Programowanie Defensywne

Modelowanie zagrożeń

Arkadiusz Chrobot

Katedra Systemów Informatycznych

18 kwietnia 2024

Plan

Wprowadzenie

Zagadnienie modelowania zagrożeń zostało już zasygnalizowane na pierwszym wykładzie. Dziś zajmiemy się nim bardziej szczegółowo. W ujęciu ogólnym czynność ta zmierza do uzyskania odpowiedzi na następujące pytania:

1. Co opracowujemy?
2. Jakie przeciwności mogą się pojawić?
3. Jak poradzimy sobie z przeciwnościami?
4. Czy nasze działania są skuteczne?

W przypadku projektu informatycznego modelowanie zagrożeń ma na celu osiągnięcie pożądanego poziomu zabezpieczeń tworzonego oprogramowania, zanim trafi ono do środowiska produkcyjnego. Jest to zatem część *aktywnego*, a nie *reaktywnego* zapewniania bezpieczeństwa.

Wprowadzenie

Zadając pierwsze pytanie ze slajdu nr 3 chcemy poznać wymagania (w szczególności przypadki użycia), projekt oprogramowania, zastosowane w nim komponenty i interakcje między nimi.
Odpowiedź na drugie pytanie pozwala odkryć potencjalne problemy, a na trzecie znaleźć środki zaradcze (ang. *countermeasures*).
Czwarte pytanie ma służyć retrospekcji, czyli sprawdzeniu na ile dobrze udało się nam zidentyfikować zagrożenia i przeanalizować możliwości zapobiegania im, a także odkryć ewentualne braki.
Proces modelowania zagrożeń ma charakter iteracyjny i powinien być powtarzany tak długo, jak długo pozostają nierozwiązane kwestie.

Wprowadzenie

Bardziej precyzyjny opis modelowania zagrożeń obejmuje następujące kroki:

1. Pozyskanie lub przygotowanie modelu systemu.
2. Identyfikacja aktywów (ang. *assets*), czyli zasobów, które wymagają ochrony.
3. Przeszukanie modelu systemu, analiza jego komponentów celem określenia potencjalnych powierzchni ataku (ang. *attack surface*) oraz granic zaufania (ang. *trust boundaries*), czyli interfejsów pośredniczących między bardziej i mniej zaufanymi komponentami w systemie.
4. Analiza odkrytych zagrożeń (realne i hipotetyczne).
5. Hierarchizacja zagrożeń.
6. Proponowanie środków zaradczych zmniejszających ryzyko wystąpienia najbardziej krytycznych zagrożeń.
7. Iteracyjne dodawanie środków zaradczych z uwzględnieniem kosztów.
8. Weryfikacja skuteczności środków zaradczych.

Model systemu

Model systemu stosowany do identyfikacji zagrożeń może mieć charakter zarówno formalny, np. diagramy przepływu danych (ang. *Data Flow Diagram* — DFD), diagramy UML, lub nieformalny model graficzny. Jego charakter nie jest ważny, poza tym że ma przedstawiać abstrakcję systemu. Istotna jest jego szczegółowość. Zbyt wiele detali powoduje zwiększenie kosztów analizy i wydłuża niepotrzebnie jej czas. Z kolei mała liczba szczegółów prowadzi do szybkiego zakończenia procesu, ale powoduje, że istotne kwestie mogą zostać pominięte. Dobry model systemu pozwala odkryć zależności między przetwarzanymi danymi i je pogrupować. Pozwala zidentyfikować procesy i ich interakcje, a także kanały komunikacyjne występujące między komponentami.

Aktywa

Aktywa są elementami systemu, które powinny podlegać ochronie. Należą do nich, między innymi, dane, urządzenia peryferyjne, moc obliczeniowa, miejsce w pamięci operacyjnej, pasmo komunikacyjne. W ramach modelowania zagrożeń należy podjąć decyzję, które z aktywów są najbardziej priorytetowe. Zastosowanie w dużym systemie ochrony wobec wszystkich może okazać się nie tylko nieekonomiczne, ale wręcz niewykonalne. Najlepiej w takim wypadku zastosować prostą metodę polegającą na przypisaniu każdemu zasobowi miary, jaką jest ... rozmiar koszulki. Najważniejsze zasoby powinny zostać oznaczone rozmiarem L. Te, które są tylko trochę mniej cenne mogą być zaznaczone jako M. Najmniej cenne, ale nadal istotne aktywa trzeba oznaczyć jako S. Oznaczenie XL należy stosować jedynie dla aktywów o znaczeniu krytycznym.

Decyzje odnośnie do stosowanych zabezpieczeń należy zacząć od aktywów L, a następnie zastosować *oportunistyczną ochronę* zasobów M. Polega ona na stosowaniu działań, które nie są kosztowne, ale przynoszą dobre rezultaty.

Aktywa

Analizując ryzyko dla aktywów, można połączyć je w grupy, jeśli posiadają one podobną charakterystykę. Należy jednak zachować ostrożność, aby nie pominąć szczegółów, którymi mogą cechować się poszczególne aktywa, a które w wyniku połączenia można utracić.
Analiza ryzyka uwzględnia triadę CIA, czyli polega na ocenie potencjalnych strat spowodowanych wyciekiem danych, nieuprawnioną ich modyfikacją lub utratą do nich dostępu (np. w wyniku zniszczenia).
Dokonując analizy należy rozpatrzeć różne punkty widzenia. Przykładowo, inaczej będzie oceniana utrata danych o obrotach firmy przez szeregowych pracowników, a inaczej przez kierownictwo, czy klientów.
Zwróćmy też uwagę, że ryzyko związane z aktywami może ulec zmianie, w zależności od tego, czy rozpatrujemy je indywidualnie, czy zbiorczo. Przykładowo, wyciek informacji o stosowanych komponentach aplikacji internetowej może być małym ryzykiem, ale w połączeniu z danymi o ich wersji może być już dużym.

Aktywa

Analiza ryzyka związanego z aktywami powinna być skoncentrowana na identyfikacji i minimalizacji powierzchni ataku (ang. *attack surface*). Jeśli np. wiele komponentów oprogramowania ma bezpośredni kontakt z Internetem, to należy się zastanowić, czy nie lepiej byłoby kierować ruch sieciowy do nich poprzez pośrednika (ang. *proxy*), który odfiltrowywałby niebezpieczne dane pochodzące z zewnątrz. Należy pamiętać, że poszczególne powierzchnie, czy nawet *wektory ataku* mogą być związane ze światem fizycznym, nie zaś informacyjnym.

Granice zaufania

Mając zidentyfikowane aktywa można przystąpić do określania granic zaufania, czyli miejsc w systemie, gdzie dochodzi do interakcji między komponentami o mniejszych uprawnieniach z komponentami o większych uprawnieniach. W każdym złożonym systemie informatycznym takie granice występują, bo są niezbędne do jego działania. Ich prawidłowe zaprojektowanie jest częścią szerszego zagadnienia znanego jako wielopoziomowa polityka bezpieczeństwa (ang. *Multilevel Security Policy.*). Jego podstawą jest model Bella-LaPaduli składający się z dwóch reguł:

prosta własność bezpieczeństwa — żaden proces nie może odczytywać danych z wyższego poziomu uprzywilejowania

własność * — żaden proces nie może zapisywać danych do niższego poziomu uprzywilejowania.

Jest to model idealny zabezpieczeń, w rzeczywistości nieosiągalny. Jednak jest on dobrym punktem wyjścia do dyskusji nad bezpieczeństwem granic zaufania.

Granice zaufania

Mając określone aktywa i granice zaufania można przystąpić do identyfikacji zagrożeń dla całego systemu. Najłatwiej jest znaleźć te, które dotyczą tych dwóch elementów, ale są również takie, które mają charakter pośredni — same w sobie nie wydają się być groźne, ale ich kombinacja może okazać się katastrofalna. Dlatego należy identyfikacje zagrożeń prowadzić na różnych poziomach szczegółowości.

Zastosowanie STRIDE

Wspomniana na pierwszym wykładzie taksonomia STRIDE jest dosyć często interpretowana jako metodologia modelowania zagrożeń. W rzeczywistości jest to klasyfikacja zagrożeń, która stanowi listę kontrolną, pozwalającą znaleźć i zidentyfikować zagrożenia. Umożliwia zastanowienie się, co może zostać sfałszowane (ang. *Spoofed*), naruszone (ang. *Tempered*), czego można się wyprzeć (ang. *Repudiated*), co może zostać ujawnione (ang. *Information disclosure*), w jaki sposób można zablokować dostęp (ang. *Denial of Service*) lub podnieść uprawnienia (ang. *Escalation of privileges*).
Analiza każdego komponentu oprogramowania z punktu widzenia zagrożeń pozwala skoncentrować się nie na tym jak ten element *działa*, ale jak jego *działanie może zostać nadużyte*. Innymi słowy, pozwala odkryć, nieoczywiste zachowanie takiego komponentu. Tę analizę warto też poprowadzić z dwóch perspektyw — ochrony i ataku [1].

Zastosowanie STRIDE

Stosując STRIDE szczególną uwagę warto zwrócić na możliwość wyparcia się działania przez użytkownika systemu. Przeciwdziałać temu powinny *dane audytowe*. Muszą one być odpowiednio szczegółowe i zapisywane w bezpiecznym miejscu. Należy zapewnić ich nienaruszalność. Bez nich przeprowadzenie analizy naruszenia bezpieczeństwa, nie wspominając nawet o udowodnieniu winy, będzie niemożliwe.

Środki zaradcze

Środki zaradcze w stosunku do zidentyfikowanych zagrożeń, mogą należeć do jednej z czterech kategorii:

1. łagodzenie (ang. *mitigate*) — zmniejszenie ryzyka przez zmianę projektu lub dodanie mechanizmów ochrony,
2. usuwanie (ang. *remove*) — jeśli zagrożone aktywa nie są koniecznie potrzebne można je usunąć, a jeśli jest to niemożliwe, to można próbować pozbawić je cech, które wiążą się z powstaniem ryzyka,
3. przeniesienie (ang. *transfer*) — odpowiedzialność za ryzyko może być przeniesiona na stronę trzecią,
4. zaakceptowanie (ang. *accept*) — jeśli ryzyka nie można usunąć bez naruszania ważnych wymagań, to należy je dobrze zrozumieć i ocenić, czy można je ponieść.

Środki zaradcze

Niekiedy możliwe jest jedynie częściowe ograniczenie ryzyka. Może ono polegać na:

1. zmniejszeniu prawdopodobieństwa wystąpienia szkody,
2. zmniejszeniu dotkliwości szkód,
3. umożliwieniu przywrócenia stanu sprzed szkody,
4. umożliwieniu wykrycia szkody.

Dane osobowe

Dane osobowe są szczególnie ważnym zasobem. Projektując ich ochronę należy rozważyć:

1. Czy ich gromadzenie i przetwarzanie na pewno jest konieczne?
2. Czy muszą być przechowywane po zakończeniu ich przetwarzania?
3. Jakie standardy i przepisy prawne muszą być przestrzegane, np. GDPR (RODO)?
4. Czy wykryto i przeanalizowano starannie wszystkie nietypowe przypadki?
5. Czy zabezpieczenia uwzględniają scenariusze rzeczywistych przypadków użycia?
6. Czy ograniczono do minimum wymianę informacji ze stronami trzecimi, w szczególności ujawnianie danych wrażliwych?
7. Czy użytkownicy zostali rzetelnie poinformowani jak i w jakim celu będą przetwarzane ich dane?

Metody

STRIDE jest na pewno jednym z najbardziej dojrzałych rozwiązań stosowanych w modelowaniu zagrożeń, ale oczywiście nie jedynym. Przegląd kilku najciekawszych można znaleźć w artykule wydanym w biuletynie Software Engineering Institute Carnegie Mellon University [2].

PASTA

PASTA (ang. *The Process of Attack Simulation and Threat Analysis*) to ▸ metodologia opracowana w 2012 roku, której cechą jest połączenie celów biznesowych i wymagań technicznych, aby zaangażować w analizę ryzyka jak największą grupę specjalistów [1]. Jej główną zaletą jest ocena zagrożeń dla aktywów z uwzględnieniem perspektywy intruza. Ta metoda skład się z 7 etapów:

1. definicja celów biznesowych,
2. określenie zakresu technicznego,
3. rozkład (ang. *factoring*) aplikacji,
4. analiza zagrożeń,
5. wykrywanie podatności,
6. analiza i modelowanie ataków,
7. analiza skutków i opracowanie środków zaradczych.

LINDDUN

LINDDUN (ang. *Linkability, Identifability, Nonrepudation, Detectability, Disclosure of Information, Unawareness, Noncompliance*) to metoda, które celem jest ocena zagrożeń dla danych, a w szczególności dla danych osobowych [1]. Składa się z sześciu kroków:

1. Przestrzeń problemu
    1. Zdefiniuj DFD
    2. Przypisz zagrożenia prywatności do elementów DFD
    3. Zdefiniuj scenariusze zagrożeń
2. Przestrzeń rozwiązań
    1. Nadaj priorytety zagrożeniom
    2. Zgromadź strategie łagodzenia
    3. Wybierz odpowiednie techniki ochrony prywatności (ang. *Privacy Enhancing Technologies* —PETs)

Proces ten jest iteracyjny.

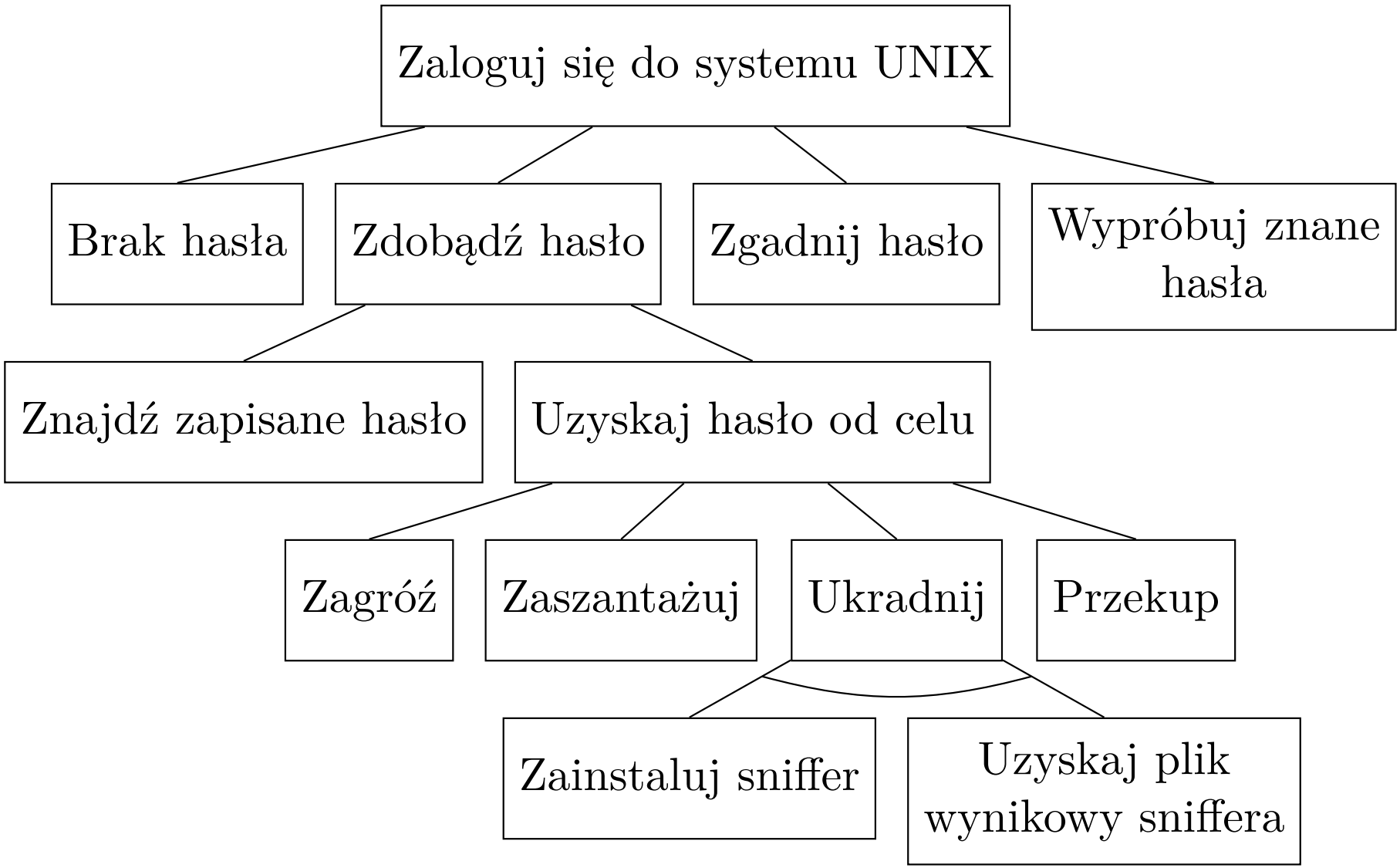
CVSS

Wspomniany na pierwszym wykładzie system CVSS służy do oceny ryzyka związanego z podatnościami, ale może być także użyty w modelowaniu zagrożeń, w połączeniu z innymi metodami [1]. Jego zaletą jest powtarzalność wyników, która tworzy wspólny poziom odniesienia.

Drzewa ataku

Drzewa ataku (ang. *attack trees*) są prawdopodobnie najstarszą metodą modelowania ryzyka, opracowaną niezależnie przez NSA i DARPA. Pozwalają one przedstawić atak na system w formie drzewa, gdzie korzeń stanowi cel ataku, a pozostałe węzły opisują drogę do jego zdobycia. (Ilustracja na następnym slajdzie na podstawie [3]).

Drzewa ataku



Persona non Grata

Ta metoda skupia się na umiejętnościach i motywacjach intruzów. Na tej podstawie pozwala ustalić zagrożenia i ryzyka. Jest odwrotnością metodyki *person*, stosowanej w podejściach zwinnych do tworzenia oprogramowania.

Karty bezpieczeństwa

Karty bezpieczeństwa (ang. *Security Cards*) nie są formalną metodą, a raczej podejściem na zasadzie „burzy mózgów”. Analitycy używając talii 42 kart starają się odpowiedzieć na pytania:

1. Kto może zaatakować?
2. Dlaczego system może być zaatakowany?
3. Które aktywa są interesujące z punktu widzenia intruza?
4. Jak takie ataki można przeprowadzić?

Aby ułatwić odkrycie zagrożeń talia kart jest podzielona na kategorie: wpływ na ludzi (9 kart), motywacja intruza (13 kart), zasoby adwersarza (11 kart) i jego metody (9 kart). Umożliwia odkrycie złożonych i nieoczywistych zagrożeń.

Bibliografia

Nataliya Shevchenko i in. “Threat Modeling: A Summary Of Available Methods”. W: *SEI Bulletin* (2018). URL: https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_524597.pdf.

Tony UcedaVelez. *Real World Threat Modeling Using the PASTA Methodology*. 2012. URL: https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf.

Łukasz Basa i in. *Wprowadzenie do bezpieczeństwa IT*. T. 1. Kraków: Securitum Wydawnictwo sp. z o.o., 2023.

Pytania

?

Koniec

Dziękuję Państwu za uwagę!