Dan Kaminsky
dan@doxpara.com
@dakami

SUMMARY

Dan Kaminsky has been a noted security researcher for over a decade, and has spent his career advising Fortune 500 companies such as Cisco, Avaya, and Microsoft. Dan spent three years working with Microsoft on their Vista, Server 2008, and Windows 7 releases.

Dan is best known for his work finding a critical flaw in the Internet's Domain Name System (DNS), and for leading what became the largest synchronized fix to the Internet's infrastructure of all time. Of the seven Recovery Key Shareholders who possess the ability to restore the DNS root keys, Dan is the American representative. Dan is presently developing systems to reduce the cost and complexity of securing critical infrastructure.

SELECTED PRESENTATIONS

- **"Introducing the Domain Key Infrastructure"** Black Hat USA 2010 – Las Vegas, NV
  Zero Configuration DNSSEC Serving, End-To-End Client Integration w/ UI Via OpenSSL and Secure Proxies, Federated OpenSSH, DNS over HTTP/X.509, Self-Securing URLs, Secure Scalable Email (Finally!)
- **Interpolique** The Next HOPE 2010 – New York, NY
  Where's The Safety in Type Safety?, Preventing Injection Attacks (XSS/SQL) With String Safety, Why Ease Of Use Matters, Automatic Query Parameterization, How LISP Was Right About Dynamic Scope, Dynamic DOM Manipulation For Secure Integration of Untrusted HTML
- **Realism in Web Defense** CONFidence 2010 – Krakow, Poland
  Why Security Fails, What's Wrong With Session Management On The Web, The Failure Of Referrer Checking, Interpreter Suicide, Towards a Real Session Context, Treelocking, The Beginnings of Interpolique
- **Staring Into the Abyss** CanSecWest 2009 – Vancouver, BC
  Middleware Fingerprinting, Firewall Rule Bypass, Internal Address Disclosure, Same Origin Attacks Against Proxied Hosts, TCP NAT2NAT via Active FTP And TCP Spoofing
- **Black Ops of PKI** Chaos Communications Congress 2009 (26c3) – Berlin, Germany
  Structural Weaknesses of X.509, Architectural Advantages of DNSSEC, ASN.1 Confusion, Null Terminator Attacks Against Certificates
- **It's the End of the Cache As We Know It** Black Hat USA 2008 – Las Vegas, NV
  DNS Server+Client Cache Poisoning, Issues with SSL, Breaking "Forgot My Password" Systems, Attacking Autoupdaters and Unhardened Parsers, Rerouting Internal Traffic
- **Ad Injection Gone Wild** ToorCon 2008 – Seattle, WA
  Subdomain NXDOMAIN injection for Universal Cross Site Scripting
- **Design Reviewing the Web** Black Hat USA 2007 – Las Vegas, NV
  DNS Rebinding, VPN to the Browser, Provider Hostility Detection, Audio CAPTCHA Analysis
- **Weaponizing Noam Chomsky, or Hacking with Pattern Languages** ShmooCon 2007 – Washington, DC
  The Nymic Domain, XML Trees For Automatically Extracted Grammar, Syntax Highlighting for Compression Depth, Live Discovered Grammar Rendering, "CFG9000" Context Free Grammar Fuzzer, Dotplots for Format Identification and Fuzzer Guidance, Tilt Shift Dotplots, Visual Bindiff

- **Pattern Recognition** Black Hat USA 2006 – Las Vegas, NV
  Net Neutrality Violation Detection, Large Scale SSL Scanning, Securing Online Banking, Cryptomnemonics, Context Free Grammar Fuzzing, Security Dotplots
- **Black Ops of TCP/IP 2005.5** Black Hat Japan 2005 – Tokyo, JP
  Worldwide DNS Scans, Temporal IDS Evasion, the Sony Rootkit, MD5 Conflation of Web Pages
- **MD5 To Be Considered Harmful Someday** Chaos Communications Congress 2004 – Berlin, Germany
  Applied Attacks Against Simple Collisions Via Malicious Appendage, Executable Confusion, Auditor Bypass, Bit Commitment Shirking, HMAC Implications, Collision Steganography, P2P Attacks Against Kazaa Hash
- **Black Ops of DNS** Black Hat USA 2004 – Las Vegas, NV
  Tunneling Audio, Video, and SSH over DNS
- **Stack Black Ops** Black Hat Federal 2003 – Washington, DC
  Generic ActiveX, SQL for Large Network Scans, Bandwidth Brokering, SSL for IDS's
- **Black Ops of TCP/IP** Black Hat USA 2002 – Las Vegas, NV
  High Speed Scanning, Parasitic Traceroute, TCP NAT2NAT
- **Gateway Cryptography** Defcon 9 2001 – Las Vegas, NV
  SSH Dynamic Forwarding, Securing Meet-In-The-Middle, PPTP over SSH