TouW Informatica Symposium

Security & Privacy in a Connected World

zaterdag 19 november 2016, 10:00-20:00

Studiecentrum Amsterdam

Op zaterdag 19 november 2016 organiseert de faculteit Informatica van de Open Universiteit samen met de studievereniging TouW het jaarlijkse symposium voor studenten, alumni en medewerkers, in studiecentrum Amsterdam (Amstelveenseweg 390, 1076 CT Amsterdam).

Security en privacy worden steeds belangrijker. Tegelijkertijd zitten onze apparaten en wijzelf steeds vaker online. Gaan deze trends wel samen?

Prof. dr. Marko van Eekelen, hoogleraar aan de OU zal de daginleiding verzorgen**.** Vervolgens zijn er lezingen door p**rof. dr. Sjouke Mauw** van de **Université du Luxembourg** en **ir. Walter Bergers** van **Madison Ghurka**. Na de lunch volgen lezingen door **dr. ir. Harald Vranken** en **dr. Gergely Alpár**, beiden van de OU.

Natuurlijk besteden we ook aandacht aan de nieuwe ontwikkelingen rond de studie. In de middag wordt in aparte parallel-sessies voor bachelor- en masterstudenten ingegaan op deze ontwikkelingen. Daarnaast is er een extra parallel-sessie voor alumni en promovendi door **dr. ir. Hugo Jonker**.

De studieadviseurs van de faculteit, **Henk Frederiks en Janine Voncken**, zijn de hele dag aanwezig om vragen rond jaarplanning, vrijstellingen en inschrijving te beantwoorden.

De dag wordt traditiegetrouw afgesloten met een huldiging van de geslaagden voor onze bachelor- en masteropleidingen. Daarna is de borrel en het gezellige buffet.

Als je alvast een indruk wilt krijgen van een dergelijk symposium kijk dan naar informatie van de OU over voorgaande symposia: http://portal.ou.nl/web/informatica/symposia

Met vriendelijke groeten,

Netty Stoelinga

namens de OU-docenten, Hugo Jonker en Lloyd Rutledge en namens het bestuur van de studievereniging TouW, Rikki Dijkman en Marcel Korpel.

AANMELDEN

Het is belangrijk dat iedereen die aan het symposium wil deelnemen zich van tevoren aanmeldt. Dat gaat door een e-mail te sturen naar Netty Stoelinga (netty.stoelinga@gmail.com). Er zijn ongeveer 100 plaatsen beschikbaar. Inschrijving gaat op volgorde van aanmelden. Wil je hierbij duidelijk aangeven welke van de parallel sessies je wilt bijwonen? En of je deelneemt aan het buffet?

De prijs voor het symposium bedraagt voor TouW leden € **30,00** inclusief buffet. Zonder buffet is het € **12,50**. Voor niet-TouW leden € **35,00** inclusief buffet en anders € **17,50**.

Over te maken naar giro 2986197 t.n.v. TouW te Eindhoven o.v.v. 'symposium 2016'

Voor overschrijvingen met IBAN nummer en overschrijvingen vanuit België:

IBAN nummer:	**NL 09 INGB 0002 9861 97**
BIC code:	**INGBNL2A**

Lid worden van TouW kan ook: de contributie bedraagt € 12,50 per kalenderjaar en kan ook overgemaakt worden naar bovenstaand gironummer, onder vermelding van 'contributie 2015'. Ook graag even aanmelden op bovenstaand e-mail adres. Als je nu lid wordt geldt ook de korting voor TouW leden.

Deelnemers die door de faculteit zijn uitgenodigd hoeven niet te betalen.

Programma

10:00	**Inloop** met koffie en thee.		
10:30	Marko van Eekelen *Hoogleraar Open Universiteit, dagvoorzitter* **Inleiding**		
11:00	Sjouke Mauw *Hoogleraar Université du Luxembourg* **Let's stick together: digitally ensuring physical proximity**		
12:00	Walter Bergers *Principal Security Consultant, Madison Ghurka* **Privacy in de praktijk**		
13:00	lunch		
14:00	Harald Vranken *Open Universiteit* **Resilience of the Internet: case studies on DNS availability and botnet detection**		
14:45	Gergely Alpár *Open Universiteit* **Cookie in the fridge – privacy problems with the Internet of Things and some ideas how to fix them**		
15:30	Koffie		
15:45	Tanja Vos *bachelor informatie sessie* **Ontwikkelingen in de bacheloropleidingen Informatica en Informatiekunde**	Bastiaan Heeren *Master informatie sessie* **Ontwikkelingen in de masteropleidingen BPM&IT, CS en SE**	Hugo Jonker *alumni en promovendi sessie* **FP-Block: usable web privacy by controlling browser fingerprinting**
16:30	Huldiging afgestudeerden.		
17:00	Netty Stoelinga **Afsluiting.**		
	Borrel en Diner		
19:30	**Sluiting**		

Hoofdsprekers

prof. dr. Sjouke Mauw
Université du Luxembourg

Sjouke Mauw is professor in security and trust of software systems at the University of Luxembourg. His current research focuses on the application of formal methods in the area of information security.

Let's stick together: digitally ensuring physical proximity

What do traditional keys, train tickets and coins have in common? They are increasingly being replaced by digital solutions, such as electronic car keys, smart tickets and contactless payment systems. Unfortunately, various physical properties that are easily verified in the traditional setting are significantly harder to achieve in the digital world. An example is the proximity of a lock and its key. In the physical world, in order to open a lock, the key needs to be physically inserted into it. However, proximity is much harder to ensure using digital means only. And indeed, relay attacks on existing electronic car keys have been found.

Over the past few decades, researchers have been studying security protocols that digitally ensure such physical properties. In this presentation I will discuss protocols for two such properties: distance-bounding protocols and grouping protocols. I will also briefly touch on their merger: distance-bounding grouping protocols.

ir. Walter Belgers
Madison Gurkha

Walter Belgers is Principal Security Consultant bij Madison Gurkha, een onafhankelijk bedrijf dat zich bezig houdt met technische IT-beveiliging. Walter is niet te vinden op Facebook.

Privacy in de praktijk

We werken steeds meer digitaal. We koppelen steeds meer aan internet. We slaan steeds meer gegevens op. Wat doet dat met onze beveiling? En met onze privacy? Walter Belgers gaat in op deze vragen met als leidraad voorbeelden die hij in het dagelijks leven om zich heen ziet.

Overige voordrachten

dr. ir. Harald Vranken, Open Universiteit
Resilience of the Internet: case studies on DNS availability and botnet detection

The central theme of this talk is the resilience of the Internet. We will start with a short introduction on the term 'resilience', which is a broad concept that covers, among others, aspects of trustworthiness and security. Next, we will present two case studies: (1) guaranteeing the availability of some vital part of the Internet infrastructure, and (2) preventing the availability of malicious services on the Internet. In the first case study we explore the impact on the availability of the .nl-domain when parts of the DNS infrastructure fail. In order to do so, we developed an analysis method to identify the name servers and resolvers involved, to map the topology of relevant parts of the Internet, and to simulate failure scenarios in which parts of the DNS infrastructure fail. Next, we applied this method to the .nl-domain. We found that the impact on availability is negligible in most failure scenarios, and that negative impacts can be avoided by simple measures. In the second case study we explore the detection of large-scale botnets. We present an ongoing research project in which we create signatures of botnets by off-line analysis of anomalies in DNS network data. Next, we apply these signatures to detect botnets in real-time at a national scale by on-line monitoring the DNS-traffic at domain name registries and Internet Service Providers (ISPs). We conclude the talk with some outlooks to future research on these topics and opportunities for graduation projects.

dr. Gergely Alpár, Open Universiteit
Cookie in the fridge – privacy problems with the Internet of Things and some ideas how to fix them

Cookies are one of the main elements of web technologies today. They make the link between web-site visitors and organisations. There are multiple things that can go wrong; and do go wrong here. The Internet of Things is a new communication platform between humans and machines. Since it has been created by the same technological trends as web cookies, they inherit some of the same problems. These problems, most related to privacy, have broad consequences. In this thought-provoking talk, I will discuss phenomena that seem to be unavoidable, yet they can (and probably should) be changed. The group that can primarily influence the current trends is exactly the group of computer scientists, that is, YOU!

dr. ir. Hugo Jonker, Open Universiteit
FP-Block: usable web privacy by controlling browser fingerprinting

Online tracking of users is used for benign goals, such as detecting fraudulous logins, but also to invade user privacy. We posit that for non-oppressed users, tracking within one website does not have a substantial negative impact on privacy, while it enables legitimate benefits. In contrast, cross-domain tracking negatively impacts user privacy, while being of little benefit to the user. Existing methods to counter tracking treat any and all tracking similar: client-side storage is blocked, or all sites are fed random characteristics to hamper re-identification. We develop a tool, FP-Block, that counters cross-domain tracking, while allowing intra-domain tracking. For each visited site, FP-Block generates a unique, consistent fingerprint: a "web identity". This web identity is then used for any interaction with that site, including for third-party embedded content. This ensures that ubiquitously embedded parties will see different, unrelatable fingerprints from different sites, and can thus no longer track the user across the web.