WSPÓLNY JĘZYK DLA INFORMACJI O INCYDENTACH BEZPIECZEŃSTWA KOMPUTEROWEGO

Incydent związany z bezpieczeństwem komputerowym to zestaw zdarzeń, które obejmują atak lub serię ataków w jednej lub wielu witrynach. Radzenie sobie z tymi incydentami jest nieuniknione dla osób i organizacji na wszystkich poziomach bezpieczeństwa komputerowego. Główną częścią radzenia sobie z tymi incydentami jest rejestrowanie i otrzymywanie informacji o zdarzeniach, które prawie zawsze występują w postaci stosunkowo niestrukturalnych plików tekstowych. Z biegiem czasu pliki te mogą zawierać dużą ilość bardzo cennych informacji. Niestety, niestrukturalna forma informacji często sprawia, że informacje o incydencie są trudne do zarządzania i wykorzystania. W tej części przedstawiono wyniki szeregu wysiłków podejmowanych w ciągu ostatnich kilku lat w celu opracowania i zaproponowania metody obsługi tych niestrukturalnych rekordów incydentów bezpieczeństwa komputerowego. W szczególności ta część przedstawia narzędzie zaprojektowane, aby pomóc osobom i organizacjom rejestrować, rozumieć i udostępniać informacje o zdarzeniach związanych z bezpieczeństwem komputerowym. Nazywamy to narzędzie wspólnym językiem dla informacji o incydentach bezpieczeństwa komputerowego. Ten wspólny język składa się z dwóch części:

1. Zestaw terminów związanych z incydentem "wysokiego poziomu"

2. Metoda klasyfikacji informacji o incydentach (taksonomia)

Dwie części wspólnego języka, terminy i taksonomia są ze sobą ściśle powiązane. Taksonomia zapewnia strukturę, która pokazuje, jak powiązane są najczęściej spotykane terminy. Wspólny język ma pomóc badaczom poprawić ich zdolność do:

* Mów bardziej zrozumiale z innymi o incydentach

* Zbieraj, organizuj i rejestruj informacje o incydentach

* Wyodrębnij dane z informacji o incydencie

* Podsumuj, udostępnij i porównaj informacje o incydencie

* Użyj informacji o incydencie, aby ocenić i zdecydować o prawidłowym przebiegu działań

* Użyj informacji o incydencie, aby określić skutki działań w czasie

Ta część zaczyna się od krótkiego omówienia, dlaczego potrzebny jest wspólny język, a następnie podsumowanie tego, jak rozwinięto wspólny język incydentów. Następnie przedstawiamy wspólny język w dwóch częściach: (1) terminy incydentów i taksonomia oraz (2) dodatkowe warunki dotyczące informacji o incydentach. Ostatnia sekcja zawiera informacje o praktycznych sposobach używania wspólnego języka.

DLACZEGO WSPÓLNY JĘZYK JEST POTRZEBNY?

Ponad 30 lat temu, bezpieczeństwo komputerów było małą, niejasną akademicką specjalnością. Ponieważ w terenie pracowało tylko kilka osób, obsługa informacji dotyczących bezpieczeństwa komputerowego mogła w dużej mierze odbywać się w sposób ad hoc. W tym środowisku osoby i grupy opracowały własne terminy opisujące informacje o bezpieczeństwie komputera. Opracowali, zgromadzili, zorganizowali, ocenili i wymienili swoje informacje dotyczące bezpieczeństwa komputerowego na wiele unikalnych i niestrukturalnych sposobów. Ten brak uogólnienia oznaczał, że informacje o bezpieczeństwie komputera zazwyczaj nie były łatwe do porównania lub połączenia, a czasami nawet do mówienia w zrozumiały sposób. Postępy w ciągu lat w uzgadnianiu względnie standardowego zestawu terminów dotyczących bezpieczeństwa komputerowego (wspólny język)

przyniosły mieszane rezultaty. Jednym z problemów jest to, że wiele terminów nie jest jeszcze w powszechnym użyciu. Innym problemem jest to, że terminy, które są w powszechnym użyciu, często nie mają standardowych znaczeń. Przykładem tego ostatniego jest termin "wirus komputerowy". Często słyszymy ten termin, nie tylko na forach akademickich, ale także w mediach i popularnych publikacjach. Okazuje się jednak, że nawet w publikacjach akademickich "wirus komputerowy" nie ma akceptowanej definicji. Wielu autorów definiuje wirusa komputerowego jako "fragment kodu, który kopiuje się do większego programu." Używają oni terminu "robak". aby opisać niezależny program, który wykonuje podobne funkcja inwazyjna (np. Internet Worm w 1988 r.). Inni autorzy używają terminu "wirus komputerowy" do opisu zarówno inwazyjnych fragmentów kodu, jak i niezależnych programów. Postęp w opracowywaniu metod zbierania, organizowania, oceny i wymiany komputera informacje dotyczące bezpieczeństwa również odniosły ograniczony sukces. Na przykład oryginalne zapisy (1988-1992) zespołu ds. Reagowania w sytuacjach kryzysowych (obecnie Centrum Koordynacji CERT lub CERT / CC) są po prostu plikiem wiadomości e-mail i innych plików wysłanych do CERT / CC. Te wiadomości i pliki zostały zarchiwizowane razem w porządku chronologicznym, bez żadnej innej organizacji. Po 1992 roku CERT / CC i inne organizacje opracowali metody organizowania i rozpowszechniania swoich informacji, ale informacje nadal trudno jest połączyć lub porównać, ponieważ większość z nich pozostaje prawie całkowicie tekstową informacją, która ma unikalną strukturę dla CERT / CC. Takie ad hoc warunki i ad hoc sposoby gromadzenia, organizowania, oceny i wymiany informacji bezpieczeństwa komputerowego nie są już odpowiednie. W projekt zaangażowanych jest zdecydowanie zbyt wiele osób i organizacji, a informacja o nich jest zbyt dużo, aby je zrozumieć i udostępnić. Dziś bezpieczeństwo komputerów jest coraz ważniejszym, istotniejszym i bardziej wyrafinowanym kierunkiem studiów. Wiele osób i organizacji obecnie regularnie gromadzi i rozpowszechnia informacje o bezpieczeństwie komputera. Informacje takie obejmują cały zakres od cech bezpieczeństwa i słabych punktów komputerów i sieci, po zachowania ludzi i systemów podczas incydentów związanych z bezpieczeństwem - zdecydowanie za dużo informacji dla każdej osoby i organizacji, aby mieć własny, unikalny język. Jednym z kluczowych elementów systematycznego postępu w każdej dziedzinie jest: opracowanie spójnego zestawu terminów i taksonomii (zasad klasyfikacji), które są stosowane w tej dziedzinie. Jest to niezbędny i naturalny proces, który prowadzi do rozwoju wspólnego języka, który umożliwia zbieranie, wymianę i porównywanie informacji. Innymi słowy, im bardziej wzrasta zakres badań, takich jak bezpieczeństwo komputerowe, tym bardziej potrzebny jest wspólny język, aby zrozumieć i komunikować się ze sobą

ROZWÓJ WSPÓLNEGO JĘZYKA

Dwa z bardziej znaczących wysiłków w procesie rozwoju tego wspólnego języka dla informacji o incydentach związanych z bezpieczeństwem komputerowym to (1) projekt klasyfikacji ponad 4 300 incydentów bezpieczeństwa w Internecie zakończonych w 1997,4 i (2) serii warsztatów w 1997 i 1998 roku zwany wspólnym projektem językowym . Uczestnikami warsztatów byli ludzie przede wszystkim z grupy badawczej ds. bezpieczeństwa i sieci w Sandia National Laboratories, Livermore w Kalifornii oraz z CERT / CC w Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania. Dodatkowy udział i przegląd uzyskali pracownicy Departamentu Obrony (DoD) oraz Narodowego Instytutu Standardów i Technologii (NIST). Wysiłki te, zmierzające do wypracowania wspólnego języka, nie były próbą opracowania kompleksowego słownika terminów. Zamiast tego uczestnicy próbowali opracować zarówno minimalny zestaw terminów "wysokiego poziomu", aby opisać ataki i incydenty związane z bezpieczeństwem komputerowym, a także schemat struktury i klasyfikacji dla tych terminów (taksonomia), które mogą służy do klasyfikowania, rozumienia, wymiany i porównywania ataków na komputer i informacje o incydentach. Uczestnicy warsztatów mieli nadzieję, że ten wspólny język zyska szeroką akceptację ze względu na swoją przydatność. Istnieją już dowody, że taka akceptacja ma miejsce, szczególnie w zespołach reagowania na incydenty i w DoD.

Aby być kompletnym, logicznym i użytecznym, wspólny język informacji o incydentach bezpieczeństwa komputerowego był oparty początkowo i przede wszystkim na teorii (tj. Był oparty a priori lub nieempirycznie). Klasyfikacja rzeczywistych informacji o zdarzeniach związanych z bezpieczeństwem w Internecie została następnie wykorzystana do udoskonalenia i rozszerzenia języka. Mówiąc dokładniej, wspólny rozwój języka przebiegał w sześciu etapach:

1. Zapisy w CERT / CC dotyczące incydentów zgłoszonych im od 1988 r. Do 1995 r. Zostały zbadane w celu ustalenia wstępnej listy terminów używanych do opisywania incydentów bezpieczeństwa komputerowego.

2. Pojęcia w tym wykazie i ich definicje zostały połączone w strukturę (wstępna taksonomia).

3. Ta wstępna taksonomia została wykorzystana do sklasyfikowania informacji w rejestrach incydentów z lat 1988-1995.

4. Wstępna taksonomia i wyniki klasyfikacji zostały opublikowane w 1997 r.

5. Seria warsztatów została przeprowadzona w latach 1997-1998 (Common Language Project) w celu ulepszenia taksonomii i dodania dodatkowych warunków.

6. Wyniki warsztatów ("wspólny język incydentów związanych z bezpieczeństwem") zostały po raz pierwszy opublikowane w 1998 r.

Taksonomia to system klasyfikacji (struktura), który dzieli wiedzę i określa relacje sztuk. Większość terminów w tym wspólnym języku dla informacji o zdarzeniach związanych z bezpieczeństwem jest ułożona w takiej taksonomii, jak przedstawiono w następnej sekcji . Klasyfikacja to proces wykorzystywania taksonomii do rozdzielania i zamawiania. Jak wspomniano wcześniej, klasyfikacja informacji przy użyciu taksonomii jest niezbędna dla informacji o incydentach bezpieczeństwa komputerowego z powodu szybko rosnącej ilości informacji i charakteru tych informacji (głównie tekstu). Klasyfikacja za pomocą wspólnej taksonomii jest omówiona w końcowej sekcji tej części. Nasze doświadczenie pokazało, że zadowalające taksonomie mają kategorie klasyfikacyjne z tymi sześcioma cechami

1. Wzajemnie wyłączne. Klasyfikowanie w jednej kategorii wyklucza wszystkie pozostałe, ponieważ kategorie się nie nakładają.

2. Wyczerpujące. Wszystkie kategorie obejmują wszystkie możliwości.

3. Jednoznaczny. Taksonomia jest jasna i precyzyjna, więc klasyfikacja nie jest niepewna, niezależnie od tego, kto dokonuje klasyfikacji.

4. Powtarzalny. Powtarzające się aplikacje skutkują tą samą klasyfikacją, niezależnie od tego, kto robi klasyfikację.

5. Zaakceptowany. Jest logiczny i intuicyjny, dzięki czemu kategorie mogą zostać ogólnie zatwierdzone.

6. Przydatne. Taksonomię można wykorzystać do uzyskania wglądu w obszar badań

Te cechy zostały wykorzystane do opracowania i oceny taksonomii w języku potocznym. Taksonomia jest jednak tylko przybliżeniem rzeczywistości i jako taka, nawet najlepsza taksonomia nie będzie cechowała się pewnymi cechami. Może to być szczególnie prawdziwe, gdy cechy sklasyfikowanych danych są nieprecyzyjne i niepewne, co jest typowe dla informacji o incydentach bezpieczeństwa komputerowego. Niemniej jednak klasyfikacja jest ważnym, użytecznym i koniecznym warunkiem wstępnym do systematycznego badania incydentów.

INFORMACJA O ZABEZPIECZENIU KOMPUTEROWYM PODATEK.

Udało się skonstruować większość terminologii we wspólnym języku dla informacji o zdarzeniach związanych z bezpieczeństwem w systematykę. Te terminy i taksonomia są przedstawione w tej sekcji.

ZDARZENIA

Działanie komputerów i sieci wiąże się z niezliczonymi zdarzeniami. W ogólnym sensie zdarzenie jest dyskretną zmianą stanu lub statusu systemu lub urządzenia. Z punktu widzenia bezpieczeństwa komputerowego zmiany stanu wynikają z działań skierowanych przeciwko określonym celom. Przykładem jest użytkownik podejmujący działanie w celu zalogowania się na konto użytkownika w systemie komputerowym. W tym przypadku, działanie podejmowane przez użytkownika polega na uwierzytelnianiu w programie logowania przez stwierdzenie, że posiada on określoną tożsamość, a następnie przedstawienie wymaganej weryfikacji. Celem tej akcji byłoby konto użytkownika. Inne przykłady obejmują liczne działania, które mogą być ukierunkowane na:

* Dane (np. Czynności do odczytu, kopiowania, modyfikowania, kradzieży lub usuwania)

* Proces (np. Działania mające na celu sondowanie, skanowanie, uwierzytelnianie, ominięcie lub zalanie działającego procesu komputerowego lub wątku wykonawczego)

* Komponent, komputer, sieć lub intersieć (np. Czynności skanowania lub kradzieży)

Zdarzenie komputera lub sieci jest zdefiniowane jako:

Zdarzenie-akcja skierowana na cel, którego celem jest zmiana stanu lub stanu celu

Istotne jest podkreślenie kilku aspektów tej definicji. Po pierwsze, aby zdarzenie miało miejsce, musi zostać podjęte działanie i musi być skierowane przeciwko celowi, ale działanie nie musi odnieść rzeczywistej zmiany stanu celu. Na przykład, jeśli użytkownik wprowadzi niepoprawną kombinację nazwy użytkownika i hasła podczas logowania do konta zdarzenie uwierzytelniające miało miejsce, ale zdarzenie nie powiodło się przy sprawdzeniu, czy użytkownik ma odpowiednie poświadczenia dostępu do tego konta. Drugim ważnym aspektem jest to, że zdarzenie reprezentuje praktyczne połączenie między działaniem i określonym celem, na który skierowane jest działanie. W związku z tym przedstawia sposób, w jaki ludzie zasadniczo konceptualizują wydarzenia na komputerach i sieciach, a także poszczególne kroki, które faktycznie mają miejsce podczas wydarzenia. Na przykład, gdy użytkownik loguje się do konta, klasyfikujemy akcję jako uwierzytelnioną, a cel jako konto. Rzeczywiste działanie, które ma miejsce, jest dla użytkownika, aby uzyskać dostęp do procesu (na przykład, program "logowanie") w celu uwierzytelnienia. Próba zobrazowania wszystkich poszczególnych kroków jest niepotrzebną komplikacją; przedstawione tutaj koncepcje wyższego poziomu mogą poprawnie i dokładnie opisać wydarzenie w formie dobrze zrozumiałej dla ludzi. Innymi słowy, sensowne jest streszczenie języka i jego struktury do poziomu, na którym ludzie zasadniczo konceptualizują wydarzenia. Na wszelki wypadek należy przedstawić dowody potwierdzające, tak aby dowody zawierały pełne wyobrażenie o tym, co się wydarzyło. Innymi słowy, abstrakcja, konceptualizacja i komunikacja powinny być stosowane tak blisko dowodów, jak to tylko możliwe. Na przykład, jeśli celem ataku jest przełącznik sieciowy, należy normalnie wyświetlić cel jako komputer lub składnik (w zależności od charakteru przełącznika), a nie sieć, ponieważ założenie, że sieć jest celem, może być niedokładną interpretacją dowodów. Innym aspektem definicji zdarzenia jest to, że nie rozróżnia on działań dozwolonych od nieuprawnionych. Większość zdarzeń, które mają miejsce na komputerach lub w sieciach, jest zarówno rutynowa, jak i autoryzowana, dlatego też nie stanowią problemu dla

specjalistów od bezpieczeństwa. Czasami jednak zdarzenie jest częścią ataku lub stanowi zagrożenie bezpieczeństwa z innego powodu. Ta definicja zdarzenia ma na celu uchwycenie zarówno autoryzowanych, jak i nieautoryzowanych działań. Na przykład, jeśli użytkownik uwierzytelnia się prawidłowo, podając prawidłową identyfikację użytkownika i kombinację hasła podczas logowania się do konta, tym użytkownikiem jest dostęp do tego konta. Może się jednak zdarzyć, że ten użytkownik podszywa się pod rzeczywistego użytkownika, po uzyskaniu identyfikatora użytkownika i hasła od podsłuchu w sieci. Tak czy inaczej, nadal jest to uznawane za uwierzytelnienie. Wreszcie, ważnym aspektem wydarzeń jest to, że nie wszystkie możliwe zdarzenia są uważane za prawdopodobne, a nawet możliwe. Na przykład akcja uwierzytelniania jest zwykle powiązana z kontem lub procesem, a nie z innym celem, takim jak dane lub komponent. Inne przykłady obejmują czytanie i kopiowanie, które są zwykle ukierunkowane na dane; powodzie, które są zwykle ukierunkowane na konto, proces lub system; lub kradzież, która jest zwykle skierowana przeciwko danym, składnikowi lub komputerowi. Definiujemy akcję i cel w następujący sposób:

Krok działania podjętego przez użytkownika lub proces w celu osiągnięcia rezultatu 11, taki jak sondowanie, skanowanie, zalewanie, uwierzytelnianie, ominięcie, fałszowanie, odczytywanie, kopiowanie, kradzież, modyfikowanie lub usuwanie.

Komputer docelowy lub logiczna jednostka (konto, proces lub dane) lub jednostka fizyczna (komponent, komputer, sieć lub intersieć).

AKCJE

Działanie to krok podjęty przez użytkownika lub proces w celu uzyskania wyniku. Akcje są inicjowane przez uzyskanie dostępu do celu, w którym dostęp jest zdefiniowany jako:

Dostęp - ustanów logiczną lub fizyczną komunikację lub kontakt.

Do zbierania informacji o celach służą dwie akcje: sonda i skan. Sonda jest działaniem mającym na celu określenie jednej lub więcej charakterystyk określonego celu. W przeciwieństwie do skanowania, które jest działaniem, w którym użytkownik lub proces uzyskuje dostęp do zestawu celów w sposób systematyczny, w celu określenia, które cele mają jedną lub więcej cech. "Sonda" i "skan" są terminami powszechnie używanymi przez zespoły reagowania na incydenty. W rezultacie mają wspólne, akceptowane definicje. Mimo to istnieje logiczna dwuznaczność: skan może być postrzegany jako wiele sond. Innymi słowy, jeśli atakujący testuje jedną lub więcej cech na wielu hostach, może to być (a) wiele ataków (wszystkie sondy) lub (b) jeden atak (skan). Ta kwestia była szeroko omawiana podczas warsztatów poświęconych projektowi językowemu, a wniosek był taki, że terminy we wspólnym języku powinny w jak największym stopniu odpowiadać ich powszechnemu użyciu. Dzięki sondom i skanom zwykle jest oczywiste, co się dzieje. Atakujący albo "odciąga się" od jednego hosta (sondy), losowo testuje wiele hostów (wiele sond), albo używa jakiegoś "automatycznego" oprogramowania, aby systematycznie szukać tej samej charakterystyki w grupie hostów (skan). W praktyce, odpowiedź na incydent, zespoły zwykle nie mają problemu z podjęciem decyzji o rodzaju akcji, z którą mają do czynienia. Dodatkową kwestią dotyczącą skanowania jest to, że określenie "systematyczny" nie ma na celu określenia określonego wzorca. Najbardziej zaawansowani atakujący próbują ukryć systematyczny charakter skanowania. Skan może początkowo wydawać się wielokrotnymi sondami. Na przykład osoba atakująca może losować skan w odniesieniu do hostów i względem testowanej cechy. Jeśli atak można określić, aby obejmował testowanie jednej lub więcej charakterystyk na grupie hostów z pewną wspólną własnością (np. Zakres adresów IP [IP]) lub jeśli testy na wielu hostach wydają się być w inny sposób powiązane (np. wspólne pochodzenie w lokalizacji i czasie), a następnie wielokrotne sondy powinny być sklasyfikowane jako skan. W przeciwieństwie do sondowania lub skanowania, działania podejmowane w celu zalania celu nie są wykorzystywane do zbierania informacji o celu. Zamiast tego,

pożądanym skutkiem powodzi jest przytłoczenie lub przeciążenie zdolności celu poprzez wielokrotne uzyskiwanie dostępu do celu. Przykładem są powtarzające się prośby o otwarcie połączeń z portem w sieci lub wielokrotne żądania inicjowania procesów na komputerze. Innym przykładem jest duża liczba wiadomości e-mail, które mogą przekroczyć zasoby dostępne dla konta docelowego.

Uwierzytelnianie to działanie podejmowane przez użytkownika w celu założenia tożsamości. Uwierzytelnianie rozpoczyna się od użytkownika uzyskującego dostęp do procesu uwierzytelniania, takiego jak program logowania. Użytkownik musi mieć określoną tożsamość, na przykład poprzez podanie nazwy użytkownika. Zwykle weryfikacja jest również wymagany jako drugi etap uwierzytelniania. W celu weryfikacji użytkownik musi udowodnić znajomość czegoś tajnego (np. hasła), udowodnić posiadanie jakiegoś tokena (np. Bezpieczna karta identyfikacyjna) i / lub udowodnić posiadanie określonej cechy (np. Wzór skanowania siatkówki) . Uwierzytelnianie może być używane nie tylko do logowania się do konta, ale także do uzyskiwania dostępu do innych obiektów, takich jak obsługa procesu lub uzyskiwanie dostępu do pliku. Innymi słowy, celem działania uwierzytelniającego jest podmiot (na przykład konto, proces lub dane), do którego użytkownik próbuje uzyskać dostęp, a nie sam proces uwierzytelniania. Aby pokonać proces uwierzytelniania, można użyć dwóch ogólnych metod. Po pierwsze, użytkownik może uzyskać prawidłową parę identyfikującą i weryfikacyjną, z której można by korzystać z uwierzytelnienia, nawet jeśli nie należy do tego użytkownika. Na przykład podczas incydentu osoba atakująca może użyć procesu działającego na komputerze hosta, który przechwytuje nazwy użytkowników, hasła i kombinacje adresów IP wysyłane w postaci zwykłego tekstu przez Internet. Atakujący może następnie użyć przechwyconych informacji do uwierzytelnienia (zalogowania) na kontach należących do innych użytkowników. Należy zauważyć, jak wspomniano wcześniej, że ta czynność nadal jest uznawana za autentyczną, ponieważ atakujący przedstawia ważne pary identyfikacyjne i weryfikacyjne, mimo że zostały skradzione.

Drugą metodą, która może być wykorzystana do pokonania procesu uwierzytelniania, jest wykorzystanie luki w celu obejścia procesu uwierzytelniania i uzyskania dostępu do celu. Pomijanie to działanie podejmowane w celu uniknięcia procesu przy użyciu alternatywnej metody uzyskania dostępu do celu. Na przykład niektóre systemy operacyjne mają luki, które atakujący może wykorzystać do uzyskania uprawnień bez faktycznego logowania się na konto uprzywilejowane. Jak omówiono w odniesieniu do uwierzytelniania, akcja obejścia niekoniecznie oznacza, że działanie jest nieautoryzowane. Na przykład, niektórzy programiści uważają, że przydatna jest metoda skrótu ("back-door") do założenia konta lub uruchomienia procesu, szczególnie podczas programowania. W takiej sytuacji działanie w celu ominięcia można uznać za dozwolone. Uwierzytelnianie i obejście to działania związane z identyfikacją użytkowników. W komunikacji sieciowej procesy również identyfikują się ze sobą. Na przykład, każdy pakiet informacji podróżujących w sieci zawiera adresy identyfikujące zarówno źródło, jak i miejsce docelowe, a także inne informacje. Przyjmuje się "poprawne" informacje w tych komunikatach, ponieważ są one generowane automatycznie. Tak więc żadne działanie nie jest uwzględnione na liście, aby opisać tę normalną sytuację. Do tych komunikatów można jednak wprowadzić niepoprawne informacje. Dostarczanie takich fałszywych informacji jest powszechnie nazywane działaniem podszywania się. Przykłady obejmują spoofing IP, fałszowanie poczty i fałszowanie DNS (Domain Name System). Spoofing to aktywny atak bezpieczeństwa, w którym jedno urządzenie w sieci podszywa się pod inną maszynę. . . . [To] zakłóca normalny przepływ danych i może obejmować wstrzykiwanie danych do łącza komunikacyjnego między innymi komputerami. Ta maskarada ma na celu oszukać inne urządzenia w sieci, aby zaakceptować oszusta jako oryginał, albo zwabić inne maszyny do wysyłania danych, albo umożliwić zmianę danych. Niektóre działania są ściśle powiązane z danymi znajdującymi się na komputerach lub sieciach, w szczególności z plikami: odczyt, kopiowanie, modyfikowanie, kradzież i usuwanie. Nastąpiło pewne zamieszanie w stosunku do tych terminów, ponieważ ich powszechne stosowanie w opisywaniu świata fizycznego różni się czasami od

powszechnego użycia opisującego świat elektroniczny. Na przykład, jeśli powiem, że osoba atakująca ukradła komputer, można założyć, że atakujący przejął w posiadanie cel (komputer) i nie pozostawił identycznego komputera w tej lokalizacji. Jeśli jednak powiem, że atakujący ukradł plik komputerowy, co to właściwie znaczy? Często przyjmuje się, że atakujący zduplikował plik i ma teraz kopię, ale oznacza to również, że oryginalny plik nadal znajduje się w pierwotnej lokalizacji. Innymi słowy, "kradzież" oznacza czasami coś innego w świecie fizycznym niż w świecie elektronicznym. Dezorientujące jest to, że istnieją różnice w znaczeniu działań w świecie fizycznym i świecie elektronicznym. Uczestnicy warsztatów próbowali pogodzić te różnice, dokładnie określając każdy termin (czytać, kopiować, modyfikować, kraść lub usuwać), aby miał on bardzo specyficzne i wzajemnie wykluczające się znaczenie, które w największym możliwym stopniu pasuje do znaczenia świata fizycznego. Odczytywanie jest zdefiniowane jako działanie w celu uzyskania zawartości danych zawartych w pliku lub innym nośniku danych. Działanie to odróżnia się koncepcyjnie od rzeczywistych fizycznych kroków, które mogą być wymagane do odczytu. Na przykład podczas odczytu pliku komputerowego plik może zostać skopiowany z pamięci do głównej pamięci komputera, a następnie wyświetlony na monitorze do odczytu przez użytkownika. Te fizyczne kroki (skopiuj plik do pamięci, a następnie na monitor) nie są częścią abstrakcyjnej koncepcji czytania. Innymi słowy, aby odczytać cel (uzyskać jego zawartość), kopiowanie pliku nie jest koniecznie wymagane i nie jest koncepcyjnie zawarte w naszej definicji odczytu. Ta sama separacja pojęć jest zawarta w definicji terminu "kopia". W tym przypadku mamy na myśli uzyskanie kopii celu bez usunięcia oryginału. Termin "kopia" nie oznacza, że treść w celu została uzyskana, tylko że kopia została wykonana i uzyskana. Aby uzyskać zawartość, plik musi zostać odczytany. Przykładem jest skopiowanie pliku z dysku twardego na dyskietkę. Kopiowanie odbywa się poprzez skopiowanie oryginalnego pliku, pozostawiając oryginalny plik nienaruszony. Użytkownik musiałby otworzyć plik i przejrzeć zawartość, aby go przeczytać.

Kopiuj i czytaj są dwiema różnymi pojęciami z kradzieży, co skutkuje tym, że atakujący przejmie w posiadanie cel, a cel staje się niedostępny dla pierwotnego właściciela lub użytkownika. Ta definicja jest zgodna z naszymi koncepcjami dotyczącymi własności fizycznej, w szczególności, że istnieje tylko jeden obiekt, którego nie można skopiować. Na przykład, jeśli ktoś ukradnie samochód, to pozbawił on właściciela jego posiadania. Kiedy mamy do czynienia z nieruchomością w formie elektronicznej, np. Plik komputerowy, często używa się terminu "ukraść", kiedy kopia jest tym, co faktycznie ma na myśli. Termin "kradzież" oznacza w szczególności, że pierwotnemu właścicielowi lub użytkownikowi odmówiono dostępu lub użycia celu. Z drugiej strony, kradzież może również oznaczać fizyczne wzięcie dyskietki, na której znajduje się plik lub kradzież całego komputera. Dwa inne działania wymagają w jakiś sposób zmiany celu. Pierwsze to działania mające na celu modyfikację celu. Przykłady obejmują zmianę zawartości pliku, zmianę hasła konta, wysyłanie poleceń w celu zmiany charakterystyk procesu operacyjnego lub dodanie komponentów do istniejącego systemu. Jeśli cel zostanie całkowicie wyeliminowany, do opisu działania zostanie użyty termin "usuń". Jak wspomniano wcześniej, różnice w użyciu terminów między światem fizycznym a światem elektronicznym są niepożądane. W związku z tym staraliśmy się być konkretni i konsekwentni w użyciu. Wynikający z tego zestaw terminów jest wyczerpujący i wykluczający się wzajemnie, ale jest sprzeczny z ziarnem w jakimś powszechnym użyciu dla elektronicznego świata, szczególnie w odniesieniu do terminu "ukraść". Sytuacja wydaje się nieunikniona. Oto kilka przykładów, które mogą wyjaśnić terminy:

* Użytkownik klika łącze do przeglądarki i widzi zawartość strony Web na ekranie komputera. Sklasyfikowalibyśmy to jako przeczytane. Podczas gdy to, co się dzieje, jest to, że zawartość strony jest przechowywana w ulotnej pamięci, kopiowana do pamięci podręcznej na dysku twardym i wyświetlana na ekranie, z logicznego (tj. Użytkownika) punktu widzenia, strona internetowa nie była skopiowane (ani skradzione). Teraz, jeśli użytkownik kopiuje plik zawartość strony WWW do pliku lub go wypisuje,

a następnie użytkownik skopiował stronę ze strony internetowej. Ponownie, byłaby to logiczna klasyfikacja akcji z punktu widzenia użytkownika.

* Użytkownik duplikuje plik, który jest zaszyfrowany. Sklasyfikowalibyśmy to jako kopię, a nie odczytano. W tym przypadku plik został odtworzony, ale zawartość nie została uzyskana, więc nie została odczytana.

* Użytkownik usuwa kilka wpisów w haśle lub pliku grupy. Czy należy to działanie opisać jako kilka akcji usuwania lub jako jedno działanie do modyfikacji? Opisywalibyśmy to działanie jako modyfikujące, a celem są dane. Nie ma tu żadnej niejednoznaczności z powodu definicji "danych". Dane definiuje się jako plik stacjonarny lub plik w tranzycie (patrz następna sekcja). Jeśli użytkownik usunie linię z pliku haseł, plik został zmodyfikowany. Akcja zostanie opisana jako usuń tylko wtedy, gdy cały plik zostanie usunięty. Gdybyśmy zdefiniowali dane, które obejmowałyby część pliku, mielibyśmy rzeczywiście niejednoznaczność.

* Użytkownik kopiuje plik i usuwa oryginał. Sklasyfikowalibyśmy to jako kradzież. Chociaż kroki zawierają kopię, a następnie usunięcie, to jest elektroniczny sposób kradzieży pliku, a zatem opis jest bardziej opisowy, jak kradzież.

Sonda - uzyskuje dostęp do celu w celu określenia jednej lub większej liczby jego cech.

W rzeczywistości termin "ukraść" jest rzadko używany (poprawnie), ponieważ osoby atakujące, które kopiują pliki, zwykle nie usuwają oryginałów. Termin "kradzież" jest często używany niepoprawnie, tak jak w "kradzieży kodu źródłowego", gdy w rzeczywistości prawidłowym terminem jest kopia. Lista działań została zaabsorbowana licznymi dyskusjami grupowymi, które trwały kilka lat, zanim zostały wprowadzone do wspólnego języka. Większość osób, które brały udział w tych dyskusjach, nie była do końca zadowolona z listy, ale jest to najlepsze, co do tej pory widzieliśmy. W szczególności lista zdaje się przechwytywać wszystkie popularne terminy z ich powszechnym użyciem (sonda, skan, powódź, podróbka, kopiowanie, modyfikowanie i usuwanie), a pozostałe terminy są logiczne (dla osób, które uczestniczyły w grupach dyskusyjnych) i są konieczne, aby kategoria działania była wyczerpująca (uwierzytelniać, ominąć, przeczytać i ukraść). Oto podsumowanie naszych definicji działań:

Sonda - uzyskuje dostęp do celu w celu określenia jednej lub większej liczby jego cech.

Skanuj - systematycznie uzyskuj dostęp do zbioru celów, aby określić, które cele mają jedną lub więcej charakterystycznych cech. Powtarza wielokrotnie dostęp do celu, aby przeładować pojemność celu.

Uwierzytelnij - przedstaw tożsamość procesowi i, w razie potrzeby, zweryfikuj tę tożsamość, aby uzyskać dostęp do celu

Pomiń - unikaj procesu, używając alternatywnej metody dostępu do celu

Podróbka-maskarady, zakładając pojawienie się innej jednostki w komunikacji sieciowej

Odczytaj - uzyskaj zawartość danych w urządzeniu pamięciowym lub innym nośniku danych.

Kopiuj - powtórz cel, pozostawiając pierwotny cel bez zmian.

Kradnij - zdobądź cel bez pozostawienia kopii w pierwotnej lokalizacji.

Zmodyfikuj - zmień zawartość lub cechy celu.

Usuń - usuwa cel lub czyni go nieodwracalnym

CELE

Uważa się, że działania są ukierunkowane na siedem kategorii celów. Pierwsze trzy z nich to "logiczne" jednostki (konto, proces i dane), a pozostałe cztery to "fizyczne" jednostki (komponent, komputer, sieć i intersieć). W środowisku wielu użytkowników konto jest domeną pojedynczego użytkownika. Ta domena obejmuje pliki i procesy, do których uzyskiwania dostępu i używania użytkownik jest uprawniony. Specjalny program rejestrujący nazwę konta użytkownika, hasło i ograniczenia użytkowania kontroluje dostęp do konta użytkownika. Niektóre konta mają zwiększone lub specjalne uprawnienia umożliwiają dostęp do kont systemowych, innych kont użytkowników oraz plików i procesów systemowych i często nazywane są kontami uprzywilejowanymi, administratora, administratora lub root. Czasami akcja może być skierowana na proces, który jest programem wykonywanym na komputerze lub w sieci. Oprócz samego programu proces obejmuje także dane programu i stos; jego licznik programu, wskaźnik stosu i inne rejestry; i wszystkie inne informacje potrzebne do realizacji programu. Akcja może wtedy polegać na dostarczeniu informacji do procesu lub komendowaniu procesu w pewien sposób. Celem działania może być dane znalezione na komputerze lub w sieci. Dane są przedstawieniami faktów, pojęć lub instrukcji w formularzach odpowiednich dla użytkowników lub procesów. Dane można znaleźć w dwóch postaciach: pliki lub dane w tranzycie. Pliki to dane określone przez nazwę i uważane za jednostkę przez użytkownika lub proces. Powszechnie uważamy, że pliki znajdują się na nośniku pamięciowym, takim jak dysk pamięci masowej, ale pliki mogą również znajdować się w niestabilnej lub nieulotnej pamięci komputera. Dane w tranzycie są danymi przesyłanymi przez sieć lub w inny sposób pochodzącymi z niektórych źródeł. Przykłady tych ostatnich obejmują dane transmitowane pomiędzy urządzeniami w komputerze i danymi znajdującymi się w polach elektromagnetycznych otaczających monitory komputerowe, urządzenia pamięci, procesory, nośniki transmisji sieciowej i tym podobne. Czasami konceptualizujemy cel działania jako nie będący bytem logicznym (konto, proces lub dane), ale raczej jako jednostka fizyczna. Najmniejszy z obiektów fizycznych jest komponentem, który jest jedną z części tworzących komputer lub sieć. Sieć jest połączoną lub wzajemnie powiązaną grupą komputerów, wraz z siecią odpowiednie elementy przełączające i łączące się gałęzie.Gdy komputer jest podłączony do sieci, jest czasami określany jako komputer-host. Jeżeli sieci są ze sobą połączone, to czasami określa się je jako intersieci. Oto podsumowanie naszych definicji celów.

* Konto - domena dostępu użytkownika na komputerze lub w sieci, która jest kontrolowana zgodnie z zapisem informacji, który zawiera nazwę konta użytkownika, hasło i ograniczenia użytkowania.

* Proces - program w realizacji, składający się z programu wykonywalnego, danych programu i stosu, licznika programu, wskaźnika stosu i innych rejestrów oraz wszystkich innych informacji potrzebnych do wykonania programu.

* Dane - reprezentacja faktów, koncepcji lub instrukcji w sposób odpowiedni do komunikacji, interpretacji lub przetwarzania przez ludzi lub w sposób automatyczny. Dane mogą mieć postać plików w pamięci ulotnej komputera lub pamięci nieulotnej lub w urządzeniu do przechowywania danych lub w postaci danych przesyłanych przez medium transmisyjne.

* Komponent - jedna z części składających się na komputer lub sieć.

* Urządzenie komputerowe - które składa się z jednego lub więcej powiązanych komponentów, w tym jednostek przetwarzania i jednostek peryferyjnych, które są kontrolowane przez programy przechowywane wewnętrznie i które mogą wykonywać znaczne obliczenia, w tym liczne operacje arytmetyczne lub operacje logiczne, bez interwencji człowieka podczas wykonywania. Uwaga: może być samodzielny lub może składać się z kilku połączonych ze sobą jednostek. Połączona z siecią lub powiązana ze sobą grupa komputerów hosta, elementów przełączających i oddziałów łączących.

* Sieci - połączona lub powiązana grupa komputerów-hostów, elementy przełączające i połączone gałęzie.

* Intersieci - sieć sieci

ATAKI

Czasami zdarzenie, które ma miejsce na komputerze lub sieci, jest częścią serii kroków mających na celu uzyskanie czegoś, co nie jest autoryzowane. To wydarzenie jest następnie uważane za część ataku. Atak ma trzy elementy.

1. Jest to seria kroków podjętych przez atakującego. Wśród tych kroków znajduje się akcja skierowana na cel (zdarzenie, jak opisano w poprzedniej sekcji), a także użycie jakiegoś narzędzia do wykorzystania luki

2. Atak ma na celu uzyskanie nieautoryzowanego wyniku, patrząc z perspektywy właściciela lub administratora danego systemu.

3. Atak to seria celowych kroków zainicjowanych przez atakującego. To odróżnia atak od czegoś, co jest nieumyślne.

Definiujemy atak w ten sposób:

Atak - seria kroków podjętych przez atakującego w celu uzyskania nieautoryzowanego wyniku.

Ataki mają pięć części, które przedstawiają logiczne kroki, które musi podjąć atakujący. Osoba atakująca używa (1) narzędzia do wykorzystania (2) podatności na wykonanie (3) akcji na (4) celu w celu uzyskania (5) nieautoryzowanego wyniku. Aby odnieść sukces, atakujący musi znaleźć jedną lub więcej ścieżek, które można połączyć (ataki), być może jednocześnie lub wielokrotnie. Pierwsze dwa kroki ataku, narzędzia i luki w zabezpieczeniach służą do wywołania zdarzenia (akcji skierowanej na cel) na komputerze lub sieci. Logicznym końcem udanego ataku jest nieautoryzowany wynik. Jeśli logicznym końcem poprzednich kroków jest autoryzowany wynik, wtedy atak nie miał miejsca. Koncepcja autoryzowanego konta nieautoryzowanego jest kluczem do zrozumienia tego, co odróżnia atak od normalnych zdarzeń, które występują. Jest to również koncepcja zależna od systemu, ponieważ to, co może być autoryzowane w jednym systemie, może być nieautoryzowane na innym. Na przykład niektóre usługi, takie jak anonimowy protokół przesyłania plików (FTP), mogą być włączone w niektórych systemach, a nie w innych. Nawet akcje, które są zwykle traktowane jako wrogie, takie jak próby ominięcia kontroli dostępu w celu uzyskania dostępu do konta uprzywilejowanego, mogą być autoryzowane w szczególnych okolicznościach, takich jak zatwierdzony test bezpieczeństwa systemu lub użycie "tylnych drzwi" podczas rozwoju. Właściciele systemów lub ich administratorzy określają, jakie działania uznają za autoryzowane dla swoich systemów, ustanawiając politykę bezpieczeństwa. Oto definicje autoryzowanych i nieautoryzowanych.

Autoryzowany - zatwierdzony przez właściciela lub administratora.

Nieautoryzowane - niezatwierdzone przez właściciela lub administratora.

Narzędzie Pierwszym krokiem w sekwencji, która prowadzi atakujących do nieautoryzowanych wyników, jest narzędzie użyte w ataku. Narzędzie to pewne środki, które można wykorzystać do wykorzystania luki w komputerze lub sieci. Czasami narzędzie jest proste, takie jak polecenie użytkownika lub atak fizyczny. Inne narzędzia mogą być bardzo wyrafinowane i skomplikowane, takie jak program konia trojańskiego, wirus komputerowy lub narzędzie rozproszone. W ten sposób definiujemy narzędzie.

Narzędzie - oznacza wykorzystanie luki w zabezpieczeniach komputera lub sieci.

Termin "narzędzie" jest trudny do zdefiniowania bardziej szczegółowo z powodu szerokiej gamy dostępnych metod wykorzystania luk w komputerach i sieciach. Kiedy autorzy sporządzają listy metod ataku, często sporządzają listy narzędzi. Bazując na naszym doświadczeniu, te kategorie narzędzi są obecnie wyczerpującą listą.

Atak fizyczny - oznacza fizyczną kradzież lub uszkodzenie komputera, sieci, jego komponentów lub systemów wspomagających (np. Klimatyzacja, energia elektryczna itp.).

Wymiana informacji - oznacza uzyskiwanie informacji od innych napastników (np. Za pośrednictwem elektronicznej tablicy ogłoszeń) lub od osób atakowanych (powszechnie nazywanych inżynierią społeczną).

Polecenie użytkownika - oznacza wykorzystanie luki poprzez wprowadzenie komend do procesu poprzez bezpośrednie wprowadzanie danych przez użytkownika w interfejsie procesu. Przykładem jest wprowadzanie poleceń UNIX przez połączenie telnet lub komendy w porcie protokołu.

Skrypt lub program - oznacza wykorzystanie luki poprzez wprowadzenie komend do procesu poprzez wykonanie pliku komend (skryptu) lub programu w interfejsie procesu. Przykładem jest skrypt powłoki wykorzystujący błąd oprogramowania, program logowania konia trojańskiego lub program do łamania haseł.

Autonomiczny agent - oznacza wykorzystanie luki poprzez użycie programu lub fragmentu programu, który działa niezależnie od użytkownika. Przykładami są wirusy komputerowe lub robaki.

Zestaw narzędzi - pakiet oprogramowania zawierający skrypty, programy lub autonomiczne agenty wykorzystujące luki w zabezpieczeniach. Przykładem jest szeroko dostępny zestaw narzędzi o nazwie rootkit.

Narzędzie rozproszone - narzędzie, które można dystrybuować do wielu hostów, które następnie można skoordynować, aby anonimowo wykonać atak na host docelowy jednocześnie z pewnym opóźnieniem.

Dotknięcie danych - oznacza monitorowanie promieniowania elektromagnetycznego emitowanego przez komputer lub sieć za pomocą urządzenia zewnętrznego.

Z wyjątkiem ataku fizycznego, wymiany informacji i kategorii danych, każda z kategorii narzędzi może zawierać inne kategorie narzędzi w sobie. Na przykład zestawy narzędzi zawierają skrypty, programy, a czasem autonomiczni agenci. Tak więc, gdy używany jest zestaw narzędzi, dołączany jest również skrypt lub kategoria programu. Polecenia użytkownika muszą być również używane do inicjowania skryptów, programów, autonomicznych agentów, zestawów narzędzi i narzędzi rozproszonych. Innymi słowy, istnieje kolejność niektórych kategorii w bloku narzędzi, od prostej kategorii poleceń użytkownika do bardziej wyrafinowanej kategorii narzędzi rozproszonych. Przy opisywaniu lub klasyfikowaniu ataku na ogół należy dokonać wyboru spośród kilku alternatyw w bloku narzędzi. Zdecydowaliśmy się sklasyfikować zgodnie z najwyższą kategorią używanego narzędzia, co sprawia, że kategorie wzajemnie się wykluczają w praktyce.

Podatność Aby osiągnąć pożądany rezultat, osoba atakująca musi skorzystać z luki w zabezpieczeniach komputera lub sieci.

Wrażliwość - słabość systemu umożliwiającego nieautoryzowane działanie.

Luka w oprogramowaniu to błąd, który pojawia się na różnych etapach rozwoju lub użytkowania. Ta definicja może być użyta do podania trzech kategorii luk:

Luka w zabezpieczeniach projektowych - luka nieodłącznie związana z projektem lub specyfikacją sprzętu lub oprogramowania, dzięki której nawet perfekcyjna implementacja spowoduje lukę.

Luka w implementacji - luka wynikająca z błędu w oprogramowaniu lub implementacji sprzętowej zadowalającego projektu.

Luka w konfiguracji - luka wynikająca z błędu w konfiguracjia systemu, np. posiadanie kont systemowych z domyślnymi hasłami, uprawnienie do zapisu na świecie dla nowych plików lub posiadanie włączone wrażliwe usługi.

Wynik nieautoryzowany Logicznym końcem udanego ataku jest nieautoryzowany wynik. W tym momencie osoba atakująca wykorzystała narzędzie do wykorzystania luki w celu spowodowania zdarzenia.

Nieautoryzowany wynik - nieautoryzowane konsekwencje zdarzenia.

Jeśli się powiedzie, atak spowoduje jedno z następujących:

Zwiększony dostęp - nieautoryzowane zwiększenie domeny dostępu do komputera lub sieci.

Ujawnianie informacji - rozpowszechnianie informacji każdemu, kto nie jest upoważniony do dostępu do tych informacji.

Uszkodzenie informacji - nieautoryzowana zmiana danych na komputerze lub w sieci.

Odmowa usługi- - celowa degradacja lub blokowanie zasobów komputera lub sieci.

Kradzież zasobów - nieautoryzowane wykorzystanie zasobów komputera lub sieci.

Pełna taksonomia informacji o zdarzeniach. Często ataki na komputery w sieci występują w charakterystycznej grupie, którą klasyfikowalibyśmy jako część jednego zdarzenia. To, co czyni te ataki grupą wyróżniającą, jest kombinacją trzech czynników, z których każdy może mieć jedynie częściową informację.

1. Może być jeden atakujący lub może być kilku napastników, którzy są w jakiś sposób spokrewnieni.

2. Atakujący może użyć podobnych ataków lub może starać się osiągnąć wyraźny lub podobny cel.

3. Witryny zaangażowane w ataki i czas ataków mogą być takie same lub mogą być powiązane.

Oto definicja incydentu:

Incydent - grupa ataków, które można odróżnić od innych ataków z powodu odrębności atakujących, ataków, celów, witryn i czasu. Atakujący lub grupa atakujących osiąga cele poprzez wykonywanie ataków. Incydent może obejmować jeden pojedynczy atak lub wiele ataków. Uniemożliwienie atakującym osiągnięcia celów można osiągnąć poprzez zapewnienie, że atakujący nie może wykonać żadnych pełnych połączeń przez siedem przedstawionych kroków. Na przykład mogą zostać przeprowadzone dochodzenia w sprawie podejrzanych o ataki terrorystyczne, systemy można okresowo przeszukiwać pod kątem narzędzi atakujących, można naprawić luki w systemie, wzmocnić kontrolę dostępu, aby uniemożliwić atakującemu dostęp do konta docelowego, pliki mogą być szyfrowane tak, jak nie prowadzić do ujawnienia, a można zainicjować publiczny program edukacyjny, aby uniemożliwić terrorystom osiągnięcie celu politycznego

Atakujący i ich cele Ludzie atakują komputery. Robią to za pomocą różnych metod i różnych celów. To, co odróżnia kategorie atakujących, to połączenie tego, kim są i jakie są ich cele (co chcą osiągnąć).

Atakujący - osoba, która próbuje jednego lub więcej ataków w celu osiągnięcia celu.

Cel - cel lub cel końcowy zdarzenia

W oparciu o ich cele podzieliliśmy atakujących na kilka kategorii:

Hakerzy - atakujący, którzy atakują komputery w poszukiwaniu wyzwań, statusu lub emocji związanych z uzyskaniem dostępu. (Uwaga: zdecydowaliśmy się użyć terminu "haker", ponieważ jest on powszechny i szeroko rozumiany. Zdajemy sobie sprawę, że bardziej pozytywne skojarzenie tego terminu było po raz kolejny szeroko akceptowane).

Szpiedzy - atakujący, którzy atakują komputery w celu wykorzystania informacji do celów politycznych.

Terroryści - napastnicy, którzy atakują komputery, aby wywołać strach, dla korzyści politycznych.

Korporacyjni najeźdźcy - pracownicy (atakujący), którzy atakują komputery konkurencji w celu uzyskania korzyści finansowych.

Zawodowi przestępcy - napastnicy atakujący komputery w celu uzyskania osobistych korzyści finansowych.

Wandale - atakujący, którzy atakują komputery, aby spowodować obrażenia.

Voyeurs - atakujący, którzy atakują komputery z powodu dreszczyku wrażliwych informacji.

Te siedem kategorii napastników i ich cztery kategorie celów, są fundamentalne dla różnicy między incydentami a atakami. Różnicę tę podsumowano w wyrażeniu "atakujący wykorzystują ataki do osiągnięcia celów"

DODATKOWE WARUNKI INFORMACJI O INCYDENTACH

Taksonomia ostatniej sekcji przedstawiała wszystkie terminy wspólnego języka bezpieczeństwa komputerowego, które opisują, jak atakujący osiągają cele podczas incydentu. Jednak, aby w pełni opisać zdarzenie, wymagane są inne, bardziej ogólne warunki. Następne rozdziały omawiają te warunki

SUKCES I PORAŻKA

Informacje o sukcesie lub porażce można zapisać na kilku poziomach ogólnej taksonomii. W najszerszym sensie ogólny sukces lub porażka wskazuje, czy jeden lub więcej napastników osiągnęło jeden lub więcej celów. Węższym celem byłoby określenie sukcesu lub niepowodzenia pojedynczego ataku poprzez ocenę, czy atak prowadzi do nieautoryzowanego wyniku. Informacje o sukcesie lub porażce mogą jednak nie być znane. Na przykład próba zalogowania się do konta root lub superużytkownika w systemie może zostać zakwalifikowana jako niepowodzenie lub jako nieznane.

NAZWA WITRYNY I WITRYNA

"Witryna" jest popularnym terminem używanym do identyfikowania organizacji internetowych oraz fizycznych lokalizacji. "Witryna" to także poziom organizacyjny administratora strony lub innego organu odpowiedzialnego za komputery i sieci w tej lokalizacji. Termin "nazwa witryny" odnosi się do części w pełni kwalifikowanej nazwy domeny w internetowym systemie nazw domen (DNS). W przypadku witryn w Stanach Zjednoczonych nazwy witryn zazwyczaj znajdują się na drugim poziomie drzewa DNS. Przykładami mogą być cmu.edu lub widgets.com. W innych krajach nazwa witryny to trzeci lub niższy poziom drzewa DNS, taki jak widgets.co.uk. Niektóre nazwy witryn występują nawet

dalej w dół drzewa DNS. Na przykład szkoła w Kolorado może mieć nazwę strony myschool.k12.co.us. Oto definicje witryny i nazwy witryny.

Witryna - poziom organizacyjny odpowiedzialny za zdarzenia związane z bezpieczeństwem; poziom organizacyjny administratora strony lub innego organu odpowiedzialnego za komputery i sieci w tym miejscu.

Nazwa witryny - część w pełni kwalifikowanej nazwy domeny, która odpowiada witrynie. Niektóre organizacje, takie jak większe uniwersytety i firmy, są wystarczająco duże, aby fizycznie podzielić się na więcej niż jedną lokalizację, z oddzielną administracją. Ta separacja nie może być łatwo ustalona. Dlatego często te różne miejsca muszą być traktowane jako jedna strona.

Inne warunki dotyczące incydentów Kilka dodatkowych warunków jest niezbędnych do pełnego opisania rzeczywistych incydentów internetowych. Pierwszy z tych terminów dotyczy dat.

Data zgłoszenia - pierwsza data zgłoszenia zdarzenia zespołowi reagowania lub innej agencji lub osobom zbierającym dane.

Data rozpoczęcia - data pierwszego znanego zdarzenia incydentu.

Data końcowa - data ostatniej znanej aktywności incydentu.

Kilka terminów dotyczy zaangażowanych stron.

Liczba witryn - ogólna liczba witryn, o których wiadomo, że zgłosiły lub w inny sposób brały udział w incydencie.

Witryny raportujące - nazwy witryn, o których wiadomo, że zgłosiły incydent.

Inne witryny - nazwy witryn, o których wiadomo, że brały udział w incydencie, ale które nie zgłosiły incydentu.

W przypadku większości zespołów reagowania na incydenty rzeczywiste nazwy witryn są uważane za informacje poufne. W naszych badaniach, w celu ochrony tożsamości witryn związanych z incydentem, dezynfekujemy informacje o witrynie, kodując nazwy witryn przed ich publicznym udostępnieniem. Przykładem może być zastąpienie nazwy witryny, takiej jak fikcyjne widgets.com, numerami i nazwą domeny wyższego poziomu, taką jak 123.com. Zespoły reagowania często wykorzystują numery incydentów do śledzenia zdarzeń i identyfikacji informacji o zdarzeniach.

Numer incydentu - numer referencyjny używany do śledzenia zdarzenia lub identyfikacji informacji o incydencie.

Ostatnim terminem, który uznaliśmy za przydatny, jest działanie korygujące, które wskazuje działania podjęte w następstwie incydentu. Działania te mogą obejmować zmianę haseł, przeładowanie plików systemów, rozmowę z intruzami, a nawet postępowanie karne. Informacje na temat działań naprawczych podjętych w trakcie lub po incydencie są trudne do uzyskania dla zespołów reagowania na incydenty, ponieważ zaangażowanie zespołu reagowania jest zazwyczaj ograniczone do wczesnych etapów incydentu. Zapisy CERT / CC wskazują, że różnorodność działań naprawczych jest rozległa, a taksonomia działań naprawczych może być pożądanym przyszłym rozszerzeniem wspólnego języka.

Działanie korygujące - działanie podjęte podczas lub po incydencie, aby zapobiec dalszym atakom, naprawić obrażenia lub ukarać przestępców.

JAK KORZYSTAĆ Z WSPÓLNEGO JĘZYKA

Ważne są dwie rzeczy, które należy podkreślić, używając wspólnego języka dla informacji o incydencie bezpieczeństwa komputera. Po pierwsze, wspólny język to naprawdę zestaw terminów wysokiego poziomu. W związku z tym nie rozwiąże wszystkich sporów dotyczących wszystkiego, co jest dyskutowane na temat bezpieczeństwa komputerowego. Na przykład wspólny język obejmuje "autonomicznego agenta" jako termin (kategorię narzędzia). Autonomiczni agenci obejmują wirusy komputerowe, robaki i tym podobne, niezależnie od tego, jak te konkretne terminy mogą być zdefiniowane. Innymi słowy, wspólny język nie próbuje rozstrzygać sporów na temat tego, co powinno lub nie powinno być uważane za wirusa komputerowego, ale raczej zajmuje się wyższym poziomem abstrakcji ("autonomiczny agent"), gdzie, jak można mieć nadzieję, może być więcej zgody i standaryzacja. Innymi słowy, uczestnicy warsztatów Common Language Project przewidywali, że osoby i organizacje będą nadal używać własnych warunków, które mogą być bardziej szczegółowe zarówno pod względem znaczenia, jak i zastosowania. Wspólny język został zaprojektowany, aby umożliwić sklasyfikowanie tych terminów niższego poziomu w ramach wspólnej struktury językowej. Drugą kwestią, na którą należy zwrócić uwagę, jest to, że wspólny język, nawet jeśli przedstawia taksonomię, nie klasyfikuje incydentu (ani pojedynczych ataków) jako jednej rzeczy. Klasyfikowanie ataków lub incydentów związanych z bezpieczeństwem komputera jest trudne, ponieważ ataki i incydenty to seria kroków, które musi podjąć atakujący. Innymi słowy, ataki i incydenty to nie tylko jedna rzecz, ale szereg rzeczy. Dlatego mówię, że wspólny język stanowi taksonomię dla informacji o incydencie bezpieczeństwa komputera. Przykład problemu można znaleźć w popularnych i prostych taksonomiach często używanych do próby klasyfikacji incydentów. Pojawiają się jako lista pojedynczych, zdefiniowanych terminów. Następujące terminy z Icove, Seger i VonStorch stanowią przykład :

Ukryte kanały ,Zanieczyszczenie danych, Degradacja usług, Denial of service ,Dumpster diving ,Podsłuch na emanacjach,Nadmiar uprawnień Nękanie Podszywanie się pod adresy IP,Logiczne bomby ,Masquerading ,Password sniffing, Przejęcie kontroli nad sesją ,Salamis, Piractwo komputerowe ,Ataki czasowe ,Analiza ruchu, Drzwi pułapkowe ,Konie trojańskie Tunelowanie, Nieautoryzowane kopiowanie danych ,Wirusy i robaki ,Podsłuch

Listy terminów nie są zadowalającymi taksonomiami do klasyfikacji rzeczywistych ataków lub incydentów. Nie mają większości z sześciu cech zadowalającej taksonomii. Po pierwsze, terminy nie wykluczają się wzajemnie. Na przykład terminy "wirus" i "bomba logiczna" znajdują się zazwyczaj na tych listach, ale wirus może zawierać bombę logiczną, więc kategorie się pokrywają. Faktyczni napastnicy zazwyczaj używają wielu metod, więc ich ataki musiałyby zostać zaklasyfikowane do wielu kategorii. To sprawia, że klasyfikacja jest niejednoznaczna i trudna do powtórzenia. Bardziej fundamentalnym problemem jest to, że przy założeniu, że można by opracować wyczerpującą i wzajemnie wykluczającą się listę, taksonomia byłaby niewystarczająco długa i trudna do zastosowania. Nie wskazywałby także na związek między różnymi typami ataków. Wreszcie żadna z tych list nie została powszechnie zaakceptowana, po części dlatego, że trudno jest uzgodnić definicję terminów. W rzeczywistości wiele różnych definicji terminów jest powszechnie używanych. Podstawowe problemy związane z tymi listami (i ich odmianami) polegają na tym, że większość incydentów wiąże się z wieloma atakami, a ataki wymagają wielu kroków. W rezultacie informacje o typowym incydencie muszą być klasyfikowane w wielu kategoriach. Na przykład jednym z ataków w incydencie może być zalew hosta, który powoduje odmowę usługi. Ale ten sam incydent może wiązać się z wykorzystaniem luki w zabezpieczeniach komputera hosta, który był specyficznym źródłem powodzi. Czy należy to uznać za powódź? Jako kompromis roota? Jako atak typu "odmowa usługi"? W rzeczywistości incydent należy sklasyfikować we wszystkich tych kategoriach. Innymi słowy, ten incydent ma wiele klasyfikacji. Podsumowując, opracowując wspólny język, stwierdziliśmy, że w odniesieniu do ataków i incydentów możemy naprawdę tylko (1) przedstawić wspólny zestaw terminów wysokiego poziomu, które są powszechnie używane i mają wspólne definicje i (2) przedstawić strukturę logiczną terminom, które

można wykorzystać do klasyfikacji informacji o incydencie lub ataku w odniesieniu do określonych kategorii. Niektóre przykłady mogą to wyjaśnić. Jak wspomniano wcześniej, większość informacji o faktycznych atakach i incydentach ma formę zapisów tekstowych. W typowym rejestrze incydentów w CERT / CC można odnotować trzy obserwacje:

1. Znaleźliśmy rootkita na hoście xxx.xxx.

2. Wysłano e-mail na konto xxx@xxx.xxx, które spowodowało awarię serwera pocztowego.

3. Prześledziliśmy atak z powrotem na nastolatka w mieście Xyz, który powiedział, że nie próbuje wyrządzić żadnych szkód, tylko stara się sprawdzić, czy może się włamać.

W przypadku obserwacji 1 sklasyfikowalibyśmy rootkita w kategorii "zestaw narzędzi" w kategorii "Narzędzie", a nazwę hosta w kategorii "komputer" w sekcji "Cel". W przypadku obserwacji 2 "powódź e-mailowa" jest konkretną instancją w "powodzi" kategorię w kategorii "Akcja", a także w kategorii "odmowa usługi" w sekcji "Nieautoryzowany wynik". co do celu obserwacji 2: czy jest to konto czy komputer? Ze względów praktycznych obserwacje zostałyby sklasyfikowane jako oba, ponieważ informacje są dostępne w obu przypadkach. Dla obserwacji 3 można wywnioskować, że jest to "haker" poszukujący "wyzwania, statusu lub emocji". Co zapewnia ten taksonomiczny proces, który ma wartość praktyczną? Po pierwsze, taksonomia pomaga nam przekazywać innym to, co znaleźliśmy. Kiedy mówimy, że rootkit jest rodzajem zestawu narzędzi, to nasz wspólny zestaw terminów ("wspólny język") zapewnia nam ogólne zrozumienie tego, co mamy na myśli. Kiedy mówi się, że 22 procent incydentów zgłoszonych do CERT / CC w latach 1988-1995 obejmowało różne problemy z hasłami (poprawna statystyka35), taksonomia okazała się przydatna w przekazywaniu cennych informacji. Zastosowanie taksonomii jest w rzeczywistości czteroetapowym procesem, który można wykorzystać do określenia największych problemów bezpieczeństwa. W szczególności proces ma na celu:

1. Spójrz na fragmentaryczne informacje w raportach incydentów.

2. Klasyfikuj te obserwacje.

3. Wykonaj badania statystyczne tych danych.

4. Skorzystaj z tych informacji, aby określić najlepszy kurs (y) działania.

Z czasem ten sam proces może zostać użyty do określenia efektów tych działań. Dwa kolejne punkty są ważne, aby podkreślić tę taksonomię. Po pierwsze, atak jest procesem, który z wystarczającą ilością informacji jest zawsze klasyfikowany w wielu kategoriach. Na przykład: w kategorii "Narzędzie", w kategorii "Podatność", w kategorii "Działanie", w kategorii "Cel" oraz w kategorii "Nieautoryzowany wynik". Po drugie, incydent może obejmować wiele, może tysiące ataków. W związku z tym informacje zebrane w incydencie teoretycznie mogłyby zostać prawidłowo zaklasyfikowane do wszystkich kategorii taksonomii. Zgodnie z tymi wytycznymi wspólny język incydentów związanych z bezpieczeństwem komputerów okazał się użytecznym i coraz bardziej akceptowanym narzędziem do gromadzenia, wymiany i porównywania informacji o bezpieczeństwie komputera. Sama taksonomia okazała się prosta i prosta w użyciu.