



CRESTCon 2012

16th February, 9.00 - 17.30
Cavendish Conference Centre, London

Agenda

09.00 - 9.30: Registration

09.30 - 9.40: Welcome

TECHNICAL STREAM

09.45 – 10.30: Finding the Weak Link in Windows Binaries
Ollie Whitehouse, Director, Recx

The advent of generic memory corruption mitigations in Microsoft Windows and Visual Studio means it can be a chore when looking where to spend effort, yet ensuring successful exploitation of discovered bugs. Ollie Whitehouse will discuss how to identify binaries that provide the highest possible likely return on investment and will also show how to identify issues with Windows binaries. This will be of particular interest to independent software vendors or end user organisations who want to gain a base level of assurance that SDLC best practices have been followed - yet source and debug symbols are not available.

10.35 – 11.20: The Security of 3D Browser Extensions
James Forshaw, Senior Security Consultant,
Context IS

Whilst recent research at Context into the recently standardised WebGL technology (which brings high performance 3D graphics to the browser) got widely publicised, not all of the research or low-level details were made public. In this presentation, James Forshaw will present new content not previously released. The research identified significant risks to the stability and security of a computer by having this extension enabled by default in Mozilla Firefox and Google Chrome; including allowing a malicious attacker to crash a user's machine or steal information which they should not be able to access.

11.20 – 11.50: Coffee

12.50 – 12.35: What makes (time) travel possible for us all!
Mike Auty and Zak Maples, Security Consultants, MWR
InfoSecurity

In their presentation, Mike Auty and Zak Staples will focus on outlining the weaknesses in the MiFare classic card that are now well publicised and will break down the complex maths and crypto goodness so the impact of the vulnerabilities can be clearly understood. They will then look in detail at one implementation of the technology and how those same flaws can be investigated and abused.

12.35 – 13.25: Lunch

**13.25 – 14.10: Targeted Malware - What does it Look Like?
Laura Aylward and Mark Nicholls, Lead Security
Consultants, Context IS**

While the term 'Advanced Persistent Threat' describes a determined and ongoing attack on an individual or organisation, Context sees it more as 'Adequate Persistent Threats'. Laura Aylward and Mark Nicholls will introduce some of the malware and tools found by Context in recent targeted attack investigation and discuss some of their interesting features, including decryption of command and control traffic; extraction of infection details from running memory; using reverse engineering to determine command and control format strings; the potential re-use of 'financial' malware for alternative means; and overcoming anti-forensic techniques. They will also look at future threats and include demonstrations of the malware in action, how they can be reverse engineered and determining the motivations of the attackers.

**14.15 – 15.00: Leaving Without a Trace
Thomas Mackenzie and Ryan Jones, Security
Consultant, Trustware Spiderlabs**

Meticulous attackers can subvert audit controls to the point where a compromise is almost undetectable. Thomas Mackenzie and Ryan Jones look at the tools and techniques which can be used by attackers to minimise evidence left behind and propose a novel strategy for managing this issue. They will also explore various evidential sources commonly used to identify the extent and method of a web application compromise and draw together the techniques used to investigate a data compromise. A new approach will be suggested that gives us the best chance of keeping logging to an absolute minimum whilst ensuring that techniques used to minimise forensic evidence left by an attack are unsuccessful.

15.00 – 15.30: Coffee

**15.30 – 16.15: USB - Undermining Security Barriers
Andy Davis, Research Director, NGS Secure**

In his presentation, Andy Davis will discuss an approach to performing platform independent USB fuzzing and include a demo showing a USB zero day threat being triggered in Windows 7. The session will include detailed information about device fuzzing and the Frisbee Lite tool that will be released at INFILTRATE in Miami in January

**16.15 – 16.45: An update from Chris Marshall, CESH
Closing address from Ian Glover, CREST
Q & A session**

16.45 – 17.30: Networking

INFOSEC STREAM

09.45 – 10.30: Cybersecurity – A Critical Business Risk Alan Calder, CEO, IT Governance

Alan Calder will review and discuss the current UK cybersecurity risks which include Advanced Persistent Threats (APT), organised crime and the risks from staff and the workforce. He will outline the challenges faced by all UK business and propose a 7-Step Cybersecurity strategy which includes technical counter-measures, staff training, incidence response planning and compliance to the ISO27001 standard. Alan is the joint author of IT Governance: A Manager's Guide to Data Security and ISO27001/ISO27002 textbook and a leading authority on the compliance and best practice associated with ISO27001.

10.35 – 11.20: To Pen Test or not to Pen Test? Duncan Alderson, Senior Associate, PwC

We live in a real-time, social networked world that supports 24/7 international business for companies of any size. We have become used to an 'always on' culture where, 5 9s (99.999%) uptime is not good enough and if a system is down income can stop dead. So, why is it that companies hesitate when it comes to Penetration Testing their business critical infrastructure - be it CRM, web application or some bigger systems such as SAP? Business critical systems should be able to suffer a single server or device outage. The magical Security Triad of CIA where most governance, compliance and certifications are based even includes Confidentiality, Integrity and of course the sometimes forgotten availability.

11.20 – 11.50: Coffee

12.50 – 12.35: How to Survive in the Cloud Michael Jordon, Principal Consultant, Context IS

What is the reality of security within cloud infrastructure as a service? Michael Jordon will present the results of a security review of four major cloud providers to determine what the issues are of using the cloud over traditional dedicated hosting and to understand what cloud nodes look like and how this changes the attack surface. The important difference between traditional hosting and cloud computing is that an attacker can sign up or compromise someone else's node to have a virtual machine on the same physical hardware and network as their target; making it a lot easier to get closer. But what do providers do to separate these nodes and how can you test this? Do these attacks work in the real world?

12.35 – 13.25: Lunch

13.25 – 14.10: Are Agile and Secure Development Mutually Exclusive? Matt Bartoldus, Director, Gotham Digital Science

Can you develop using Agile and also be secure? Agile development methodologies are being increasingly adopted by organisations that believe they can bring more speed and flexibility to teams when delivering projects. But if not performed correctly Agile methods can come across as a mask for: 'do as fast as you can with a vague plan and little documentation'. Matt Bartoldus will look into the fundamental concepts of Agile security practices and Agile Project Management and ask whether these concepts can be applied to the information security world.

**14.15 – 15.00: Rapid Response to Incidents and [Rapid] Deployment of Countermeasures
Konrads Smelkovs, Advisor, KPMG**

In his presentation, Konrad Smelkovs will discuss an approach, tools and their customisation, as well as process challenges to rapidly respond to a wide breach of computer network security. A case study of an incident and will be used to look at lessons learned – what was done well and what could have been done better.

15.00 – 15.30: Coffee

**15.30 – 16.15: No Guts, No Glory - Securing Your Network Military Style
Matt Summers, Lead Technical Specialist, VISA**

Security is adversarial by nature. Throughout history there have been military leaders that were all highly trained; however, some failed where others succeeded. From Custer to Montgomery, one strategic decision can stand between legendary greatness and epic defeat. Everything from technology to training, if you don't have a strategy then you could be setting yourself up for your last stand. Matt Summers will look at military tactics how they can be applied to information security and help build a stronger organisation. You are either the attacker or defender. Do you want to become Custer or Montgomery?

**16.15 – 16.45: An update from Chris Marshall, CESH
Closing address from Ian Glover, CREST
Q & A session**

16.45 – 17.30: Networking