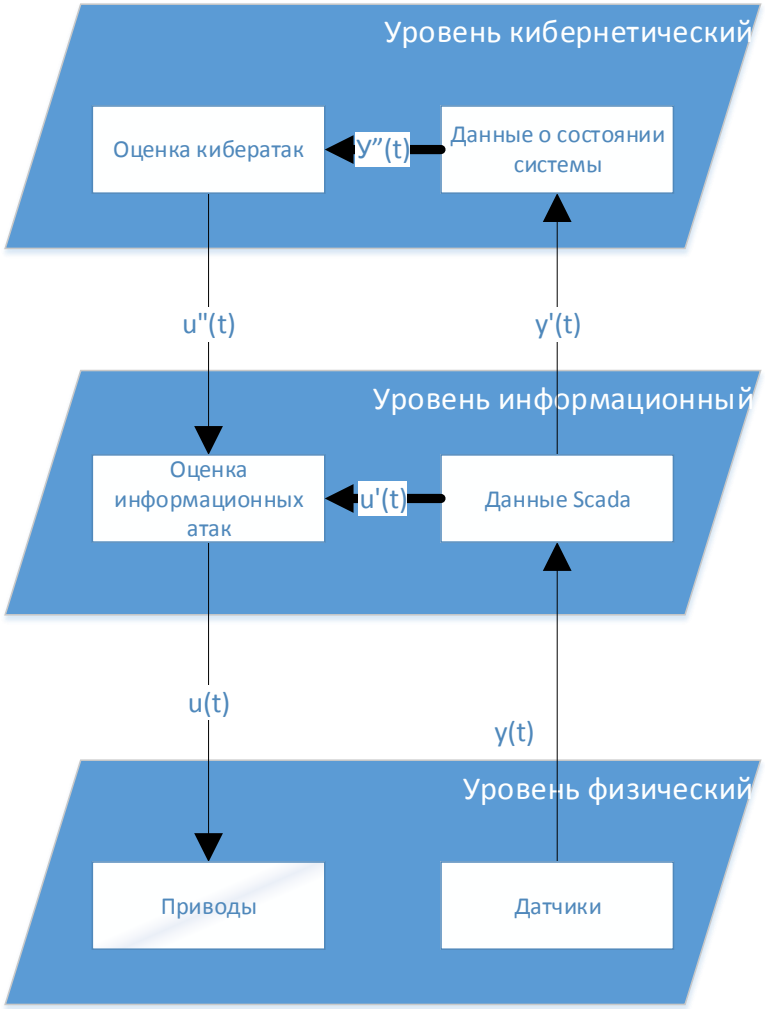
ИЕРАРХИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ КИБЕРСИСТЕМЫ

1) Атаки на информационном уровне и атаки на кибернетическом уровне следует выявлять раздельно.

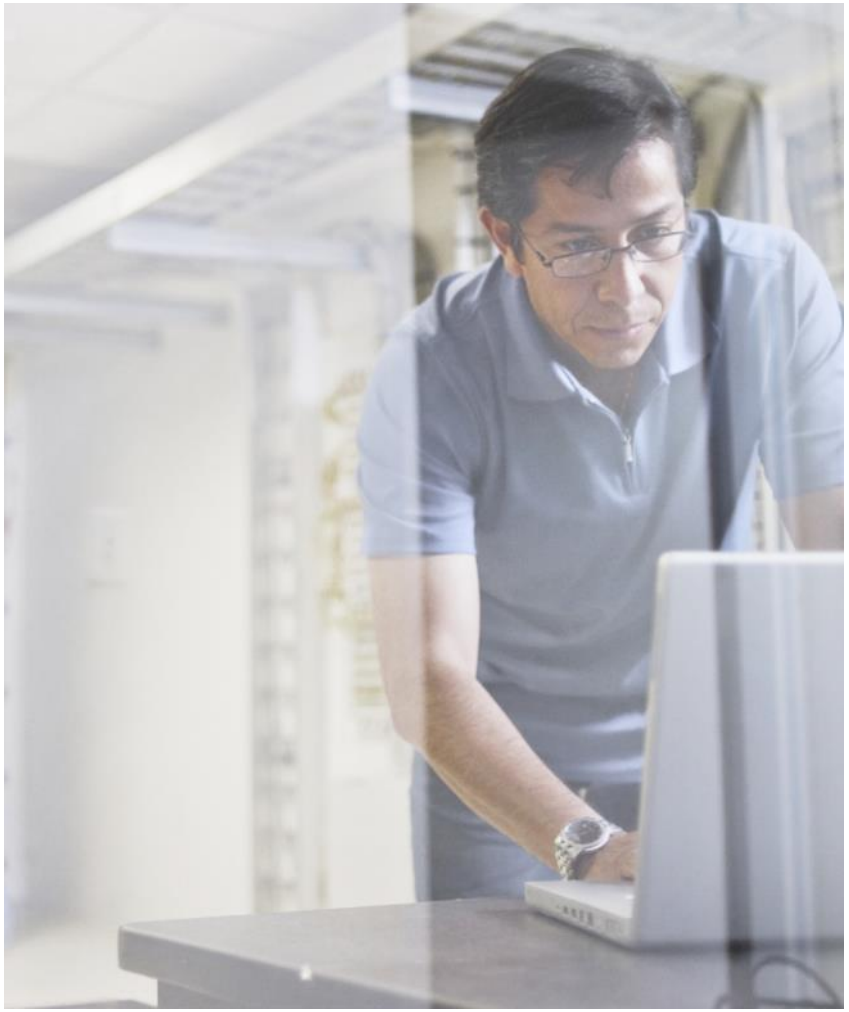
2) Атаки на информационном уровне можно выявлять для широкого круга систем.

3) Решатель объединяет результаты выявления информационных атак и кибератак.

4) В случае отсутствия информации о протоколе прикладного уровня, следует выполнять оценку на основании интегральных характеристик трафика.



ВЫЯВЛЕНИЕ АТАК НА ИНФОРМАЦИОННОМ УРОВНЕ



1) Типовые атаки на стек TCP\IP

2) Атаки на открытые промышленные протоколы, основанные на отклонении трафика от спецификации

3) Выявление аномалий статистик трафика для закрытых промышленных протоколов

KASPERSKY lab

ПРОТОКОЛ MODBUS

порт TCP 502

связь HMI(master) и PLC(slave), в виде (Master IP, Slave IP)

Поля:

- Transaction Identifier - 2 байта,
- Protocol Identifier - 2 байта (значение 0)
- Unit Identifier – 1 байт, используется для адресации slave

Request: отправляется master к slave для начала транзакции

Response: сообщение ответа, отправляемое slave к master

Indication: сообщение запроса, отправляемое slave к master

Confirmation: сообщение ответа, отправляемое master к slave

Transaction Identifier	Protocol Identifier	Length Field	Unit Identifier	PDU (data)	Checksum

MODBUS PDU

Function Code – (1 байт). Определено 19 из 127 возможных значений кода функции. (1, 2, 3, 4) – операция чтения, (5) – операция записи.

Payload – (переменный размер, до 252 байтов) содержит параметры, специфичные для кода функции. Read (Function Codes 1, 2, 3, 4) нагрузка состоит из двух полей: Reference Number и Bit/Word Count. Reference Number определяет адрес памяти, с которого начинается чтение.

Bit/Word Count определяет количество считываемых объектов.

В ответе содержится 2 поля - Byte Count и Data.

Сообщение Write кроме области памяти содержит значения, которые должны быть записаны.

ПОДХОД К ПОСТРОЕНИЮ ПРАВИЛ

- для описания поведения следует использовать набор конечных автоматов, включающий по 1 автомату на взаимодействие master – slave.
- в соответствии со спецификациями протокола Modbus можно описать нормальное поведение конечного автомата, т.е. разрешенные функции перехода для любого состояния
- любые отклонения от нормального поведения можно считать аномалиями и признаками атаки.

НОРМАЛЬНЫЕ ПЕРЕХОДЫ ДЛЯ MODBUS

Для каждого запроса должен быть отклик, изменяющий состояние взаимодействие по протоколу.

Если в некотором состоянии предыдущий запрос дублируется, то состояние не изменяется

Если в некотором состоянии предыдущий отклик дублируется, то состояние не изменяется

Запросы и отклики должны быть корректно сформированы в соответствии с правилами RFC для протокола Modbus

УТОЧНЕНИЕ АВТОМАТА В ЗАВИСИМОСТИ ОТ СИСТЕМЫ

HMI периодически опрашивает PLC с использованием одинаковых команд

конечный автомат, построенный для протокола в соответствии с RFC может быть уточнен для конкретной системы

для того, чтобы построить один конечный автомат требуется около 100 сообщений обмена между адресатами

аномалия может быть выявлена как неожиданный переход или некорректное сообщение

переходы полученного автомата могут оцениваться с использованием вероятностей, а отклонения – с использованием цепочек Маркова

АНАЛИЗ ТРАФИКА В СИСТЕМАХ АСУ ТП. ПРИМЕРЫ

Проверка	Атрибуты	Оценка	Интерпретация
Роль хоста в сети при нормальном поведении	Количество соединений Количество портов источника Количество портов приемника	Отклонение параметров	Изменение роли хоста
Оценка разброса адресов приемников	Оценивается энтропия IP адресов назначения	Рост энтропии	Сканирование
Характеристика сетевого соединения	Среднее количество пакетов для потока	Малое значение	Отказ в обслуживании
Характеристика сетевого соединения	Размер пакетов	Отклонение от распределения	Изменение сервиса на хосте

KASPERSKY lab

ВЫЯВЛЕНИЕ КИБЕРАТАК

1) Возможно для известных промышленных протоколов.
2) Возможно с использованием методов машинного обучения

- Определение типов переменных на основе наблюдения за системой в процессе обучения: управляющие, оповещающие, измерительные, состояния.
- В соответствии с группой можно сделать предсказания их будущего поведения: изменение постоянное и равномерное во времени, дискретные, константные.
- Выявление отклонения поведения

3) Возможно на основании информации о нормальном процессе для защищаемого объекта

КИБЕРФИЗИЧЕСКАЯ СИСТЕМА

$x_{k+1} = Ax_k + Bu_k$, $y_k = Cx_k + e_k$

$x_k \in R^n$ – вектор состояния,

$u_k \in R^n$ - вектор управляющего воздействия

$y_k \in R^p$ - вектор выхода

$e_k \in R^p$ - вектор атак

$A \in R^{n \times n}$, - связь состояний

$C \in R^{p \times n}$

Подделка нарушителем сигнала: $y' \neq y$, $u' \neq u$

DOS атака $y' = -y$, $u' = -u$

$K \subseteq \{1, \ldots, p+n\}$ – множество атакуемых сенсоров и контроллеров

Functional Safety: $\exists\{x_i\}: X_{min_i} \leq x_i \leq X_{max_i}$

(A, B, C), $\{u_k\}$ - выполняется $\{x_i\}$

LET'S TALK?

Kaspersky Lab ZAO
10/1, 1st Volokolamsky Proezd,
Moscow, 123060, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com