# JOOP BAUTZ INFORMATION SECURITY AWARD
# JURY RAPPORT 2007

**De Jury van de Joop Bautz Information Security Award 2007 is na ampel beraad tot de eenstemmige conclusie gekomen dat zij voor de Joop Bautz Information Security Award 2007 nomineert:**

## *Marc Stevens*

**voor zijn master thesis getiteld: "On Collisions of MD5"** [1]

De Jury overweegt hierbij het volgende:

In 2007 werd het voor de zesde maal mogelijk om kandidaten voor te dragen voor de Joop Bautz Information Security Award, een prijs ingesteld door 4 instellingen, actief op het gebied van informatiebeveiliging in Nederland (PvIB, ISACA, NOREA en ECP.nl).
De toetsingscriteria hiervoor luiden:

- **Theorie:** vernieuwing, originaliteit, bronnengebruik, aanpak, presentatie
- **Praktijk**: originaliteit, effectiviteit & efficiency, "zitten we er op te wachten"
- **Instrumentarium**: originaliteit, nauwkeurigheid, toepasbaarheid, gemak
- **Relevantie**: maatschappelijk draagvlak, kostenfactoren, werkingssfeer, acceptatie

Na bestudering van de in totaal 15 voordrachten heeft de jury er vijf genomineerd, waaronder de voordracht van **Marc Stevens.** De Jury overweegt bij het werkstuk van Marc het volgende. Zijn werkstuk betreft een technisch-wiskundig onderwerp met mogelijk grote impact op het dagelijks gebruik van informatietechnologie. Op tal van manieren gebruiken wij daarin hash functies (niet van Marokkaanse, Libanese of lokale herkomst), d.w.z. een vorm van eenrichtingsversleuteling, bijv. in wachtwoord-encryptie. Een paar jaar geleden ontdekte een Chinese wetenschappster, mevrouw Xiaoyun Wang, dat het mogelijk is bekende Public Key encryptie toepassingen te kraken, middels de "collision" methodiek. Marc heeft haar vinding verfijnd en toegepast op het MD5 algoritme, in 1991 ontworpen door Ronald Rivest en sindsdien uitgegroeid tot de facto standaard voor hashing. Gebruikmakend van de rekenkracht van vele PC's via het HashClash project binnen het BOINC raamwerk (een vrijwillige vorm van samenwerking, waarbij loze rekenkracht om niet ter beschikking van een onderzoeker wordt gesteld) bleek Marc in staat de tijd benodigd voor een "collision", oftewel een voorspelbare in plaats van een onvoorspelbare uitkomst aanmerkelijk terug te brengen. Dit leverde hem o.a. uitnodigingen voor internationale fora en artikelen in zeer prestigieuze tijdschriften op.

De Jury beoordeelde zijn werkstuk met de kwalificatie theoretisch uitstekend en mogelijk van grote invloed op de toekomst van beveiligingsoplossingen voor standaardsituaties. Marc heeft met zijn werk aangetoond dat de Nederlandse wetenschapsbeoefening op het gebied van cryptologie - hoeksteen van de veiligheid van vrijwel al ons gebruik van informatietechnologie – volwaardig meetelt. Dat geeft oranjegevoel dat uitgaat boven een andere nationale trots, het verschijnsel "coffeeshops"…..

De Jury van de Joop Bautz Information Security Award 2007

Mr. P. van Dijken (voorzitter) K.F. Rorive (secretaris)

[1]) Afstudeer thesis Technische Universiteit Eindhoven, Afdeling Wiskunde en Computer Wetenschap, Eindhoven juni 2007. Begeleiders waren Prof. Dr. Ir. H.C.A. van Tilborg, Dr. B.M.M. de Weger en drs. G. Schmitz.