Good morning, my name is Stephen Toulouse, and I'm known by my nickname "Stepto" which is also my email name.

Before I begin justifying your being awake this early with a hopefully pithy and thought-provoking talk, I wanted to tell you a quick story about my flight out here.

It was an 8am flight so I was already kind of bitchy and cranky because if there's anything I hate more than repeatedly being punched in the throat, it's air travel.

Sure enough, the pilot comes on after we're all seated. "The flight plan computer in the cockpit has a non recoverable fault," and they were going to have to, get this, reboot the airplane. Sound familiar? I felt like they were calling our own support. "Have you tried turning it off and back on?"

For those not familiar with rebooting an airplane, I sure wasn't, this involved turning the plane off, turning the plane on again, and waiting for the flight team to recertify the flight. This process takes 30 to 40 minutes.

That didn't work. So they came on the speakers and said well, we're going to….try it again. So seriously, they rebooted the plane, AGAIN. And it didn't work.

The pilot came on and said well folks, rebooting hasn't fixed the problem so we're going to potentially have to cancel the flight but first we're going to…reboot it one last time.

And that time it worked. [Slide: Third time worked? They must have known a Microsoft employee was on board]

So let me start off telling you what I do for Microsoft. I'm the Lead Program Manager for policy and enforcement on the Xbox LIVE service. [Slide: Translation: BANHAMMER] Previously I was a program manager and communications manager for security response for Microsoft [Slide: Translation: MOUTHPIECE] So when they asked me to come here and talk to you guys, at first I was a little stuck for what to talk about. [Slide: Was actually stuck on level three of Portal.]

So I thought well, I'll talk about some history. Explore some myths and things we learned, and then I can point out something that surprised me when I "left" security, the fact that the baggage I took with me was incredibly helpful.

[Slide: HISTORY]

So, what is my security expertise? You see, I didn't start out in security. Because I think there's two types of us out there, those that came into computer security and those who have always been there.

My involvement in computer security at Microsoft wasn't really a natural career path for me. I got interested in security when I got hacked.

Back in 2001 I was working in Microsoft's office in Texas, doing technical writing and training development for operating systems. And on the side I ran a little IRC chat server for friends and IT pro's

across the country to just hang out and share knowledge or whatever. [Slide: Rarer than a blue steak: a quality Win32 IRC Daemon. For good reason]

And there was this one member of the chat man, this one guy, who was constantly griefing about the fact I was running a Windows 2000 IRC server. I mean non-stop; "worst operating system ever, worst security ever, blah blah blah". One day I got fed up. I went to the server, checked Windows Update to make sure it had everything, and finally told the guy "ok look, either put a file on my hard drive or tell me the contents of a file on my hard drive or shut up"

30 minutes later he gave me the contents of an .ini file in my system directory.

You see back then, not all security updates were propped to Windows update. You had to run a manual command line file, hfnetchk, to understand if you needed an update and sure enough I'd missed the Unicode update MS00-078. And because I was a terrible system administrator [Slide: and an awful human being] I was running IIS 5 without even knowing it.

So as I was paving the machine I kept thinking, wow, if a Microsoft employee can't get this right, how in the world can our customers get it right?

Now, I had no idea the security landscape. Oh I mean I knew that from time to time my company tended to treat security issues as a PR problem. I knew that certain companies out there who shall remain nameless proclaimed their software to be "unbreakable" [Slide: Rhymes with Shmoracle] or were pressuring researchers to not present their findings through legal means [Slide: Rhymes with Crisco] or that some companies were even doing a horrible combination of all three! [Slide: Pic of Justin Long]

But I knew I wanted to help, both out of my own embarrassment and because I wanted to learn. Oh, by the way the kid that hacked into my server grew up to become the sound designer on a game you might have heard of [Slide: hi res graphic of Bioshock logo] so he did good.

Anyways. I interviewed with the Microsoft Security Response Center in summer of 2002 for a Program Manager role and moved up to Seattle in fall of 2002. I learned how to triage vulnerabilities incoming to secure@microsoft.com, and one day they had me do the press calls for a week's releases and bam, that became my job as well, describing the scope and impact of the vulnerabilities to journalists.

This was actually a great move by Microsoft. There was no way for me to treat these as a PR problem because I was scared shitless just to be on the phone with a reporter. The reporter would say "So, what can an attacker do?" me (sweating): "ANYTHING THEY WANT"

Reporter: Which customers are affected? Me(sweating): "ALL OF THEM".

Along with everybody else on the team I wrote security bulletins, drove product teams through release plans to produce updates, and handled release every week. [Slide: Trivia: The song we always played while bulletins and updates propped was "Yo, Pumpkinhead!" from the Cowboy Bebop soundtrack]

My first experience with any type of crisis was…Slammer, just a month or two into the job. Between juggling selling my house in Dallas and all the other stuff that comes with a move I was having a new stereo installed in my Jeep. So I woke up early the morning of January 25th 2003, and tried to log into mail and couldn't. I figured it was because the temp house I was in had bad wiring, and went to have the stereo work done. So they tear apart my car and I'm kind of geeking out watching them do all the stuff and they then proceed to rebuild it and the first thing they hooked together was the radio, which I rarely listened to anyway. "pssht The Internet today was taken down by a worm in Microsoft's SQL server software"

I start screaming "put the car back together put the car back TOGETHER!!!"

So I'm racing down I-5 to get to campus and assist in the recovery, etc. And we made it painfully through that experience and we learned a ton of things.

The first thing we learned was to create a much broader plan for incident response than we had. So we developed the Microsoft Internet Security Emergency Response plan [Slide: M.I.S.E.R.] Well, the executive leadership didn't like that name for some reason [Slide: M.I.S.E.R. (Y)] so we went with Software Security Incident Response Plan, or SSIRP.

Which in Microsoft speak was quickly verb'd. "Are we SSIRPing?" "Have we SSIRPed?" This was the process we used to respond to Blaster and Sasser, and it continues to be refined and improved to this day.

It was also at this time that the finishing touches were being put on the Security Development Lifecycle. We moved to monthly releases, and began providing malware removal tools. The rest, as they say, is history.

[Slide: MYTHS and MISTAKES]

So being the accidental security guy I really threw myself into it. And I discovered pretty quickly that computer security, as a subset of being a computer professional, was very much a "drink from the fire hose experience all the time". And along the way, as I began to meet and truly understand security researchers, I quickly discovered mistakes we were making, as well as some myths.

[Slide: MYTH #1: Microsoft hates security researchers

Mistake #1: We didn't work to understand them]

Thankfully, I think this one has pretty much been debunked thanks to the outstanding efforts our ecosystem team has done over the years but I want to bring it up here because of the mistake part. If you go back to 2003 I was always mystified by people saying we hated security researchers. Our rules for handling communications with researchers were to always be professional, get back to them with status and updates in a timely manner, have them test our updates. I mean, it looked to me like we were being really supportive.

But the reality was we were just being an interface. We weren't working to really understand what motivates researchers and where the trends were going in security research. And so we got over that by creating the Blue Hat internal security conference twice a year, where security researchers present to both developers and execs in the company. And we started making a concerted effort to be present at security conferences all over the world, talking and engaging with researchers to get their view on how we could improve. I'm not saying Microsoft is the single greatest company in the history of the world in regards to our relationship with researchers, but we've learned. But the team in Microsoft that created that outreach deserves credit for wanting to understand researchers.

[Slide: Myth #2: The SDL is a failure, critical vulns are still present

Mistake #2: Not making the SDL more public, more quickly]

Myth #2 really bugs me and I still hear it to this day when I state that I believe other companies should either adopt the security development lifecycle or develop and publish their own. The SDL process is not a panacea, it's a quality driver that is designed to be adaptable over time to reduce classes of mistakes. I think today's Microsoft products are light years more secure than previous ones at a baseline.

But it took us forever to really get it out in front of people in a way they could adopt it. I mean we could say all day we created it and it has benefits but getting it out there so companies developing in house tools could use it, or small and large software firms could consume it, add to it, etc, was way too long in coming. My work on the SDL has been very tangential, to be clear I am just in awe of the entire team that works on it because those are some Crackerjack folks. But the key is, no one else is leading in this space in the software vendor world. The SDL architects are key.

[Slide: Myth #3: Microsoft has the Trustworthy Computing Group, but does the rank and file understand security?

Mistake #3: Not setting the example of aggressive security knowledge "pollination" in the company]

This leads me into the final part of my talk, which is sort of wrapped up in the title. I've heard this before, people have said to me up front. Sure, you have a group within Microsoft that's a central hub of security, but do the people writing the code understand security?

And the answer to that is yes. Just because a lot of the SDL work occurs in TwC doesn't mean people aren't there in the product groups grokking security. I think that's one of the main reasons that Bluehat is so successful. It's one thing to read a paper describing a broad class of vulnerability that might affect your code. It's quite another thing to sit there in the audience and watch as a researcher demonstrates to you and your peers how shoddy assumptions lead to customers getting owned. So for people out there, don't just bring in security researchers for pen testing or contract work.

Our mistake is not setting an example for every company on how to distribute security knowledge. Not to say our method is by any means perfect, but since the creation of TwC, it's served almost as a training academy for security knowledge. People leave TwC and go on to become great product leaders or

developers in different business groups. Microsoft and our customers benefit every day when people leave core security roles to go on to product teams and support teams, and new people take their place.

I can't tell you how different things are now internally at Microsoft. How many security alumni there are out there who didn't need to have a security researcher brought to them, they've gone out to understand the trends. If I had one piece of advice to give it's to encourage your security teams to sabbatical with other groups in the company. Encourage them to move on and see other aspects of things.

The skills we have as security professionals are portable to so many other aspects of computer professional work. I never really realized it until I made the decision to leave security.

Which brings me to baggage. By the time Vista shipped I was worn down. I was finding myself becoming "that guy" who says "but we've always done it that way" [Slide: and get off of my lawn!]

I helped the Xbox team get through a minor privacy issue they had and they said hey, we're expanding a lot of the work we're doing for safety, etc on Xbox LIVE would you like to come over and work with us. hrmm let me think about it…OK OK OK OK.

My lifelong passion is video games so I leapt at the chance. I figured, what could be further from computer security than the entertainment group? Their concept of "bad news" was people buying too many copies of a game and it's scarce. You've all heard it right? All heard the phrase, "once you get into security you never really leave it". I think that's really the wrong way to put it. I would say, once you leave computer security you're going to bring some baggage with you. But it's good baggage.

The first thing you bring with you is the concept of misuse of functionality. My team's first task was to build a scalable enforcement tool for the service to replace the existing toolset. The tool would consume text data from the internal complaint database, and render it for judgment by our agents. Oh I was so happy to be working on a tool where my security knowledge could come into play. I had the team setup the database just the way I thought it should be. I had the web client designed to run on 64bit Vista in low rights IE. I code reviewed and we ran some pen testing to make sure people couldn't misuse the application or anyone else other than my team couldn't try to wreak havoc with it. It was isolated from any customer facing interfaces.

Finally we were done. The tool consumed input from a trusted database and rendered it, and things went perfectly. Did you know the first rule of gun safety is that the gun is always loaded? The computer security correlary to that is the data is never trusted, even when it's trusted. One day the webUI for the tool just refused to render. No matter who logged in. I couldn't figure it out until I remembered something key: the tool was simply displaying text from a database. Text the users had entered into their profile fields. That's when I found that someone had set their biography field to this: [Slide: <style type="text/css"> .penis { height: 1000px; width: 300px; overflow: into your moms mouth;]

And of course, our web client tried to render it and got stuck. So I implemented a check to render the input differently. My dev asked what made me think to check for script. All I could think of was to say "it's what I would done if I was breaking it"

The second thing you bring with you is an understanding of unintended consequences. We'd received some feedback from customers that finding friends on the service was harder perhaps than they wanted it to be. So the product team came up with a great feature to make it easier to find like-minded gamers. They called it "Friends of friends". Basically you could now see the friends of everyone on your friends list, dramatically expanding the pool of people you might want to game with. The problem, we security minded folk pointed out, was with luminaries, celebrities, and families. These are people most likely to not want to be as discoverable in that manner. It's especially sensitive with families who would want to restrict children's friends lists. So we provided ways online to turn the feature off before we ever shipped it so people who didn't want it, never had to deal with it.

The final thing I think you take with you wherever you go is that if you're in security, you care about the customer in the end. Now the word customer can have many different meanings. It can be an individual user, a group of users, or the company that pays you to protect their network. But the point is because we play in a realm where the stakes are so high, our professionalism and our focus is oriented to doing the job well, and always learning about the environment we operate in. I encourage you all to explore great opportunities because I think our entire ecosystem benefits when people dedicated enough to come and learn and speak at conferences such as this share their expertise. And who knows, maybe one day I'll go back into a more computer security oriented role. But for now I've got a plane to catch, I hear there are some jerks in Halo3 who need a good banx0ring.

[Slide: Thank you.]

Thank you all for coming this morning.

[this document was written on an HP 2133 using Windows Vista x86 and Open Office 3.0 RC4]