Hacker Court

BLACK HAT BRIEFINGS

Hacker Court

The passage of the US Patriot Act has broadened Law Enforcement powers and increased the penalties for computer crime. Computer forensics experts are essential to analyze and interpret technical data in simple terms that jurors, attorneys and judges can understand. It's one thing to analyze and interpret technical evidence for your peers – it's much more difficult to explain it to the average grandmother.

Black Hat has traditionally been a meeting of computer security professionals and hackers, with the intent to share knowledge of how "the other side" operates. The Hacker Court organization reflects this philosophy by presenting issues from both prosecution and defense in computer crime cases. Many computer forensic presentations are one-dimensional viewpoints, usually from the Law Enforcement perspective. Hacker Court represents both prosecution and defense and includes professionals from both sides.

This presentation will enact a courtroom environment, complete with judge, jury, attorneys, and witnesses to demonstrate key issues in computer crime cases. There is no pre-determined outcome, but we try to make the case interesting enough that both sides can make a good argument. 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. For example, in a real court case, a juror would not be allowed to go to the bar for a drink during testimony.

In the spirit of producing a realistic case, we have included fictitious news articles, Press Releases and an Indictment which the general public would typically have available before a case. Please read these over before the presentation to help us expedite the presentation. None of the events portrayed actually occurred and all similarity to persons living or dead is purely coincidental. So there.

For information about the Hacker Court organization, contact hackercourt@wkeys.com.

Players

Producer: Carole Fennelly
EmCee: Simple Nomad
Judge: Chief U. S. District Court Judge Philip M. Pro
Court Clerk: Caitlin Klein
Federal Marshal: Jack Holleran
Prosecutor: Richard Salgado
Defense Attorney: Jennifer Granick
Defendant: Weasel
Victim (Prosecution Witness): Brian Martin
CEO Getta Entertainment (Prosecution): Richard Thieme
Factual Witness (Prosecution): Ryan Bulat
Case Officer (Prosecution): Jesse Kornblum
Expert witness (Prosecution): Edward Castanova (expert on gaming economy)
Expert witness (Defense): Jonathan Klein
Technical Assistant: Inertia

Special Acknowledgement: Although not appearing in Hacker Court '03, Paul Ohm and Miles Roberts of the Department of Justice contributed significantly to legal research for the case.

Speaker's Bios:

Carole Fennelly (producer and contact):
fennelly@wkeys.com
Carole Fennelly is co-founder of the Wizard's Keys security consulting firm which has been providing security expertise to Fortune 500 clients in the New York Metropolitan area for more than ten years. Ms. Fennelly has also published numerous articles for IT World, Sunworld and Information Security Magazine. She has been a speaker at Blackhat and many other security conferences. She has over 20 years experience as a Unix Systems administrator specializing in security.

Richard Thieme
rthieme@thiemeworks.com
Richard Thieme is a business consultant, writer, and professional speaker focused on "life on the edge," in particular the human dimension of technology and work. He is a contributing editor for Information Security Magazine. Speaking/consulting clients include: GE Medical Systems; Los Alamos National Laboratory; Apache Con; Microsoft; Network Flight Recorder; System Planning Corporation (SPC); InfraGard; Firstar Bank; Financial Services - Information Sharing and Analysis Center (FS-ISAC); Psynapse/Center for the Advancement of Intelligent Systems; Cypress Systems; Assn. for Investment Management and Research (AIMR); Alliant Energy; Wisconsin Electric; UOP; Ajilon; OmniTech; Strong Capital Management; MAPICS; Influent Technology Group; FBI; US Department of the Treasury; the Attorney General of the State of Wisconsin; and the Technology, Literacy and Culture Distinguished Speakers Series of the University of Texas.

Jennifer Granick
jennifer@granick.com
Jennifer Stisa Granick is the Litigation Director of the public interest law and technology clinic at Stanford Law School's Center for Internet and Society. Ms. Granick's work focuses on the interaction of free speech, privacy, computer security, law and technology. She is on the Board of Directors for the Honeynet Project and has spoken at the NSA, to law enforcement and to computer security professionals from the public and private sectors in the United States and abroad. Before coming to Stanford Law School, Ms. Granick practiced criminal defense of unauthorized access and email interception cases nationally. She has published articles on wiretap laws, workplace privacy and trademark law.

Jonathan Klein
klein@wkeys.com
Jonathan Klein is president and co-founder of Wizard's keys, a security consultancy located in New Jersey. 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 independent consulting as a method of achieving both. Jon has participated in forensic investigations on behalf of the Federal Defender's Office in Manhattan , 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
jericho@attrition.org
Brian Martin is an outspoken security consultant
in the Washington DC area. Brian has the relatively unique experience of being on both sides of an FBI investigation.. His daily work takes him in and out of commercial and government networks, usually without sparking law enforcement investigation. His work revolves around making recommendations based on cynical review of network and system security. He will be survived by his three cats and his EverQuest character.

Jesse Kornblum
jesse.kornblum@ogn.af.mil
SA Kornblum is the Chief, Computer Investigations and Operations for the Air Force
Office of Special Investigations. A graduate of the Massachusetts Institute of Technology, he has experience running intrusion investigations and supporting other agents
in more traditional investigations. He is currently responsible for
developing tools and techniques to allow agents to conduct investigations.

Jack Holleran
jholleran@comcast.net
Jack Holleran, CISSP, currently teaches Information Security at several colleges
and the Common Body of Knowledge review for ISC2. In a past life, he was
the Technical Director of the National Computer Security Center at the National
Security Agency and Chair of the National Information Systems Security Conference.

Richard P. Salgado
Richard.Salgado@usdoj.gov
Richard Salgado serves as Senior Counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice. Mr. Salgado specializes in investigating and prosecuting computer network cases, such as computer hacking, denial of service attacks, illegal sniffing, logic bombs, viruses and other technology-driven privacy crimes. Often such crimes cross international jurisdictions; Mr. Salgado helps coordinate and manage the investigation and prosecution of those cases. Mr. Salgado participates in policy development relating to emerging technologies such as the growth of wireless networks, voice-over Internet Protocol, surveillance tools and forensic techniques. Mr. Salgado serves as a lead negotiator on behalf of the Department in discussions with communications service providers to ensure that the ability of the Department to enforce the laws and protect national security is not hindered by foreign ownership of the providers or foreign located facilities. Mr. Salgado also regularly trains investigators and prosecutors on the legal and policy implications of emerging technologies, and related criminal conduct. Mr. Salgado is an adjunct law professor at Georgetown University Law Center where he teaches a Computer Crime seminar, and is a faculty member of the SANS Institute. Mr. Salgado graduated *magna cum laude* from the University of New Mexico and in 1989 received his J.D. from Yale Law School.

Weasel
weasel@nmrc.org
Weasel is a freelance security consultant specializing in Intrusion
Detection, Policy, Incident Response, Digital Forensics, Penetration

Testing, and Security Awareness. He is also a charter member of an industry Information & Sharing Analysis Center and is a member of Nomad Mobile Research Centre.

Ryan Bulat
shadow@wkeys.com
Ryan Bulat is an intern at Wizard's Keys, where he is responsible for web site support. His interests are in Science and Technology as well as programming (C). When school doesn't intrude, he is also an avid gamer who wonders why game stats aren't included in college admissions along with SAT scores.

Edward Castanova
ecastronova@fullerton.edu
Edward Castronova, PhD, has been an Associate Professor of Economics at Cal State Fullerton since the fall of 2000. From 1991 to 2000, he was an Assistant and later Associate Professor of Public Policy at the University of Rochester.

Paul Ohm
Paul Ohm used to write code for a living. Then he went to law school, and he's never really been the same. He now works for the U.S. Department of Justice.

Myles Roberts
Myles Roberts attends the School of Law at the University of Virginia and serves as an intern to the Computer Crime and Intellectual Property Section at the U.S. Department of Justice. Prior to law school, Mr. Roberts worked at the Federal Aviation Administration and ran their Internet perimeter. He hopes to represent the first computer program that claims protection under the 13th Amendment.

Disclaimer:
This article is a work of fiction written by Carole Fennelly for Hacker Court, an organization of computer crime experts that produces simulated courtroom cases for the Black Hat conference. The events described here never occurred and all quotes are fictitious. The persons described are fictitious and any resemblance to real persons, dead or alive, is purely coincidental. For information about this article, please contact fennelly@wkeys.com

FOR IMMEDIATE RELEASE

Contact:
I. Ben Dover
Press Office
Getta Entertainment Enterprises
1313 Las Vegas Blvd, South,
Las Vegas, NV 89109
Phone: 900-555-GETTA(W) (900-555-4388)
900-555-1212(H)
http://www.GettaEntertainment.com
GettaLife@GettaEntertainment.com

Las Vegas April 1, 2001, 3:42 am PDT

LAS VEGAS, Nevada, April 1 /PR-BS/ Getta Entertainment, the world leader in online gaming, announces today the appointment of Richard Baggins as new CEO of Getta Entertainment, which earlier this year became a publicly traded company. Mr. Baggins replaces Getta founder, John Getta, who will stay on until year-end to ensure a smooth transition.

Mr. Getta is stepping down after more than 5 years as CEO citing “personal reasons” for leaving. Mr. Getta is best known for developing the online role-playing game “GettaLife”, a multi-player adventure game with over half a million subscribers world-wide. “I founded Getta Entertainment with just a few devoted staff members who helped me take this to the top”, Mr. Getta remarked, “Many of our staff volunteered their time to help develop and guide the game play to what it is today – a virtual world more real to our subscribers than the physical world. I’d like to take this opportunity to extend my heart-felt gratitude to those people who made this company what it is today.”

Richard Baggins, newly appointed CEO commented, "I am humbled to be taking over Getta Entertainment as its CEO and lead visionary", "I intend to develop this gaming space to a degree never before seen in the online gaming world, bringing greater value to the shareholders and investors. The name "Getta" is more than a brand, it's a legacy, a standard - a bright flaming torch lighting the way for all who hope to contribute to online gaming in a positive way. It is a privilege to ensure the profitability of the company while serving young people in America and the world by creating and sustaining an environment in which they can explore viable options for advancing in life, build character by learning how to play the game of life and win in a an ethical manner,

and otherwise develop the character traits that all parents want to see in their children. I see this work as a public trust and I intend to use the most creative talent available to deliver a gaming platform to the world that would make my momma proud. I know Getta's shoes are huge and I can never hope to fill them, but I do hope with unfeigned humility to advance the platform he has built in a way that honors and extends his extraordinary vision, while maintaining share value."

About Getta Entertainment

Getta Entertainment, founded by legendary gamer John Getta in 1995, develops and markets online subscriber games played by subscribers around the globe. "GettaLife", the premier multi-player role playing adventure, has been voted "Massive Multiplayer Online Role-Playing (MMORPG) Game of the Year" by prestigious gaming magazines, including Getta Entertainment's own "GettaClue". GettaLife's players assume the role of a self-created avatar, traveling through the game's virtual world to develop attributes and acquire equipment. Players often spend days - turning into years - performing Quests to gain experience and rare items. Earlier this year, Getta Entertainment announced plans for a new role-playing game called "Phlite Simulator", where players assume roles as fighter pilots tasked with military missions.

Disclaimer:
This article is a work of fiction written by Carole Fennelly for Hacker Court, an organization of computer crime experts that produces simulated courtroom cases for the Black Hat conference. The events described here never occurred and all quotes are fictitious. The persons described are fictitious and any resemblance to real persons, dead or alive, is purely coincidental. For information about this article, please contact fennelly@wkeys.com

FUD NEWS

Cyber-thugs Mug Gamer
By Cy Berfud

Horrified, Brian Martin found himself lying naked in a field, all his worldly possessions stolen, his virtue violated. What would he do? There were no police to call, no one to come to his aid, as he lay defenseless against attack. This was no ordinary mugging, but the work of cyber-thugs who cyber-raped and mugged his virtual persona.

Mr. Martin is a subscriber of the hugely popular online role-playing game by Getta Entertainment known as "GettaLife". Returning from a week- long conference, he logged in to the game todiscover his game character had been stripped of all its virtual-worldly possessions. Worse, he lost experience and what's referred to as "faction" in the game – a virtual rape of his character.

"I've been violated", a shaken Mr. Martin confessed, "It's bad enough they stole some pretty valuable stuff – that could be replaced. I can't replace the damage to my character's reputation and faction in game. No one will ask me to raid with them now."

J.B. Weasel, 30, was arrested by Federal Agents at his home in Palestine W. Virginia at the request of AFOSI Special Agent Jesse Kornblum. Mr. Weasel is the alleged mastermind of a plot to enact revenge on Mr. Martin in retaliation for a gang-like dispute in the popular online game, "GettaLife".

"GettaLife" is a global, multi-player adventure game where players assume the role of a self-created avatar, traveling through the game's virtual world, fighting monsters and searching for treasures. Players join "guilds", an online version of a club. Like street gangs, these guilds often develop rivalries with other guilds. On the advanced play, characters perform quests to increase their game status and win items with special attributes providing greater abilities in game. Players often spend days, weeks - even months – performing these quests and certain items are very difficult to acquire.

Prosecutor Richard Salgado contends Mr. Weasel, incensed when Mr. Martin exploited a feature in the game thereby gaining a contested item, directed a 17-year-old guild protégé to hack the game server and strip Mr. Martin's character of all equipment leaving him defenseless against attack in the game. The protégé, whose name was withheld because of his age, has agreed to cooperate with prosecution.

Weasel, leader of the premier guild, makes no secret of his disdain for Mr. Martin but denies hacking the server.
Interviewed at his home in Palestine, West Virginia, Mr. Weasel became emotional as he stood on his porch here overlooking the tobacco fields and cattle pastures, “Martin is grasping at straws! He's simply picking me out of the crowd because of pre-conceived notions of who I am. I'm sure if someone were to break into his house, take his company parking spot, or kick his dog, I would be at the top of his list of suspects, regardless of the evidence or the lack thereof. He’s a lamer - not a gamer!”

The GettaLife game server was allegedly hacked by Mr. Weasel, a former member of the original GettaLife team hired by Getta Entertainment founder John Getta. Weasel left Getta Entertainment shortly after John Getta was replaced as CEO by business tycoon Richard Baggins.
Interviewed at Getta Entertainment’s corporate headquarters in Las Vegas, Baggins stressed his commitment to GettaLife.
"We have built the platform for GettaLife to be a kind of exploratorium for young and old to play in ways that life itself does not always afford. It is built out of air, thin air, out of what they tell me we call pixels, and in order to hold that sky city up there we need rules and rules require integrity and the acceptance of responsibility on the part of Gettazens ... an affectionate name for the population of all of our subscribers..”

Richard Baggins has been instrumental in improving Getta Entertainment’s stock value after a dismal start. Vowing full cooperation with law Enforcement, Baggins remarked, “ I am glad to say that 98% of our members are rule-observing, law-abiding Gettazens. But, as in life itself, that remaining two per cent, a mere handful of despicable scum-sucking miscreants, try to ruin it for the rest of us. Whether its drive-by shootings that kill five-year-olds on their porches, would-be terrorists doing surveillance on dams, power stations, bridges, large banks and holding companies, natural gas pipelines, our food supply, the water that we drink, the very air that we breathe ... excuse me, whether it's them or the kind of assassin that takes a life in an online game and steals the food accumulated by a player and eats it online with the kinds of noxious odors and offensive noises only our virtual platform makes available (GettaSenseAround – ™) ... those people must be apprehended, tried and convicted, and made example of. They must be punished and punished in public if at all possible so others know the penalties for violating the trust, the sacred handshake, that is the basis of global free markets."

Mr. Weasel has been charged with three counts of conspiracy, leading to over $5000 in damages. Trial begins at the Black Hat conference at Caesar’s Palace in Las Vegas 4:45pm on July 30, 2003 with the Honerable Phillip M. Pro presiding. Mr. Weasel’s attorney, Jennifer Granick, expressed confidence her client would be exonerated, stating, “This case is grasping at pixels. There is no proof my client committed any crime, much less proof of a crime itself. After all – it’s just a game. Pixels aren’t purchased in a store. We will prove that the Emperor has no clothes.”

DISCLAIMER: The following document is a **fictionalized indictment** used as the basis for a mock trial at the Black Hat 2003 conference. The events described did not occur. The characters are fictional and any resemblance to any person, living or dead, is purely coincidental.

Approved: _____
RICHARD SALGADO
Assistant United States Attorney

Before: HONORABLE PHILLIP M. PRO
Chief United States District Court Judge
District of Nevada

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

UNITED STATES OF AMERICA	)	
- v -	)	INDICTMENT
J.B. Weasel a/k/a "Weasel"	)	

COUNT ONE
(Conspiracy to defraud and obtain something of value via unauthorized access to a protected computer)

The Grand Jury charges that at all times relevant to the indictment:

Background

1. Getta Entertainment was a corporation, which business includes owning and operating online games for multiple players.

2. GettaLife is a global, multi-player adventure game that takes place in a fictional world in the fantasy genre similar to "Lord of the Rings." Players assume the role of a self-created

avatar through their computer, traveling through the game's virtual world, fighting monsters, searching for and accumulating treasures, acquiring money for use in the game, acquiring status and socializing with other the avatars of other players.

3. Players often worked together in a "guild," an online club of players who cooperate in completing quests.

4. Defendant J.B. Weasel was 30 years old at the time of the offense. The defendant was employed at Getta Entertainment as a GettaLife gaming designer and programmer from October 31, 1995 to December 31, 2001. Defendant was also one of the original players of GettaLife.

5. Defendant was the leader of the most powerful GettaLife guild. As leader, his power over his guild was great: he determined which events they would participate in and would lead quests for special items, deciding which guild member was to benefit from the quest.

6. Some players sold their avatars, attributes and items for use in game in exchange for actual money through real-world transactions facilitated by websites such as gameauctions.com. Therefore, players who had put little or no time into the game could immediately acquire powerful avatars, rare attributes and valuable items, with no need to join guilds or successfully complete lengthy quests.

7. Defendant was very vocal in his disapproval of purchasing avatars, attributes and items. The defendant expressed disdain for players who took shortcuts in the game by purchasing their characters from online auction sites or by using methods not intended in the original plan for the game. Defendant blamed CEO Baggins for allowing the practice to expand unabated.

8. Defendant grew his character, "Weasel," over several years of play. Weasel achieved a high status within GettaLife without purchasing enhancements or by using methods not intended in the original plan.

9. Brian Martin's character ("Jericho") achieved a high status within the game by Mr. Martin's purchase of enhancements and using techniques unintended by the game's designers.

10. The defendant spent several months working on a quest, but Mr. Martin used an unintended technique to take the object of the quest at the end of the defendant's endeavor, thereby surpassing the defendant's character in status.

11. On bulletin posts, emails and online chat, the defendant condemned Mr. Martin's actions, vowing revenge. Many of these feuds took place on online message boards showing the ongoing dispute between the defendant and Mr. Martin. The defendant's computer had game logs showing arguments between the defendant and Mr. Martin.

12. Getta trusted an Air Force computer in order to provide non-classified data for another Getta game, Phlite Simulator. The Air Force computer resided inside the Air Force public address space, but outside the Air Force's internal network.

The Conspiracy and Its Objects

13. Ryan Bulat was a member of the defendant's guild and played a character named "Terron." Mr. Bulat regarded the defendant as his mentor. In discussions with the defendant, he offered to help get revenge on Mr. Martin.

14. Mr. Bulat and the defendant ("the conspirators") knowingly and intentionally conspired and agreed with each other to access a protected computer without authorization and

obtain something of value with intent to further a fraud.

Means and Methods of the Conspiracy

15. Mr. Bulat's home computer and the defendant's computer contained hacking tools and exploit code for a Unix-based system.

Overt Acts

16. On or around the week before August 5, 2002, the conspirators gained unauthorized access to the Air Force computer. Mr. Bulat's ISP showed that the unique IP addressed assigned to Mr. Bulat at time of break-in matched the unique IP address of the system that gained unauthorized access.

17. The conspirators sold almost all items from the character played by Mr. Martin ("Jericho") at an online auction site (gameauctions.com) for $3,000.

18. The rare item stolen from Mr. Martin was found on the defendant's character.

19. The conspirators deleted the Air Force system's log file that would have shown a connection from Mr. Bulat's computer at the time of the intrusion.

(Title 18 United States Code, Sections 371 and 1030(a)(4).)

COUNT TWO
(Conspiracy to cause harm via unauthorized access to a protected computer that results in at least $5,000 of loss)

The Grand Jury further charges:

20. The allegations of paragraphs one through sixteen and nineteen are repeated and re-alleged as if fully set forth in this count.

21. Mr. Bulat and the defendant knowingly and intentionally conspired and agreed with each other to intentionally access a protected computer without authorization and recklessly cause damage which equaled or exceeded $5,000.

(Title 18 United States Code, Sections 371 and 1030(a)(5)(A)(ii),(a)(5)(B)(i).)

COUNT THREE
(Conspiracy to Access a Government Computer)

The Grand Jury further charges:

22. The allegations of paragraphs one through sixteen and nineteen are repeated and re-alleged as if fully set forth in this count.

23. Mr. Bulat and the defendant knowingly and intentionally conspired and agreed with each other to access without authorization a non-public computer that is exclusively for the use of the United States Air Force.

(Title 18 United States Code, Sections 371 and 1030(a)(3).

_____
FOREPERSON

_____
RICHARD SALGADO
Assistant United States Attorney

DATED: _____