Joel Eriksson

Objective

To keep challenging myself, and continue evolving as a
vulnerability researcher and reverse-engineer.

Education

1998 - 2001	Computer Engineering - University of Gävle, Sweden
1995 - 1998	Natural Sciences Programme - Polhemsskolan, Gävle, Sweden

Awards & Honors

2015	Winner of SweCTF
2014	2nd place in Codegate Quals
2013	Winner of Black Knight challenge (nSense)
2013	3rd place in SECUINSIDE Finals in South Korea
2011	Winner of PlaidCTF
2008	Speaker at the RSA Conference in San Francisco
2007	Speaker at BlackHat Europe in Amsterdam
2007	Speaker at BlackHat USA in Las Vegas
2007	Speaker at DefCon in Las Vegas

Resources

Homepage	ClevCode.org
LinkedIn	Joel Eriksson
Twitter	@OwariDa

Profile

Although I have 19 years under my belt working in the IT-security field, with a personal interest that goes beyond even that, my current experience is not my primary strength. My strength lies in the fact that I delve deeper, and that I have the desire and ability to rapidly acquire the knowledge and understanding that I need for the tasks I face.

I perform vulnerability research, reverse-engineering, malware analysis and exploit development. While the last of these may only be relevant in itself to a few of our clients, it is key to my understanding of IT security on a deeper level than most.

I am able to identify flaws, and potential solutions, in systems from the design level down to the raw bits and bytes. I also know cryptography on a level that allows me to discover common flaws in cryptosystems, and what kind of cryptographic primitives that should be used and which ones that should be avoided.

Vretgränd 17 · 753 22 Uppsala · Sweden
🖂 je@clevcode.org ☎ +46 760-152 942

Work Experience

Period	January 2011 — Present	
Employer	ClevCode AB	Uppsala, Sweden
Job Title	Founder and CEO	

Examples of projects I've been involved in during my time at ClevCode are:

- Vulnerability research
- Network security assessments
- Application security assessments
- Exploit development (Windows, Linux, OS X)
- Building and optimizing a GPU-based cracker system
- Reverse-engineering applications (Windows, Linux, OS X)
- Reverse-engineering parts of the Samsung S3 baseband (ARM)

Besides the projects I have been involved in on a professional basis, I also participate in IT security competitions around the world on a regular basis. I am currently competing with the team HackingForSoju, that was ranked between #4-#7 in the world during our most active period in 2013, according to the official ranking at http://www.ctftime.org/. I have also participated in non-team based competitions, such as the Black Knight challenge and SweCTF, and was the sole winner of each. I am also building a new team called ClevCode Rising, with people that I am acting as a mentor for.

Solving the problems in these kind of competitions involves analyzing binaries and source code to identify vulnerabilities, developing exploits and defeating exploit mitigation mechanisms, reverse-engineering various types of code (x86, x86_64, ARM, MIPS, custom architectures) for Windows, Linux, *BSD, Android, iOS (iPhone/iPad), NDS and Cisco IOS to mention a few, identify and exploit flaws in cryptosystems, find and exploit web application vulnerabilities and to solve forensics based challenges.

Software development is a natural part of the vulnerability research process, and a number of custom tools are developed using programming languages such as C, C++, Python, Perl and Assembler. To truly understand IT security on a deeper level, one has to have a deep understanding of both code and the inner workings of the operating systems that are used.

Period	June 2006 — January 2011	
Employer	Bitsec AB	Stockholm, Sweden
Job Title	Co-founder, CTO and R&D Officer	

Examples of projects I was involved in during my time at Bitsec are:

- Incident response
- Vulnerability research
- Network security assessments
- Application security assessments
- Reverse-engineering Windows malware
- Reverse-engineering applications (Linux, Windows, OS X)
- Exploit development (Windows, Linux, OS X, *BSD, iOS)
- Teaching (vulnerability research, reverse-engineering)

I was also responsible for leading our R&D team, that worked on projects involving vulnerability research and reverse-engineering. Vulnerability research includes finding new vulnerabilities, developing exploits and bypassing exploit mitigation mechanisms. To find new vulnerabilities we used methods such as code auditing, reverse-engineering, fuzzing, instrumentation and other forms of static and dynamic analysis methods.

Reverse-engineering projects involved both searching for vulnerabilities, and determining any proprietary protocols and algorithms that are being used in order to assess their security.

Other responsibilities included finding other suitable members of the R&D team and to assess the technical skill level of applicants. For this purpose, I devised a public challenge that to this day has only been solved by a few. It involved reverse-engineering a binary and exploit a specially designed vulnerability, that required the challenger to go beyond the known and ordinary methods. It set the focus on understanding and thinking further, rather than just being able to apply a known and documented method.

We presented the results of some of the research we did at conferences such as BlackHat, DefCon and the RSA conference. This involved kernel vulnerabilities, malware analysis and exploitation. Some of the research I did regarding exploiting vulnerabilities on the iPhone led to articles and TV news reports here in Sweden.

Period	January 2003 — June 2006	
Employer	Bitnux AB	Gävle, Sweden
Job Title	Co-founder and CEO	

Examples of projects I was involved in during my time at Bitnux are:

- Web application development
- Network security assessments
- Application security assessments
- Exploit development (Linux, Windows)
- Application development (Linux, Windows)
- Reverse-engineering applications (Linux, Windows)
- System and security administration (Linux, Windows)
- Teaching (vulnerability research, reverse-engineering)

Bitnux started out being mainly focused on systems development. We developed web based database applications managing invoices, real estate and expenses, to mention a few. We developed a variety of custom solutions to optimize the workflow within large economy departments, where there is a lot of work automating handling, converting and distributing various forms of data from one system to another. I developed back end systems using mainly C, C++, Bash and Perl.

As my main focus has always been vulnerability research, I was soon able to get clients within this area as well. Instead of using traditional PR methods I decided to activate myself on the large and well known IT security related mailing lists, where I published detailed security advisories about vulnerabilities I found, and other findings. A couple of examples:

0xbadc0ded Advisory #02 - Dropbear SSH Server <= 0.34
DailyDave: Gemini (AKA academic security)

On the site I built for the purpose of publishing my advisories, I also published challenges for other vulnerability researchers and exploit developers. I knew how important it was to build a network, not just with potential clients, but with other skilled IT security researchers. I was particularly focused on finding other skilled researchers in Sweden.

There were, and still are, very few security researchers with a deep technical understanding of complex security vulnerabilities and potential exploit mitigations. So, when I found anyone with potential I made sure I stayed in touch, and invited them to my private IRC server. I used the IRC server to keep in touch with both the few other Swedes I found with potential, and international contacts from various countries. I built a team on this foundation, and published some of their contributions as well, in the form of challenges and vulnerability advisories.

Period	June 2001 — December 2002	
Employer	Utilator AB	Gävle, Sweden
Job Title	Software Developer, System and Security Administrator	

Examples of projects I was involved in during my time at Utilator are:

PSI Unix client for eHem Home. Implemented services such as programmable scenarios, lock guard and alarms. Controlling units and sensors through X10. Web interface for realtime surveillance of units and sensors status. Introduced SSL protected synchronization to the eHem portal. Developed in POSIX-compatible C, and used under Linux, OpenBSD, Windows (cygwin) and uClinux. For uClinux, the MMU-less Coldfire CPU was used.

Secure Channel System PKI based security solution to TCP/IP enable Solid's RS232-based central units, with strong encryption and two-way authentication. Enables connections between geographically separated locking systems, remote administration and interfacing with Web Booking System.

Web Booking System Plugin to the Secure Channel System to web enable Solid's Soliwash-centrals for booking laundry rooms and other shared spaces. Enabled booking requests and event logs over TCP/IP. Can also be used stand alone.

SecMsg Bridge Part of Alleato Access. Bridge between VCU (Virtual Central Unit) and DAC-GW (Door Access Control Gateway) that controls locks, alarms and relays connected to the door and reader. Communicates over TCP/IP with the VCU and via SecMsg with the DAC-GW, part of an OSGi framework.

Tank Automated installation and configuration of Linux boxes, using a serial console and root filesystem over NFS. Associats MAC address to pregenerated SSH keys, SSL certificates and a unique Box ID, that are transferred over RS232 for security reasons.

BoxCfg Centralized configuration of Unix systems in a hierarchical database. Affected services and subsystems are automatically notified when relevant variables have been changed. Templates with a custom made embedded scripting language are used for configuration files and rc-scripts, for maximum flexibility. Used through its C API and CLI applications, for network, system and application configuration on Service Gateways.

BoxCmd General TCP/IP based interface with SSL authentication for access to BoxCfg and other services on the system. Two-way authentication is used, just as in other PKI based solutions I have developed, so that neither the client nor the server can be impersonated. Ability to nest calls through several boxes, which makes a hierarchical network of trust possible.

Home Gateway Custom Linux distribution and applications for Geode based gateway, with features such as data acquisition, door phone with streaming video (Bewator + Axis), a locked down browser (Opera) and connections to Web Booking System and eHem Home. System and application configuration gathered in SQL database on central server, with a Message Broker forwarding messages.

Period	May 1999 — March 2001	
Employer	TeleBudget AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	IT-security, C++, Perl, Bash, CGI, Unix (Solaris)	
	System and security administration, maintenance of webchat.	

Period	February 1999 — January 2001	
Employer	FMG AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	IT-security, Perl, Bash, C, Unix (Solaris, OpenBSD)	
	System and security administration.	

Period	May 1999 — November 2000	
Employer	Bizitel AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	Dialogic, C, VOS, Windows NT, Unix (SCO), MS/DOS	
	Development and maintenance of a teleconferencing application.	

Period	June 1999 — April 2000	
Employer	TeleBudget AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	Dialogic, C, VOS, Windows NT, MS/DOS	
	Development and maintenance of a teleconferencing application.	

Period	February 2000	
Employer	Säkerhet & Sekretess (Security & Secrecy)	
Job Title	Freelance Writer	
Keywords	IT-security, writer	
	Wrote an article about IDS and security scanners (issue 2/2000).	

Period	March 1999 — August 1999	
Employer	Dagens Kommunikation (Today's Communication)	
Job Title	Freelance Writer	
Keywords	IT-security, writer, editor	
	Issued and sent out warnings about recent security flaws to subscribers of DK.	

Period	November 1998 — August 1999	
Employer	EttNet AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	IT-security, Portmaster, Perl, Bash, Unix (Solaris, FreeBSD)	
	System and security administration.	

Period	June 1998 — May 1999	
Employer	TeleNext AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	Dialogic, VOS, C++, IT-security, Unix (Solaris), MS/DOS	
	System and security administration, maintenance of webchat.	

Period	June 1998 — May 1999	
Employer	TeleNext AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	Dialogic, VOS, C++, IT-security, Unix (Solaris), MS/DOS	
	System and security administration, maintenance of webchat.	

Period	August 1998 — May 1999	
Employer	Fordonskammaren AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	Delphi, SQL, Paradox, MS/DOS, Windows	
	Development of database management software in Borland Delphi.	

Period	April 1999	
Employer	Confidential	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	IT-security, Unix (Linux)	
	Secured main Linux server. Participated in meeting as support regarding security related issues.	

Period	March 1999	
Employer	Säkerhet & Sekretess (Security & Secrecy)	
Job Title	Freelance Writer	
Keywords	IT-security, writer	
	Wrote an article about the Melissa virus (issue 3/1999).	

Period	January 1998 — May 1998	
Employer	TeleNext AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	C++, CGI, Unix (Linux, Solaris)	
	Development of webchat in C++.	

Period	July 1997 — August 1997	
Employer	Oy Snellman Ab	Jakobstad (Pietarsaari), Finland
Job Title	Freelance Consultant	
Keywords	IT-security, Unix (AIX, SCO), Windows NT	
	IT-security consulting. Hardening of server security. Auditing for vulnerabilities. Development of backup system.	

Period	July 1997	
Employer	FMG AB	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	IT-security, Unix (Solaris)	
	IT-security consulting. Hardening of server security.	

Period	May 1996	
Employer	IDG	Stockholm, Sweden
Job Title	Freelance Consultant	
Keywords	IT-security, Unix (Solaris), Windows NT	
	IT-security consulting. Black box network security check.	

Languages

Swedish	Mother tongue
English	Fluent
Japanese	Beginner

Skills

Operating Systems	Linux, Windows, OS X, iOS, Android, Solaris, FreeBSD, OpenBSD, NetBSD, AIX, SCO, HP-UX, IRIX, Ultrix, DG/UX, HP-UX, QNX, ...
Programming Languages	C, C++, Python, Perl, Assembly (x86/x64/ARM), Bash, Sed, Awk, Pascal, Object Pascal (Delphi/Kylix), Java, PHP, Tcl, Expect, Lua, Prolog, SQL, ...
Reversing / Debugging	IDA Pro, Hex-Rays, OllyDbg, GDB, WinDBG, SoftICE, DynamoRIO, PIN, BinNavi, BinDiff, Immunity Debugger, PaiMei, 010 Editor, LordPE, ImpREC,...
Security Tools	OpenSSL, IPTables, IPF, Snort, Tripwire, GRSecurity, PAX, S/Key, RSA SecurID, TrueCrypt, Nmap, Metasploit, CANVAS, SPIKE, Peach, ...
Development Tools	VIM, GCC, Visual Studio, Xcode, Eclipse, Wing IDE, Delphi, NASM, Yasm, GAS, Lex/Flex, Yacc/Bison, ...
Virtualization	VMWare, VirtualBox, Parallels, QEMU, Bochs, LXC, Xen, ...

Publicity

English

http://www.telegraph.co.uk/technology/internet/10468112/The-internet-mystery-that-has-the-world-baffled.html
http://www.washingtontimes.com/news/2013/nov/26/secret-society-seeks-worlds-smartest-cicada-3301-r/
http://www.blackhat.com/html/bh-europe-07/bh-eu-07-speakers.html#Eriksson
http://www.defcon.org/html/defcon-15/dc-15-speakers.html#Eriksson
http://www.wired.com/threatlevel/2008/04/researcher-demo/
http://www.darknet.org.uk/2008/04/hackers-could-become-the-hacked/
http://www.theguardian.com/technology/blog/2008/apr/12/letshackthehackerssaysjoe
http://www.cyberpunkreview.com/news-as-cyberpunk/hackers-get-hacked-or-turnabout-is-fair-play/

Swedish

http://www.aftonbladet.se/nyheter/article17921597.ab
http://www.tv4play.se/program/nyhetsmorgon?video_id=2494551
http://www.idg.se/2.1085/1.377394
http://www.idg.se/2.1085/1.384830/
http://www.svt.se/nyheter/sverige/smarta-telefoner-latta-att-hacka (also on TV)
http://www.mobil.se/guider/din-smarta-mobil-snart-hackad-1.382389.html
http://www.idg.se/2.1085/1.104180
http://www.idg.se/2.1085/1.101336