

# Hacker Court 2007: The Case of a Thousand Truths

## **Background:**

Expertise in computer forensic technology means nothing if the jury doesn't understand the testimony. Presenting technical evidence in a courtroom is a far cry from presenting a technical paper at Black Hat. Sure, a computer professional may understand the importance of full headers in tracing email origins, but a jury has no clue. The real challenge in the field of computer forensics is translating complicated technical evidence in terms your typical juror would understand.

This particular case involves a person who is unlucky enough to have his name on the TSA's terrorism watch list and gets his laptop seized and searched at the border when coming home from abroad. As it turns out, he's not a terrorist and there are no contraband images on his computer, but the forensics expert does discover MMORPG cheat tools--tools which the suspect has used to build a large and growing kingdom in a popular MMORPG as the notorious "Crimson Knight". He is charged with a CFAA violation (Computer Fraud and Abuse Act).

This presentation will enact a courtroom environment, complete with judge, attorneys, and witnesses to demonstrate key issues in computer crime cases. While we strive to make case arguments and legal issues as accurate as possible, some liberties are taken to streamline the presentation and keep it entertaining. The presentation will be in two parts: the mock trial, followed by a panel discussion.

In the spirit of producing a realistic case, we have included a fictitious Indictment which the general public would typically have available before a case. None of the events portrayed actually occurred and all similarity to persons living or dead is purely coincidental.

For more information about this presentation, please contact Carole Fennelly (fennelly at wkeys dot com).

## **Cast:**

<b>Judge:</b>	<b>Richard Salgado</b>
<b>Clerk:</b>	<b>Caitlin Klein</b>
<b>Defense:</b>	<b>Kevin Bankston</b>
<b>Prosecution:</b>	<b>Jennifer Granick</b>
<b>Defendant:</b>	<b>Ryan Bulat (playing "David Nelson" aka</b>
<b>"Crimson Knight")</b>	
<b>Agent Smith (TSA):</b>	<b>Brian Martin</b>
<b>Forensic Expert:</b>	<b>Jesse Kornblum</b>
<b>CEO:</b>	<b>Richard Thieme</b>
<b>IT Director:</b>	<b>Jon Klein</b>
<b>Defense Expert:</b>	<b>Simple Nomad</b>
<b>Producer:</b>	<b>Carole Fennelly</b>

**Non-Appearing contributors:**

**Legal input:**  
**Jury Instructions:**

**Paul Ohm**  
**Merlin Arduini**

### **Case Summary:**

**David Nelson**, a young software engineer from Las Vegas, was coming home from a beach vacation when he went through U.S. customs. Not only was his (very common) name on the TSA's "selectee list" of potential security threats [this is an actual example of a common name that is on the list; David Nelsons get hassled all the time], but he also fit the profile as having a possible link to contraband material.

David was directed into a side room by **Agent Smith** of the TSA for a pat-down and a search of his bags. He was quite irate at this treatment--"This is ridiculous! I'm just trying to come home--hey! Don't open that bag!" TSA personnel opened the bag anyway, but didn't find anything immediately interesting. They did, however, find a laptop computer, a video camera, a digital camera, and lots and lots of SD cards and mini-DV tapes. The TSA then booted the computer--again despite

Nelson's objections--and did a quick search for types of media that might contain child porn or terrorist plans. They didn't find any, though they did find a bit of regular porn. They checked the memory of the cameras, but only found scenic vistas of jungles and beaches. The TSA personnel were still suspicious and annoyed by David's continuing (and increasingly insulting) demands that they stop searching his stuff and let him go. They did let him go--but they kept the computer and the media for a more in-depth search, promising to return it all to him as soon as they'd conclusively determined that there was no contraband data [alternatively, we could have them mirror all his data but give the computer back--we've heard reports of that].

The next day, David Nelson secured the representation of famed defense attorney **Kevin Bankston**, who raised a firestorm in the press and prompted readers to flood the TSA with complaints. Of course, this only put more pressure on the TSA personnel to find something incriminating on the computer and justify their suspicions about Nelson. And they did--sort of.

The government filed an affidavit that it had discovered evidence of computer fraud on the computer that required further investigation. That was quickly followed by the indictment of David Nelson--also known as "The Crimson Knight" in Getta Entertainment's Masters of Mayhem MMORPG--for violations of the Computer Fraud and Abuse Act.

Despite searching all of Nelson's equipment, the government had not found one iota of child porn or information regarding any terrorist threats. What they did find was that Nelson was a huge Masters of Mayhem fan, and they discovered a broad range of software that David had coded to cheat in the game. Nelson was authorized to access MoM's servers--he paid for his subscription--but once in game, he cheated mercilessly. Using the tools that he created, along with some others he found on some private hacker boards he frequented (where he also distributed copies of his own tools), he was accumulating unearned experience points and unearned gold, and receiving unfair advantages in battles by creating new and powerful spells, weapons, and non-player characters to support him. As a result, he'd built a large kingdom for

himself in the game and had become quite notorious as an aggressively growing power in the virtual World. Although a few had suspected he was cheating, most simply regarded him as an incredibly experienced and powerful player. Naturally, the indictment was big news in the gaming community and in the blogosphere: "The Crimson Knight Unmasked as a Fraud!" and the legal/tech/civlib community: "Cheat in a Video Game and Go to Jail?" and "The War on Terror Stumbles into the Virtual World: Real Terror List Accidentally Snags Virtual 'Terrorist'."

Notably, the Crimson Knight's cheating didn't cause any direct damage to MoM's servers or technically degrade their performance any more than his playing without cheating would have (although MoM did have to spend some money analyzing the systems and patching the vulnerabilities revealed after Nelson's arrest). **Nor did he** ever sell or intend to sell any of his ill-gotten gains in the real-world economy--for him; it was always about the game--although he could have made a mint if he had. Finally, his cheats didn't take gold or weapons or anything else directly from other players--rather, they only gave him a tactical advantage. However, this tactical advantage *did* enable him to use those items to kill other players and take their stuff...

**Kevin Bankston** signed on to represent David in his criminal trial, up against **Jennifer Granick**.

Bankston railed to the press: "This is an outrage! They unconstitutionally seize David Nelson's computer based on a bogus watch list and baseless profiling, and *this* is what they come up with to cover their rears? What's next, arresting people for cheating at Monopoly?" Despite such criticism, DOJ didn't relent and the case proceeded to trial.

Some of the CFAA issues raised here----was the access authorized or unauthorized? Was Nelson's conduct fraudulent, and was the object of that fraud worth more than \$5000/year as the statute requires? And/or did he knowingly or recklessly cause damage to MoM's servers, even though the only damage was to the quality of play for non-cheating users who had to face the unfairly super-powered Crimson Knight? And/or did he violate the CFAA prohibition against trafficking in "information through which a computer may be accessed" by sharing his tools on some leet hacker boards? And, ultimately, the broader policy question: should violating a game's Terms of Service really rise to the level of felony fraud?

This issue ties directly into a case (US v Arnold) that is currently being briefed in front of the 9th circuit, which may be discussed during the post-presentation panel discussion. Here's a blog post to introduce you to the decision being appealed: <<http://volokh.com/posts/1160582029.shtml>>.

## ***Trial schedule***

**COURT CALLED TO ORDER (MS. KLEIN):**

**JUDGE SALGADO REMARKS** (normally instructions to the jury):

**OPENING REMARKS (PROSECUTOR GRANICK):**

**OPENING REMARKS (DEFENSE BANKSTON):**

**GOVERNMENT WITNESSES:**

**RICHARD THIEME**

**DEFENSE CROSS OF THIEME**

**JON KLEIN**

**DEFENSE CROSS OF KLEIN**

**AGENT MARTIN**

**DEFENSE CROSS OF MARTIN**

**JESSE KORNBLUM**

**DEFENSE CROSS OF KORNBLUM**

**{BREAK}**

**DEFENSE WITNESSES**

**SIMPLE NOMAD**

**GOVERNMENT CROSS OF NOMAD**

**CLOSING REMARKS (GRANICK):**

**CLOSING REMARKS (BANKSTON):**

**JUDGE SALGADO'S COMMENTS:**

**PANEL PRESENTATION**

***Bios:***

**Carole Fennelly**

*Carole Fennelly is an information security professional with over 25 years of hands-on experience in the computing technology field. Starting as a Unix System Administrator in 1981, she was drawn into the developing information security field as the commercial Internet grew. She is the author of numerous articles for IT World, SunWorld and Information Security Magazine. A frequent speaker at security*

conferences, such as the Black Hat Briefings, her technical background includes in-depth security and administration knowledge of UNIX operating systems.

### **Richard Salgado**

*Richard P. Salgado is a Senior Legal Director with Yahoo! Inc., where he focuses on worldwide data security and international law enforcement compliance matters. Prior to joining Yahoo!, Mr. Salgado served as Senior Counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice. As a federal prosecutor, Mr. Salgado specialized in investigating and prosecuting computer network cases, such as computer hacking, illegal computer wiretaps, denial of service attacks, malicious code and other technology-driven privacy crimes. Mr. Salgado also regularly speaks on the legal and policy implications of searching and seizing computers and electronic evidence, emerging surveillance technologies, digital evidence and related criminal conduct. Mr. Salgado is a lecturer in law at Stanford Law School, where he teaches a Computer Crime seminar; he previously served as an adjunct law professor at Georgetown University Law Center and George Mason Law School, and as a faculty member of the National Judicial College. Mr. Salgado is also a Certified Instructor with the SANS Institute. He received his J.D. from Yale Law School.*

### **Kevin Bankston**

*Kevin Bankston, a staff attorney specializing in free speech and privacy law, was the Electronic Frontier Foundation's Equal Justice Works/Bruce J. Ennis Fellow for 2003-05. His fellowship project focused on the impact of post-9/11 anti-terrorism laws and surveillance initiatives on online privacy and free expression. Before joining EFF, Kevin was the Justice William J. Brennan First Amendment Fellow for the American Civil Liberties Union in New York City. At the ACLU, Kevin litigated Internet-related free speech cases, including First Amendment challenges to both the Digital Millennium Copyright Act (Edelman v. N2H2, Inc.) and a federal statute regulating Internet speech in public libraries (American Library Association v. U.S.). Kevin received his J.D. in 2001 from the University of Southern California Law Center, and received his undergraduate degree from the University of Texas in Austin.*

### **Jennifer Granick**

*Jennifer Stisa Granick joined Stanford Law School in January 2001, as Lecturer in Law and Executive Director of the Center for Internet and Society (CIS). She teaches, speaks and writes on the full spectrum of Internet law issues including computer crime and security, national security, constitutional rights, and electronic surveillance, areas in which her expertise is recognized nationally. Granick continues to consult on computer crime cases and serves on the Board of Directors of the [Honeynet Project](#), which collects data on computer intrusions for the purposes of developing defensive tools and practices. She was selected by Information Security magazine in 2003 as one of 20 "Women of Vision" in the computer security field. She earned her law degree from University of California, Hastings College of the Law and her undergraduate degree from the New College of the University of South Florida.*

### **Jonathan Klein**

*Jonathan Klein is a Director of Security Solutions with Calence Inc, a networking company located in Tempe Arizona. Jon has been a software developer in the Unix/C*

environment for over 20 years. During that time, he has developed custom security software for several large financial institutions and held key roles in numerous application deployments. Facing the choice of a management career that would remove him from hands-on technical work, Jon chose consulting as a method of achieving both. Jon has participated in forensic investigations on behalf of the Federal Defender's Office in Manhattan and with private attorneys, discovering there is more to being a technical witness than purely technical knowledge. Most recently, he served as defense expert witness in U.S. vs. Oleg Zezev, the Russian citizen accused of hacking into Bloomberg LLP and making extortion demands.

#### **Brian Martin:**

Brian Martin is an outspoken senior security consultant with the Ethical Hacking group at BT IN(<http://bt.ins.com>). With over ten years of professional security assessment experience, he has had the opportunity to provide cynical review of network and physical security for all types of business, government agency and military facility. Martin's training and articles have given people an accurate and honest picture of the dismal state of Information Security across all industries. In his spare time, he is the content manager for the Open Source Vulnerability Database (<http://www.osvdb.org>) and a champion of small misunderstood woodland creatures.

#### **Jesse Kornblum**

Jesse Kornblum is a Principal Computer Forensics Engineer for ManTech SMA's Computer Forensics and Intrusion Analysis Division. Based in the Washington DC area, his research focuses on computer forensics and computer security. In 2007 he published the "Buffalo" paper on Windows memory analysis, striking fear into the hearts of both rootkit authors and Bovinae lovers everywhere. He has authored a number of computer forensics tools including both md5deep and ssdeep, two widely used hashing suites. Previously he has served as a Computer Crime Investigator for the United States Air Force, an instructor at the Naval Academy, and the Lead Information Technology Specialist for the Department of Justice Computer Crime and Intellectual Property Section. His favorite part of coming to Las Vegas is eating at IN-N-OUT Burger.

#### **Simple Nomad**

Simple Nomad is one of the world's most intriguing hackers. Intriguing means old, right? Working for Vernier Networks by day and hacking for NMRC by night, he lives in his own world of wonder and intrigue, conspiracy and paranoia, death and taxes. He has done hackerish things for years, enjoys a good Vodka, and regularly speaks at security conferences and speaks to the press about security issues.

#### **Ryan Bulat**

Ryan Bulat used to major in Computer Science until he decided that he much preferred to be a writer. However, five years of Hacker Court have turned him to The Dark Side. He is presently a pre-law student at Monmouth University in New Jersey.

#### **Caitlin Klein**

Caitlin Klein is an honor-roll student at a private school in New Jersey and still finds time to devote to dance, guitar, horseback-riding and her level-70 Hunter on World of Warcraft. She is frequently mistaken for an undercover FBI agent. She despises blond jokes and the fact that most girls don't play video games. Caitlin drinks a lot of coffee.

***The following contributed significantly to the presentation but were unable to appear:***

***Paul Ohm***

*Paul Ohm joined the faculty of the CU School of Law in Spring of 2006. He specializes in the emerging field of computer crime law, as well as criminal procedure, intellectual property, and information privacy.*

*Prior to joining CU he worked as an Honors Program trial attorney in the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. Professor Ohm is a former law clerk to Judge Betty Fletcher of the U.S. Ninth Circuit Court of Appeals and Judge Mariana Pfaelzer of the U.S. District Court for the Central District of California. He attended the UCLA School of Law where he served as Articles Editor of the UCLA Law Review and received the Benjamin Aaron and Judge Jerry Pacht prizes. Prior to law school, he worked for several years as a computer programmer and network systems administrator, and before that he earned undergraduate degrees in computer science and electrical engineering.*

***Merlin Arduini***

*Merlin Arduini is a student at the University of Colorado School of Law. He has a BA in Mathematics, and is formerly a firmware engineer. He would rather be a fish.*