

JOOP BAUTZ INFORMATION SECURITY AWARD JURY RAPPORT 2009

De Jury van de Joop Bautz Information Security Award 2009 is na ampel beraad tot de eenstemmige conclusie gekomen dat zij voor de Joop Bautz Information Security Award 2009 nomineert:

Thijs Kinkhorst en Michael van Kleij

voor hun afstudeerthesis getiteld: "Detecting the ghost in the browser: Real time detection of drive-by infections" ¹

De Jury overweegt hierbij het volgende:

In 2009 werd het voor de achtste 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-EPN).

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 8 voordrachten heeft de jury er 3 genomineerd, waaronder de voordracht van Kinkhorst en Kleij. De Jury overweegt bij het gezamenlijke werkstuk van deze auteurs het volgende.

Het doel van hun werkstuk betrof een studie naar het detecteren van "drive-by" infecties op basis van gemeten eigenschappen van Internetverkeer. Daartoe ontwikkelden zij een methodiek die kansrijk bleek in het vroegtijdig ontdekken van typische Internet gerelateerde "malware", zo kansrijk zelfs dat een gespecialiseerde dienstverlener op het gebied van informatiebeveiliging (Fox-IT) al begonnen is met concrete implementatie. Zij tekenen daarbij aan dat het verschijnsel "drive-by" infecties zeer actueel is, het een nieuwe manier van besmetten betreft waartegen firewalls geen bescherming bieden en die gebruik maken van bekende en minder bekende kwetsbaarheden in browsers en browser plugins. De auteurs betogen dat hun methode beoogt robuust te zijn tegen de vele, zeer snelle veranderingen in infectueuze software en eenvoudig te implementeren en bij te werken.

De Jury beoordeelt dit werkstuk met de kwalificatie zeer goed op alle criteria van de Award. De Jury overweegt daarbij dat het werkstuk een mooie balans bevat tussen theorie en praktijk, de methodiek een nieuwe aanpak betreft, en die daarom nog wel in een laboratorium fase verkeert. Maar gegeven het feit dat wij allemaal vele malen per dag browsers aanklikken en browser plugins gebruiken, gaat het om een zeer praktisch en innovatief werkstuk van mogelijk grote maatschappelijke waarde, dat hopelijk zal bijdragen aan veilig gebruik van Internet.

Kortom, het betreft een goed onderbouwd werkstuk over een actueel thema met hoge maatschappelijke relevantie, met een aantal vernieuwende inzichten.

De Jury van de Joop Bautz Information Security Award 2009

Mr. P. van Dijken (voorzitter)

K.F. Rorive (secretaris)

¹) Afstudeerthesis Faculteit Natuurwetenschappen, Wiskunde en Informatica, Universiteit van Amsterdam, begeleider dr. Ir. C.Th.A.M. de Laat, voorjaar 2009