POSTER: Critique of the CISSP Common Body of Knowledge of Cryptography

Stephan Neuhaus
Communication Systems Group
Eidgenössische Technische Hochschule Zürich
Gloriastrasse 35, 8095 Zürich, Switzerland
neuhaust@tik.ee.ethz.ch

Gabriela Gheorghe
Interdisciplinary Center for Security, Reliability, and Trust, University of Luxembourg
4 Rue Alphonse Weicker, L-2721 Luxembourg
gabriela.gheorghe@uni.lu

ABSTRACT

Many security job ads mention that security certificates are regarded as assets, giving the candidate an advantage. For some high-profile jobs, certification may even be required.

No matter where one stands on the subject of certification, the assumption is that the imparted knowledge is at least factually correct. We examine the cryptography section in the Common Body of Knowledge (CBK) underlying the most sought-after certification, the CISSP, issued by the International Information Systems Security Certification Consortium, Inc., or "(ISC)^2"[1][2] [4].

We find many mistakes, some positively dangerous: people who believe what they read there will build systems that are *less* secure than they would have built if they had looked to, say, Wikipedia instead. They include: a confusion of encryption and authentication; an unconditional recommendation of RC4 for key sizes over 128 bits; a belief that block ciphers are inherently stronger than stream ciphers; and many more. These mistakes are elementary and appear in the third edition of the CBK, indicating that two preceding editing cycles were not enough to remove them. This shows that no one knows or cares that the material is wrong.

This poses dilemmas for graduates and companies. Graduates can either obtain a CISSP despite the factual inaccuracies, thereby surrendering at least part of their professional integrity; or they can try to tough it out, thereby lowering their chances of getting a high-profile security job. Companies must either keep using the CISSP, knowing that they have been taught some dangerous nonsense, or find another way to assess a candidate's security knowledge.

[1]This is the official spelling, which we will use consistently throughout.
[2](ISC)^2, CISSP, and CBK are registered trademarks of the Information Systems Security Certification Consortium, Inc.

CCS'13, November 4–8, 2013, Berlin, Germany.

http://dx.doi.org/10.1145/2508859.2512499.

Categories and Subject Descriptors

K.6.1 [**Project and People Management**]: Staffing, Training; K.6.5 [**Security and Protection**]; K.7.3 [**Testing, Certification, and Licensing**]

General Terms

Security, Certification, Management, Standardization

Keywords

Security Certification, Cryptography

1. INTRODUCTION

For many HR departments, certifications are the simple answer to the questions of how to assess someone who applies for a security job, and how to filter out more experienced candidates from the newcomers. First, a trusted third party is vouching for the technical competence of the candidate. Second, one common prerequisite for certification is a certain job experience. Additionally, certifications need to be renewed periodically, ensuring that the candidate's knowledge is current.

One important certification is the Certified Information Systems Security Professional (CISSP), offered by the (ISC)^2. Founded in 1988, the (ISC)^2's self-stated mission is to

> make society safer by improving productivity, efficiency and resilience of information-dependent economies through information security education and certification.

The (ISC)^2's main educational vehicle is the "(ISC)^2 Common Body of Knowledge", or CBK. In the (ISC)^2's words,

> (ISC)^2 develops and maintains the (ISC)^2 CBK, a compendium of information security topics. The CBK is a critical body of knowledge that defines global industry standards, serving as a common framework of terms and principles that our credentials are based upon and allows professionals worldwide to discuss, debate, and resolve matters pertaining to the field. Subject matter experts continually review and update the CBK.[3]

The CBK for the CISSP is organised into ten so-called domains, such as Access Control, Application Development

[3]This quote and the previous ones are from `https://www.isc2.org/aboutus/default.aspx`

Security, Telecommunications and Network Security, and Cryptography. Demonstration of knowledge of the CBK is required to pass the CISSP certification test.

The most recent version of the "Official (ISC)^2 Guide to the CISSP CBK" is the third edition, published in December 2012 [4]. This means that two editing cycles have presumably been used to "review and update" the material by "subject matter experts". We believe that the third edition of a book published by a self-styled "elite" organisation of experts, on a topic where details matter so much, should be about as error-free as it gets.

We only have the Kindle edition of the CBK, so we can only give "location markers" instead of page numbers. We will write them like so: [L. 12345].

All quotes from the CBK have been carefully checked to be letter-accurate (but errors may still have occurred). This includes any stylistic, spelling, or grammar issues.

2. CRYPTOGRAPHY

In addition to the selection of dangerous errors cited below, this section also contains a number of annoyances[4], which mainly betray a lack of care, and "wait, what?" moments, where the text makes no sense at all. These, and more dangerous errors, will feature on the final poster.

By *dangerous errors* we mean errors that, if believed and applied by students, result in system that are *less* secure than if they hadn't had that wrong information or had looked it up in a reliable reference. Or even a not necessarily reliable one: as of today, the relevant Wikipedia articles were all more accurate than what we read in the CBK.

Relative Strengths of Block and Stream Ciphers. The author seems to believe that block ciphers are inherently stronger than stream ciphers:

> Most block ciphers use a combination of substitution and transposition to perform their operations. This makes block ciphers relatively stronger than most stream-based ciphers, but more computationally intensive and usually more expensive to implement. This is also why many stream-based ciphers are implemented in hardware, whereas a block-based cipher is implemented in software. [L. 15034]

We found nothing in the peer-reviewed literature that would support such statements. Also, if block ciphers were slower than stream ciphers, wouldn't it make more sense to implement block ciphers in hardware rather than the already-fast stream ciphers?

Encryption and Authentication. One beginner's mistake is to assume that symmetric encryption per se can help with authentication or freshness:

> If two parties share a symmetric key, and they have been careful not to disclose that key to anyone else, then when they transmit a message from one to another, they have assurance that the message is indeed from their trusted partner. [L. 15242]

Related to this is the notion that modifying an encrypted message in transit makes it completely undecipherable, thus providing integrity checking:

> In many cases, they would also have some degree of confidence in the integrity of the message, because any errors or modifications of the message in transit would render the message undecipherable. With chaining-type algorithms, any error is likely to destroy the remainder of the message. [L. 15224]

A modified ciphertext will decipher just fine, it's just that some of the deciphered data will be junk. Also, some chaining modes like Cipher Block Chaining have a self-healing property where a modified ciphertext block leads to only a small number of corrupted decrypted plaintext blocks.

RC4. In the section on RC4 [L. 15572], we read:

> If RC4 is used with a key length of at least 128 bits, there are currently no practical ways to attack it; the published successful attacks against the use of RC4 in WEP applications are related to problems with the implementation of the algorithm, not the algorithm itself.

To cite just one example of many, the Fluhrer-Mantin-Shamir attack [3] is now 12 years old, and while it *also* attacked WEP, it identified "a large number of weak keys", that were then used to "mount related key attacks with practical complexities". Since then, other attacks have come to light; thus *all* use of RC4 is banned in the Microsoft Secure Software Development Lifecycle [5] since at least 2007[5] because it is too difficult to use securely.

3. COMMUNITY REACTIONS

The CISSP *certification* (as opposed to the CBK) has been criticised from many angles for many years; it has even spawned a humorous YouTube video in which a CISSP uses his plastic CISSP card like a police badge and storms into rooms shouting "everyone step away from the encryption keys and put the server down!"[6]. We will not go into that and focus on criticisms of the CBK.

At Def Con 20, Timmay gave a talk entitled "Why You Should Not Get a CISSP" [6]. In this talk, the presenter argued that the CBK was not up-to-date, but didn't comment on the accuracy of its official guide.

Factual criticism of the CBK is nonexistent; we couldn't even find an independent review of the book, not even on Rob Slade's otherwise excellent "CISSP by domain" pages[7].

4. CONCLUSIONS

It is very tempting to ignore these mistakes on the grounds that they fall outside the area of specialisation of a typical CCS attendee and are thus properly someone else's problem. But such complacency would be wrong.

First of all, formulations like "relevant security qualifications (CISSP) are considered an advantage" are commonly

[4]Having to deal with a text whose sample plaintexts include "I Hate Bed Time" [L. 15089] is an annoyance in itself.

[5]http://www.acsac.org/2007/workshop/Howard.pdf

[6]https://www.youtube.com/watch?v=8DZkpynFhak

[7]http://victoria.tc.ca/int-grps/books/techrev/mnbksccd.htm

found in security job ads[8][9][10]. While certainly not all CISSPs believe in or endorse the mistakes that are found in the CBK, some undoubtedly do, since that's what they read in the $(ISC)^2$'s *official* guide (a point to which we will return later). And these people might get the jobs that you or your graduates aren't getting, simply because they have a certificate that is based at least in part on dangerous errors.

How big is the problem? The $(ISC)^2$ has grown to be internationally recognized, as stated on their webpage:

> We provide [...] Gold Standard credentials to professionals in more than 135 countries. [...] And we're proud of our membership—an elite network of nearly 90,000 certified industry professionals worldwide.

We couldn't find the exact reasons for this recognition, other than historical: the U.S. DoD Directive 8570.1 of 2004 [2, AP2.1.3] encouraged that DoD employees working in information assurance should have certifications from bodies that have been ANSI/ISO/IEC 17024 accredited. Also in 2004, $(ISC)^2$'s CISSP was one of the first certifications to be thusly accredited. However, this accreditation is just a standard of managing personnel certification programmes and gives no indication about the quality of the technical content.

According to Robert Half's 2012 Salary Guide[11], security professionals are in the top five most wanted professionals in the US, and certification is required for positions such as Chief Security Officer or Information Systems Security Manager. Given that it is used by the US Department of Labor to forecast the job market[12], certification has a definite impact on hiring of graduates.

Also, certificate holders earn more: the job search engine SimplyHired notes that CISSP holders can earn between $80000 and $87000 on average, while in related jobs the average is only $78000[13].

To see how many CISSP employees are there from another angle, we used LinkedIn data from simple queries when logged in. We queried for keywords (CISSP, and other acronyms for security certifications), locations and names of well known companies, and also tried to see how many people had additional certifications; see Table 1. We found that around 25,000 people had some certifications other than CISSP. The numbers suggest that few professionals only have a CISSP, and confirm that public bodies tend to ask for certifications more than other employees.

Informally however, we found lots of forum discussions on the topic of security certifications. They are esentially split in two categories: those discussions where someone who has already gained a security certification asks the world "what's the next certification to beef up my CV?", and the discussions on the utility of CISSP-like credentials. In this last case, we found that professionals with system administration experience dismiss the relevance of screening just for CISSP when hiring security staff, for the reason that CISSP training does not touch upon aspects such as operating system security, or technical security details. We even found a blog entry [1] where the CISSP-holding author explains that CISSP has failed at both measuring technical competence, as well as measuring the grasp of security principles. The irony of this situation is in that people who do not believe in the technical value of this certification still take it, and defend its code of ethics as its only advantage compared to other security certifications. But the only real hurdle to getting the CISSP is the test, and not adherence to the code of ethics, which is ambiguous in any case [6].

Certification	LinkedIn members
CCNA	300456
CompTIA	101415
CCNP	84232
CISSP	82779
CISA	59691
CISSP and (CEH or CISM or CISA)	24966
CISM	21019
CEH	20689

Table 1: LinkedIn members with IT certifications.

Two editing cycles have gone by, allowing ample time to check the material (or have it checked) and to react to reports of inaccuracies. But this opportunity was passed up.

The material we have surveyed is not just any publication by the $(ISC)^2$; it is their *official* guide to the CISSP CBK, and is thus endorsed by them. From this review of the crypto chapter, it follows that the $(ISC)^2$ endorses rubbish. We believe that the $(ISC)^2$ should revise the entire section thoroughly, and probably the rest of the CBK, while they're at it.

5. REFERENCES

[1] Richard Bejtlich. CISSP: Any value? `http://taosecurity.blogspot.com/2005/06/cissp-any-value-few-of-you-wrote-me.html`, June 2005. visited June 2013.

[2] U.S. Department of Defense. Dod 8570.01-m information assurance workforce improvement program. `http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf`, December 2005.

[3] Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. In *Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, SAC '01, pages 1–24, London, UK, 2001. Springer-Verlag.

[4] Steven Hernandez, editor. *Official* $(ISC)^2$ *Guide to the CISSP CBK*. $(ISC)^2$ Press, third edition, December 2012. Kindle edition.

[5] Michael Howard and Steve Lipner. *The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software*. Microsoft Press, June 2006.

[6] Timmay. Why you should not get a CISSP. `http://attrition.org/security/conferences/why_you_should_not_get_a_CISSP-public.pdf`, July 2012. Talk at Def Con 20.

[8] `http://www.jobat.be/en/windows-security-specialist/job_653229.aspx`

[9] `http://www.indeed.com/cmp/H2H-Technology/jobs/Cyber-Security-Engineer-4ffec9aa5de920ef`

[10] `http://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/122112-Emory-InfoSecSpecialist.pdf`

[11] `http://www.nwoinnovation.ca/upload/documents/rht_salaryguide_2012.pdf`

[12] `https://ccpdfs.s3.amazonaws.com/guide-securityplus.pdf`

[13] `http://www.simplyhired.com/a/salary/search/q-cissp`