BU Security Group Doctoral Subject Exam in Cryptography and Information Security, 2015

Professors Canetti, Goldberg, Reyzin, and Triandopoulos

1 Announcement

The Doctoral Subject Exam in Cryptography will take place in December 2015 or January of 2016 at a date to be determined by the faculty administering it. The goal of the exam is to test the students' preparedness for conducting research within the security group. Students intending to take the exam should contact Professors Canetti, Goldberg, and Reyzin by the end of October. Post-master's students are expected to pass this exam in their second year; post-bachelor's students can (but are not encouraged to) wait until their third year. Students are strongly encouraged to join forces and organize a reading group to study for this exam.

Structure of the exam: The exam will consist of two parts. The first part will be in-class (closed book), lasting 2-3 hours; it will require a basic understanding of all the topics below. The second part will be take-home (open book), lasting 2 days; it will consist of more in-depth questions, but you will be able to omit two topics out of topics 3–6. We will ask you to let us know in advance which topics you will choose, so we can prepare the exam accordingly.

2 Topics Covered

Below is the list of topics covered.

1. The union of the contents of BU CAS CS 538 as taught by Leo and Ran. The material appears in the online class notes at:
   - `http://www.cs.bu.edu/~reyzin/teaching/cryptonotes/`
   - `http://www.cs.tau.ac.il/~canetti/f08.html`
   - `http://www.cs.tau.ac.il/~canetti/f09-materials/f09-scribe3.pdf`
   - `http://www.cs.tau.ac.il/~canetti/f09-materials/f09-scribe4.pdf`
2. The contents from BU CAS CS 558 as taught by Sharon, specifically
   - TLS, Certificates, PKI infrastructures, and their vulnerabilities
   - Web security (cross-site scripting, cross-site request forgery, SQL injection, cookies, web tracking, the risk of mixing HTTP and HTTPS content.)
   - network security (BGP security (BGPSEC, RPKI), DNS security (DNSSEC), IPSec, distributed DoS attacks and DoS amplification.

   Possible references for this material include Section 2 of [AM01] for DNSSEC, Chapter 19 of [Sta11] for IPsec, [KLS00] for secure BGP, Chapter 16 of [Sta11] for TLS.
3. Correctness of outsourced computation: the definition of PCPs and main result (without constructions/proofs) ([Din07, Section 1] has a concise introduction); the Kilian/Micali protocol for succinct arguments for NP [Mic00].

4. Key exchange: the basic Diffie-Hellman protocol (which assumes authenticated communication channels between the parties) and challenges in designing protocols when such channels do not exist, as explained in chapters 1–5 `http://webee.technion.ac.il/~hugo/sigma-pdf.pdf`. The setting of password-based key exchange, as explained in Section 1 of `http://eprint.iacr.org/2010/368.pdf`.

5. Real/ideal paradigm for multiparty computation and the problems of composition, as explained in chapters 1–5 of `http://eprint.iacr.org/2006/465`.

6. The basic principles of the following attacks: buffer overflow (stack-smashing/return-oriented programming), cross-site scripting, side channels (power consumption/timing/caching).

References

[AM01] G. Ateniese and S. Mangard. A new approach to dns security (dnssec). In *Proceedings of the 8th ACM conference on Computer and Communications Security*, pages 86–95. ACM, 2001.

[Din07] Irit Dinur. The PCP theorem by gap amplification. *J. ACM*, 54(3):12, 2007.

[KLS00] S. Kent, C. Lynn, and K. Seo. Secure border gateway protocol (s-bgp). *Selected Areas in Communications, IEEE Journal on*, 18(4):582–592, 2000.

[Mic00] Silvio Micali. CS proofs. *SIAM Journal on Computing*, 30(4):1253–1298, 2000.

[Sta11] W. Stallings. *Cryptography and network security, Fifth Edition*, volume 5. Prentice hall, 2011.