										s
News	Blog	White Papers	Webcasts	Test Center	Technologies	Tech Watch	Video	J Deep Dives	More	

#### InfoWorld Home / Security / Security Adviser / In his own words: Confessions of a cyber warrior



Security Adviser ROGER GRIMES

JULY 09, 2013

# In his own words: Confessions of a cyber warrior

A longtime friend working as a cyber warrior under contract to the U.S. government provides a glimpse of the front lines

57

By Roger A. Grimes | InfoWorld

Follow @rogeragrimes

Print 30 Comments

Much of the world is just learning that every major industrialized nation has a state-sponsored cyber army -- though many of the groups, including team USA, have been around for decades.

I've met a few cyber warriors. As you might imagine, they can't talk much about their duties. But if you work shoulder to shoulder with them long enough, certain patterns emerge. For starters, there are a lot of them. They are well armed with cyber weaponry, and they're allowed to experiment and hack in ways

that, as we all now know, might be considered illegal in some circles.

[It's over: All private data is public | Learn how to secure your systems with the Web Browser Deep Dive PDF special report and Security Central newsletter, both from InfoWorld.]

I've been a longtime friend to one cyber warrior. On condition of anonymity, he agreed to be interviewed about what he does for a living and allowed me to record our conversation on a device he controlled, from which I transcribed our conversation. I was able to ask clarifying questions the next day.

We met in person in my boat off the coast of Florida, which might sound very clandestine, except that our primary goal was to catch some fish. It's interesting to note that he did not want me to contact him by email or phone during the months leading up to this interview or for a few months after, even though what he revealed does not disclose any national security secrets. The following is an edited version of our conversation. Certain inconsequential details have been altered to protect his identity.

Grimes: Describe yourself and your occupation.





## Recent Posts

- The one security technology that actually works
- In his own words: Confessions of a cyber warrior
- Stop your privacy from being buried alive
- Why bug bounties aren't a cure for broken software

List of all recent posts

## Most Popular

- In his own words: Confessions of a cyber warrior
- 7 predictions for the iPhone 5S
- The weirdest, wackiest, and coolest sci/tech stories of 2013 so far
- The top 16 iPhone app battles
- Coming soon! 10 tech blockbuster movies

**Cyber warrior:** Middle-aged, white male, not married. Somewhat smart. Music lover. Lifetime hacker of all things. Currently working on behalf of armed services to break into other countries' computer systems.

Grimes: What is your background? How did you learn to hack?

**Cyber warrior:** I got into computers fairly early in my life, though I grew up in a foreign country. My dad split when I was young, and my mom worked a lot. I got into computers by visiting one of the few Radio Shacks near my neighborhood. The sales guy hated me at first because I was always on their computers, but after I taught him a few things, we became good friends for years. I realized I had an aptitude for computers ... that most of the adults around me did not have. By the time I was 15, I had dropped out of school (it wasn't as big of a deal in the country I was in, as it is in most developed countries), and I was working a full-time job as the head IT guy at a federal hospital.

I was hacking everything. I hacked their systems, which wasn't too much of a problem because I was already the head IT guy. They had lost some of the admin passwords to the network and other computer systems, so I had to use my hacking skills to reclaim those systems. I hacked everything: door locks, Master locks, burglar alarms -- anything. For a while, I thought I was a master spy and thief, even though I never stole anything. I would spend all my earnings on buying security systems, install them in my house, then spend all my time trying to bypass them without getting caught. I got pretty good, and soon I was breaking into any building I liked at night. I never got caught, although I did have to run from security guards a few times.

Grimes: What did you like hacking the most: security systems or computer systems?

Cyber warrior: Actually, I loved hacking airwaves the most.

		1 2 3 4	next page ›
Tags: Secur	ity, Hacking, Government		
Print	30 Comments		
	57		

FREE InfoWorld Download: Selecting the Right Cloud Step by Step Guide

From CIO.com

## From CSO Online

- 13 Steps to Help You Deal With Losing Your IT Job
- Microsoft: Purges, Personalities, 'Pursuing Other Opportunities'
- Time and Distance Enemies of Agile Project Management
- Why SaaS HR Software Is Ready to Take Off
- » Read more at CIO.com

- Telltale signs of ATM skimming
- 20 security and privacy apps for Androids and iPhones
- Big screen con artists: 7 great movies about social engineering
- Social media risks: The basics
- » Read more at CSO Online

- 10 Must Haves for Secure EMM paper | White Paper
- Dell Software | Webcast
- How to Build a Massively Scalable Next-Generation Firewall | White Paper
- Protecting personally identifiable information | White
  Paper
- Five tips to reduce risk from modern web threats | White Paper
- Web security buyers guide | White Paper

See all White Papers / Webcasts

## IT Jobs

Information Technology **Project Coordinator Full-time** Glenwood Springs, CO - Valley View Hospital

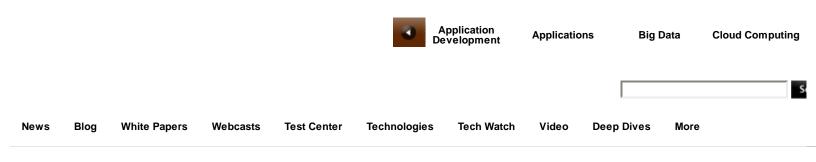
Information Technology (IT) Internship (Enterprise Network Services) Miami, FL - Assurant

Information Technology **Engineer 3 4** Long Beach, CA - Boeing

Information Technology **Technician 1** Pullman, WA - Washington State University

Information Technology Manager (Quality Assurance) Houston, TX - Halliburton

## O Additional Resources



#### InfoWorld Home / Security / Security Adviser / In his own words: Confessions of a cyber warrior



Security Adviser ROGER GRIMES

JULY 09, 2013

# In his own words: Confessions of a cyber warrior

## A longtime friend working as a cyber warrior under contract to the U.S. government provides a glimpse of the front lines

By Roger A. Grimes   Infoworld	Follow @rogeragrimes	
Print   30 Comments	57	Like 580
<pre>c previous page</pre>	1 2 3 4	next page >

#### Grimes: You mean 802.x stuff?

**Cyber warrior:** How cute. How quaint. No, I liked hacking everything that lives in the sky. Computer wireless networks are such a small part of the spectrum. I bought literally dozens of antennas, of all sizes, from small handheld stuff to multi-meter-long, steel antennas. I put them all in a storage shed I rented. I put the antennas up on the roof. I don't know how I didn't get in trouble or why the storage shed people didn't tell me to remove the antennas. I had to learn about electricity, soldering, and power generation. I had dozens of stacked computers. It was my own little cloud, way back when. I would listen for all the frequencies I could. I was next to an airbase and I captured everything I could.

Back then a lot more was open on the airwaves than today. But even the encrypted stuff wasn't that hard to figure out. I would order the same manuals as the equipment they were using and learn about backdoors in their equipment. I could readily break into most of their equipment, including their high-security telephone system. It was fun and heady stuff. I was maybe 16 or 17 then. I was living and sleeping in the shed more than at my home.

One day I started to see strange cars show up: black cars and trucks, with government markings, like out of movie. They cut the lock off my shed and came in the door. My loft was up near the rafters, so I scooted over into the next storage area, climbed down, and went out the side door at the far end of the shed area. I walked off into desert and never went back. I must have left \$100,000 worth of computers, radio equipment, and oscilloscopes. To this day, I don't know what happened or would have happened had I stayed -- probably not as much as I was worried about.

Grimes: Then what did you do?

**Cyber warrior:** My mom got married to my stepdad, and we moved back to the States. I was able to get a computer network admin job pretty quickly. Instead of hacking everything, I started to build



### Recent Posts

- The one security technology that actually works
- In his own words: Confessions of a cyber warrior
- Stop your privacy from being buried alive
- Why bug bounties aren't a cure for broken software

List of all recent posts

## Most Popular

- In his own words: Confessions of a cyber warrior
- 7 predictions for the iPhone 5S
- The weirdest, wackiest, and coolest sci/tech stories of 2013 so far
- The top 16 iPhone app battles
- Coming soon! 10 tech blockbuster movies

operating systems. I'm a big fan of open source, and I joined one of the distros. I wrote laptop drivers for a long time and started writing defensive tools. That evolved into hacking tools, including early fuzzers.

Eventually I got hired by a few of the big **penetration-testing companies**. I found out that I was one of the elite, even in a group of elites. Most of those I met were using tools they found on the Internet or by the companies that hired us, but all that code was so [messed up]. I started writing all my own tools. I didn't trust any of the hacking tools that most penetration testers rely on. I loved to hack and break into to things, but to be honest, it was pretty boring. Everyone can break into everywhere -- so I made it a game. I would only break in using tools that I built, and I would only consider it a success if none of my probes or attacks ended up in a firewall or other log. That at least made it more challenging.

#### Grimes: How did you get into cyber warfare?

**Cyber warrior:** They called me up out of the blue one day -- well, an employment agency on behalf of the other team. They were offering a lot more money, which surprised me, because I had heard that the guys working on behalf of the feds made a lot less than we did. Not true -- it's certainly not true anymore, if you're any good.

I had to take a few tests. I had a few problems getting hired at first because I literally didn't have a background: no credit, no high school or college transcripts. Even the work I had done was not something you could easily verify. But I scored really well on the tests and I was honest on what I had done in the past. They didn't seem to care that I had hacked our own government years ago or that I smoked pot. I wasn't sure I was going to take the job, but then they showed me the work environment and introduced me to a few future coworkers. I was impressed.

cprevious page		1 2 3 4	next page >
Tags: Securit	y, Hacking, Gov	ernment	
Print	30 Comments		
	57	Like 580	

#### FREE Downloads: InfoWorld Special Reports

- Cloud Computing in 2012
- Developers Survival Guide
- Mobile Management Expert Guide

## Section From Clo.com

## From CSO Online

- 13 Steps to Help You Deal With Losing Your IT Job
- Microsoft: Purges, Personalities, 'Pursuing Other Opportunities'
- Time and Distance Enemies of Agile Project Management
- Why SaaS HR Software Is Ready to Take Off
- » Read more at CIO.com

- Telltale signs of ATM skimming
- 20 security and privacy apps for Androids and iPhones
- Big screen con artists: 7 great movies about social engineering
- Social media risks: The basics
- » Read more at CSO Online

- 10 Must Haves for Secure EMM paper | White Paper
- Dell Software | Webcast
- How to Build a Massively Scalable Next-Generation Firewall | White Paper
- Protecting personally identifiable information | White Paper
- Five tips to reduce risk from modern web threats | White Paper
- Web security buyers guide | White Paper

See all White Papers / Webcasts

## O IT Jobs

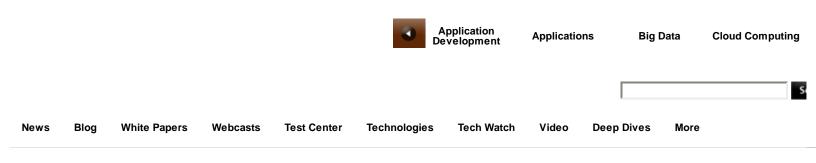
Information Technology **Project Coordinator Full-time** Glenwood Springs, CO - Valley View Hospital

Information Technology (IT) Internship (Enterprise Network Services) Miami, FL - Assurant

Information Technology **Engineer 3 4** Long Beach, CA - Boeing

Information Technology **Technician 1** Pullman, WA - Washington State University

Information Technology Manager (Quality Assurance) Houston, TX - Halliburton



Follow @rogoragrimos

#### InfoWorld Home / Security / Security Adviser / In his own words: Confessions of a cyber warrior



Py Poger A. Grimes | InfoWorld

Security Adviser ROGER GRIMES

JULY 09, 2013

# In his own words: Confessions of a cyber warrior

A longtime friend working as a cyber warrior under contract to the U.S. government provides a glimpse of the front lines

By Roger A. Grimes   InfoWorld	Follow @rogeragrimes	
Print   30 Comments	57	Like 580
<pre>oprevious page</pre>	1 2 3 4	next page >

#### Grimes: Explain.

**Cyber warrior:** They had thousands of people just like me. They had the best computers. They had multiple supercomputers. They had water-cooled computers running around on handtrucks like you would rent library books. The guys that interviewed me were definitely smarter than I was. I went from always being the smartest guy wherever I worked to being just one of the regular coworkers. It didn't hurt my ego. It excited me. I always want to learn more.

Grimes: What happened after you got hired?

**Cyber warrior:** I immediately went to work. Basically they sent me a list of software they needed me to hack. I would hack the software and create buffer overflow exploits. I was pretty good at this. There wasn't a piece of software I couldn't break. It's not hard. Most of the software written in the world has a bug every three to five lines of code. It isn't like you have to be a supergenius to find bugs.

But I quickly went from writing individual buffer overflows to being assigned to make better fuzzers. You and I have talked about this before. The fuzzers were far faster at finding bugs than I was. What they didn't do well is recognize the difference between a bug and an exploitable bug or recognize an exploitable bug from one that could be weaponized or widely used. My first few years all I did was write better fuzzing modules.

Grimes: How many exploits does your unit have access to?

**Cyber warrior:** Literally tens of thousands -- it's more than that. We have tens of thousands of ready-to-use bugs in single applications, single operating systems.

Grimes: Is most of it zero-days?



### Recent Posts

- The one security technology that actually works
- In his own words: Confessions of a cyber warrior
- Stop your privacy from being buried alive
- Why bug bounties aren't a cure for broken software

List of all recent posts

## Most Popular

- In his own words: Confessions of a cyber warrior
- 7 predictions for the iPhone 5S
- The weirdest, wackiest, and coolest sci/tech stories of 2013 so far
- The top 16 iPhone app battles
- Coming soon! 10 tech blockbuster movies

**Cyber warrior:** It's all zero-days. Literally, if you can name the software or the controller, we have ways to exploit it. There is no software that isn't easily crackable. In the last few years, every publicly known and patched bug makes almost no impact on us. They aren't scratching the surface.

Grimes: What do you like hacking now?

**Cyber warrior:** Funny enough, it's a lot of wireless stuff again: public equipment that everyone uses, plus a lot of military stuff that the general public knows nothing about. It's mostly hardware and controller hacking. But even that equipment is easy to exploit.

Grimes: Does your team sometimes do illegal things?

**Cyber warrior:** Not that I know of. We get trained in what we can and can't do. If we do something illegal, it's not on purpose. Well, I can't speak for everyone or every team, but I can tell you the thousands of people I work with will not do anything intentionally illegal. I'm sure it happens, but if it happens, it's by mistake. For instance, I know we accidentally intercepted some government official's conversations one day, someone high-level. We had to report it to our supervisors and erase the digital recordings, plus put that track on our red filter list.

**Grimes:** You say you don't do anything illegal, but our federal laws distinctly say what we cannot offensively hack other nations. And we are hacking other nations.

**Cyber warrior:** They say we can't hack other nations without oversight. John Q. Public and John Q. Corporation can't hack other nations, but our units operate under laws that make what we are doing not illegal.

cprevious page		1 2 3 4	next page >
Tags: <mark>Secur</mark> i	ity, Hacking, Gover	nment	
Print	30 Comments		
	57	Like 580	

FREE InfoWorld Download: Selecting the Right Cloud Step by Step Guide

## From CIO.com

## Section From CSO Online

Androids and iPhones

about social engineering

» Read more at CSO Online

Social media risks: The basics

Telltale signs of ATM skimming

20 security and privacy apps for

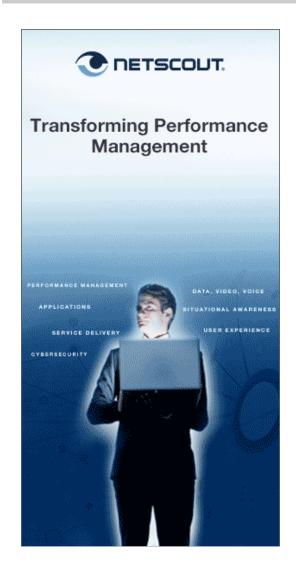
Big screen con artists: 7 great movies

- 13 Steps to Help You Deal With Losing Your IT Job
- Microsoft: Purges, Personalities, 'Pursuing Other Opportunities'
- Time and Distance Enemies of Agile Project Management
- Why SaaS HR Software Is Ready to Take Off
- » Read more at CIO.com

## O Additional Resources

- 10 Must Haves for Secure EMM paper | White Paper
- Dell Software | Webcast
- How to Build a Massively Scalable Next-Generation Firewall | White Paper
- Protecting personally identifiable information | White Paper
- Five tips to reduce risk from modern web threats | White Paper
- Web security buyers guide | White Paper

See all White Papers / Webcasts



## 🛛 IT Jobs

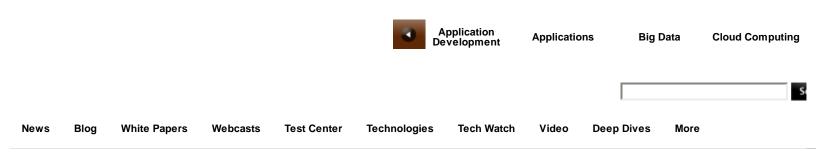
Information Technology **Project Coordinator Full-time** Glenwood Springs, CO - Valley View Hospital

Information Technology (IT) Internship (Enterprise Network Services) Miami, FL - Assurant

Information Technology **Engineer 3 4** Long Beach, CA - Boeing

Information Technology **Technician 1** Pullman, WA - Washington State University

Information Technology Manager (Quality Assurance) Houston, TX - Halliburton



#### InfoWorld Home / Security / Security Adviser / In his own words: Confessions of a cyber warrior



Security Adviser ROGER GRIMES

JULY 09, 2013

## In his own words: Confessions of a cyber warrior

A longtime friend working as a cyber warrior under contract to the U.S. government provides a glimpse of the front lines

By Roger A. Grimes   InfoWorld		Follow @rogeragrimes	
Print   30 Comments	57	Like 580	
· previous page	1 2 3 4		

Grimes: I know you from many years ago, and I think the young you would revile hacking any government by any government. I think I heard you say this many times, and you were passionate about it.

Cyber warrior: I'm still passionate about it, but the older self realizes that the young self didn't have all the facts. We have to do what we do because [other nation states and other armies] are doing it. If we didn't, we would literally be dead. It's already something that I don't know if we are winning. I know we have the best tools, the best people, but our laws actually stop us from being as good as we could be.

Grimes: What about your job would surprise the average American?

Cyber warrior: Nothing.

Grimes: I really think the average American would be surprised you do what you do.

Cyber warrior: I don't agree. I think everyone knows what we have to do to keep up.

Grimes: What does your work location look like?

Cyber warrior: I work in obscure office park in Northern Virginia. It's close to DC. There's no lettering or identifiers on the building. We park our cars in an underground garage. There are about 5,000 people on my team. I still work for the same staffing company I was hired by. My badge does not say "U.S. government" on it. We are not allowed to bring any computers, electronics, or storage USB drives into the building. They aren't even allowed in our cars, so I'm the guy at lunch without a cellphone. If people were to look around, they could spot us. Look for the group of people being loud that don't have a single cellphone out -- no one texting. Heck, they should let us carry cellphones just so we don't look so obvious.



## Recent Posts

- The one security technology that actually works
- In his own words: Confessions of a cyber warrior
- Stop your privacy from being buried alive
- Why bug bounties aren't a cure for broken software

List of all recent posts

## Most Popular

- In his own words: Confessions of a cyber warrior
- 7 predictions for the iPhone 5S
- The weirdest, wackiest, and coolest sci/tech stories of 2013 so far
- The top 16 iPhone app battles
- Coming soon! 10 tech blockbuster movies

Grimes: What do you do for a hobby?

**Cyber warrior:** I play in a hardcore rap/EDM band, if you can imagine that. I play lots of instruments, make beats and percussion stuff. I wish I could make more money doing music than hacking. I'm even considering now leaving my job and doing music. I don't need much money. I have enough for retirement and enough to support my lifestyle.

Grimes: What do you wish we, as in America, could do better hacking-wise?

**Cyber warrior:** I wish we spent as much time defensively as we do offensively. We have these thousands and thousands of people in coordinate teams trying to exploit stuff. But we don't have any large teams that I know of for defending ourselves. In the real world, armies spend as much time defending as they do preparing for attacks. We are pretty one-sided in the battle right now.

Grimes: What do you think of Snowden?

Cyber warrior: I don't know him.

Grimes: Let me clarify, what do you think of Snowden for revealing secrets?

Cyber warrior: It doesn't bother me one way or the other.

Grimes: What if it could lead to your program shutting down? You'd be without a job.

**Cyber warrior:** There's no way what we do will be shut down. First, I don't intentionally do anything that involves spying on domestic communications. I don't think anyone in my company does that, although I don't know for sure. Second, it would be very dangerous to stop what we do. We are the new army. You may not like what the army does, but you still want an army.

If I was out of job I'd just get better at playing my instruments. I like to hack them, too.

This story, "In his own words: Confessions of a cyber warrior," was originally published at InfoWorld.com. Keep up on the latest developments in network security and read more of Roger Grimes' Security Adviser blog at InfoWorld.com. For the latest business technology news, follow InfoWorld.com on Twitter.

revious page	1 2 3 4
Tags: Security, Hacking, Governmer	nt
Print   30 Comments	
57	Like 580

FREE InfoWorld Download: Selecting the Right Cloud Step by Step Guide

## Section From CIO.com

## From CSO Online

- 13 Steps to Help You Deal With Losing Your IT Job
- Microsoft: Purges, Personalities, 'Pursuing Other Opportunities'
- Time and Distance Enemies of Agile Project Management
- Why SaaS HR Software Is Ready to Take Off
- » Read more at CIO.com

- Telltale signs of ATM skimming
- 20 security and privacy apps for Androids and iPhones
- Big screen con artists: 7 great movies about social engineering
- Social media risks: The basics
- » Read more at CSO Online

- 10 Must Haves for Secure EMM paper | White Paper
- Dell Software | Webcast
- How to Build a Massively Scalable Next-Generation Firewall | White Paper
- Protecting personally identifiable information | White
  Paper
- Five tips to reduce risk from modern web threats | White Paper
- Web security buyers guide | White Paper

See all White Papers / Webcasts

## 🛛 IT Jobs

Information Technology **Project Coordinator Full-time** Glenwood Springs, CO - Valley View Hospital

Information Technology (IT) Internship (Enterprise Network Services) Miami, FL - Assurant

Information Technology Engineer 3 4 Long Beach, CA - Boeing

Information Technology **Technician 1** Pullman, WA - Washington State University

Information Technology Manager (Quality Assurance) Houston, TX - Halliburton

## O Additional Resources

#### WHITE PAPER

#### Service Desk Comparative Report

#### See All Jobs » Post a job for \$295 »

job title or company	location	Go
Jobs powered by Sin	nplyHired	

Gartner's recent magic quadrant for IT Service Support Management included no vendors as leaders or innovators. Learn why and how ITinvolve is delivering an innovative service desk solution that empowers IT staff through social collaboration and visualization to improve incident analysis and triage to speed incident resolution time.

#### Read now »

Comments powered by	Our Commenting Network   Policies   Privac	
Add New Comment	Login	
Type your comment here.		
You must verify your Disqus Profile ema	ail address before your comments are approved.	

#### Ted Thomas

Entertaining? Definitely. True? Parts of it probably are, but then, lies are mostly the truth with important bits broken off.

Here's a thought experiment: imagine 5000 mostly men working in a building who are as smart, accomplished (and arrogant) as this guy appears to be. For over a month now, a high-school dropout hiding in a Russian airport has made them all look like fools. (They can hack anything, remember?) Forget the \$ or resume chops-- it's the CHALLENGE of Edward Snowden's continued freedom to f\*\*k with their employer that must be driving them to ... fail? Why does Snowden still exist! Shouldn't something have blown up several weeks ago and "solved" this issue??

Perhaps Snowden really is as smart as he appears to be (he's still alive & free, or at least so we're told), and he really has deep encrypted NSA destroying secrets in multiple places around the world, to be released at his sudden death. If so, that would validate Mr. Cyber's last point-- the U.S. hasn't done a good job on defense.

But -- we already knew that.

#### **Gary Wickmiller**

this is a hoax article. really read what the guy claims he did between the ages of 15 - 16 years old, and you'll stop reading there.

Nice reading, a bit PR, but I suspect that large part of the real deal nowdays is no longer hacking hidden information but rather mining by relevance disclosed behavioral big data, which is nowhere mentioned here.

#### **Phone Source**

Everybody who is hired by the U.S. government as a cyber warrior needs to bear in mind that it is against the law to divulge secrets like Edward Snowden did.

#### Rbudrick

There is an incredible amount of identifying info in this interview, unless it was a lot of disinformation. Guaranteed, nation states have read this, identified the interviewee and are trying to get intel on/hack the nondescript office park building right now.



#### Herb LeBurger

It's hardly news that US intelligence agencies have people in nondescript office park buildings in the DC area.



Ugh, this guy sounds like Bill Paxton's character from the movie "True Lies" with an extra helping of arrogance, buzz words and bullocks. Each time he says "computer" replace it with the word "cyber" it not only makes re-reading the article more fun but is in and of itself a fun word to say.

Cyber, Cyber, Cyber!

#### Kamisori

in a room full of it security experts the most interesting one is the silent guy in the corner who doesnt need to brag around ...



#### Rudston

"We have tens of thousands of ready-to-use bugs ... all zero-days".

If that database ever gets hacked or leaked it's going to cause mayhem.



#### **Roger Grimes**

You might be surprised by how many pen testing companies, who have a record of their client's vulnerabilities gets stolen by other hackers all the time. Other hackers intentionally break into those companies seeking that data, and have found it again and again.



#### Rudston

In your article you say that the person you were interviewing was not directly employed by the US Government, but left it unclear as to whether he actually worked on site at a Government facility. The mention of supercomputers (plural) being available for use implies a generous budget, so we have to assume he does. In that case the likelihood of data theft is remote but, as the case of Edward Snowden demonstrates, not impossible.

The fact remains that some organisation has accumulated a huge number of coding vulnerabilities and is prepared to use them to create exploits malware. And this is a good thing? I doubt that the answer would be "Yes" if the organisation with the exploits were in another country, even if that country was a friend of the united States.

Still, it means the purveyors of security solutions are never going to be short of threats to counter, and that must be good for business.

And all because programmers aren't trained not to write sloppy code, and software testing is rushed through in order to meet product release deadlines ...

#### PC\_Backup

#### Anyone catch this gem?

First, he says he doesn't do anything illegal intentionally, then a bit later he states "our units operate under laws that make what we are doing not illegal."

In other words, they do lots of things that are illegal for the public, but they have laws that define anything they do as being legal for them - what a loophole!



#### **Roger Grimes**

He also said that they have unintentionally done things that they had to report, so there are boundaries.



#### PC\_Backup

Yeah, I saw that too, but it's important to acknowledge that we really have no idea where those boundaries fall.



**Roger Grimes** 

Read any James Bamford book. It will depress you.

	Anon
	I didn't know Roger started writing fiction.
	Bob
	I call BS this whole story. Bad PR move for pro-NSA stuff and such. Shame on you Grimes.
	Wtf
	scare tactics
	Weaver2
	Why should we believe any of this is real?
	Richard Lawson
	This is BS and if he was dumb enough to give an interview they already have this idiot
V Subs	scribe by email S RSS
	Load more comments

## Sponsored Technology Links

Cervalis-S.S.A.E. 16 data centers keep critical IT applications running.	Powerful and secure remote support with LogMeIn Rescue - Try it free
A Simpler Way to Share Flash Cache Using Your Existing SAN	Watch Perforce Webinar   Swarm Code Collaboration for Agile Teams
Share best practices and drive change at Enterprise CIO Forum	Adobe® ColdFusion® Builder™ 2 helps develop ColdFusion apps faster.
Drive business transformation now at Enterprise CIO Forum	The benefits and challenges of deploying a hybrid cloud infrastructure.
Connect with global CIOs now at Enterprise CIO Forum	Cisco Nexus 1000V and virtual network overlays ease cloud transition.
Cisco Nexus 1000V delivers data center consistency to the cloud.	Panasonic Toughbook® mobile computers are built to keep you running.
Transform enterprise IT with ServiceNow. See how easy IT can be.	Intel ProLiant - Speed through data-intensive workloads with HP ProLiant
Unleash the power of HP Converged Infrastructure. Learn More	servers. Learn More