thái SUBSCRIBE
a donut lover

Làm an toàn thông tin thì học gì?

May 02, 2012

1 Giới thiệu

Tôi nhận được thư từ của nhiều bạn hỏi về việc nên học gì và như thế nào để có thể tìm được việc làm và làm được việc trong ngành an toàn thông tin (information security). An toàn thông tin là một ngành rộng lớn với rất nhiều lĩnh vực. Những gì tôi biết và làm được chỉ gói gọn trong một hai lĩnh vực. Có rất nhiều mảng kiến thức cơ bản mà tôi không nắm vững và cũng có nhiều kỹ năng mà tôi không thạo. Hack tài khoản Yahoo! Mail là một trong số đó. Tôi cũng không biết cách tìm địa chỉ IP của bạn chat :-(.

Xét theo năm mức ngu dốt thì tôi nằm ở mức "1OI - thiếu kiến thức" ở hầu hết các lĩnh vực trong an toàn thông tin. Cũng có lĩnh vực tôi nằm ở mức "2OI - thiếu nhận thức". Nhiều lần đọc sách vở hoặc nói chuyện với đồng nghiệp, tôi hay nhận ra rằng có nhiều thứ tôi không biết là tôi không biết. Theo ý của anh Ngô Quang Hưng thì đây là chuyện bình thường:

> *Dân máy tính thường phải đọc/học rất nhiều để theo kịp sự phát triển với tốc độ ánh sáng của ngành mình. Trong quá trình này, với mỗi vấn đề X của ngành, ta sẽ chuyển dần dần từ 3OI xuống 1OI. Sau đó, nếu X là cái mà ta thật sự thích hoặc cần cho công việc thì sẽ chuyển nó lên 0OI.*
>
> *Rất nhiều sinh viên và nghiên cứu sinh KHMT ở mức 3OI khi mới bắt đầu đi học. Sau đó họ tìm hiểu về quá trình nghiên cứu, quá trình tìm các vấn đề và hướng nghiên cứu mới, quá trính cập nhật kiến thức về ngành của mình, và chuyển dần các thứ lên 2OI. Để có một quá trình hiệu quả từ 3OI lên 2OI không*

dễ chút nào. Ví dụ đơn giản: các journals, conference nào trong ngành mình là có giá trị, làm thế nào để tìm đọc các bài trong chúng, phương pháp lọc bài đọc thế nào, vân vân.

Tôi thấy anh Hưng nói có lý, nên mục tiêu chính của bài viết này là cung cấp một quá trình hiệu quả để bớt ngu về an toàn thông tin.

2 Làm an toàn thông tin là làm gì?

Tôi muốn viết phần này vì nhiều người tưởng tôi làm bảo vệ khi tôi nói tôi làm security. Ngoài ra có lẽ là do thị trường việc làm an toàn thông tin ở Việt Nam không phong phú nên hầu hết đều nghĩ rằng làm an toàn thông tin nghĩa là đảm bảo an toàn hệ thống mạng (network/system security), trong khi thực tế đây chỉ là một trong số rất nhiều công việc trong ngành.

Trong bốn phần nhỏ tiếp theo, tôi sẽ giới thiệu bốn nhóm công việc chính trong ngành. Đối với mỗi nhóm công việc, tôi sẽ bàn một chút về triển vọng nghề nghiệp ở Việt Nam và Mỹ, hai nơi mà tôi có dịp được quan sát. Nếu bạn không biết bạn thích làm gì thì cứ chọn một công việc rồi làm thử. Các công việc này đều có liên quan nhau, nên kiến thức mà bạn học được trong quá trình thử vẫn hữu ích cho những nghề khác.

2.1 An toàn sản phẩm (product security)

Công việc chính của nhóm này là làm việc với các đội phát triển sản phẩm để đảm bảo sản phẩm làm ra an toàn cho người dùng và an toàn cho hệ thống của công ty, cụ thể là:

- Kiểm định mã nguồn và thiết kế của sản phẩm
- Phát triển các giải pháp kỹ thuật và quy trình phát triển phần mềm an toàn để phát hiện và ngăn chặn những kỹ thuật tấn công đã biết
- Đào tạo nhân lực để nâng cao nhận thức về an toàn thông tin cũng như kỹ năng viết mã an toàn
- Nghiên cứu các hướng tấn công mới có thể ảnh hưởng hệ thống sản phẩm và dịch vụ của công ty

Tóm gọn lại thì nhóm này chuyên tìm lỗ hổng và kỹ thuật tấn công mới. Đây là công việc của tôi và tôi thấy đây là công việc thú vị nhất trong ngành :-).

Ở Mỹ thì thông thường thì chỉ có các hãng có phần mềm và dịch vụ lớn như Facebook, Google, Microsoft, Oracle, v.v. hay các tập đoàn tài chính ngân hàng lớn mới có đội ngũ tại chỗ để đảm nhiệm công việc này. Các công ty nhỏ thường chỉ thuê dịch vụ của các công ty tư vấn. IBM và Big Four đều có cung cấp dịch vụ tư vấn này. Dẫu vậy nếu được chọn lựa thì tôi sẽ chọn làm cho các công ty chuyên sâu như Matasano, iSec, Leviathan, Gotham, IOActive, Immunity, v.v.

Ở Việt Nam thì thị trường việc làm cho người làm an toàn sản phẩm có vẻ ảm đạm hơn. Cho đến nay tôi biết chỉ có một vài công ty ở Việt Nam là có nhân viên chuyên trách lĩnh vực này. Các công ty khác (nếu có quan tâm đến an toàn thông tin) thì hầu như chỉ tập trung vào an toàn vận hành. Các công ty tư vấn an toàn thông tin ở Việt Nam cũng không tư vấn an toàn sản phẩm, mà chỉ tập trung tư vấn chung chung về các quy trình và tiêu chuẩn an toàn thông tin.

2.2 An toàn vận hành (operations security)

Công việc chính của nhóm này là đảm bảo sự an toàn cho toàn bộ hệ thống thông tin của doanh nghiệp, với ba nhiệm vụ chính:

- Ngăn chặn: đưa ra các chính sách, quy định, hướng dẫn về an toàn vận hành; kiện toàn toàn bộ hệ thống thông tin, từ các vành đai cho đến máy tính của người dùng cuối; cấp và thu hồi quyền truy cập hệ thống; quét tìm lỗ hổng trong hệ thống, theo dõi thông tin lỗ hổng mới và làm việc với các bên liên quan để vá lỗi, v.v.
- Theo dõi và phát hiện: giám sát an ninh mạng.
- Xử lý: phản hồi (incident response) và điều tra số (digital forensics) khi xảy ra sự cố an toàn thông tin, từ tài khoản của nhân viên bị đánh cắp, rò rỉ thông tin sản phẩm mới cho đến tấn công từ chối dịch vụ.

Đây là công việc khó nhất, nhưng lại ít phần thưởng nhất của ngành an toàn thông tin.

Tương tự như trên, chỉ có các hãng lớn của Mỹ mới có đội ngũ tại chỗ để phụ trách toàn bộ khối lượng công việc đồ sộ này, nhất là mảng xử lý và điều tra. Đa số các công ty chỉ tập trung vào ngăn chặn và sử dụng dịch vụ của bên thứ ba cho hai mảng còn lại. Các hãng như Mandiant, Netwitness hay HBGary cung cấp dịch vụ điều tra các vụ xâm nhập và có rất nhiều hãng khác cung cấp dịch vụ giám sát an ninh mạng.

Ở Việt Nam thì thị trường việc làm cho người làm an toàn vận hành tương đối phong phú hơn so với an toàn sản phẩm. Các công ty và tổ chức tài chính lớn đều có một vài vị trí chuyên trách về an toàn vận hành. Đa số người làm về an toàn thông tin ở Việt Nam mà tôi biết là làm trong lĩnh vực này. Dẫu vậy hầu như chưa có ai và công ty tư vấn nào làm về phản hồi và điều

tra sự cố.

2.3 Phát triển công cụ (applied security)

Công việc chính của nhóm này là phát triển và cung cấp các công cụ, dịch vụ và thư viện phần mềm có liên quan đến an toàn thông tin cho các nhóm phát triển sản phẩm sử dụng lại.

Nhóm này bao gồm các kỹ sư nhiều năm kinh nghiệm và có kiến thức vững chắc về an toàn thông tin, viết mã an toàn và mật mã học. Họ phát triển các thư viện và dịch vụ dùng chung như phân tích mã tĩnh - phân tích mã động (static - dynamic code analysis), hộp cát (sandboxing), xác thực (authentication), kiểm soát truy cập (authorization), mã hóa (encryption) và quản lý khóa (key management), v.v.

Đây là dạng công việc dành cho những ai đang viết phần mềm chuyên nghiệp và muốn chuyển qua làm về an toàn thông tin. Đây cũng là công việc của những người thích làm an toàn sản phẩm nhưng muốn tập trung vào việc xây dựng sản phẩm hơn là tìm lỗ hổng.

Rõ ràng loại công việc này chỉ xuất hiện ở các công ty phần mềm lớn. Ở các công ty phần mềm nhỏ hơn thì các kỹ sư phần mềm thường phải tự cáng đáng công việc này mà ít có sự hỗ trợ từ nguồn nào khác. Ở Việt Nam thì tôi không biết có ai làm dạng công việc này không.

2.4 Tìm diệt mã độc và các nguy cơ khác (threat analysis)

Ngoài an toàn sản phẩm ra thì đây là một lĩnh vực mà tôi muốn làm. Công việc chính của nhóm này là phân tích, truy tìm nguồn gốc và tiêu diệt tận gốc mã độc và các tấn công có chủ đích (targeted attack). Mã độc ở đây có thể là virút, sâu máy tính, hay mã khai thác các lỗ hổng đã biết hoặc chưa được biết đến mà phần mềm diệt virút thông thường chưa phát hiện được. Các loại mã độc này thường được sử dụng trong các tấn công có chủ đích vào doanh nghiệp.

Tôi nghĩ rằng sau hàng loạt vụ tấn công vừa rồi thì chắc hẳn các công ty lớn với nhiều tài sản trí tuệ giá trị đều muốn có những chuyên gia trong lĩnh vực này trong đội ngũ của họ. Ngoài ra các công ty chuyên về điều tra và xử lý sự cố như Mandiant, HBGary hay Netwitness mà tôi đề cập ở trên đều đang ăn nên làm ra và lúc nào cũng cần người. Các công ty sản xuất phần mềm diệt virút dĩ nhiên cũng là một lựa chọn.

Ở Việt Nam thì tôi nghĩ hầu hết doanh nghiệp vẫn chưa thấy được nguy cơ đến từ các cuộc tấn công có chủ đích, thành ra họ sẽ không tuyển người chuyên trách vấn đề này. Tôi cũng không biết có công ty tư vấn nào ở Việt Nam chuyên về điều tra và xử lý sự cố hay không. Tôi nghĩ lựa chọn khả dĩ nhất cho những người thích mảng công việc này là các công ty phần mềm diệt virút.

Tuy nhiên cũng cần lưu ý rằng trong vài năm gần đây ở Việt Nam còn xuất hiện những loại mã độc nhắm vào đông đảo người dùng máy tính bình thường. Vấn nạn này có lẽ sẽ còn kéo dài trong nhiều năm tới và lẽ đương nhiên "phe ta" lúc nào cũng cần thêm những chiến sĩ lành nghề như anh TQN. Thành ra dẫu triển vọng nghề nghiệp không sáng sủa cho lắm, nhưng tôi rất hi vọng sẽ ngày càng nhiều người tham gia vào việc phân tích các mã độc nhắm vào người dùng máy tính ở Việt Nam. Đối với tôi họ là những người hùng thầm lặng, chiến đấu đêm ngày với các "thế lực thù địch" để bảo vệ tất cả chúng ta.

3 Học như thế nào?

Đa số những bạn viết thư cho tôi đều đang học đại học ngành CNTT và tất cả đều than rằng chương trình học quá chán, không có những thứ mà các bạn muốn học. Tôi nghĩ đây là một ngộ nhận.

Hối tiếc lớn thứ nhì trong sự nghiệp học tập mấy chục năm của tôi là đã không học nghiêm túc khi còn là sinh viên (hối tiếc lớn nhất là tôi đã không nghỉ hẳn, nhưng đó là một câu chuyện dài khác). Tôi cũng đã nghĩ rằng chương trình học ở đại học là lạc hậu và không cần thiết. Bây giờ nhìn lại thì tôi thấy nội dung và cách dạy của từng môn học thì đúng là lạc hậu (chỉ có mấy môn triết học Mác-Lênin là bắt kịp ánh sáng thời đại), nhưng toàn bộ giáo trình đại học vẫn cung cấp được một cái sườn kiến thức rất cần thiết cho một kỹ sư an toàn thông tin.

Ở đại học người ta có cách tiếp cận top-down, nghĩa là dạy từ đầu đến cuối những kiến thức nằm trong chương trình. Điều này dễ dẫn đến tình trạng là người học phải học những kiến thức mà họ không thấy cần thiết. Nếu chương trình học cũ kỹ và không có nhiều thực hành, hoặc người dạy không chỉ ra được bức tranh toàn cảnh, vị trí hiện tại của người học và bước tiếp theo họ nên làm là gì thì người học sẽ dễ cảm thấy rằng họ đang phí thời gian học những kiến thức vô bổ.

Trong khi khi đi làm thì cách tiếp cận là bottom-up, nghĩa là lao vào làm, thấy thiếu kiến thức chỗ nào thì học để bù vào chỗ đó. Lúc này tôi hoàn toàn chủ động trong việc học và tôi cũng hiểu rõ tôi cần học cái gì và tại sao. Điều thú vị là mỗi khi truy ngược lại nguồn gốc của những kiến thức tôi cần phải có, tôi thường thấy chúng nằm trong chương trình đại học.

Ví dụ như tôi muốn luyện kỹ năng dịch ngược mã phần mềm (reverse code engineering - RCE) thì tôi thấy rằng tôi cần phải có kiến thức về tổ chức và cấu trúc máy tính. Hoặc nếu tôi muốn học về mật mã học thì tôi phải học lý thuyết tính toán, mà khởi nguồn là lý thuyết automata. Nhưng tại sao trước đó tôi cũng đi làm nhưng không thấy được những lỗ hổng kiến thức này? Tôi nghĩ là do tôi làm không đủ sâu. Ví dụ như nếu bạn suốt ngày chỉ lập trình PHP thì bạn sẽ không thể hiểu được tại sao phải nắm vững tổ chức và kiến trúc máy tính. Hoặc giả

như công việc của bạn là sysadmin thì cũng sẽ rất khó để bạn thấy được tại sao cần phải học lý thuyết automata.

Những gì tôi nói lan man ở trên có thể tóm gọn lại thế này:

- Học dựa theo chương trình đại học. Nếu bạn đang học đại học các ngành công nghệ thông tin, khoa học máy tính hay toán tin thì nên tập trung vào việc học các môn trong trường. Các học liệu trong phần 4 cũng được soạn theo các đại học lớn trên thế giới.
- Học kiến thức căn bản thật vững (cái gì là căn bản thì xem phần 4), những món còn lại khi nào cần (căn cứ vào nhu cầu công việc) thì hẵng học.
- Tìm dự án lề (side project) mà bạn thích để làm để có thể nhanh chóng nhận ra những mảng kiến thức còn thiếu.
- Thời điểm tốt nhất để học một cái gì đó là khi bạn đang là sinh viên. Thời điểm tốt thứ hai là ngay bây giờ!

Các lớp mà tôi liệt kê trong phần 4 đa số là của đại học Stanford. Bạn không cần phải đến tận nơi, ngồi trong lớp mới có thể học được. Tôi thấy trong nhiều trường hợp thì bạn chỉ cần đọc lecture notes, sách giáo khoa mà lớp sử dụng rồi làm bài tập đầy đủ thì vẫn sẽ tiếp thu đủ kiến thức. Một số lớp mà tôi liệt kê dưới đây được dạy miễn phí rộng rãi trên Coursera.

Bạn có thể tham khảo chương trình SCPD nếu muốn học chung với các sinh viên Stanford khác. Đây là chương trình học từ xa thông qua video. Buổi sáng lớp diễn ra thì buổi chiều bạn đã có video để xem. Thi cử như các sinh viên chính quy khác và điểm phải trên B mới được học tiếp. Đây là chương trình mà tôi theo học. Điểm thú vị là mỗi học kỳ bạn chỉ cần lấy một lớp, nhưng Stanford vẫn sẽ cho bạn xem video của tất cả các lớp khác.

Ngoài Stanford và Coursera ra, bạn cũng có thể tham khảo các lớp trên Udacity, OCW và MITx. Khi tôi đang viết những dòng này thì MIT và Harvard công bố dự án edX. Chúng ta đang sống trong một thời đại cực kỳ thú vị! Bây giờ chỉ cần bạn chịu học thì muốn học cái gì cũng có lớp và học liệu miễn phí. Nhưng mà học cái gì bây giờ?

4 Học cái gì?

Có ba món quan trọng cần phải học: lập trình, lập trình và lập trình! Để làm việc được trong ngành này, bạn phải yêu thích lập trình. Không có cách nào khác. Thề luôn!

Tôi dành khá nhiều thời gian tìm hiểu giáo trình khoa học máy tính của các trường đại học lớn trên thế giới và tôi thấy tất cả các môn học đều có phần bài tập là lập trình. Học cái gì viết phần mềm cho cái đó. Học về hệ điều hành thì phần bài tập là viết một hệ điều hành. Học về

mạng thì viết phần mềm giả lập router, switch hay firewall. Cá nhân tôi cũng thấy rằng lập trình là cách tốt nhất để tiếp thu kiến thức một môn học nào đó, biến nó thành của mình. Nói cách khác, lập trình là một cách mã hóa tri thức khá hiệu quả.

Ngoài ra nhìn vào mô tả công việc ở phần 2, bạn cũng có thể thấy kỹ năng lập trình quan trọng đến dường nào, bởi hầu hết các vấn đề và giải pháp của an toàn thông tin là đến từ phần mềm. Rõ ràng muốn tìm lỗi của phần mềm thì bạn phải hiểu được phần mềm thông qua mã nguồn trực tiếp hay trung gian của nó. Rất có thể bạn sẽ không phải lập trình hàng ngày, nhưng bạn phải viết được những công cụ nhỏ hay những thư viện hỗ trợ cho công việc và các lập trình viên khác.

Vậy làm thế nào để lập trình giỏi? Câu hỏi này làm tôi nhớ đến câu chuyện cười về ông lập trình viên không thể ra khỏi phòng tắm vì trên chai dầu gội có ghi hướng dẫn sử dụng là "cho vào tay, xoa lên đầu, xả nước và lập lại". Từ khóa trong câu chuyện này là "lập lại": muốn giỏi lập trình thì cách tốt nhất là lập trình nhiều vô!

Nhưng mà lập trình bằng ngôn ngữ gì bây giờ? Đây là câu hỏi dễ làm cho các lập trình viên oánh nhau nhất ;-). Cá nhân tôi thấy rằng người làm an toàn thông tin bây giờ cần phải thông thạo C, x86 Assembly, Python (hoặc Ruby) và JavaScript. Tôi có nói lý do tại sao trong phần giới thiệu sách tiếp theo.

Lập trình

- Brian Kernighan, Dennis Ritchie, *The C Programming Language (2nd Edition)*: kinh điển và phải-đọc cho tất cả những ai muốn học C! Linus Torvalds từng nói rằng "[...] *all right-thinking people know that (a) K&R are _right_ and (b) K&R are right*". Tôi đã từng rất sợ C (vì nghĩ nó phức tạp), và cuốn này giúp tôi không còn sợ nữa.

- Randal Bryant, David O'Hallaron, *Computer Systems: A Programmer's Perspective*: cuốn này được dùng cho lớp CS107. Đọc cuốn này và làm bài tập của lớp CS107 sẽ rèn cho bạn kỹ năng lập trình C và x86 Assembly. Sau khi đọc cuốn này, bạn sẽ biết tại sao có lỗi tràn bộ đệm và cách khai thác chúng. Tôi rất thích các chương nói về x86 và sự liên kết giữa các công cụ như preprocessor, compiler và linker.

- David Hanson, *C Interfaces and Implementations*: muốn mau "lên cơ" bida thì phải thường xuyên xem người khác chơi để mà học "đường" mới. Tương tự, muốn giỏi lập trình thì phải thường xuyên đọc mã của những cao thủ. David Hanson là một cao thủ C và cuốn sách này sẽ chỉ cho bạn nhiều "đường" mới trong việc sử dụng C. Tôi thích các bài tập của cuốn sách này. Tôi nghĩ chỉ cần luyện các bài này là đủ để trở thành một lập trình viên C hạng lông.

- Justin Seitz, *Gray Hat Python: Python Programming for Hackers and Reverse Engineers*: cuốn này sẽ giúp bạn sử dụng Python để viết những công cụ nho nhỏ mà bất kỳ ai làm an toàn thông tin cũng sẽ phải viết một vài lần trong đời.

- Douglas Crockford, *JavaScript: The Good Parts*: JavaScript là ngôn ngữ thống trị WWW. Nếu bạn muốn làm an toàn (ứng dụng và trình duyệt) web thì bắt buộc phải thành thạo ngôn ngữ. Cuốn sách rất mỏng này của tác giả JSON giới thiệu đầy đủ những vấn đề mà người làm an toàn ứng dụng cần phải biết về JavaScript. Cuốn này có thể dùng làm sách giáo khoa thay cho cuốn "Javascript: The Definitive Guide" trong lớp CS142 (xem bên dưới). Đọc cuốn này tôi mới hiểu closure là gì và bản chất prototypal của JavaScript.

- Sẽ đọc: những cuốn được giới thiệu ở đây.

Hệ điều hành

- Abraham Silberschatz, Peter Galvin, and Greg Gagne, *Operating System Concepts, 8th Edition Update*: cuốn này là giáo trình của lớp CS140. Tôi nghĩ không cần đọc cuốn này, chỉ cần đọc notes và làm bài tập (viết các phần khác nhau của một hệ điều hành!) là đủ. Đây là một lớp nặng. Tôi theo đuổi lớp CS140 này giữa chừng thì phải dừng lại do không có đủ thời gian.

- Intel Software Developer Manuals: tôi thấy nên đọc tài liệu của 80386 trước, rồi sau đó hẵng đọc tài liệu của các CPU mới hơn.

- Red Hat, *Introduction to System Administration*: tôi rất thích chương nói về "philosophy of sysadmin" của cuốn này và tôi nghĩ kỹ năng quản trị hệ thống là cực kỳ cần thiết khi muốn nghiên cứu các kỹ thuật tấn công/phòng thủ mới. Không thể làm an toàn vận hành nếu không có kỹ năng quản trị hệ thống.

Mạng máy tính

- Richard Stevens, *TCP/IP Illustrated Vol I*: cuốn sách này quá nổi tiếng rồi nên tôi nghĩ không cần phải giới thiệu. Tôi chưa đọc Vol II, III nhưng nhất định sẽ tìm đọc trong thời gian tới. Lớp CS144 dùng một cuốn sách khác. Tôi chưa học lớp này, nhưng tôi thấy bài tập của họ khá thú vị.

- Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent, Ronald W. Ritchey, *Inside Network Perimeter Security, 2nd Edition*: tôi thích cuốn này vì nó viết rất dễ hiểu về các vấn đề và công cụ thường gặp trong an toàn mạng.

- Sẽ đọc: Fyodor, *Nmap Network Scanning*.

Sau khi đã có những kiến thức cơ bản ở trên, bạn có thể theo đuổi lớp CS155. Lớp này có trên Coursera với tên Computer Security. Song song với lớp CS155, bạn có thể tìm đọc các sách sau:

Tìm lỗi phần mềm

- Mark Dowd, John McDonald, Justin Schuh, *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*: Kinh điển và phải-đọc! Cuốn này là kinh thánh của lĩnh vực an ninh ứng dụng. Tôi thích nhất phần nói về tràn số nguyên và những vấn đề của ngôn ngữ C trong cuốn này.
- Dafydd Stuttard, Marcus Pinto, *The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws*: cuốn này tập trung vào ứng dụng web. Tôi không đọc cuốn này kỹ lắm, mà chỉ thường dùng nó để tham khảo. Dẫu vậy tôi nghĩ nó là một cuốn giới thiệu tốt cho những ai mới bắt đầu.
- Michal Zalewski, *The Tangled Web*: cuốn này mới xuất bản gần đây nhưng đã ngay lập tức trở thành kinh điển! Cuốn này đúc kết quá trình nghiên cứu về an ninh web trong vài năm trời của một trong những hacker xuất sắc nhất thế giới. Tôi nghĩ chỉ cần đọc cuốn này là bạn đã có thể bắt đầu tìm lỗ kiếm tiền được rồi. Cuốn này và cuốn ở trên được dùng làm sách giáo khoa của lớp CS142.
- Sẽ đọc: Tobias Klein, *A Bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security*

Dịch ngược mã phần mềm

- Eldad Eilam, *Reversing: Secrets of Reverse Engineering*: mặc dù có rất nhiều người viết về RCE nhưng tôi thấy đây là cuốn duy nhất hệ thống hóa được các bước quan trọng cần phải làm khi cần dịch ngược mã của một tệp chương trình nào đó.
- Chris Eagle, *The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler*: IDA Pro là công cụ tốt nhất để làm RCE và đây là cuốn sách tốt nhất về IDA Pro. Nắm vững C và x86 Assembly thì chỉ cần đọc cuốn này là bạn có thể bắt đầu RCE các phần mềm phức tạp.
- Tham khảo các tài liệu về dịch ngược mã phần mềm của lớp PenTest của đại học NYU.
- Sẽ đọc: Michael Sikorski, Andrew Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*

Điều tra số (digital forensics)

- Brian Carrier, *File System Forensic Analysis*: Brian Carrier là tác giả của bộ công cụ forensic nổi tiếng The Sleuth Kit. Cuốn này đã giúp tôi "khai quật" được một đoạn video bị xóa lưu trong một máy camera quay lén các máy ATM.

- Sẽ đọc: Cory Altheide, Harlan Carvey, *Digital Forensics with Open Source Tools*

Mật mã hóa

- Niels Ferguson, Bruce Schneier, *Practical Cryptography*: tôi có nhiều kỷ niệm đẹp với cuốn này ;-). Hầu hết các kết quả làm việc của tôi trong vài năm vừa rồi là nhờ vào việc đọc cuốn này. Tôi chép lại đây giới thiệu rất hay của một người bạn: "*The best security books, you can read "inside out", taking any recommendation on what to do and looking for people to do the opposite to find flaws. "Firewalls and Internet Security" was like that. So was "Practical Unix Security", and so is TOASSA. This is that book for crypto. It's also the one book on crypto you should allow yourself to read until you start actually finding crypto flaws.*"

- Jonathan Katz, Yehuda Lindell, *Introduction to Modern Cryptography: Principles and Protocols*: đây là sách giáo khoa của lớp CS255. Lớp này là lớp Cryptography trên Coursera.

Chú ý đây là những cuốn sách tập trung vào công việc hàng ngày và sở thích của tôi -- nói cách khác, còn thiếu nhiều sách của các mảng công việc khác. Dẫu vậy tôi nghĩ những cuốn sách này sẽ giúp bạn có được một kiến thức nền tảng vững chắc để từ đó theo đuổi các nghề nghiệp khác nhau trong ngành an toàn thông tin. Trong thời gian tới tôi sẽ cập nhật thêm những cuốn sách mà tôi đang và sẽ đọc. Nếu bạn biết sách nào hay thì hãy giới thiệu cho tôi.

Ngoài ra trong các sách mà tôi vừa liệt kê không có cuốn sách toán (và lý thuyết khoa học máy tính) nào cả. Tôi nghĩ bạn sẽ tự có câu trả lời cho câu hỏi "Có nên học toán hay không?" khi bắt đầu học mật mã. Về hai mảng này thì tôi rất thích lớp "Great Ideas in Theoretical Computer Science" của Scott Aaronson và cuốn "A Computational Introduction to Number Theory and Algebra" của Victor Shoup. Thích đến nỗi tôi phải viết đoạn này chỉ để nhắc đến chúng ;-). Tôi cũng đã từng dành ra nhiều tháng để đánh vật với Introduction to the Theory of Computation của Michael Sipser. Nhưng thôi, tôi không muốn giới thiệu sách toán nữa vì tôi rất dốt món này!

5 Bắt đầu nói nhảm và hết

Phew! Không ngờ là tôi cũng viết được cho đến đây (hi vọng là bạn vẫn đang đọc!). Tôi định viết dông dài về thái độ học tập này nọ, nhưng thôi bài đã dài và nhiều thông tin rồi, nên tôi chỉ nói ngắn gọn thế này:

Cái mà tôi vừa "vẽ" ra là một con đường. Thú thật là tôi không biết đích đến của nó là gì -- tôi

chỉ biết rằng hành trình mà tôi đã đi qua (và hi vọng là những chặng đường sắp tới) đã mang đến cho tôi rất nhiều niềm vui -- niềm vui của một con người đi khám phá thế giới, chinh phục những thử thách, để rồi chia sẻ những câu chuyện hay ho với tất cả mọi người.

Mỗi ngày tôi đều dành thời gian đọc sách, làm bài tập, viết mã hoặc chứng minh một cái gì đó. Không ai bắt tôi phải làm những chuyện đó. Có những thứ tôi học cũng không (hoặc chưa) có liên quan gì đến công việc. Tôi học chỉ vì tôi thích và tò mò. Tôi học vì tôi muốn hiểu thêm những thứ mà tôi cho là hay ho. Tôi học vì tôi muốn đi mãi, đi mãi, đi đến tận cùng những cái mà người ta viết trong sách, để xem ở đó có gì hay không.

Hôm rồi tôi đọc một mẩu chuyện về Richard Feynman, trong đó có đoạn kể về lúc Feynman bị bệnh gần đất xa trời, ông tâm sự rằng, "[I'm going to die but I'm not as sad as you think because] when you get as old as I am, you start to realize that you've told most of the good stuff you know to other people anyway". Đương nhiên những gì tôi biết làm sao mà "good" bằng những gì Feynman biết, nhưng dẫu sao thì tôi cũng sẽ học theo Feynman: có biết chuyện gì hay ho thì kể cho nhiều người khác cùng biết. Bài này là một chuyện như thế.

Happy hacking!

(cảm ơn đại ca M. đã đọc và sửa bản nháp của bài này)

Quang Le said...

Thanks Thái, bài viết rất hay, hay đến nỗi mình phải comment :). Esp thanks for the SCPD link. Hope to see you again sometimes (maybe in US ;)

6:03 PM

hoàng anh vũ said...

Bài viết thực sự hay và ý nghĩa! Anh cho em copy về blog của em nha. Để khi nào đó em ngồi đọc lại. Cám ơn anh đã viết bài!

12:23 AM

anuunh said...

Cám ơn anh vì những chia sẻ rất bổ ích cho bản thân em và nhiều bạn trẻ khác. Em thích nhất đoạn này: "Mỗi ngày tôi đều dành thời gian đọc sách, làm bài tập, viết mã hoặc chứng minh một cái gì đó. Không ai bắt tôi phải làm những chuyện đó. Có những thứ tôi học cũng không (hoặc chưa) có liên quan gì đến

công việc. Tôi học chỉ vì tôi thích và tò mò. Tôi học vì tôi muốn hiểu thêm những thứ mà tôi cho là hay ho. Tôi học vì tôi muốn đi mãi, đi mãi, đi đến tận cùng những cái mà người ta viết trong sách, để xem ở đó có gì hay không" bởi nó như gợi ra cách để trở thành một người - như anh bây giờ.

1:05 AM

Lê Tâm said...

Cám ơn anh rất nhiều :) Em đã, đang và sẽ luôn đọc những chia sẻ cực kỳ thú vị của anh :)

2:05 AM

Lê Tâm said...

Cám ơn anh rất nhiều :) Em đã, đang và sẽ luôn đọc những chia sẻ cực kỳ thú vị của anh :)

2:06 AM

chairuou said...

Đồng chí hắc cơ Việt Nam bật chức năng share với +1 cái đê.

2:42 AM

mitmat said...

Cảm ơn bạn lần đầu tiên mình đọc hết một bài viết dài như vậy ^^:G)

1:34 AM

brother said...

cảm ơn anh vì bài viết hay

12:18 AM

Nguyen Ngoc Hue said...

Bài viết rất hay và bổ ích. Mình cũng rất thích CNTT nhưng tiếc rằng mình lại học Cơ khí. Đang định học thêm CNTT không biết có phù hợp không. Mong đại ca cho vài lời khuyên. Thanks

7:21 PM

Nguyen Ngoc Hue said...

This comment has been removed by the author.

7:23 PM

vhtk said...

Anh Thái và mọi người ơi!
Em rất muốn đọc cuốn "The_C_Programming_Language" nhưng tìm ở đâu Việt Nam thì có ạ? Em tìm mãi không ra ạ. Mọi người biết ở đâu có chỉ giùm em!

6:52 AM

RacTun said...

Minhh nghi cac ban SV nen Nghi hoc va doc cac cuon sach cua Thai de nghi cho nhuyen cung du roi. Ban than minh cung rat lay lam tiec ko tu bo dai hoc som, tam bang dai hoc chi lam vui gia dinh.

10:23 AM

Minh said...

1 bài viết rất bổ ích. không những chỉ áp dụng cho ngành an toàn thông tin mà còn cho các ngành học khác.

11:57 PM

PFH said...

bài này rất hay và hữu ích cho ai theo attt

9:10 PM

vhtk said...

Em đã đọc bài viết này lần thứ 3. Nhưng bây giờ em mới tập trung được. Cảm ơn anh Thái! Em sẽ lao vào học ngay. Chờ những bài viết khác của anh.

8:47 PM

Hoàng Minh said...

Thanks,bài viết hay lắm

7:55 PM

Anonymous said...

LK xin cảm ơn a đã dành nhiều thời gian viết bài. Tuy nhiên e có 1 ý kiến thế này. Bài viết nó gì đó nó hơi xa với cái title. Em đọc tiêu đề mãi mà ko hiểu phải đọc kỹ nội dung. ^..^Seo web gia re. Mình làm bên bộ phận kinh doanh thiết kế website vì thế ai cần thiết kế website giá rẻ thì ủng hộ mình nha

5:59 PM

Unknown said...

em thực sự thích cái cách tư duy của anh, anh có thể cho em xin FB, Y!M or số điện thoại đc k ạ, em muốn tham khảo thêm 1 số thứ về ngành IT nói chung

9:07 PM

Unknown said...

Hi, minh co do bai viec cua ban va thay rat huu ich. Nhat la ve nhung quyen sach ma moi nguoi co the tham khao.

Minh chuyen ve java va cung co tiep xuc voi ma hoa kha nhieu va co nhieu hung thu voi ma hoa du lieu va an toan thong tin. Hien gio minh cung dang danh thoi gian hoc python nen co le minh se thu voi Python Programming for Hackers and Reverse Engineers xem the nao.

Minh cung co tham gia mot so khoa hoc online ma Thai da de cap o tren. Cam thay hau het khoa hoc deu rat thu vi. Minh da thu qua Udacity, Coursera va Edx. Co le cach day cua Udacity rat tot voi beginners. Va Coursera thi co kha nhieu khoa hoc tap nham nen cung phai tim kiem kha khi. Edx thi con moi nen rat it khoa hoc. Ngoai ra minh cung thay staford co cung cap mot so khoa hoc mien phi tren trang chu cua ho ma khong public tren coursera.

Anyway, chuc Thai thanh cong trong cong viec va cuoc song.

3:09 AM

lam said...

Bài viết của a rất hay :)
Vui vì biết đc blog này của a:D
Cũng khá lo bởi vì không biết mình sẽ đi được tới đâu trong cái chặng đường đầy chông gai này :)

Have a good day !

6:38 AM

TRẦN HOÀI AN said...

hờ hờ, cảm ơn đại ca vì bài viết hữu ích và thực tế này!
Em cũng học ngành MIS bên đH Kinh tế TP.HCM.
Tương lai thật mù mịch nhưng " Tôi học chỉ vì tôi thích và tò mò. Tôi học vì tôi muốn hiểu thêm những thứ mà tôi cho là hay ho ". NghĨ như vậy có vẻ tốt hơn cho cái đầu e bây giờ!

1:37 AM

Luan Huynh said...

Sao a Thái không thử đi dạy nhỉ ?

11:35 PM

Thiện Lê Văn said...

tuyệt vời! cám ơn anh nhiều!

4:44 AM

Thất Đặng said...

cảm ơn bài viết của anh rất nhiều. bài viết tuy dài, nhưng thật sự là cách viết của anh rất lôi cuốn, và những thông tin anh cung cấp thật bổ ích, khiến em không thể không đọc kỹ từng chữ được.

Một từ về cảm nhận sau khi đọc xong đó là thật sự rất phấn khích :) Mong anh sẽ chia sẻ thêm nhiều kinh nghiệm cho cộng đồng hơn nữa. Chúc anh sức khỏe và thành đạt :)

Liên kết: cách trị rụng tóc ở nữ

10:02 AM

van trong Nguyen said...

em rất cảm ơn anh vì bài viết rất hay và chi tiết. em đang muốn theo học bảo mật mà chưa biết bắt đầu từ đâu.
Mong anh đừng xóa hay ẩn bài viết này đi nhé! Em còn có cơ hội đọc lại nữa.
Em cảm ơn anh!

7:23 PM

miendathua said...

Cho mình hỏi muốn đăng ký các khóa học của Standford thì đăng ký thế nào nhỉ

9:04 PM

fanta toan said...

Anh cho em hỏi Cuốn sách mà anh đang đề cập đến trong Đoạn Trích cuốn nào ạ?
Trích:
"Cuốn sách rất mỏng này của tác giả JSON giới thiệu đầy đủ những vấn đề mà người làm an toàn ứng dụng cần phải biết về JavaScript"

7:26 PM

Thành Phạm said...

em rất cảm ơn anh về bài viết đã cho em thấy nhiều thứ bổ ích em tks anh nhiều

5:03 AM

Vu Huu said...

Đây là lần đầu tiền em vào blog của anh, em thực sự rất ngưỡng mộ anh và bị cuốn hút bởi bài viết của anh. Em chúc anh sức khoẻ để có nhiều bài viết hay, nhiều đóng góp cho cộng đồng Việt. Cảm ơn anh !

12:57 AM

Thu Nguyen Minh said...

Thank you very much

11:52 AM

Thanh Ngoc said...

Cảm ơn anh. Bài viết của anh rất hay và giúp em rất nhiều.

9:50 AM

Hien Hoang said...

không phải dân lập trình oder cntt nhưng đọc cũng thấy hay hay
....thích....
TÔI ĐỌC CHỈ VÌ TÔI THÍCH VÀ TÒ MÒ
TÔI ĐỌC VÌ TÔI MUỐN HIỂU NHỮNG THỨ TÔI CHO LÀ HAY HO
Và vì nó có liên quan tới ng mà tôi quan tâm...

3:44 PM

Hien Hoang said...

không phải dân lập trình oder cntt nhưng đọc cũng thấy hay hay
....thích....
TÔI ĐỌC CHỈ VÌ TÔI THÍCH VÀ TÒ MÒ
TÔI ĐỌC VÌ TÔI MUỐN HIỂU NHỮNG THỨ TÔI CHO LÀ HAY HO
Và vì nó có liên quan tới ng mà tôi quan tâm...

3:45 PM

Anonymous said...

e rất ghét lập trình và không biết tí gì về lập trình, vậy e nên bỏ đh không anh. e cũng đang học chuyên ngành an toàn thông tin.

1:52 AM

Học viện Kỹ thuật mật mã said...

Chào bạn, bài viết của bạn thực sự rất bổ ích.
Bạn có thể chia sẻ thêm về các địa chỉ đào tạo An toàn thông tin tại Việt nam được không?
Chắc hẳn các bạn trẻ đam mê An toàn thông tin rất quan tâm đến điều này.

7:46 PM

duy nq said...

anh Thái mà viết một bài về quản trị thời gian thì hay quá

7:41 AM

Mr.Why said...

Dù không giỏi tiếng anh nhưng e sẽ cố gắng đọc cuốn: The C Programming Language (2nd Edition)
Cảm ơn những dòng chia sẻ của a <3

5:55 PM

Khoi Bui said...

Cám ơn anh đã mở đường cho thế hệ sau, chúc anh luôn vui :)

7:59 AM

Anonymous said...

cảm ơn a.dù chưa hiểu được nhiều nhưng sẽ cố gắng đọc lại nhiều lần để hiểu.đã lâu chưa đọc hết 1 bài dài như này

9:43 PM

Khánh Minh Trương Nguyễn said...

Cám ơn anh đã viết bài!Đây là lần đầu tiên em vào blog của anh, em thực sự rất ngưỡng mộ anh và bị cuốn hút bởi bài viết của anh. Em chúc anh sức khoẻ để có nhiều bài viết hay, nhiều đóng góp cho cộng đồng Việt. Cảm ơn anh !

8:39 PM

Hải Yến Trịnh said...

Cảm ơn anh ạ 😍😍😍 em đã đọc đi đọc lại bài viết này của em khoảng chục lần rồi :😁😁😁😁 em thực sự rất thích ghé qua blog của anh vì học hỏi được rất nhiều kiến thức và kinh nghiệm ạ 😇😇😇

5:09 AM

Tuấn Nô Bi said...

Có ai biết các trung tâm nào ở hà nội dạy về an toàn thông tin mà uy tín không ạ. Chỉ em với em đang định học ở bách khoa aptech trên đường hoàng quốc việt mà không biết chỗ này ra sao

11:12 PM

Nguyễn Hiền said...

Cảm ơn anh đã chia sẽ kinh nghiệm cho em.
Bản thân em cũng là một SV an toàn thông tin, nhưng anh có thể cho em biết có thể liên lạc với anh như thế nào được không? Vì e có một số thắc mắc muốn hỏi?

8:36 AM

phuong thao said...

Hi a, a cung biet a TQN? Hien a y can nhung ng ban co chung tieng nói để động viên a ý tìm lại tự tin làm viec IT! Please help him!!!!

9:23 PM

Hoàng Tiến Công said...

Bài viết hay lắm ạ.Cảm ơn a.

11:37 AM

Quân Huỳnh Ngọc said...

Cho em hỏi khóa CS107 mình đọc Ebook rồi làm bài tập của khóa thôi hả anh ? Có cần xem video không ? Mà e cũng không biết làm sao để có SUnet ID để xem video nữa. Em cảm ơn !

8:23 PM

LangThang said...

cảm ơn anh. đọc đi đọc lại cả trên hva lẫn ở đây, bắt tay vao đọc và thực hành

9:18 AM

Hoà Hoàng Văn said...

làm sao em có thể liên lạc hỏi anh về một số vấn đề.

11:15 PM

Thai Duong said...

Email của tôi là thaidn@gmail.com.

8:19 AM

Lê Việt Hào said...

cảm ơn anh. bài viết hay lắm

10:58 AM

Thanh Tung Nguyen said...

Anh ơi cho em hỏi: Nếu muốn làm về tìm lỗi sản phẩm hay phân tích mã độc liệu có cần biết nhiều các Algorithms không ạ ? Thực sự em đang học môn này mà thấy nó rộng quá...

9:29 PM

Thùy Nguyễn said...

Minhh nghi cac ban SV nen Nghi hoc va doc cac cuon sach cua Thai de nghi cho nhuyen cung du roi. Ban than minh cung rat lay lam tiec ko tu bo dai hoc som, tam bang dai hoc chi lam vui gia dinh.

2:48 AM

Hoang Nguyen Dinh said...

Em cảm ơn anh ạ. Em cũng đang là sinh viên IT chuyên ngành ATTT, và đang cảm thấy các môn học ở trường rất mông lung. Sau khi đọc bài của anh em cảm thấy yên tâm tư tưởng học tập hơn ạ =))), có cái nhìn tổng quan hơn nhiều, Cảm ơn anh

9:08 AM

Hoang Nguyen Dinh said...

This comment has been removed by the author.

9:09 AM

CTy Cp Ổn Áp Biến Áp Standa Việt Nam said...

Bạn ơi cho mình hỏi: Nếu muốn làm về tìm lỗi sản phẩm hay phân tích mã độc liệu có cần biết nhiều các Algorithms không? Thực sự mình cũng đang học môn này mà thấy nó quá rộng.
standa

4:17 PM

Unknown said...

Anh có thể làm thêm bài viết nói về ngành hệ thống thông tin được không anh ??? Bài viết thật sự rất hay và ý nghĩa

6:25 PM

Unknown said...

em mới hc ngành an toàn thông tin nhưng bài viết của anh rất hay!!!! e cảm ơn ạ

9:54 AM

Unknown said...

E mới học ngành an toàn thông tin. Bài viết của a rất hay và rất hữu ích cho e. Em cảm ơn anh rất nhiều ạ!!!

9:56 AM

Thanh Tuấn Lê said...

Em không biết nói gì hơn anh ạ. Xin cảm ơn anh một cách chân thành !

6:31 PM

Mrd Blog said...

Chẳng có gì ngoài hai chữ cảm ơn. Thật sự bài viết rất ý nghĩa và hữu ích. Cảm ơn anh rất nhiều !

5:43 AM

Backlink AZ said...

Cảm ơn bác Thái, bác cho anh em sáng mắt ra nhiều. Cảm ơn blog của bác.
Em cũng là một trong những người thấy hối tiếc khi không học chăm chỉ khi ở Đại học, và ngày nay, các bạn trẻ đều đi trên vết xe đổi đó.
Chúc bác sức khỏe và nhiều thành công.

6:55 PM

Post a Comment

Powered by Blogger

About me

Tôi vốn xuất thân là chuyên gia bảo mật công nghệ thông tin, nhưng vì cuộc sống mưu sinh nên chạy show ca hát, nổi tiếng qua bài Gọi đò. Sau này may mắn lấy được vợ đẹp, được bảo lãnh qua ở bên Canada. Ở đây ít show, người ta không mời đi hát nữa. Tôi trở lại công việc cũ, giờ làm việc cho Google.

Nếu bạn thích những gì tôi viết ở đây, hãy mua hoặc tặng 10.000 đồng cho một người bán dạo mà bạn gặp trên đường hôm nay.

I'm a security researcher, best known for my attacks on SSL/TLS: BEAST, CRIME, and POODLE. I was half of the team that discovered the crypto vulnerability in ASP.NET that affected millions of websites and won the Pwnie Awards of 2010.

I'm a staff software engineer at Google and lead of Project Wycheproof and Tink. My goal is to help everyone use crypto correctly everywhere.

Popular Posts

BEAST

September 25, 2011

So we gave a talk and a live demo at ekop… ...

[redacted]

READ MORE

Chào Thủ tướng!

January 19, 2019

Hôm trước tôi hỏi:

Ngoài lưu trữ dữ liệu nội ...

READ MORE

Library

Security Research

The POODLE attack
The CRIME attack
BEAST: Surprising Crypto Attack Against HTTPS
Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET
Practical Padding Oracle Attacks
Flickr's API Signature Forgery Vulnerability
Zombilizing The Web Browsers Via Flash Player 9
Giám sát an ninh mạng
Một phương pháp chống DDoS bằng xFlash
Lỗ hổng nghiêm trọng của SSL/TLS