

مقدمه ای بر رایانش امن یا Security Engineering



مهندیار افتخاری نیا
دبير انجن علمي رشته مهندسی کامپیوتر

رایانش امن چیست؟

رایانش امن یا مهندسی امنیت فرآیند ترکیب کنترل های امنیتی در یک سیستم اطلاعاتی است. یک سیستم اطلاعاتی را میتوان از ابعاد مختلفی بررسی کرد که در ادامه به آن خواهیم پرداخت.



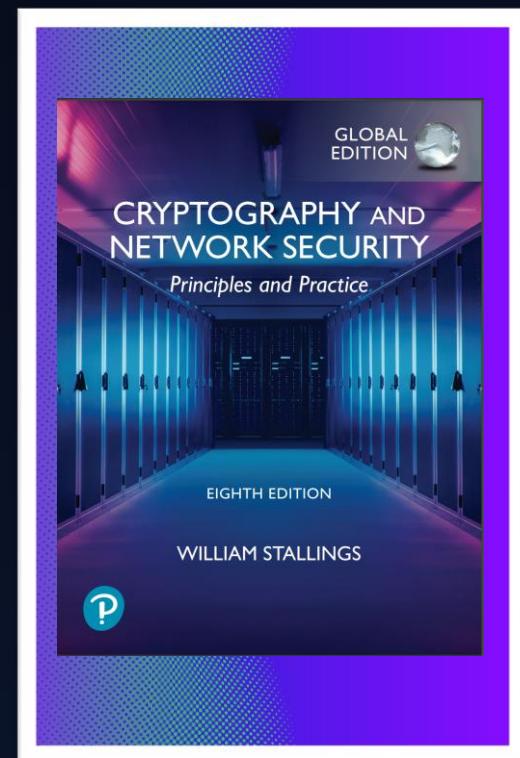
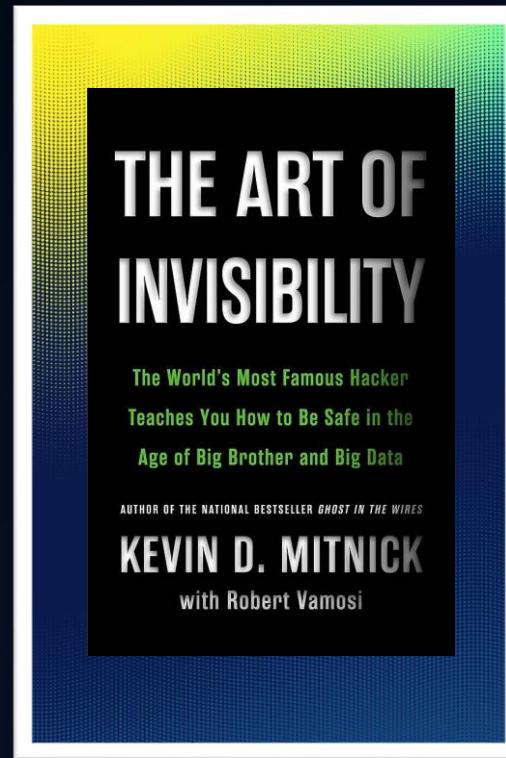
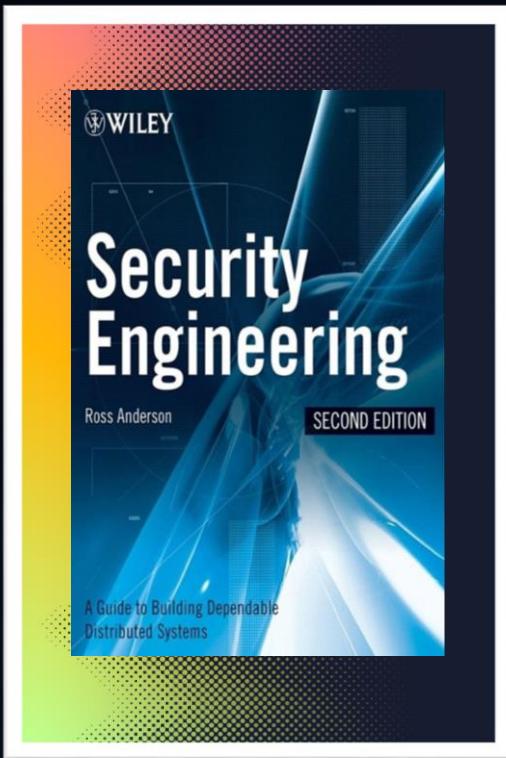
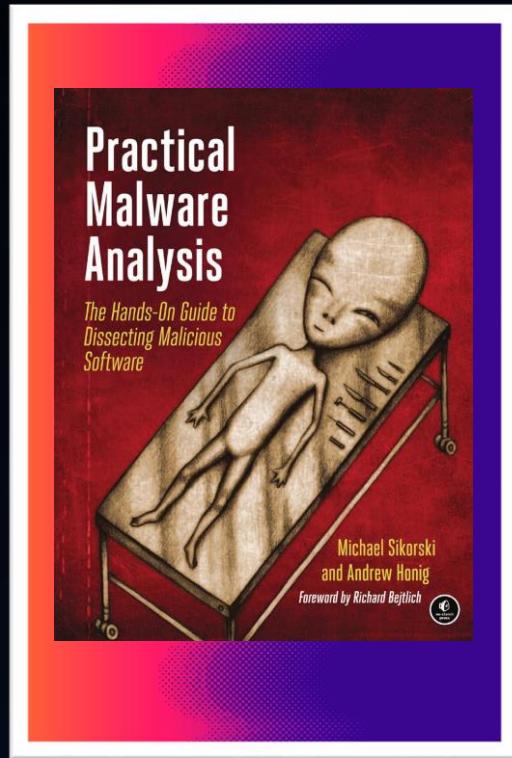
فرصت های شغلی

Bug bounty : در این روش یک متخصص امنیت به دنبال پیشنهاد هایی برای اشکال زدایی یک سامانه اطلاعاتی است و بسایت ها و سامانه های مختلفی در جهان پیشنهاد های بررسی امن بود سرویس و اشکال زدایی سامانه خود را میدهند

متخصص امنیت در شرکت های زیر ساخت : در این گونه شرکت ها که دارای زیر ساخت و مراکز داده هستند نقش افرادی که متخصص امنیت شبکه یا زیر ساخت هستند پر اهمیت است.

متخصص امنیت در زیر ساخت های دولتی و صنایع نظامی : امروزه در زیر ساخت های دولتی و صنایع نظامی محترمانگی اطلاعات و امن بودن سیستم های اطلاعاتی داری اهمیت بسیار زیادی است.

معرفی منابع برای یادگیری



ژرال های علمی معتبر

1.

ELSEVIER

Computers and Security

0167-4048 , Bimonthly

2.

IEEE

IEEE Transactions on Information
Forensics and Security

1556-6013 , Monthly

3.

acm
Association for
Computing Machinery

ACM Transactions on Privacy and
Security

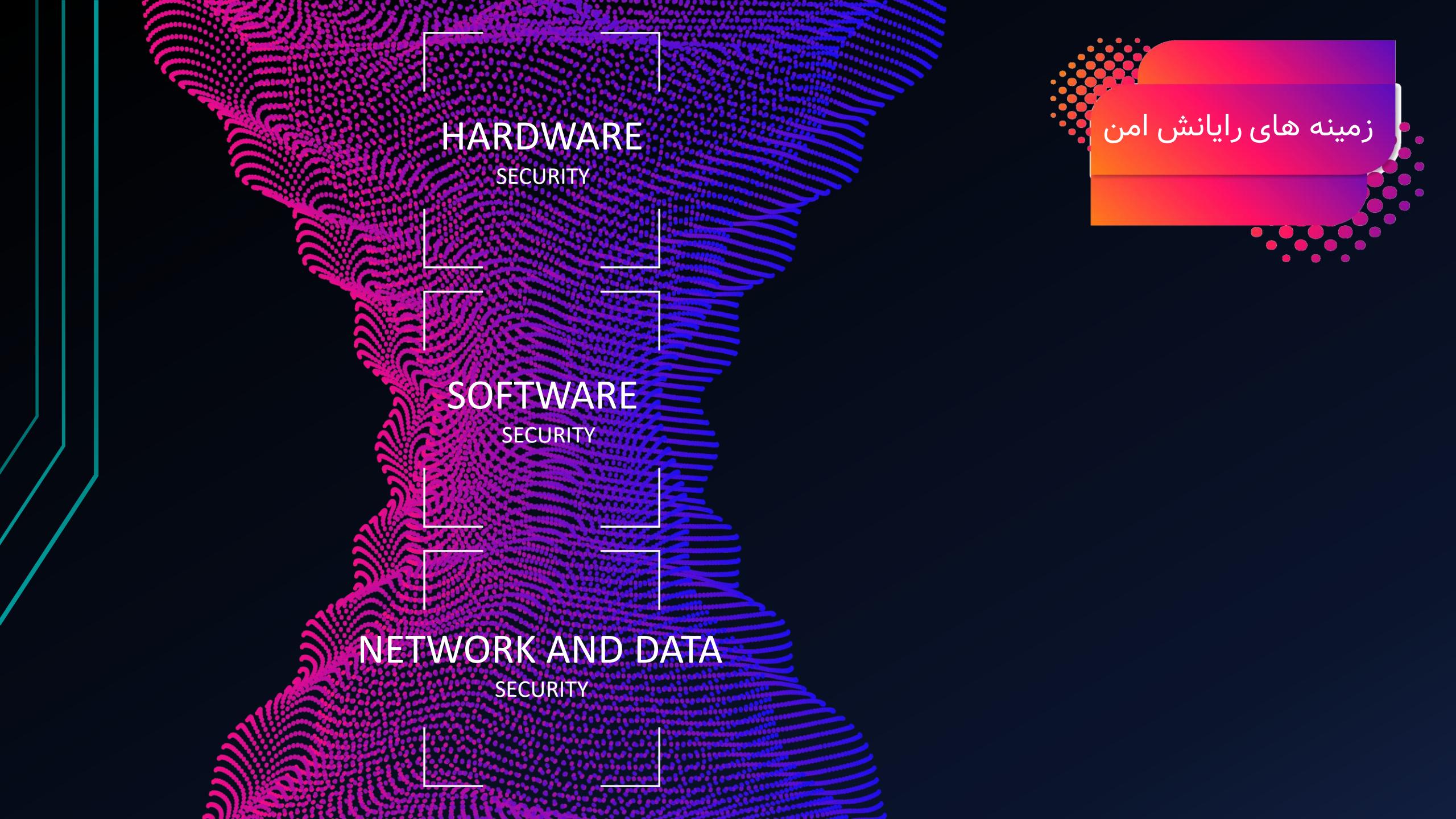
2471-2566

4.

Springer

Journal of Cryptographic Engineering

2190-8508



زمینه های رایانش امن

HARDWARE

SECURITY

SOFTWARE

SECURITY

NETWORK AND DATA

SECURITY



Hardware Attacks

Side channel effect

در این روش متهاجم به دنبال یافتن هرگونه اطلاعات از طریق سخت افزار یک سیستم است

:Side channel effect



Timing Attack

Power Consumption Attack

ElectroMagnetic Attack

Hardware Attacks

Spectre and meltdown

در این نوع از حمله سخت افزاری میتوان تمام اطلاعات و خانه های حافظه فرآیند ها دیگر را واکشی کرد

سری های مختلفی از پردازنده اینتل و Arm درگیر این حمله بحرانی شدند

حمله Meltdown باعث دسترسی به فضای حافظه کرنل یا هسته میشود و حمله Spectre باعث ایجاد دسترسی به فضای حافظه بقیه فرآیند ها میشود



Hardware Attacks

Pacman

این نوع از حمله برای اولین بار بر روی پردازنده بر پایه Apple M1 یا Arm معرفی شد
نقص در Pointer Authentication (PAC) باعث ایجاد چنین حمله ای میشود



Software Attacks

در این روش مهاجم به دنبال رسیدن به خواسته های خود از طریق دستکاری در کدها یا خرابکاری است

حملات در این بخش به دو قسمت تقسیم میشود:

حملات بر پایه User mode

حملات بر پایه Kernel mode

Software Attacks

Malware

یا بدافزار نرم افزاری است که به دنبال ایجاد کارهای مخرب یا جاسوسی از قربانی در کامپیوتر است بد افزار ها معمولا خود به چند دسته تقسیم میشوند.

در بعضی از موارد بدافزار از توابع سیستمی یا رابط برنامه نویسی سیستم عامل بهره میبرد که در این صورت ممکن است دسترسی آن را دوچندان کند.



Software Attacks

Operating System Attack

حملات مبتنی بر سیستم عامل معمولاً با استفاده از توابع سیستمی یا رابط برنامه نویسی سیستم عامل که میتواند دسترسی سطح کاربر یا هسته سیستم عامل را داشته باشد به اهداف خود میرسند.

DLL HIJAKING

DLL INJECTION

BUFFER
OVERFLOW

ASYNCHRONOUS
PROCESS RUNNING

Data and Network Security



امنیت مبتنی بر داده و شبکه جز مهمترین مسائل رایانش امن به حساب می آید.

امنیت شبکه در حقیقت فرآیند برقراری اتصالی امن بین دو یا چند کامپیوتر یا دستگاه الکترونیکی است و امنیت داده دارای چندین مبحث است که مهمترین آن محرومگی داده است

Network Attack Types

Distributed Denial of service(DDOS)

Man in The Middle(MITM)

Dns Spoofing

Exhaustive key search(Brute Force)

Spywares(Rats,Keyloggers,Remote Execution)

رمزنگاری دانشی است که به بررسی و شناختِ اصول و روش‌های انتقال یا ذخیرهٔ اطلاعات به صورت امن می‌پردازد

Asymmetric

RSA
DH
ECDH
X25519

Symmetric

AES
DES
3DES
BLOWFISH
RC4

رمزنگاری مدرن به دو دستهٔ رمزنگاری با کلید متقارن و رمزنگاری با کلید نامتقارن تقسیم می‌شود

رمزنگاری با کلید متقارن خو به دو دستهٔ
رمزنگاری جریانی یا Stream cipher
و رمزنگاری بلوکی یا Block cipher تقسیم می‌شود