Everything You Need to Know About the New CISSP Exam

Doug Landoll
CEO
Lantego
April 25, 2015

www.lantego.com
(512) 633-8405
dlandoll@lantego.com
Session Agenda

• CBK & Question Depth
• 2015 CBK
• New Test Question Formats
• Study Strategies
• Test Taking Strategies
Common Body of Knowledge

- “Mile wide and an inch deep”
  - Lots of vocabulary
- Minimal numbers and form
  - No port #s, No RFC #s
- Know your history
  - Classic definitions
  - Old criteria (e.g. Orange Book)
Preparation Process

• Learn in groups and relationships
  • Look for relationship between terms and principles, across domains, and in practice.

• Learn and build mnemonics
  • Use memory devices such as anagrams, drawings, and phrases.
  • Many of these will be presented in class
  • Compiling these together is referred to as creating your data dump sheet
Data Dump Sheet Example

OSI (TCP) Stack
A
P (A)
S
T (H)
N (I)
D (N)
P

Virtual Addressing
A: ld 3 -> A
D: ld 108(3) -> A
I: ld 507(108(3)) -> A
R: ld (100+8)(3) -> A

Biometrics
(I) FRR; (II) FAR
CER:FRR=FAR
Most Eff: RIP
Most Acc: VSHK

Models
BLP©
No read up
No write down

Biba (I-1)
No read down

CW(I3)
No write up

Concept DE RM
Imp. RI SK

Modes of Ops
Ded/SH/Compartment/MLS

DRP Test Types
Check/Walk/Sim
Parallel/Full/Real

Planning
Strategic/Tactical
Operational

Risk
ALE=SLExARO
SLE=AVxEF
SV=(ALE-ALE”)-Cost

Early Crypto
Trans: Skytale
Sub: Caesar
#sub: Polybus
Polysub: Vigenere

Fires
A(sh): Paper: Soda, Water
B(arrel): Liquid: Soda, CO2, Halon
C(ircuit): Electric: Halon, CO2,

Physical #’s
Temp: 70-74
Humid: 40-60
Light: 2x8
Fence: 3-4, 6-7, 8+

Network, peripherals, workstations
trusted processes
Audit, I&A, ...

SK
S -> RM -> O

TCB/TSF
Trusted System/TOE
Security Perimeter

ACL

CL
# 2015 Common Body of Knowledge

<table>
<thead>
<tr>
<th>2015 CBK</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and Risk Management</td>
<td>Legal,</td>
</tr>
<tr>
<td>Asset Security</td>
<td>Risk Management</td>
</tr>
<tr>
<td>Security Engineering</td>
<td>Cryptography</td>
</tr>
<tr>
<td>Communication and Network Security</td>
<td>Physical Security</td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>Security Architecture</td>
</tr>
<tr>
<td>Security Assessment and Testing</td>
<td>Telecommunications</td>
</tr>
<tr>
<td>Security Operations</td>
<td>Access Control</td>
</tr>
<tr>
<td>Software Development Security</td>
<td>BCP</td>
</tr>
<tr>
<td></td>
<td>Operations</td>
</tr>
</tbody>
</table>

**8 Domains vs. 10 Domains – Who Cares!**
2015 CBK: What’s New: Topics

• 3rd Party Risk Management
• BYOD Risks
• IoT
• Software Defined Networks
• Cloud Identity Services (OAuth 2.0)

Maybe + 4%
Access Control

• Mostly Vocabulary
  • Passwords: Static, Dynamic, Cognitive, vs. Passphrases, Hashes, Thresholds
  • Biometrics: Effective: RIP; Accepted: VSHK
  • Strong Auth
  • IdM: Ident, Authent, Auth (x.500, LDAP, XML, SPML, SAML, SOAP)
  • Policies: DAC, MAC, RBAC
  • SS: Kerberos, KryptoKnight, SESAME

NTX ISSA Cyber Security Conference – April 24-25, 2015
Architecture

- Computer Architecture
  - CPU
  - Operating System
- System Architecture
  - System boundaries
  - Security policy models
  - Modes of operation
- System Evaluation & Accreditation
  - System Evaluation
  - Certification & Accreditation
- Enterprise Architecture
- Architecture Threats
## Architecture: Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Attributes</th>
<th>Policy</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Matrix</td>
<td>S, O, accesses</td>
<td>C: DAC</td>
<td>Rows: CLs, Columns: ACLs</td>
</tr>
<tr>
<td>BLP</td>
<td>S,O,a; no read up, no write down</td>
<td>C: DAC, MAC</td>
<td></td>
</tr>
<tr>
<td>Biba</td>
<td>S,O,a; no read down, no write up</td>
<td>I: Auth changes</td>
<td>Flips BLP</td>
</tr>
<tr>
<td>Clark Wilson</td>
<td>S,O,a; no read down, no write up</td>
<td>I: Auth changes, no mistakes, data consistency</td>
<td>Well-formed transactions, separation of duty</td>
</tr>
<tr>
<td>Non Interference</td>
<td>Inputs (cmds), Outputs (views)</td>
<td>I: Auth changes, C: MAC</td>
<td>Useful in CCA, Not lattice</td>
</tr>
<tr>
<td>Information Flow</td>
<td>Objects, info flow</td>
<td>I: Auth changes, C: MAC</td>
<td>Useful in CCA, Not lattice</td>
</tr>
</tbody>
</table>
Cryptography

**Symmetric**
- DES, TDES, AES, IDEA
- Blowfish, RCx, CAST, SAFER, Serpent

**Hybrid**
- A-DH, RSA, El Gamal, ECC, LUC, Knapsack

**Keyed Hash**
- MAC, HMAC

**Hash**
- MD5, RIPEMD, SHA-x

**Digital Signature**
- DSS, RSA-DS, DSA
# Telecommunications

## Telecommunications & Network Module Review Sheet

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
<th>Technology</th>
<th>Protocol</th>
<th>Equipment</th>
<th>TCP/IP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 Application</td>
<td>provides user access to comm. services</td>
<td>HTTP, FTP, TFTP, SMTP, SNMP, Telnet, S/MIME, PEM, SET, S-HTTP, S-RPC, PGP</td>
<td>Gateways Application-level Gateway FW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6 Presentation</td>
<td>ensures compatible syntax</td>
<td>GIF, MIDI, MPEG, EBCDIC, ASCII</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Session</td>
<td>Coordinates dialog between applications</td>
<td>NFS, SQL, RPC</td>
<td>Gateways Circuit-level Gateway FW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Transport</td>
<td>ensures end-node to end-node data transfer</td>
<td>VOIP (TCP/UDP)</td>
<td>Packet-filtering Firewall</td>
<td>Host-to-Host Transport</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Network</td>
<td>selects and manages route</td>
<td>Virtual Circuits</td>
<td>RIP, OSPF, BGP</td>
<td>Routers Gateway, Switch, Packet-filtering Firewall</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Data Link</td>
<td>reliable data delivery over point-to-point link</td>
<td>leased lines, ISDN, DSL, SMDS, ATM</td>
<td>SLIP, PPP, X.25, Frame Relay, SDLC, HDLC, ARCnet, Ethernet, Token Ring, FDDI, PPTP, L2F, L2TP, PAP, CHAP</td>
<td>Bridge Switch DTE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 Physical</td>
<td>sends and receives bits across the network</td>
<td>HSSI</td>
<td>NIC, cable connectors Repeater Hub</td>
<td>Network Access contains routines for physically accessing the network</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**NTX ISSA Cyber Security Conference – April 24-25, 2015**

@NTXISSA
# Legal

<table>
<thead>
<tr>
<th>Type</th>
<th>IP Protected</th>
<th>Term</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent</td>
<td>Invention</td>
<td>20 years Patent &amp; Trade Office</td>
<td>1st to file vs invent &lt; 1 year of 1st Public Use</td>
</tr>
<tr>
<td>Copyright</td>
<td>Works of authorship</td>
<td>Life + 70; 95 yrs Library of Congress</td>
<td>Fair Use International DMCA</td>
</tr>
<tr>
<td>Trademark</td>
<td>Right to distinguish goods and services</td>
<td>10 years (+) PTO Option file</td>
<td>Distinctiveness (TM) (R) Dilution</td>
</tr>
<tr>
<td>Trade Secret</td>
<td>Proprietary Information</td>
<td>None</td>
<td>Requirements • Commercially viable • Not in public domain • Reasonable protection</td>
</tr>
</tbody>
</table>
Operations

(Learning) Discovery

Enumeration

Vulnerability Mapping

Exploitation

Report to Management

- Newsgroups
- Domain name registries
- Ping sweep, trash INT

- Port Scanning
- OS fingerprinting

- Vulnerability Scanning
- Casing

- Exploit vulnerabilities
- Social Engineer
- Escalate privileges
New Test Question Formats

• Majority: Multiple Choice, 4 candidate answers, pick one

• New Questions:
  • Scenario
  • Drag and Drop
  • Hot Box
Scenario Questions

• Description:
  • Situational: 1-2 paragraphs describing an environment, results of an audit, etc.
  • 3-5 questions on the scenario

• Tactics:
  • Read the question first
  • Consider “operational” issues (tradeoffs)
Drag and Drop

Which algorithms below are examples of symmetric cryptography?

- Advanced Encryption Standard
- Rivest Shamir Adleman
- Diffie Hellman
- El Gamal
- Data Encryption Standard
Hot Spot

The diagram below is a design of a Public Key Infrastructure to secure internet transactions. Within the design is a Certificate Authority, a Registration Authority, and a Validation Authority.

Click on the location of the registration authority.
Study Strategies

• Register NOW
  • Allows for study planning
  • Commits you to the process of successfully studying

• Develop a study plan
  • Available days
    • Number of days from now until the exam date – work and family commitments
  • “Rule of 12” (Now Rule of 10?)
    • Divide you available days by 12 to get study “units”
    • Use 1 unit for each domain
    • Use 2 units for full length exams and data dump
Study Strategies (2)

• Utilize ALL sources
  • CISSP Study book(s)
  • Question resources
    • Book CD, www.cccure.org,
    • StudIScope
    • Course slides and notes

• Take unit and mixed unit exams often
  • Mix it up, not same questions over and over
  • Aim for 80% - 85% in all units
Study Strategies (3)

• Use memory devices
  • Acronyms
    • Word-based
      • DEER MRS CARBIDS
      • Use ANAGRAM solvers to create your own
    • Sentence-based
      • Please Do Not Take Sales People’s Advice
      • Plain Brown Potatoes Raise Plain Thin Men
  • Other Mnemonics
    • Phrases
      • “Reading is simple”
      • Link(in) Tunnel
    • Diagrams
      • Concentric squares, ACM
Test Taking Strategies

• The Day Before
  • Get a good rest
  • Check out the testing center location

• The Day of...

<table>
<thead>
<tr>
<th>What to Bring</th>
<th>What NOT to Bring</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Registration paper work</td>
<td>• Cell phone</td>
</tr>
<tr>
<td>• Snack &amp; Drink</td>
<td>• Digital watch</td>
</tr>
<tr>
<td>• Jacket or sweater</td>
<td></td>
</tr>
</tbody>
</table>
Test Taking Strategies (2)

• Other possible issues
  • Noise from nearby construction or weekend event
  • Temperature
    • Dress in layers (bring a jacket)
  • White board and Marker
    • Ensure you have a good one
Test Taking Strategies (3)

• **Data Dump Strategy**
  • Prior to answering any questions
  • Recall and document diagrams, lists, charts, and other mnemonics

• **Three Pass Method** (Consider this)
  1. Answer obvious questions, update diagrams
  2. Answer all but the most difficult questions
  3. Complete all questions
Test Taking Strategies (4)

• Individual Question Strategy
  • Read question carefully
    • Find keywords and questions (e.g., not, best, first)
    • Read ALL candidate answers – do not jump to first good one
  • Use candidate answers as a clue
    • Look for slight difference between candidate answers
    • Eliminate clearly wrong answers first
      • Phases/steps: key on obvious wrong answers (e.g., report before analysis)
Test Taking Strategies (5)

• Individual Question Strategy (cont.)
  • Use information contained in questions and answers
    • Update diagrams and lists
  • Don’t “argue” with the test
    • Decide what answer ISC2 is looking for
    • “Dumb it Down”
Test Taking Strategies (6)

- Drag and Drop Questions
  - Essentially a matching exercise
  - Easier than normal questions
  - Make simplest / most obvious match first

- Scenario Questions
  - Find the question first.
  - Then go back and get relevant data
  - Usually operational questions
    - security/usability tradeoffs,
    - risk-based decisions,
    - application of principles
Pearson VUE Screen

Section Review

Instructions
Below is a summary of your answers. You can review your questions in three (3) different ways.

The buttons in the lower part of the screen allow you to:
1. Review all of your completed questions.
2. Review questions that you marked as incomplete.
3. Review questions that are flagged.

End Review

You have chosen to end the current review, but have 3 incomplete questions. If you click Yes, you will NOT be able to return to this review.

Are you sure you want to end this review?

[Yes] [No]
The Collin College Engineering Department

Collin College Student Chapter of the North Texas ISSA

North Texas ISSA (Information Systems Security Association)

Thank you