Jaarverslag 2007

Ei/Ψ is formeel van start gegaan op 1 oktober 2007. Dit is de dag dat Sandro Etalle voor 0.5 fte begonnen is als Security hoogleraar bij Informatica.
De periode okt.- dec. kenmerkt zich vooral door typische aanvangsverschijnselen: werving personeel, interne verhuizingen, e.d.

Activiteiten voor 1-10-2007

Nadat Ei/Ψ het groene licht had gehad van het FB (dec. 2006), zijn de volgende stappen ondernomen:

- Verkennende gesprekken over mogelijke samenwerking door Henk van Tilborg met: Baeten (FM), Brinksma (ESI), Jonker (Philips), Lukkien (SAN), Linartz (Philips), Rijnsoever (Philips), Schimmel (LaQuSo).
- Ontwikkeling Ei/Ψ logo.
- Ontwikkeling van plannen voor een "Grand Opening".
- Voorbereidende gesprekken tussen Van Tilborg en Etalle (2x),

Wetenschappelijke activiteiten na 1-10-2007

- Eerste Security Seminar bijeenkomst op 12 dec.
  Skoric (Philips) spreekt over *Security with noisy data*.
- C&C Ph.D. bijeenkomsten op 1 okt., 9 okt., 5 nov., 3 dec.
- Cryptography Working Group (4 sprekers) in Utrecht op 5 okt. en 7 dec.
- Minicursus "Cryptography" door Maurer en Renner (8-12 okt.)
- Promotie Ellen Jochemsz (*Cryptanalysis of RSA variants using small roots of polynomials*) op 4 okt.
- Promotie Andrey Sidorenko (*Design and analysis of provably secure pseudorandom generators*) op 29 okt.
- Afstudeervoordracht door Peter van Liesdonk (*Anonymous and fuzzy identity-based encryption*) op 22 okt.
- Afstudeervoordracht door Mark Baaijens (*Prepare for VoIP Spam*) op 30 nov.
- Bezoekers: Dan Bernstein 1/10-31/12.

Organisatorische activiteiten na 1-10-2007

- Werving UD Security, resulterend in aanstelling van Jerry den Hartog.
- Werving Spiessens als Postdoc (4 jaar) op Poseidon project.
- Werving Trivellato als Ph.D. student op Poseidon project.
- Werving Elahi als PhD student op PEARL project.
- Werving Pontes als PhD student op S-mobile project.
- Werving Peter Schwarbe als Ph.D. student op CACE project.

- Werving Michael Naehrig als Ph.D. student.
- Aanvraag (en honorering) van computercluster door Lange en De Weger voor grootschalig rekenen (voor Hash Clash, Edwards curve method of factorization, eBats, etc.).
- Vergaderingen van Ei/Ψ-top (Etalle, Jacobs, Lange, Tilborg) op 19 sept. en 3 okt.
- Uitwerking plannen van de Grand Opening op 21 en 22 april. Programma is klaar, voorlopige aankondiging is uitgezonden, contact met de pers is gezocht.
- Gesprekken met Paul Overbeek over eventueel deeltijdhoogleraarschap.
- Informele openingsborrel op 3 oktober.
- Opzetten webpagina (door Klooster en Kortsmit)
- Afspraken over secretariële ondersteuning.

Lopende en gehonoreerde projecten

- TAS3IP/Trust Management (EU Integrated Project), 2008-2012.
- PRIAM – Privacy Issues and Ambient intelligence (INRIA), 2007-2008.
- CACE - Computer Aided Cryptography Engineering (EU-project, FP7); aanvang 1-1-2008.
- SecureSCM –Secure Supply Chain Management (EU-project, FP7); aanvang 1-2-2008.
- ECRYPT - Network of Excellence in Cryptography (EU-project)
- ECRYPT II - Network of Excellence in Cryptography (EU-project, FP7); aanvang in de zomer van 2008.
- Pearl – Privacy Enhanced security Architecture for RFID labels (STW/Sentinels project), 2007-2008.
- S-Mobile - Security of Software and Services for Mobile Systems (STW/Sentinels project), 2007-2011.
- PINPASJC - Program Inferred Power Analysis in Software -- JavaCard (STW/Sentinels project), 2005-2008.
- SEDAN - SEarchable DAta eNcryption (STW/Sentinels project), 2007 -2011.
- PASC - Practical Aspects of Secure Computation, (STW/Sentinels project), 2006 - 2009
- POSEIDON - System Evolvability and Reliability of Systems of Systems (ESI/Thales), 2007-2011.
- DIAMANT, Cryptologie hoogleraar, 2006-2011.
- NIRICT, Embedded System Security hoogleraar 2007-2012.

Huisvestiging

- Met ingang van 1 okt. is Sandro Etalle gehuisvest op 9.83 en is Bart Jacobs verhuisd naar 9.86. Hiervoor waren enige verhuizingen op vloer 9 (noordzijde) nodig. Hiermee is het bij elkaar brengen van de leerstoelen Security en C&C gerealiseerd.
- De GEWIS ruimte is volledig gerenoveerd en met ingang van 1 dec. zijn de Ph.D. studenten daar werkzaam. De bilocatie wordt door iedereen als een nadeel ervaren. Communicatie verloopt minder spontaan, maar o.a. door gezamenlijke theepauzes ’s

middags proberen we dit effect te minimaliseren. De faculteit heeft kosten nog moeite gespaard om 8.79 goed in te richten. Jammer genoeg verloopt de afwerking langzaam.
- Plannen om 8.74 in te richten voor de verdubbeling van het aantal Ph.D. studenten zijn geïnitieerd.

Media
- Het werk van Benne de Weger, zijn afstudeerder Mark Stevens, en Arjen Lenstra over hash clashes van MD5 heeft geleid tot uitgebreide rapportage in de media: De Automatiseringsgids 49 (7 dec.), The Economist (12 dec.), De Pers (12 dec.), Cursor (20 dec.), Eindhovens Dagblad (28 dec.) .
- Quotes van Bart Jacobs wordt aangehaald in Trouw (12 dec.)

papers:
* Bernstein, D.J., Birkner, P., Lange, T., Peters, C.P. (2007). Optimizing double-base elliptic-curve single-scalar multiplication. In K.
Srinathan, C. Pandu Rangan, M. Yung (Eds.), Progress in Cryptology - INDOCRYPT 2007 (Proceedings 8th International Conference on Cryptology in India, Chennai, India, December 9-13, 2007). (Lecture Notes in Computer Science, Vol. 4859, pp. 167-182). Springer.

* Bernstein, D.J., Lange, T. (2007). Faster addition and doubling on elliptic curves. In K. Kurosawa (Ed.), Advances in Cryptology - ASIACRYPT 2007 (Proceedings 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Sarawak, Malaysia, December 2-6, 2007). (Lecture Notes in Computer Science, Vol. 4833, pp. 29-50). Springer.
This paper is invited to the Journal of Cryptology as one of the two best papers of Asiacrypt 2007.

* Bernstein, D.J., Lange, T. (2007). Inverted Edwards coordinates. In S. Boztas, H. Lu (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Proceedings 17th International Conference, AAECC-17, Bangalore, India, December 16-20, 2007). (Lecture Notes in Computer Science, Vol. 4851, pp. 20-27). Springer.

invited talks at:
* Explicit Methods in Number Theory In honour of Henri Cohen
* SAGE Days 6: Cryptology, Number theory, and Arithmetic Geometry
* Kolloquium über Kombinatorik
* Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17)

- **TAS3**

  EU Integrated Project
  Duration: January 2008 until December 2012

- **PRIAM: Privacy Issues and AMbient intelligence**

  INRIA/Univ. St. Etienne collaboration, funded by INRIA
  Duration: January 2007 until December 2008
  Contact: Sandro Etalle

- Further information: http://priam.citi.insa-lyon.fr/

National Funding

- **POSEIDON: System Evolvability and Reliability of Systems of Systems**

  ESI/Thales collaboration, funded by BSIK
  Duration: June 2007 until June 2011
  Contact: Sandro Etalle

  The Poseidon project rises to the challenge to discover new ways on how to build advanced systems of systems, and therefore on how to allow for flexibility, adaptability and evolvability in systems of systems while ensuring reliability -- a crucial requirement, not only in the domain of maritime safety systems that provides Poseidon's exemplary application and the industrial laboratory needed for its success.
  Further information: http://www.esi.nl/poseidon.

- **PEARL: Privacy Enhanced security Architecture for RFID Labels**

  TU/e/RUN/TUD collaboration, funded by STW/Sentinels under project nr. EIT.7639
  Duration: January 2007 until January 2011
  Contact: Sandro Etalle

  http://www.pearl-project.org/

- **S-Mobile: Security of Software and Services for Mobile Systems**

  VU collaboration, funded by STW/Sentinels under project nr. VIT.7627
  Duration: January 2007 until January 2011
  Contact: Sandro Etalle.

- **PINPASJC: Program Inferred Power Analysis in Software -- JavaCard**

TU/e/RUN collaboration, funded by STW/Sentinels under project nr. TIF.6687
Duration: January 2005 until December 2008
Contact: Sandro Etalle/Jerry den Hartog

http://www.win.tue.nl/pinpasjc/.