Rob King

Contact Information

E. jking@deadpixi.com

P. 512-917-4476

Highlights

- Nearly twenty years' experience in information security and software development.
- Awarded Innovator of the Year by 3Com for security work.
- Took a leading role in designing the product that won SC Magazine's Data Extrusion Product of the year.
- Author of the innovative Giles production rule system compiler.
- Invited to speak over a dozen times at industry and academic conferences like BlackHat and ShmooCon, as well as by organizations like the United States Department of Defense, the United States Army, USENIX and the IEEE.
- Published numerous peer-reviewed articles and papers.
- Extensive experience with a variety of programming languages, with recent focus on C, Python, and JavaScript/ECMAScript.
- Extensive experience with all levels of network theory and usage, with a strong focus on traffic analysis and identification and on network architecture and design.
- Author of several open source tools.
- Performed multi-year, in-depth, novel research for organizations like the Defense Advanced Research Projects Agency (DARPA) and TippingPoint DVLabs.
- Discovered several privately- and publicly-disclosed security vulnerabilities in a variety of popular applications.
- Acted as co-editor and contributor to one of the largest security industry newsletters, read by over 250,000 subscribers weekly.
- Extensive experience with Unix and Linux, both as a user and a developer.

Experience

Senior Researcher (Aug 2011 - Present)

KoreLogic, Inc., Austin, TX, USA

- As part of a multi-year contract with the Defense Advanced Research Projects Agency (DARPA), developed the Detecting Insider Repository Tampering (DIRT) system. DIRT was groundbreaking research and practical development into monitoring the security of the software development lifecycle.
    - Performed extensive research into the software development lifecycle, identifying points of interest for security analysis.

    - Participated in regular Independent Verification and Validation (IV&V) exercises with DARPA, MIT Lincoln Labs, and the Air Force Research Laboratory. These independent reviews always ranked the results very highly.
    - Wrote thousands of lines of code in C, Perl, Python, and Bourne Shell for various tasks throughout the DIRT system.
    - Created a complete, order-insensitive, time-efficient, transactional, data-safe event correlation engine to detect patterns of behavior in large data sets.
    - Helped create a corpus of attacks against source code management systems, including Git, CVS, and Subversion.
    - Helped architect and build a complete appliance from the ground up designed to operate in highly secure environments.
    - Wrote hundreds of signatures for this engine to detect suspicious behaviors in forensic data.
    - Helped design a comprehensive and automated test suite for the DIRT system.

- Created the open source Giles production rule system compiler, which can be used to create highly efficient event correlation engines and expert systems.
    - Giles turns normal SQL databases into self-contained production rule systems by creating complex schemas that implement a variant of the Rete algorithm. Users interact with these systems as they would normal databases, meaning users can deploy complex event correlation engines wherever they could deploy a normal database.
    - Performed novel and extensive research into search algorithms and query optimization algorithms as part of the optimizer for the Giles compiler. This included creating a variant of the Rete algorithm amenable to runtime optimization by modern database query analyzers.
    - Wrote and optimized countless complex SQL queries (primarily for SQLite) to illustrate and develop optimization strategies for the Giles compiler.

- Was a founding member of the KoreLogic Rapid Application Development (KRAD) group.
    - Wrote the custom, highly-secure web application server system for KRAD in Python. This system was designed to work in multilevel secure environments.
    - Implemented a complete Design-by-Contract system for Python using Python class and function decorators.
    - Created a powerful and novel database abstraction layer that adapts any Python DB-API module into a consistent API. This abstraction layer allowed the use of arbitrarily complex SQL on the back end (while still maintaining abstraction), meaning that it can easily adapt to existing databases.

- Helped build MASTIFF Online, a web-based interface for the MASTIFF malware analysis framework.

- Administered the KRAD core database management systems (PostgreSQL and various SQLite databases).

- Helped administer numerous Gentoo Linux systems, both physical and virtual.
- Helped create a system of created-on-demand Linux Containers to isolate mutually untrusted processes.
- Worked with reverse-engineering and forensic analysis of various applications, including mobile applications on Android.
- Supported numerous KoreLogic research and consulting projects, with services ranging from ad hoc code development to forensic data analysis.

Infrastructure and Security Architect (Nov 2010 - Aug 2011)

ATX Innovations/Tabbed Out, Austin, TX, USA

- Acted as a technical, architectural, and development lead in a fast-paced startup environment that developed the TabbedOut mobile payment application.
- Helped design and implement a highly-secure and scalable payment network transmitting payment between arbitrary endpoints, including customers and retailers.
    - Helped design the overall architecture of the system, including mechanisms for maintaining complete encryption of payment data, including guarantees of perfect forward secrecy and certificate-based identity management for endpoints.
    - Designed, built, tested, and secured a hybrid multi-threaded and event-based, non-blocking routing mechanism to handle high volumes of traffic between arbitrary endpoints. The primary language of implementation was C, and development targeted Linux systems.
- Wrote numerous integration adaptors to attach various Point-of-Sale (POS) systems to the TabbedOut infrastructure. Primary languages of implementation included C#, REBOL, and Python.
- Helped develop the TabbedOut mobile application for both iOS and Android. This included Objective-C, C, and Java development.
- Performed extensive, low-level protocol analysis and validation to ensure correctness of the various actors on the TabbedOut payment network.

DVLabs Architect, *Principal Researcher*, and *Researcher* (Feb 2005 - Nov 2010)

TippingPoint DVLabs (now HP), Austin, TX, USA

- Worked as a technical and research lead for one of the most respected information security labs in the industry.
- As Architect, participated in the TippingPoint Core Architecture Team, which was responsible for the current and future core design of the TippingPoint Intrusion Prevention System (IPS) and related products.
- Responsible for the formalization of the syntax and semantics of the TippingPoint internal signature language.

- Implemented and maintained the core TippingPoint signature compiler, which was the tool that turned high-level traffic signatures into a form consumable by the IPS.
    - Created extensive formal specifications for the syntax and semantics of the language.
    - Implemented a formal verification mechanism for compiler output.
    - Developed, maintained, and deployed a complete web-based, concurrent multi-user integrated development environment for signature development. This environment managed the complete signature development lifecycle, from authoring to compilation to deployment.
    - Analyzed and developed various optmization strategies for the compiler to increase signature performance.
    - Primary languages of implementation were JavaScript, Lua, and Python.

- Co-founded the CustomDV and WebAppDV groups, which provided customized TippingPoint signature sets to clients.
    - Awarded the 3Com Innovator of the Year for the founding of the CustomDV group.
    - The use of the CustomDV service as part of TippingPoint's Data Leakage Prevention offering helped win TippingPoint SC Magazine's Data Leakage/Extrusion Prevention Product of the Year for 2010.

- Developed the "SCREAM" technique for rewriting regular expressions to detect their original matching inputs when those inputs have been encoded in various position-dependent block encodings.

- Wrote hundreds of traffic analysis signatures for the TippingPoint IPS.
    - Performed in-depth traffic analysis using a variety of network analysis tools.
    - Reverse-engineered numerous vulnerable programs to determine how to exploit these vulnerabilities and write signatures to detect these attacks.

- Wrote thousands of lines of code for various TippingPoint tools and various ad hoc projects.

- Discovered several publicly- and privately-disclosed vulnerabilities in high-profile software targets.
    - Performed static and live analysis on various applications.
    - Performed research into bypassing reverse engineering countermeasures.

- Wrote a complete framework for the statistical analysis of encrypted network traffic and techniques for detecting the type of encrypted protcol.
    - Built a large and diverse training corpus of encrypted and plaintext network traffic for training and analysis purposes.
    - Wrote a complete framework for statistical analysis in Python.

Senior Network and Security Engineer (Apr 2002 - Feb 2005)

Whole Foods Market, Austin, TX, USA

- Helped design, build, maintain, and secure the core network for Whole Foods Market, connecting all of the various Whole Foods locations.

    - Wrote thousands of lines code code to automate network and server management (primarily in Python, C, Lua, and Bourne shell).
    - Administered hundreds of Cisco routers and firewalls, and Linux and Solaris servers.
    - Built one of the largest (at the time) Cisco-based IP/VPN networks in the world (earning a Cisco Certified Network Professional (CCNP) certification in the process).
    - Administered core DNS and NTP services for the company.
    - Integrated various acquisitions' networks, creating a nationwide multi-protocol network including IBM SNA, AppleTalk, IPX, and IP networks.
    - Maintained heavily isolated network links for credit card processing.
    - Performed incident response and post-mortem analysis of network and security incidents.

- Built the Whole Foods Market core network monitoring system from scratch.
    - Acted as coordinator to develop requirements for such a system from all stakeholders in the company.
    - Wrote thousands of lines of code to implement network and server monitoring. This includes reporting, historical monitoring data, and performance profiling statistics.

Senior Network and Security Engineer (Apr 2001 - Apr 2002)

InterTransact (European Fund Services), Munsbach, Grand Duchy of Luxembourg

- Designed, built, maintained, and secured a network facilitating bank-to-bank transfers across the European Union in a fast-paced startup environment.
    - Built a multi-layer, fault-tolerant, highly siloed network, with multiple redundant components from different vendors (primarily Cisco, CheckPoint, and F5) to isolate failure modes.
    - Administered dozens of Solaris and BSD/OS (BSDi) servers.

- Wrote extensive documentation and facilitated ongoing audits to comply with banking regulations.

- Wrote thousands of lines of code to automate network and server management, as well as helping develop the core InterTransact application. Primary languages were Python, Java, and Bourne shell.

- Provided consulting expertise for InterTransact clients.

Security Engineer (Jan 2000 - Apr 2001)

Exodus Telecommunications, Austin, TX and Boston, MA, USA

- Acted as a member of the firewall design and management team.
    - Administered dozens of Exodus-provided firewalls for clients (primarily CheckPoint and Cisco).
    - Performed low-level traffic analysis to verify firewall configuration.
    - Developed custom firewall rule sets for Exodus clients, including extremely large, multi-homed deployments for clients like American Airlines and Ford.

    - Performed firewall rule audits and provided consultation and advice for improvements.
    - Acted as a rapid-response team member, providing analysis and remediation after security incidents involving Exodus clients.

- Wrote large amounts of ad hoc software to automate firewall management.

- Administered several Solaris servers.

Senior Technical Administrator (May 1999 - Jan 2000), *Junior Technical Administrator* (May 1998 - May 1999)

PERnet Telecommunucations, Nederland, TX, USA

- Acted as primary technical engineer for what was at the time the largest Internet Service Provider (ISP) in southeast Texas.
    - Administered dozens of FreeBSD servers providing ISP services, including mail (SMTP/IMAP/POP3), DNS, web hosting, and authentication (RADIUS).
    - Administered various network components, including large-scale Cisco routers and Ascend line concentrators.
    - Wrote large amounts of ad hoc software to automate server and network management.

- Wrote custom FreeBSD kernel components to support auditing and enhanced security modes.

- Wrote a custom RADIUS authentication server to support remote authentication services.

- Wrote a custom, database-backed multiprotocol webmail system to provide email services for PERnet clients. The server components (for IMAP, POP3, and an MDA for Sendmail) were written in C++, while the web interface was written in Perl. The storage backend was abstracted to work with either MySQL and PostgreSQL.

Talks, Appearances, and Publications

Crack Me If You Can (Team presentation with KoreLogic)

- DefCon 20, Las Vegas, NV, USA, Jul 26 2012

Presented as a contest to illustrate the state of the art in large-scale, offline password cracking.

Building a Better Mousetrap: Effective Techniques in Intrusion Prevention (with Rohit Dhamankar)

- Black Hat USA 2011, Las Vegas, NV, USA, Jul 30 2011
- Black Hat USA 2010, Las Vegas, NV, USA, Jul 31 2010
- SANS Network Security 2009, San Diego, CA, USA, Sep 18 2010
- Black Hat USA 2009, Las Vegas, NV, USA, Jul 25 2009
- Black Hat USA 2008, Las Vegas, NV, USA, Aug 1 2008

Presented effective tools for developing intrusion prevention and detection signatures for a variety of network IPS/IDS tools. Topics covered included in-depth network traffic analysis, complex regular expression development, and optimization techniques for different IPS/IDS systems.

The Pixaxe Declarative Web Framework

- USENIX WebApps 10, Boston, MA, USA, Jun 23 2010
- Associated preceedings

Introduces and describes the Pixaxe web application framework. This framework combines a complete Parsing Expression Grammar (PEG) combinator library in pure ECMAScript with a declarative data query and extraction language (called Esel) for hierarchical data sets and an in-browser templating framework based on such expressions. The framework allows modelling web applications in a traditional model-view-controller fashion. Views were Esel expressions, the syntax of which was a perfect superset of XHTML; evaluating such expressions had the side effect of rendering the page. The framework provided automatic model synchronization and performed all templating and rendering inside the browser, resulting in extremely efficient bandwith usage for applications.

Implementing SCREAM

- Erlang Factory, San Francisco, CA, USA, Mar 25 2010

Describes the implementation strategies used to implement the SCREAM technique at TippingPoint, which provided a real-world example of an unusual use of Erlang.

Static Analysis of Regular Expressions for Encoding

- IEEE Joint Communications and Signal Processing, Austin, TX, USA, Feb 18 2010
- By special invitation of the United States Army, presented to the United States Department of Defense (other agencies attending), The Pentagon, Arlington County, VA, USA Jan 28 2009

Discussed mechanisms for statically analyzing regular expressions to transform them into other expressions matching the original expressions' input when this input had been encoded in various ways. These techniques allowed the development of low-level traffic analysis and data-mining signatures that could work on encoded data without first decoding it, for use in environments where decoding was impossible or expensive.

Encrypted Protocol Identification by Statistical Analysis (with Rohit Dhamankar)

- Black Hat USA 2007, Las Vegas, NV, USA, Aug 1 2007
- ShmooCon 2007, Washington, DC, USA, Mar 23 2007

Described techniques for detecting the type of plaintext protocol in use in an encrypted stream, via statistical analysis of still-visible attributes like packet size and inter-packet delay. In all, packets were stored in a ten-dimensional space, with machine learning/clustering algorithms used to find likely protocol candidates. Practical applications of this research were discussed, including detecting anomalous usage of well-known ports and detecting botnet control channels.

@RISK: The Conensus Security Alert

- Co-editor and contributor from 2005 - 2009

Acted as a co-editor and contributor for this weekly newsletter covering new vulnerabilities discovered over the last week. Read by over 250,000 subscribers weekly, *@RISK* is one of the most popular information security newsletters in the world.

SANS Top-20

- Co-editor and contributor from 2005 - 2009

This special report produced by the SANS Institute every year discussed the twenty most severe security vulnerabilities discovered that year, as determined by a panel of information security experts.

Selected Public Advisories

- CVE-2011-0234 *Multi-Platform WebKit Memory Corruption Vulnerability*
- CVE-2009-1717 *Apple Terminal xterm Resize Escape Sequence Memory Corruption Vulnerability* (remotely exploitable via the default handling of *telnet://* URLs)
- CVE-2009-0950 *Apple iTunes Multiple Protocol Handler Buffer Overflow Vulnerabilities*

Selected Open Source Software

The Giles Production Rule System Compiler
: A compiler that turns normal relational databases into complex production rule systems, usable for artificial intelligence and event correlation applications.

Deadpixi Sam
: An updated version of the *sam* text editor, originally deployed as part of Ninth Edition Research Unix from Bell Labs. This version adds scalable font support, clean bi-endian 64-bit support, configurable Unicode codepoint composition, and other improvements.

Pixaxe, Jenner, Esel, and Kouprey
: Pixaxe is a declarative web application framework with innovative features. The templating (Jenner), data querying and extraction (Esel), and parsing (Kouprey) components are usable separately.

DPGC
: A simple tri-color garbage collection library.

KL-EL
: A library implementing a compiler and interpreter for a small, statically-typed expression language that is easily embeddable in larger applications.