08:30

Registration opens

Coffee, tea and croissants will be served.

09:00

Welcome

Conference starts!

09:15

Scott Helme
Security Researcher

What We've Learned From Billions of Security Reports

Running one of the largest security reporting platforms of its kind, we handle billions of security reports for our customers every single month. Come and learn how we've scaled from handling 10,000 reports per month to 10,000 reports per second and the many evolutions our infrastructure has gone through. Alongside that come and see how, with our bird's-eye view of such a diverse ecosystem, we've helped identify malware in a multinational organisation, had a malicious browser plugin taken down and much more!

10:15

Monica Verma
PwC Digital Trust

Building an agile Security Organization

In 2017, Vipps was carved out from DNB. It is now owned by multiple banks, and Vipps has had to re-engineer its approach to Security Governance. PwC had been contracted by Vipps in Winter 2017 to build an agile Information Security Management System (ISMS). Additionally, PwC was engaged to help with the implementation of metrics & security monitoring within the organization, handling security incident operations and assisting Vipps with ISMS and Security Governance following the merger. In this talk, we'll go through the business case of how we built agile ISMS, how PwC intends to support Vipps' ISMS and Security Architecture, and how this could transform the way Vipps is seen and experienced by its customers.

11:15

Andrew Martin
Control Plane

The State of Your Supply Chain

Container security often focuses on runtime best-practices whilst neglecting delivery of the software in the supply chain. Application, library, and OS vulnerabilities are a likely route to data exfiltration, and emerging technologies in the container ecosystem offer a new opportunity to mitigate this risk. Treating containers as immutable artefacts and injecting configuration allows us to "upgrade" images by rebuilding and shipping whole software bundles, avoiding configuration drift and state inconsistencies. This makes it possible to constantly patch software, and to easily enforce governance of artefacts both pre- and post-deployment. In this talk we detail an ideal, security-hardened container supply chain, describe the current state of the ecosystem, and dig into specific tools. Grafeas, Kritis, in-toto, Clair, Micro Scanner, TUF, and Notary are covered, and we demo how to gate container image pipelines and deployments on cryptographically verified supply chain metadata.

12:15

Chris Dale
Netsecurity

When exploits are blind

Demonstration based presentation. Only intro and outro powerpoint slides. Demonstrate user enumeration using timing attacks. Especially prominent when companies have implemented bcrypt/scrypt/pbkdf#2. Attack vector which is very useful in many cases today, notably against Lync/Skype4B installations today. Further password spray into a solution. Discover, analyze and fully exploit reverse-shell command injection. How to find these across large systems? How dose vulnerability scanners work, and how do they detect this? Introduction to Burp Collaborator. Introduction to script for merging attack data into hundreds of Burp Collaborators. Discover, analyze and fully exploit blind SQL Injection. Demonstrating Burp Intruder cluster bomb attack to enumerate out table data.

13:00

Lunch break

13:45

Erlend Oftedal
Blank AS

Modern Web Application Vulnerabilities

With the emerging popularity of bug bounty programs, lesser known and even brand new vulnerability classes are gaining popularity. This talk will give a walk-though of some of these vulnerabilities, how they occur in modern web applications and how they can be found and fixed.

14:45

Alan Saied
Visma

Machine Learning for Security

The ability to mathematically classify patterns, predict events and/or identify abnormalities within a wide range of data is known as Machine Learning. For the purpose of this conference , we explain the power of data and how it can be used with Machine Learning models to identify abnormal behaviour within complex environments. We also explain the ingredients and the steps required to build a Machine Learning models to serve security tasks. This will further be followed by its complications in terms of false positives, accuracy of detection and validity of model and how this can be improved.

15:45

Patricia Aas
TurtleSec

Linux Security APIs and the Chromium Sandbox

The Linux Security and Isolation APIs have become the basis of some of the most useful features server-side, providing the isolation required for efficient containers. However, these APIs also form the basis of the Chromium Sandbox on Linux, and we will study them in that context in this talk.

16:45

Audun Ytterdal
Schibsted Media Group

VG under Attack! War Stories from the Ops Trenches

A collection of old and new war stories from Norways largest news site as seen from the perspective of the VG/Schibsted operation including stuff like Nazis, Pink Blogs, Anonymous, FBI, and how to build you own DDOS canon.

17:30

Closing

17:45

After-party

Come party with us in the basement at UiO

Platinum sponsor

mnemonic

Gold sponsors

f5

vipps

Standard sponsors

BEKK

blank

Klaveness Digital

SCHIBSTED MEDIA GROUP

Venue sponsor

UiO

Main page photo by Benson Kua