

Open Security

Why not?

T-DOSE 2015 - 29-11-2015

Asim Jahan (<http://jahan-is.com/>)

Maikel Mardjan (<https://nocomplexity.com>)

Open Security

Open Reference
Architecture
for Security
and
Privacy



Why?

Companies keep getting hacked. And that's music to the ears of the executives and investors in cybersecurity companies.

February has been a phenomenal month for the overall stock market. The [S&P 500](#) is up about 6%. But companies that help mitigate the damage from major attacks have done even better.

Sponsored Links



Here Are All The Dishwashing Tips You...
Huffington Post



14 Bathroom Inventions You Didn't Realize You...
Huffington Post



8 Moments In Life That Actually Matter...

There is a relatively new exchange-traded fund for cybersecurity companies. The ticker symbol, appropriately, is [HACK \(HACK\)](#). It has surged nearly 17% in February.

The massive data breach at health insurer Anthem ([ANTM](#)) earlier this month is one reason why the stocks have done so well.

<http://money.cnn.com/2015/02/27/investing/cybersecurity-stocks-hack/>

Here's why companies are still getting hacked

COMMENTARY

Ken Levine, president and CEO, Digital Guardian

Wednesday, 4 Nov 2015 | 1:54 PM ET



<http://www.cnbc.com/2015/11/04/cybersecurity-heres-why-companies-are-still-getting-hacked-commentary.html>

Nine Out of Ten of the Internet's Top Websites Are Leaking Your Data

November 2, 2015 // 11:50 AM EST

The vast majority of websites you visit are sending your data to third-party sources, usually without your permission or knowledge. That's not exactly breaking news, but the sheer scale and ubiquity of that leakage might be.

Tim Libert, a privacy researcher with the University of Pennsylvania, has [published new peer-reviewed research](#) that sought to quantify all the “privacy compromising mechanisms” on the one million most popular websites worldwide. His conclusion?

<http://motherboard.vice.com/read/9-out-of-10-of-the-internets-top-websites-are-leaking-your-data>

THE  TIMES

Crime

[News](#) | [Opinion](#) | [Business](#) | [Money](#) | [Sport](#) | [Life](#) | [Arts](#) | [Puzzles](#) | [Papers](#) | [Irish news](#) |

Tuesday, November 17

Welcome to your preview of The Times

Vodafone hack puts 2,000 bank customers at risk

<http://www.thetimes.co.uk/tto/news/uk/crime/article4602083.ece>



JPMorgan Tied to Largest Cyberattack Ever

By Jennifer LeClaire / NewsFactor Network



PUBLISHED:
NOVEMBER
10
2 0 1 5

Prosecutors yesterday announced charges connected to massive network intrusions at U.S. financial institutions, brokerage firms and major news publications, among other companies. And the latest headlines suggest that the massive 2014 JPMorgan hack was linked to the largest cybersecurity

THIS IS THE
NEW NORMAL

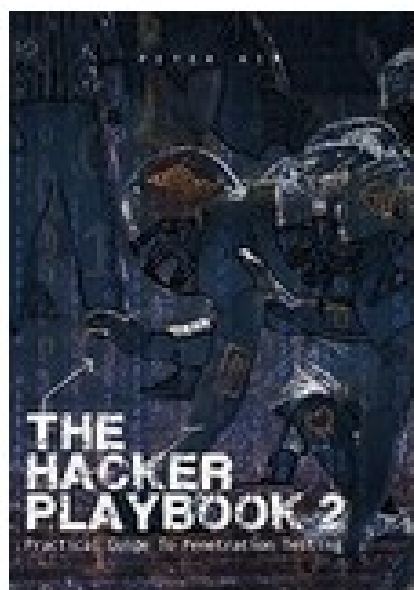
Agenda

- Why another reference architecture?
- What is an open reference architecture for security and privacy?
- The power of a good solution architecture for solving security and privacy challenges
- Current security and privacy attack vectors (with real nasty examples!)
- Security principles and reuse
- Advantage / disadvantage of using OSS security products
- Determining quality of OSS for security and privacy applications
- Common used OSS security applications

So

***Why another Reference
Architecture for
Security and Privacy?***

We have books!



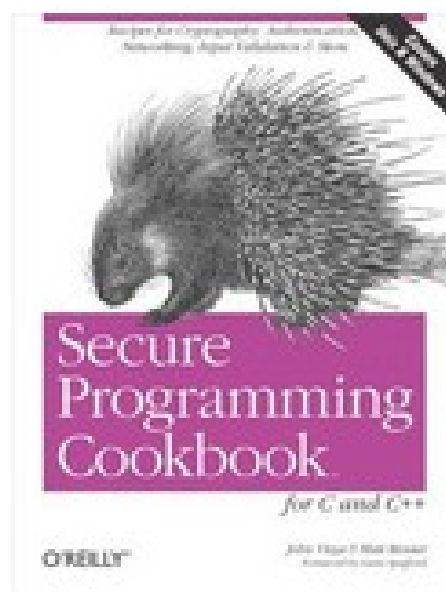
The Hacker Playbook 2:
Practical Guide To
Penetration Testing

› Peter Kim

★★★★★ 53

Kindle Edition

\$14.19



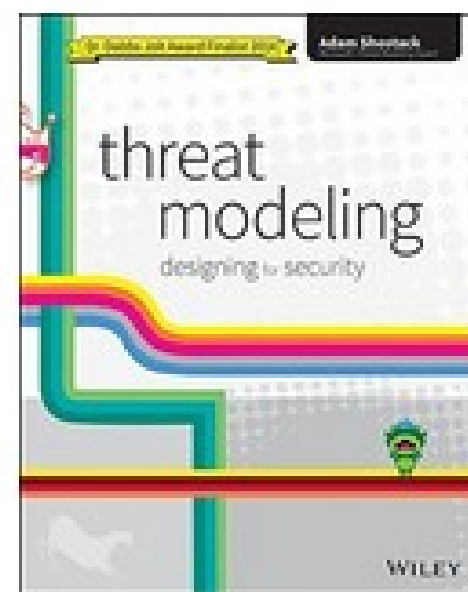
Secure Programming
Cookbook for C and C++:
Recipes for...

› John Viega

★★★★★ 11

Kindle Edition

\$50.05



Threat Modeling: Designing
for Security

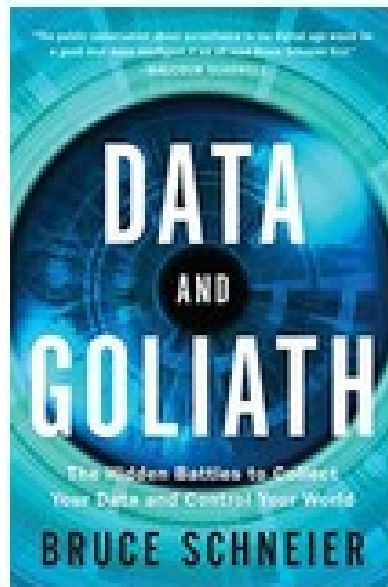
› Adam Shostack

★★★★★ 21

Kindle Edition

\$50.05

We have many more books...



Data and Goliath: The Hidden Battles to Collect Your Data and Control...

> Bruce Schneier

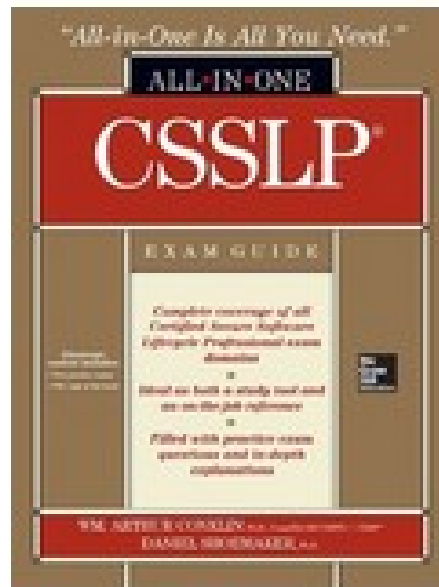
★★★★☆ 83

#1 Best Seller in Science

& Technology Law

Kindle Edition

\$13.99



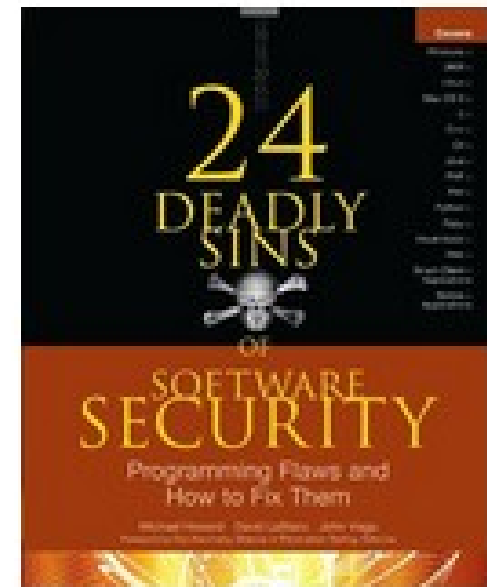
CSSLP Certification All-in-One Exam Guide

> Wm. Arthur Conklin

★★★★★ 5

Kindle Edition

\$58.08



24 Deadly Sins of Software Security: Programming Flaws and How to Fix...

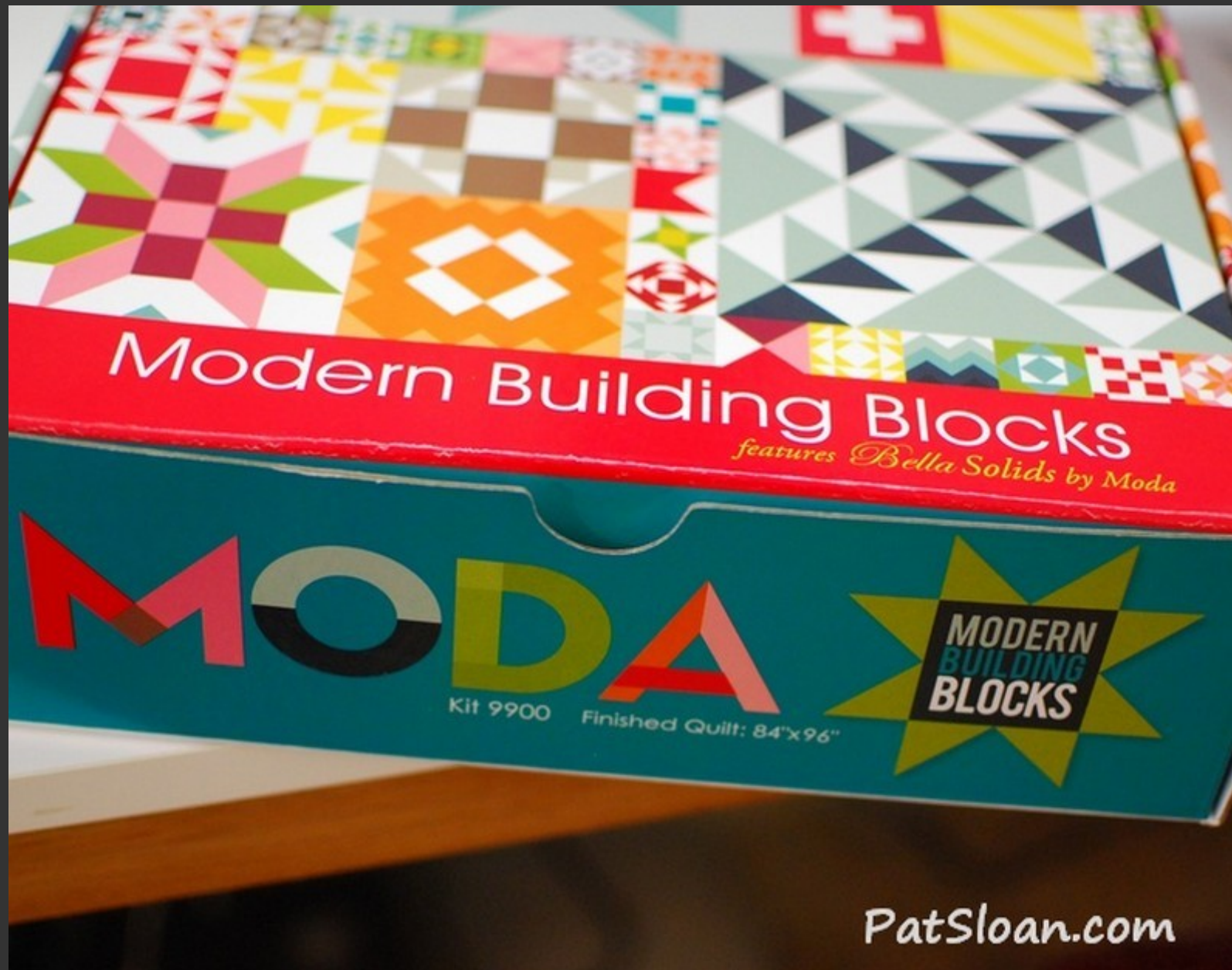
> Michael Howard

★★★★☆ 10

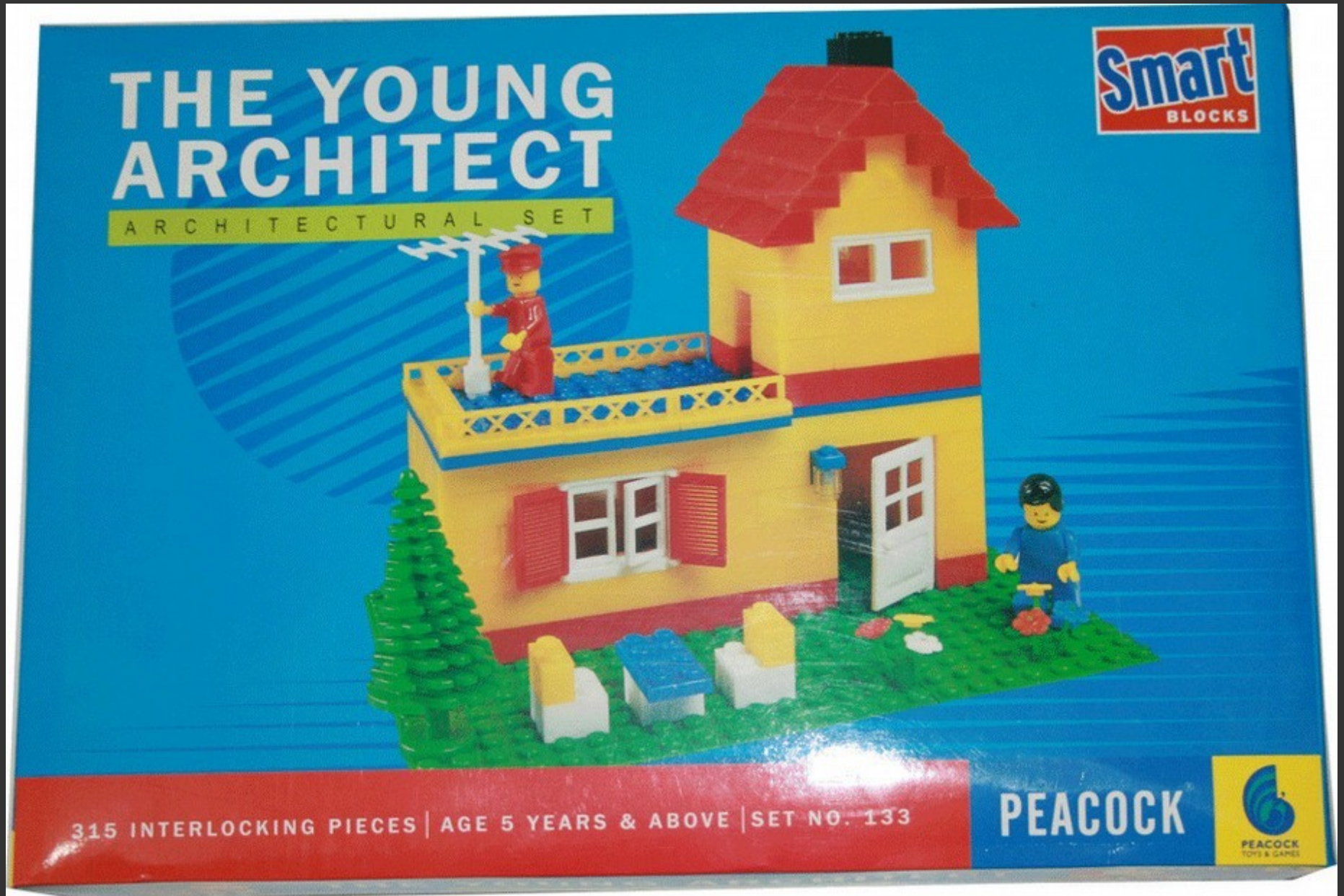
Kindle Edition

\$50.44

Use of a reference architecture



Security design should be fun! (again)



Agenda

- Why another reference architecture?
- **What is an open reference architecture for security and privacy?**
- The power of a good solution architecture for solving security and privacy challenges
- Current security and privacy attack vectors (with real nasty examples!)
- Security principles and reuse
- Advantage / disadvantage of using OSS security products
- Determining quality of OSS for security and privacy applications
- Common used OSS security applications

Domain related, not company related!

Why? - Context

Governance / Operations

What? - Conceptual

How? - Logical

With what?
Physical

Business

Data Architecture

Application Architecture

Technology Architecture

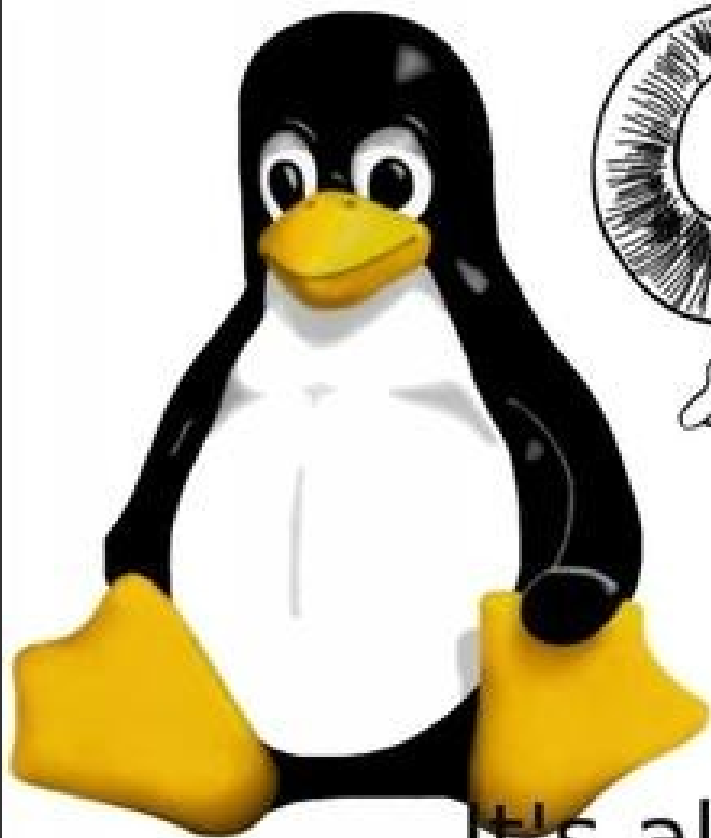
The power of open!



WIKIPEDIA
The Free Encyclopedia

Ask me about

Free Software



It's all about freedom.



LICENSES

MOST FREE



ATTRIBUTION

CC BY

This license lets you distribute, remix, tweak, and build upon the original work, even commercially, as long as you credit the original creation. This is the most accommodating of licenses offered.



ATTRIBUTION-SHAREALIKE

CC BY-SA

This license lets you remix, tweak, and build upon the original work even for commercial purposes, as long as you credit the original work and license your new creations under the identical terms. This license is often compared to "copyleft" free and open source software licenses. All new works based on the work should carry the same license, so any derivatives will also allow commercial use. This is the license used by Wikipedia.



ATTRIBUTION-NODERIVS

CC BY-ND

This license allows for redistribution, commercial and non-commercial, as long as it is passed along unchanged and in whole, with credit to the original work.



ATTRIBUTION-NONCOMMERCIAL

CC BY-NC

This license lets you remix, tweak, and build upon the original work non-commercially. Your new works must be non-commercial and acknowledge the original work, but you don't have to license your derivative works on the same terms.



ATTRIBUTION-NONCOMMERCIAL-SHAREALIKE

CC BY-NC-SA

This license lets you remix, tweak, and build upon the original work non-commercially, as long as you credit the original work and license your new creations under the identical terms.



ATTRIBUTION-NONCOMMERCIAL-NODERIVS

CC BY-NC-ND

This license is the most restrictive of the six main licenses, only allowing you to download the original work and share it with others as long as you credit the original work. You can't change the original work in any way or use it commercially.

LEAST FREE

Agenda

- Why another reference architecture?
- **What is an open reference architecture for security and privacy?**
- **The power of a good solution architecture for solving security and privacy challenges**
- Current security and privacy attack vectors (with real nasty examples!)
- Security principles and reuse
- Advantage / disadvantage of using OSS security products
- Determining quality of OSS for security and privacy applications
- Common used OSS security applications

REUSE



REDUCE

RECYCLE

Agenda

- Why another reference architecture?
- What is an open reference architecture for security and privacy?
- The power of a good solution architecture for solving security and privacy challenges
- **Current security and privacy attack vectors (with real nasty examples!)**
- Security principles and reuse
- Advantage / disadvantage of using OSS security products
- Determining quality of OSS for security and privacy applications
- Common used OSS security applications

And when there is still a minute left, we do of course some demo's!











First Public Windows 8 Secure Boot Bypass (Aug 2013)

```
BIOS Exploit
[+] loaded exploits.bios.bh2013
[+] imported chipsec.modules.exploits.bios.bh2013
[*] BIOS Region: Base = 0x00200000, Limit = 0x007FFFFFFF

[*] Reading 0x80 bytes from BIOS region in ROM (address 0x20F000)..
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff |
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff |
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff |
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff |
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff |
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff |
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff |

[+] Checking protection of UEFI BIOS region in ROM..
[spi] UEFI BIOS write protection enabled but not locked. Disabling..
[!] UEFI BIOS write protection is disabled
[*] Writing payload to BIOS region (address 0x20F000)..

[*] Reading BIOS back (address 0x20F000)..
20 20 49 4e 20 59 4f 55 52 20 42 49 4f 53 20 20 | IN YOUR BIOS
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 |
20 20 44 4f 4e 27 54 20 57 4f 52 52 59 21 20 20 | DON'T WORRY!
59 4f 55 52 20 4f 53 20 42 4f 4f 54 20 48 41 53 | YOUR OS BOOT HAS
20 20 42 45 45 4e 20 53 45 43 55 52 45 44 20 20 | BEEN SECURED
20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 |
20 42 4c 41 43 4b 20 48 41 54 20 32 30 31 33 20 | BLACK HAT 2013
ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff |
```

[A Tale Of One Software Bypass Of Windows 8 Secure Boot](#)

PILLON

PUZZLE




© Vodafone Inc., the Vodafone logo and how are part of the trademarks of the Vodafone Group.
Bluetooth workmark and logo are owned by the Bluetooth SIG, Inc. and any use of such
Ericsson Mobile Communications AB is under license.
iX, Doo and Motion Eye are trademarks of Sony Corporation.

V800 Ebony Black
Mobile Phone GSM 900/1800/1900&UMTS
DPY 101 2790/1 R4A DE

S/N: CB50ZZLXXX

IMEI: 35488500 - 148888 - 7


 Bluetooth 
CE 0682


8 95673 46852 3
Made in China

..Or in words

- Analysis of vulnerabilities in compiled software without source code
- Anti-forensic techniques
- Automated probes and scans
- Automated widespread attacks
- Client validation in AJAX routines
- Cross-site scripting in AJAX
- Cryptographic Performance Attacks
- Cyber-threats & bullying (not illegal in all jurisdictions)
- DoS Attacks
- Email propagation of malicious code
- Executable code attacks (against browsers)
- Exploiting Vulnerabilities
- GUI intrusion tools
- Industrial espionage
- Internet social engineering attacks
- Malicious AJAX code execution
- Network sniffers
- Packet Manipulation
- Packet spoofing
- Parameter manipulation with SOAP
- Replay Attack
- RIA thick client binary vector
- Rogue Master Attack

- Analysis of vulnerabilities in compiled software without source code
- RIA thick client binary vector
- Rogue Master Attack
- RSS Atom Injection
- Session-hijacking
- Sophisticated botnet command and control attacks
- Spoofing
- Stealth and other advanced scanning techniques
- Targeting of specific users
- Web service routing issues
- Wide-scale trojan distribution
- Wide-scale use of worms
- Widespread attacks on DNS infrastructure
- Widespread attacks using NNTP to distribute attack
- Widespread, distributed denial-of-service attacks
- Windows-based remote access trojans (Back Orifice)
- WSDL scanning and enumeration
- XML Poisoning
- XPATH injection in SOAP message

IS Threat?





Agenda

- Why another reference architecture?
- What is an open reference architecture for security and privacy?
- The power of a good solution architecture for solving security and privacy challenges
- Current security and privacy attack vectors (with real nasty examples!)
- **Security principles and reuse**
- Advantage / disadvantage of using OSS security products
- Determining quality of OSS for security and privacy applications
- Common used OSS security applications

THE POWER OF PRINCIPLES

12 Principles Guaranteed to
Bring You Great Success



BRIANHOLMES

Executive Coach • Business Coach



International
Edition

Principles of Electric Circuits

CONVENTIONAL CURRENT VERSION

Ninth Edition

Thomas L. Floyd



What are security principles?

Principles are statements of direction that govern selections and implementations.

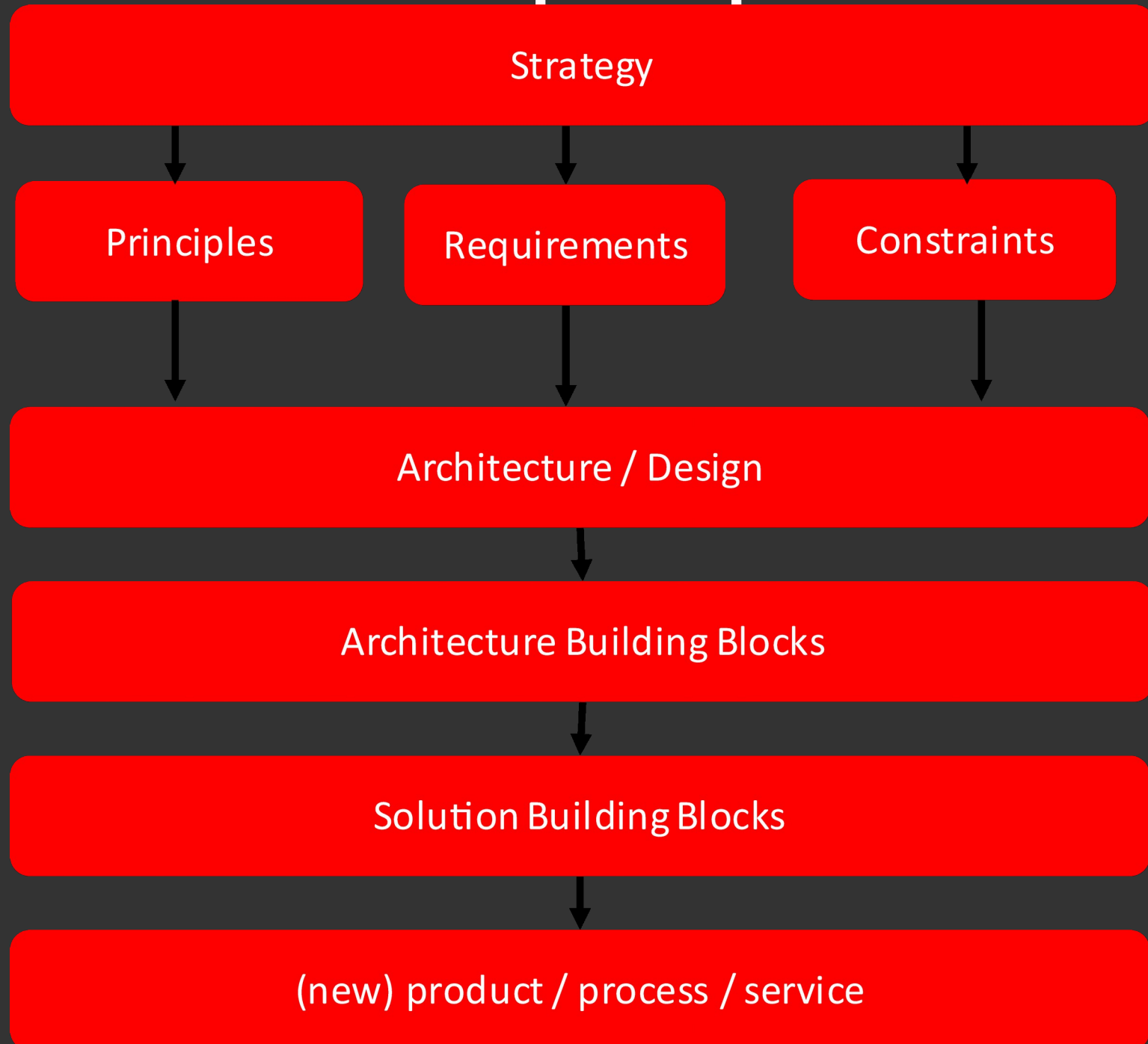
Principles are used within business design and successful IT projects.

Definition:

A principle is a qualitative statement of intent that should be met by the architecture.

Security architecture principles are used to translate selected alternatives into basic ideas, standards, and guidelines for simplifying and organizing the construction, operation, and evolution of systems.

Place of principles



Principle (Example)

Name Principle	Avoid security by obscurity
Statement	Security measurements should be open and transparent.
Rationale	<ul style="list-style-type: none">• Assume attackers will have source code (also for closed source software).• Assume attackers will have complete design and network topologies.• Open security design promotes cycle of improvement faster.• Assume sensitive information regarding security measurements are leaked or sold.
Implications	<ul style="list-style-type: none">• Do not document secrets and configuration policies (settings) in security designs.• Never store secrets (e.g. passwords) on systems.• Involve internal and external SME to evaluate the strength and weakness of a security design. (design review).• Security should always be tested by experts (open or not).• Periodically pentest the security implementation, use different companies instead of always the same.

Principle (Example-2)

Name Principle	Data in transit protection
Statement	Data in transit needs protection
Rationale	Consumer data transiting networks should be adequately protected against tampering and eavesdropping via a combination of network protection and encryption.
Implications	If this principle is not implemented, then the integrity or confidentiality of the data may be compromised whilst in transit.

Agenda

- Why another reference architecture?
- What is an open reference architecture for security and privacy?
- The power of a good solution architecture for solving security and privacy challenges
- Current security and privacy attack vectors (with real nasty examples!)
- Security principles and reuse
- **Advantage / disadvantage of using OSS security products**
- Determining quality of OSS for security and privacy applications
- Common used OSS security applications



OpenSSH Vulnerability

Exploit to Crack Server Passwords



CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Reset Password](#) [Activate Account](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

[Vulnerability Search](#)

[By Microsoft References](#)

Top 50 :

[Vendors](#)

[Vendor Cvss Scores](#)

[Products](#)

[Product Cvss Scores](#)

[Versions](#)

Other :

[Microsoft Bulletins](#)

[Bugtraq Entries](#)

[CWE Definitions](#)

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2014

Go to year: [1999](#) [2000](#) [2001](#) [2002](#) [2003](#) [2004](#) [2005](#) [2006](#) [2007](#) [2008](#) [2009](#) [2010](#) [2011](#) [2012](#) [2013](#)

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Internet Explorer	Microsoft	Application	243
2	Linux Kernel	Linux	OS	133
3	Chrome	Google	Application	127
4	Iphone Os	Apple	OS	120
5	JRE	Oracle	Application	115
6	JDK	Oracle	Application	115
7	Mac Os X	Apple	OS	114
8	Firefox	Mozilla	Application	108
9	Apple Tv	Apple	Application	81
10	Ubuntu Linux	Canonical	OS	79
11	Flash Player	Adobe	Application	76
12	Safari	Apple	Application	69
13	Thunderbird	Mozilla	Application	64
14	Mysql	Oracle	Application	63
15	Owncloud	Owncloud	Application	58
16	Fusion Middleware	Oracle	Application	57



It's real!

- Open Source software is created by communist to destroy our world.
- Open Source software is made by hobbyist.
- Open Source software is made by hackers and hackers are bad. Especially when it comes down to security and privacy.
- Open Source software is never maintained.
- Open Source software is free, so it can not have any value.
- Quality of Open Source software is dramatic. Do does hackers known how to spell quality at all?
- Using Open Source makes you depended of the good will of hackers.
- Using Open Source for security or privacy protection gives unacceptable high risk, since the whole world can hack me now instantaneously.
- Using Open Source is an extra thread for my security or privacy.

Imitation infrared detector
FAKE ALARM



**LED
FLASHING**

Outdoor security

Open and transparent..



Learning, Collaboration, and



Mistakes



Agenda

- Why another reference architecture?
- What is an open reference architecture for security and privacy?
- The power of a good solution architecture for solving security and privacy challenges
- Current security and privacy attack vectors (with real nasty examples!)
- Security principles and reuse
- Advantage / disadvantage of using OSS security products
- **Determining quality of OSS for security and privacy applications**
- Common used OSS security applications

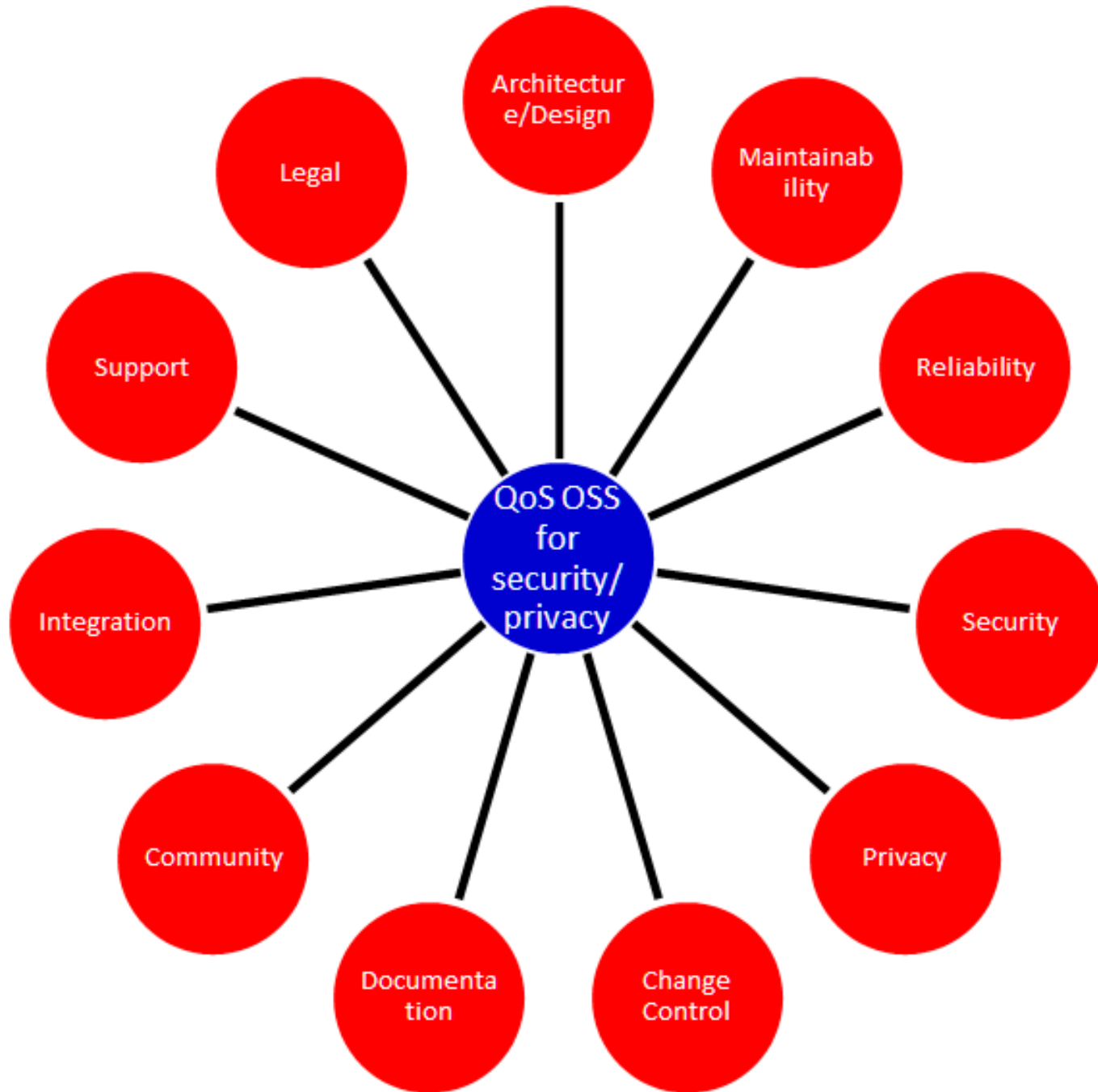
The blind men and the elephant



We are all different and with different goals, budgets and ***THREATS!***



QoS OSS Security & Privacy

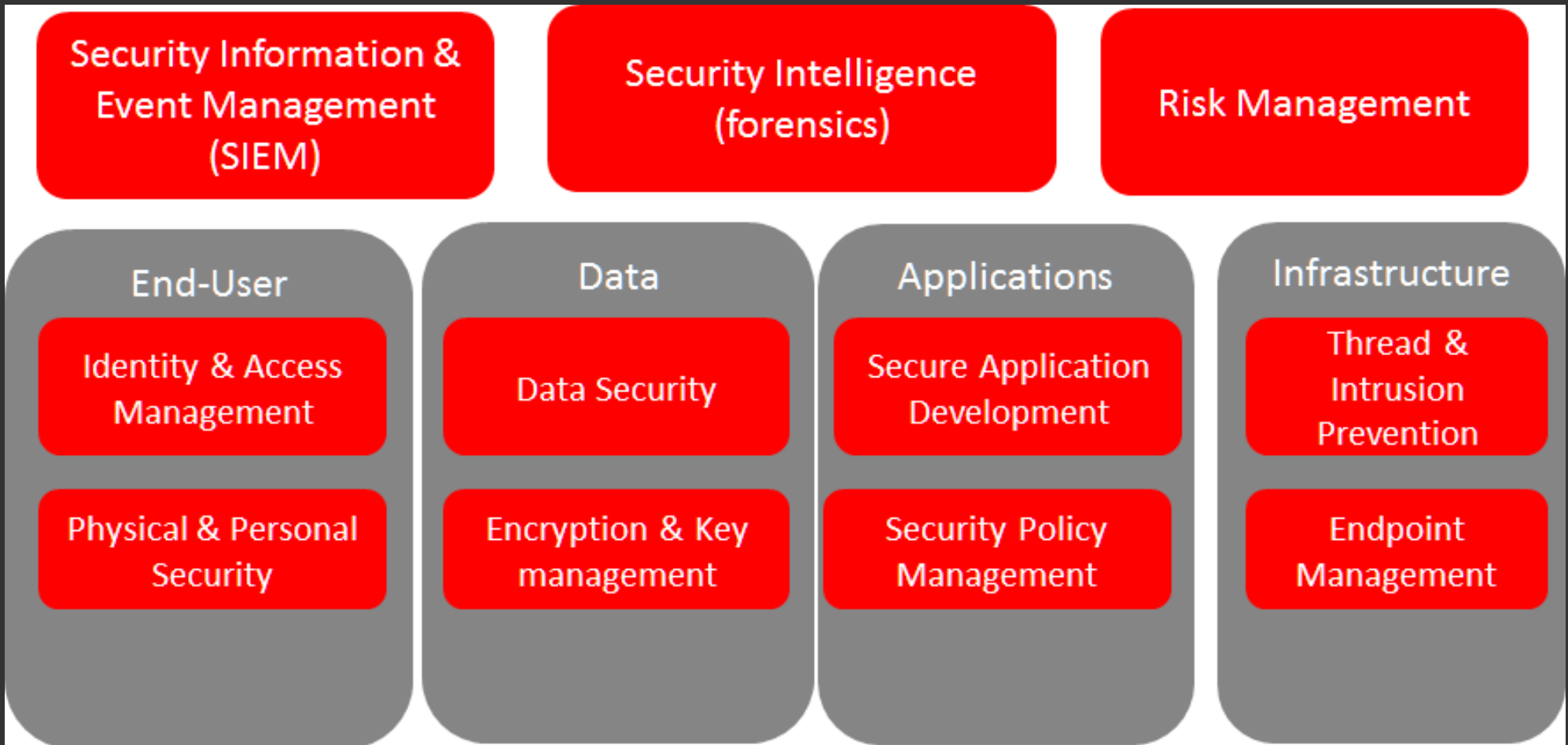


Agenda

- Why another reference architecture?
- What is an open reference architecture for security and privacy?
- The power of a good solution architecture for solving security and privacy challenges
- Current security and privacy attack vectors (with real nasty examples!)
- Security principles and reuse
- Advantage / disadvantage of using OSS security products
- Determining quality of OSS for security and privacy applications
- **(Not So) Common used OSS security applications**

Reference Solution Framework...

- Note: Selecting solutions should never be your first step!
- Just a first try:



There are far too many ?!

Take a look at:

- Bosun. Bosun is an open-source, MIT licensed, monitoring and alerting system by Stack Exchange. (<http://bosun.org/>)
- Gryffin. Gryffin is a large scale web security scanning platform. Created by Yahoo, and since September 2015 available as open source.(
<https://github.com/yahoo/gryffin>)
- SIMP (The System Integrity Management Platform)
(<https://github.com/NationalSecurityAgency/SIMP>)
- Streisand is software for setting up secure connections with your friends. A bit like TOR. (<https://github.com/jlund/streisand>)
- ...

Agenda

- Why another reference architecture?
- What is an open reference architecture for security and privacy?
- The power of a good solution architecture for solving security and privacy challenges
- Current security and privacy attack vectors (with real nasty examples!)
- Security principles and reuse
- Advantage / disadvantage of using OSS security products
- Determining quality of OSS for security and privacy applications
- (Not So) Common used OSS security applications

No Excuse!

Download the:

Open Reference Architecture for Security and Privacy

(no strings attached!)

But of course, better is to...



Contribute!

You can contribute using the following Github repository:

<https://github.com/nocomplexity/SecurityPrivacyReferenceArchitecture>

#tdose

Thank (in advanced) you all for your
great contributions!

*Now we want to try to give an answer to your
brilliant:*

Questions!