
The Microsoft Ecosystem Strategy (EcoStrat) team hosts an annual security conference called BlueHat. The goal of the BlueHat conference is to educate Microsoft engineers, executives, and invited guests, on current and emerging security threats in an effort to help address security issues in Microsoft products and services to better protect customers.

The following selection of talks were the most compelling and talked-about from BlueHat v12, and are now available to view online here.

## Fraud and Abuse: A Survey of Life on the Internet Today

*Ellen Cram Kowalczyk, Principal Security Program Manager Lead, Microsoft*

Kowalczyk kicked off BlueHat v12 in the morning with a look at two of the most difficult security issues facing our customers today. When you're in the process of becoming the leading devices and services company, this is the sort of thing that's on your mind every morning.

WATCH IT ON DEMAND

## Social Authentication

*Alex Rice, Product Security, Facebook*

Over the past year, Facebook engineers have been working on various attempts to expand authentication from "something you know" to "someone you know." Rice's talk demonstrates some of the results and details the lessons his company has learned along the way.

WATCH IT ON DEMAND

## Scriptless Attacks: Stealing the Pie Without Touching the Sill

*Mario Heiderich, Dr.-Ing, Ruhr-University in Bochum, Germany*

Removing JavaScript from the cross-site scripting equation doesn't necessarily take away the XSS pain, as Dr. Heiderich demonstrates. Learn how attackers can use seemingly benign features to build side-channel attacks that can measure and exfiltrate data from even well-protected sites – and find out what can be done to stop it.

WATCH IT ON DEMAND

## Stuff My Cloud Evangelist Says… Just Not My CSO

*Chris Hoff, Senior Director and Security Architect, Juniper Networks*

In front of an audience evenly divided between developers and security folk, Chris Hoff laid out the differences in worldview between the two – yes, there are a few – and how those translate into the world of cloud computing. More secure? Less secure? Let the debate begin…

WATCH IT ON DEMAND

## Don't Stand So Close to Me: An Analysis of the NFC Attack Surface

*Charlie Miller, Systems Software Engineer, Twitter*

Near-field communication (NFC) technology is growing in popularity, with mobile devices leading the communications charge. But when you tap your phone to an NFC-enabled terminal to make a credit-card payment, how do you know you haven't been owned – or worse? Miller looks at how NFC technology expands the potential attack surface for mobile devices.

WATCH IT ON DEMAND

## Building Trustworthy Windows Store Apps

*David Ross, Principal Software Security Engineer, Microsoft and Crispin Cowan, Senior Program Manager, Windows Security, Microsoft*

The Windows Store environment is designed to protect consumers' machines and data from individual apps, but that puts serious responsibility on developers to use secure coding practices. Ross and Cowan look at what that means and how developers can approach the challenge without tears.

WATCH IT ON DEMAND

## Why UEFI?

*Matthew Garrett, Senior Software Engineer, Nebula*

The Unified Extensible Firmware Interface (UEFI) brings far greater security to the firmware environment, letting developers build security policies that extend all the way into the most basic layers of shipped code. But do we lose platform differentiation in the process? Garrett details why that's not necessarily the case.

WATCH IT ON DEMAND

## Pass the Hash and Other Credential Theft and Reuse: Preventing Lateral Movement and Privilege Escalation

*Patrick Jungles, Security Program Manager, Microsoft*

Credential theft and re-use attacks have gained in popularity in recent years, and there's nothing tastier for some attackers than your delicious, delicious hashes. Jungles, the Microsoft PM who led the company-wide workgroup that researched and released our recent pass-the-hash whitepaper, presents an overview of the group's findings.

WATCH IT ON DEMAND

## Why Johnny Can't Patch: And What We Can Do About It

*David Seidman, Senior Security Program Manager, Microsoft*

Microsoft works hard to develop and release security bulletins as soon as we're aware of a vulnerability that needs addressing. So how is it some users remain vulnerable to issues for which the cure has existed for months, if not years? Seidman dives deep into who doesn't patch, why, and what might change their ways.

WATCH IT ON DEMAND

## Security at Microsoft

The Microsoft Security Response Center (MSRC) is part of Microsoft's Trustworthy Computing (TwC) group. The MSRC is on alert 24-hours a day, 365-days of the year, identifying, monitoring, resolving, and responding to security incidents and Microsoft software security vulnerabilities, and responds to over 100,000 customer emails annually. To report a vulnerability in a Microsoft security vulnerability please email secure@microsoft.com.

The Microsoft Ecosystem Strategy (EcoStrat) team, is part of the MSRC and works with security experts from all over the world in order to better understand how vulnerabilities affect our customers, our products and the Internet as a whole. The EcoStrat team is one of the groups responsible for securing Microsoft's current and future products. BlueHat v13 is scheduled for December 12-13, 2013, and is invitation only.

Emily Anderson

Security Program Manager, MSRC, Microsoft