ĐẠI HỌC BÁCH KHOA HÀ NỘI

Cơ sở An toàn Thông tin

Sách Giáo trình

Nguyễn Khanh Văn

Hà nội - 2014

đại thể hiện qua việc liên tục kết nối với các bài toán thực tế hiện nay. Những vấn đề được chọn trình bày kỹ lưỡng đều thuộc về cơ sở của lĩnh vực, những phần mang tính nâng cao thường được điểm qua hoặc đưa ra như những câu hỏi và bài tập mở rộng.

Về lý thuyết mật mã, một nền tảng căn bản của an toàn thông tin (ATTT), các khái niệm cơ bản sẽ được đề cập bao gôm: hệ mã hoá đối xứng, mã hoá phi đối xứng (khóa công khai), hàm băm, chữ ký điện tử... Các mô hình phát triển hơn sẽ được giới thiệu là vấn đề trao chuyển khoá và giao thức mật mã (cryptographic protocol). Bên cạnh đó các nền tảng cơ sở khác của ATTT như xác thực (authentication), điều khiển quyền truy nhập (access control), các mô hình an toàn mạng, mã độc và tấn công lợi dụng cũng là các chủ đề trọng tâm.

Giáo trình này được đưa xuất bản lần đầu nên không tránh khỏi những khiếm khuyết nhất định, tuy nhiên nó cũng là kết quả của sự tổng hợp các kiến thức và kinh nghiệm của nhiều năm giảng dạy của tác giả tại Đại học Bách Khoa Hà nội về chủ đề An toàn thông tin (bắt đầu từ năm 1998). Đặc biệt, do tính gấp rút của thời gian, một số phần trình bày là tài liệu giảng dạy đã được viết từ những năm 1998-2000, nên nội dung có thể chưa hoàn toàn cập nhật, hoặc cô đọng hơn các phần khác, thiếu các diễn giải chi tiết, nhiều vấn đề chỉ nêu mà chưa minh hoạ. Chúng tôi hy vọng sẽ bổ sung và làm tốt hơn trong các lần tái bản sau.

Mong thu nhận được thật nhiều ý kiến đóng góp cụ thể của các bạn độc giả. Ý kiến gửi về xin chuyển qua địa chỉ cơ quan hoặc các địa chỉ E-mail sau:

TS. Nguyễn Khanh Văn
601- nhà B1, Bộ môn Công nghệ Phần mềm
Viện Công Nghệ Thông tin & Truyền Thông
Đại học Bách Khoa Hà nội, 1 Đại Cồ Việt, Hà nội, Việt nam
Email: vannk@soict.hust.edu.vn; van.nguyenkhanh@hust.edu.vn

Xin Cám Ơn Bạn Đọc!

- Chiếm đoạt (usurpation): kẻ tấn công sửa đổi thông tin điều khiển qua đó cướp đoạt quyền điều khiện hệ thống hoặc phá hỏng hay làm ngừng trệ hệ thống

Trong các loại tấn công nói trên lại có nhiều dạng tấn công cụ thể, hoặc mô hình cụ thể khác nhau. Các dạng tấn công bóc tin mật thường là thụ động, tức là kẻ địch không sửa đổi thông tin. Các dạng tấn công khác, chủ động tác động lên thông tin và dữ liệu, thường là nguy hiểm hơn, tùy vào mức độ tác động. Thậm chí kẻ địch có thể tác động lên thông tin để tìm cách thao túng toàn bộ kênh thông tin mà các bên tham gia liên lạc không hề biết. Điển hình nhất là sơ đồ tấn công N-CQ J-[JLL wtlD-man-in-the-middle attack), trong đó kẻ tấn công nham hiểu, có khả năng xen vào giữa hai bên A và B, bóp méo thông tin gửi từ cả hai phía mà không để lộ ra. Cơ chế bóp méo hai phía này là rất nham hiểm, khiến cho cả hai bên không thể nhận ra, vì hai sự bóp méo từ hai phía là rất khớp nhau, không để xảy sai lệch.

Để đảm bảo bao quát hết các mối đe dọa và có giải pháp chắc chắn, cần lưu ý hai nguyên tắc quan trọng trong đánh giá phân tích các mối đe dọa:

- Phải tính đến tất cả các khả năng mà kẻ địch có thể thâm nhập. Kẻ địch thường thử mọi cách có thể được để hòng thâm nhập phá hoại cho nên không được phép giả sử rằng kẻ sẽ tấn công chỉ ở một số điểm này mà không ở những chỗ khác, nói cách khác phải đề phòng cả những khả năng khó tin nhất. Nguyên tắc này làm cho việc thẩm định về bảo mật trở nên rất khó, do tất cả các khả năng bị phá hoại phải được tính đến.
- Tài sản phải được bảo vệ cho đến khi hết giá trị sử dụng hoặc hết ý nghĩa mật.

Nếu chúng ta không đứng vững trước các loại tấn công trên, nhiều thiệt hại trong hệ thống máy tính có thể xảy ra:

1. Xoá: kẻ địch xoá tệp dữ liệu quan trọng hoặc sao chép đè.
2. Sửa đổi:

- Sửa đổi chương trình có thể gây ra chương trình bị treo ngay lập tức hoặc một thời điểm nào đó sau này (logic bomb -"mìn hẹn giờ"). Hoặc là nó có thể khiến cho chương trình hoạt động và tạo ra những hiệu ứng không trong thiết kế, chẳng hạn như sửa đổi trái phép quyền truy nhập.

- Sửa đổi dữ liệu có thể gây ra bằng nhiều hình thức: nhồi nhét để chế biến các thông báo giả (salami attack).

3. Can thiệp: Ăn trộm chương trình, dữ liệu. Phá hoại tính bí mật của các dữ liệu thông qua cá phương pháp nghe trộm (wiretaping, monitoring, electromagnetic radiation...)

Rất khó phát hiện những xâm phạm vào tính nguyên vẹn của tài sản vì chương trình/dữ liệu không hề bị thay đổi mà chỉ bị lộ bí mật.

- Truyền dự liệu giữa các điểm phân tán dễ làm bộc lộ dữ liệu, tạo nên nhiều điểm tấn công cho những kẻ xâm nhập để sửa đổi dữ liệu.
- Chia sẻ tài nguyên và điều khiển truy nhập trở nên một vấn đề hóc búa.

A &KtQK ViFK Yj Fk FKÃ

Khởi nguồn của một giải pháp ATTT là việc xây dựng một bộ chính sách. Chính sách(policy) là một phát biểu ở mức khái quát, qui định những điều nên làm và không nên làm. Một định nghĩa khái quát về giải pháp ATTT chính là tập hợp các chính sách xây dựng nó. Chính sách này được xây dựng trên cơ sở đã khảo sát phân tích kỹ các mối đe dọa tiềm năng. Chính sách chỉ là một phát biểu chỉ ra sự yêu cầu, mong muốn của lãnh đạo tổ chức. Tự nó không thực hiện được chính nó, mà cần một Fï FKG (mechanism) hoạt động, cài đặt cụ thể để có thể áp đặt những yêu cầu, mong muốn này vào đời sống công việc hàng ngày của tổ chức và hệ thông thôn tin của nó. Cơ chế thể hiện một hệ thống qui định chi tiết, trong đó bao gồm những qui định kỹ thuật và những qui định mang tính thủ tục.

Thông thường đưa ra tập chính sách không phải là một cá nhân nào đó, mà (và nên) là một hội đồng, qui tụ các chuyên gia và lãnh đạo quản lý, không chỉ trong giới hạn chuyên môn công nghệ thông tin mà còn các mảng khác như nghiệp vụ, tài chính, quản lý, nhân sự. Tức là mọi mặt hoạt động của công ty, vì an ninh thông tin chung sẽ ảnh hưởng và bị ảnh hưởng tới mọi khía cạnh, góc độ trong một hệ thống doanh nghiệp, tổ chức. Chính sách có thể biểu đạt bằng nhiều ngôn ngữ khác nhau, có thể bằng các mệnh đề toán học, chính xác cao nhưng khó hiểu, hoặc ngôn ngữ tự nhiên, dễ hiểu nhưng dễ gây nhập nhằng, thiếu chính xác. Vì vậy người ta đã thiết kế công cụ riêng, được gọi là ngôn ngữ chính sách (policy languages) để đảm bảo sự cân bằng giữa tính chính xác và sự dễ hiểu.

Vì có thể được tạo ra từ nhiều nguồn gốc, nhiều quan điểm của nhiều chuyên gia lĩnh vực khác nhau, các chính sách có thể mâu thuẫn nhau, dẫn tới khó khăn trong việc tích hợp chung vào hệ thống. Sự vênh nhau trong chính sách có thể dẫn tới những điểm yếu, những "lỗ hổng" tiềm năng mà một kẻ đối địch có thể khai thác để tấn công. Những điểm yếu hay "lỗ hổng" này thường được gọi là điểm dễ bị tổn thương, nhạy cảm về ATBM (security vulnerability). Vì vậy trong việc xây dựng chính sách, khâu tích hợp cần được làm rất cẩn thận để phát hiện và giải quyết các bất đồng có thể nảy sinh giữa các chính sách (thường tạo ra bởi các chuyên gia ở lĩnh vực khác nhau).

Mục đích chung của giải pháp an toàn thông tin chính là bảo vệ hệ thống, mà nói cho cùng chính là bảo vệ sự toàn vẹn của các chính sách an toàn, không để cho chúng bị vi phạm. Dưới góc độ này, chúng ta có thể thấy 3 mục tiêu cụ thể là: 1) phòng chống không cho kẻ tấn công có thể vi phạm (đấy là lý tưởng nhất); 2) phát hiện tấn công vi

phạm (càng sớm càng tốt); và 3) khôi phục sau tấn công, khắc phục hậu quả: sau khi đẩy lùi tấn công, khắc phục tình hình, khôi phục sự đảm bảo của các chính sách.

A .LÇP WUD Yj .LÇP VRiW

Chỉ có chính sách và cơ chế là chưa đủ vì trong thực tế, một cơ chế xây dựng nên có đáp ứng tốt hoặc tồi cho việc đảm bảo áp đặt được chính sách đó. Ta cần phải có công cụ kiểm tra, đánh giá độ đáp ứng của cơ chế đối với việc áp đặt chính sách, tức là trả lời câu hỏi "liệu có thể tin đến mức độ nào khả năng một hệ thống có đáp ứng đúng những yêu cầu đặt ra cho nó?". Công cụ kiểm trả và kiểm soát (assurance) sẽ cho phép ta điều khiển tốt hơn việc đồng khớp được chính sách và cơ chế. Để làm được điều này, các kỹ thuật tiêu biểu của công nghệ phần mềm có thể được áp dụng trong toàn bộ quá trình xây dựng giải pháp phần mềm; đó là các bước kỹ thuật: xây dựng ÿ ? F W(specification), W K L (design) G Fj L (implementation).

Đặc tả là một kỹ thuật đi liền với pha S K kQ W t F K (requirement analysis) trong công nghệ phần mềm. Các yêu cầu ở đây chính là các chính sách (thường phát biểu ở dạng khái quát) và các đặc tả sẽ cho phép mịn hóa các yêu cầu thành các yêu cầu nhỏ hơn, các bước công việc với yêu cầu riêng phải làm để thỏa mãn được 1 yêu cầu khái quát của chính sách. Các đặc tả cũng có thể được biểu đạt được bằng cả 2 ngôn ngữ, hình thức (mệnh đề toán học) và phi hình thức (ngôn ngữ tự nhiên), và cũng có thể ở các cấp độ khác nhau của khái quát (high-level) hay chi tiết, cụ thể (low-level). Đặc tả khái quát thường dùng cho mô tả hệ thống chung hoặc các modul phân hệ lớn, còn đặc tả chi tiết áp đụng cho các mo-dul, thành tố nhỏ bên trong.

Thiết kế là công việc đưa ra các kiến trúc, các mô hình cài đặt nhằm đảm bảo hệ thống hoạt động đúng theo yêu cầu của đặc tả. Thông thường bản thiết kế là một tập hợp các sơ đồ thể hiện việc giải quyết theo từng mức trừu tượng. Ban đầu hệ thống được nhìn như một sơ đồ khái quát cao, sau đó sẽ được làm mịn dần bằng các sơ đồ bộ phận chi tiết hơn, có mức trừu tượng thấp dần, cho đến khi đạt mức chi tiết có thể sử dụng trực tiếp cho việc lập trình tạo mã cho hệ thống máy tính. Việc cài đặt là sự hiện thực hóa các sơ đồ chi tiết, cho từng phân hệ, từng module, và tích hợp lại.

Quá trình thực hiện giải pháp thông qua các mức đặc tả, thiết kế và cài đặt, sẽ giúp cho việc kiểm soát được dễ dàng, vì tất cả mọi khâu thực hiện đều có định nghĩa rõ ràng, cái vào, cái ra cụ thể, cũng như bộ tài liệu xây dựng dần, chu đáo. Phương châm chung là mỗi công việc to hay bé phải có đặc tả yêu cầu và mô hình thực hiện, từ đó dễ dàng đánh giá chất lượng sản phẩm cuối và độ thỏa mãn với mục tiêu ban đầu.

A ;XQJ TXDQK FKë ÿÅ ÿLÅX KjQK RSHUDWLRQDO LVVXHV

Phân tích chi phí-lợi nhuận (cost-benefit analysis)

Đây là một chủ đề quan trọng, phải được xem xét kỹ càng khi lựa chọn giải pháp. Giải pháp cho ATTT đối với một hệ thống cụ thể có thể có nhiều, có thể do tổ chức tự xây dựng nên, hoặc do các công ty tư vấn khuyến nghị, mỗi giải pháp sẽ có những yêu-nhược điểm riêng cùng với giá thành khác nhau. Đôi khi một giải pháp đơn giản là không làm gì mới cả, cũng là một giải pháp chấp nhận được, nêu phân tích cho thấy chi phí để khôi phục hệ thống (chẳng hạn như chỉ là việc quét, diệt virus và cài lại các phần mềm thông dụng) là rẻ tiền hơn so với các giải pháp ATTT được nêu.

Phân tích rủi ro (risk analysis)

Đây cũng là một vấn đề điển hình thường được cân nhắc trước khi đầu tư cho một giải pháp an ninh, thường là tốn kém đáng kể. "Có bảo vệ hay không?"," bảo vệ đến mức độ nào?" là các câu hỏi cần quyết định. Dựa vào việc phân tích rủi ro sẽ có thể xảy ra nêu không thực hiện biện pháp cụ thể nào đó, người ta có thể đưa ra quyết định tương ứng, để chọn lựa giải pháp hiệu quả nhất, vừa giảm thiểu rủi ro, vừa không gây chi phí lớn quá mức chịu đựng.

Va chạm với luật và lệ

Một số công ty đa quốc gia thường gấp vấn đề này khi phát triển một chính sách an toàn chung trên nhiều quốc gia mà họ đặt tổ chức kinh doanh. Nhiều khi những chính sách bảo mật đã được hoàn thiện và chấp nhân tại chính quốc và 1 số quốc gia nào đó lại không thể được chấp nhận, hoặc gây sự phản đối nào đó (do các lề thói, thói quen không thành văn) ở môi trường của một quốc gia mà công ty này bắt đầu khai phá thị trường. Vì vậy những chính sách ATTT cũng cần phải được xem xét lại, có sự thương lượng và chỉnh nắn cho phù hợp với môi trường mới. Công ty Google vì đã không làm tốt điều này mà phải rút, không tổ chức kinh doanh tại thị trường Trung Quốc.

Các vấn đề xung quanh con người và tổ chức

Quyền lực và trách nhiệm. Hai điều này phải sánh đôi cân bằng. Một người được trao trách nhiệm phụ trách về an ninh thông tin, thường là một chuyên gia ICT có tuổi đời còn trẻ, cũng phải được trao một quyền lực đúng mức căn cứ theo hệ thống cấp bậc trong tổ chức. Thiếu quyền lực tương ứng phù hợp, người dù có năng lực cao cũng không thể hoàn thành trách nhiệm khó khăn, đặc biệt trong một địa hạt mà sự thiếu hiểu biết về nó có thể có ở các cấp rất cao. Chẳng hạn nếu một vị trí lãnh đạo của công ty coi thường không tuân thủ qui định nào đó (ví dụ như về lựa chọn mật khẩu) mà phụ

trách về an ninh đặt ra, thái độ đó sẽ lây lan ra các nhân viên khác, làm phá vỡ sự nghiêm minh chặt chẽ cần thiết để đảm bảo các chính sách được tuân thủ.

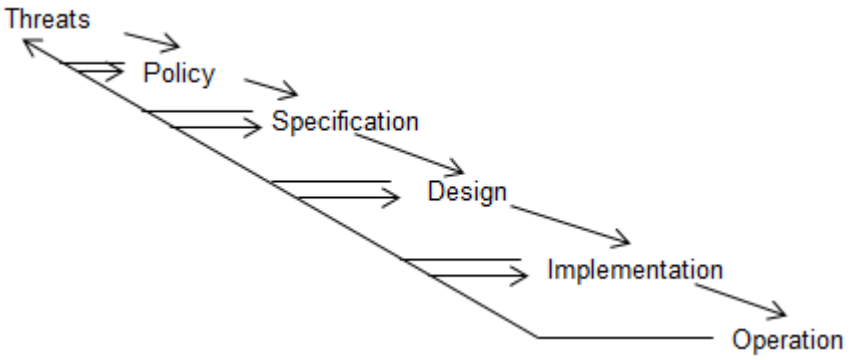
Ảnh hưởng của động cơ lợi nhuận. Các công ty doanh nghiệp thường bị lôi kéo rất mạnh bởi động cơ phải đầu tư cho có lãi, không đầu tư nhiều tiền vào dự án nào khi không sinh được lợi nhuận. Điều đó tạo một tình thế trớ trêu vì đầu tư vào ATTT sẽ tiêu tốn nhiều tiền mà không sinh ra lợi nhuận trực tiếp; người ta thường chỉ thấm thía sự cần thiết của ATTT khi đã bị thiệt hại đáng kể do bị tấn công khai thác các điểm yếu của hệ thống thông tin.

Quan hệ giữa con người. Các giải pháp cần có các chính sách thỏa đáng xem xét các mối đe dọa có thể đến từ các đối tượng con người khác nhau; người ta thường tập trung quan tâm đến các khả năng tấn công từ bên ngoài mà ít chú ý đến các khả năng tấn công từ bên trong. Những mối đe dọa từ phía bên trong đương nhiên là nguy hiểm hơn nhiều, và nên nhớ chúng có thể đến từ không chỉ nhân viên hiện thời của tổ chức, công ty mà còn từ các nhân viên cũ, đã thôi việc hoặc đã bị sa thải (loại này còn nguy hiểm hơn do bất mãn gây ra).

Chế tạo quan hệ xã hội (social engineering) là một chủ đề đáng nói ở đây: kẻ tấn công có thể giả mạo và bịa đặt những mối quan hệ với các cá nhân có vị trí quan trọng của một tổ chức, và thông qua đó lừa gạt các nhân viên quản trị ICT (thường còn trẻ) để chiếm quyền điều khiển các tài khoản quan trọng, và ăn cắp thông tin qui giá của công ty.

A 9 z Q J ÿ á L D Qông tin j Q W K

Toàn bộ khảo sát trên cho chúng ta một bức tranh toàn thể về quá trình xây dựng một giải pháp an toàn thông tin. Tóm tắt lại, quá trình này gồm các bước: khảo sát tìm hiểu các mối đe dọa → xây dựng chính sách bảo vệ → xây dựng đặt tả yêu cầu từ khái quát đến cụ thể → xây dựng thiết kê mô hình → cài đặt giải pháp → vận hành và điều hành. Quá trình này có thể lặp lại nhiều lần tạo thành các chu trình, được gọi là vòng đời an toàn thông tin. Sự lặp lại nảy thông thường được tiến hành khi có những yêu cầu mới nảy sinh, hoặc những sự thay đổi, đổi mới đến từ phía môi trường công việc, nghiệp vụ. Sự thay đổi của các chức năng thuần túy nghiệp vụ có thể dẫn đến những mối đe doại mới, tức là làm nảy sinh việc cập nhật và hoàn thiện bộ chính sách, … tức là chúng ta bắt đầu một chu trình mới để cập nhật lại giải pháp ATTT.



Hình vẽ 1. Vòng đời an toàn

B 1Ä1 7¦1* &j 6â &1ê $à, .ú 6l $1 72 THÔNG TIN

Ở trên chúng ta đã làm quen với một cách nhìn toàn thể vào bài toán xây dựng giải pháp an toàn thông tin cho một hệ thống thông tin cụ thể, nó thể hiện phần nào cái toàn cảnh, khó khăn và thách thức mà một người chuyên gia ATTT (chịu trách nhiệm cao) phải đương đầu. Một kỹ sư trẻ mới tốt nghiệp đại học thì không bị yêu cầu phải có những kiến thức đủ sâu và rộng để bao quát hết, nhưng khung nhìn trên cho thấy thực tế đòi hỏi những gì ở một chuyên gia ATTT, và tạo ra động lực để một sinh viên có thể phấn đấu trong quá trình học đại học cũng như đoạn đường rèn luyện lâu dài sau đó để có thể trở thành một chuyên gia thực thụ.

Giáo trình này sẽ cung cấp cho các bạn sinh viên một cơ sở ban đầu về học vấn, về các phương pháp kỹ thuật cơ bản trong an toàn thông tin, và quan trọng nhất là một phương pháp tư duy phân tích bài bản, hệ thống để từ đó các bạn có thể tự mình tiếp tục rèn luyện, hoàn thiện tới những trình độ cao hơn trong nghệ nghiệp chuyên môn, đặc biệt là khi đã có cơ hội cọ sát thực tế khi đã ra trường.

Mục này sẽ đưa ra một cái nhìn lướt về các kiến thức cơ sở sẽ được trình bày trong toàn giáo trình. Với người kỹ sư, có 4 thuật ngữ và cũng là phạm trù cơ bản khi nói về ATTT là: điểm yếu, dễ tổn thương (vulnerability) của hệ thống; mối đe dọa (threat); tấn công (attack); và biện pháp phòng chống (control, security measure). Ba phạm trù đầu phản ánh các mức độ của kiến thức của chúng ta khi khảo sát các khả năng một hệ thống có thể bị tấn công cho đến khi những loại tấn công thực sự đã xảy ra. Mục 1 của chương này đã giới thiệu khá rõ nét về các phạm trù này.

Phạm trù cuối bao gồm tất cả những phương pháp có thể có để loại trừ các mối nguy hiểm và các tấn công thực sự. Có thể tạm liệt kê các biện pháp để điều khiển kiểm soát an toàn và bảo mật của một HTTT như sau:

1. Điều khiển thông qua phần mềm:

- Các tiêu chuẩn về mã hoá, kiểm tra và bảo trì.