

**DARPA Tech, DARPA's 25<sup>th</sup> Systems and Technology Symposium  
August 9, 2007**

**Anaheim, California**

**Teleprompter Script for Lt Col Michael VanPutte, USA, Program  
Manager, Strategic Technology Office – Networks Presentations**

"Clean Slate –  
Enabling a Secure Global Information Grid"

» **MICHAEL VANPUTTE:**

You've all heard today about the work at DARPA to harness the advantages of information technology to serve our military men and women.

While our military command-and-control is predicated on safe and secure information sharing, there is one inescapable fact that can easily render this technological edge null and void --

***our adversaries enjoy the asymmetrical advantage in the information battlespace, an advantage that we gave them.***

**Where we are today?**

Think for a minute about the Defense Department's information systems.

Most of them operate on commercial off-the-shelf products – basically the same as those in your home or office.

These operating systems, applications and protocols are fundamentally insecure ...

and were never designed for hostile environments.

They were designed for the lowest common commercial denominator, compatible with every version of diverse hardware and software.

They are optimized to play games, track stock portfolios, and guard against the loss of personal information;  
but we need them to  
fight wars, find enemies, and protect national security information.

The requirements of the marketplace are not the demands of the battlespace –  
and the resulting information systems are placing our nation –  
and our men and women in uniform – at risk.

Whether DoD networks or corporate networks,  
we must have confidence in the information and systems.

We've seen the result of the current paradigm,  
how susceptible we are to a seemingly unending stream of denial of service attacks ...  
cyber crime ...  
harassing spam ...  
and cyber espionage.

This threat is real and becoming increasingly stealthy, more insidious and more destructive.

Today's commercial computers have components manufactured by dozens of companies with instructions burned into the hardware.

We have no way of assuring the security of component parts,  
even before the machine is assembled –  
and no way of ensuring it isn't compromised when it is assembled.

Our operating systems and applications are no better.

Essentially, we are asking our military to purchase systems that are insecure and input that insecurity right into the foundation of our warfighting network.

The commercial solution – the one we have employed up until now – is to address each threat with additional, individual plug-in security solutions, better firewalls ...  
more robust anti-viral systems ...  
more effective intrusion detection.

To date, the result is a patchwork defense characterized by high costs, reduced synergy, and an ever-increasing burden on our people and equipment –  
all of which still buys us only temporary relief in a never-ending contest to stay ahead of the next attack.

We're still vulnerable and have no idea of the state of our security.

Our cyber warfighters work relentlessly to patch every known security hole and maintain 24-7 vigilance while our adversaries develop a single exploit, and attack at the time and place of their choosing.

That's about  
as asymmetric  
as warfare gets.

But we are taking the wrong approach –  
***you can't make a system more secure by making it more complex.***

We've been trying to build security around fundamentally insecure concepts and machines and no matter what new locks we put on the

doors, attackers will still be able to exploit the basic blueprint of the house to break in.

### **DARPA's Challenge**

We cannot let this continue ...  
we need a revolutionary, disruptive change.

The most critical challenge is to develop a secure DoD-specific workstation –  
what I call ***clean slate***.

Let me explain what I mean by ***clean slate***.

The complexity of today's commercial systems is the root of the problem.

This complexity comes from gaming, entertainment and backwards compatibility.

But these are not the requirements of a weapon system.

So by eliminating these requirements ***clean slate*** will vastly reduce complexity to a level that can be mitigated.

The underlying theme of the ***clean slate*** architecture is that all components are *mutually suspicious cooperating components*.

That is, components are given the least amount of privilege necessary to perform their function.

Key to this is the concept of bottom-up compartmentalization.

Less trusted components are never permitted to compromise the entire

system.

All components – hardware, operating system, drivers, and applications -- are segmented from each other and permitted the minimal authority to accomplish their tasks.

Perhaps **Clean slate** is a general-purpose machine specification placed on the open market and fabricated anywhere in the world, mass-produced commodity hardware – much like PDAs are mass produced today.

The chipset could be completely separated from the instruction set so there is no chance for deliberate imbedded vulnerabilities.

When a **clean slate** device arrives, the system capabilities and security is verified through a formal automated process – providing a secure foundation that would extend from workstations in the Pentagon to hand-held devices used by our deployed soldiers.

Another challenge is to develop a provably secure processor coding and instruction set that would be *flushed* onto **clean slate** – in effect installing our intellectual property onto the machine after delivery and taking the foreign fabrication problem off the table.

Perhaps this revolutionary system would flash a static, secure micro-**kernel**, or secure miniature operating system.

This secure micro-**kernel**, unlike today's commercial systems, would be **provably secure** – and when combined with strict, hardware enforced compartmentalization eliminates many of the threats to DoD's operational network from viruses, worms, root-kits, bots and other

malicious intruders.

Since these machines would be made exclusively for military use, the applications only need to support critical features like email, web browsing, and document reading and editing.

Soldiers who require additional functionality – such as in-house developed databases or other legacy applications that lack a web interface – would access them through a secure “virtual machine.”

Every time a user requests an application, the machine creates a new instance, secured by hardware, protected in its own memory space – preventing our adversaries from obtaining a persistent presence on the network, even on insecure applications.

This custom hardware and compartmentalization will come with some cost, such as speed; however there are other offsetting payoffs.

For example, we can “buy speed” since we eliminate most of the security controls, patching, daily updates and other administrative burdens on today’s machines and administrators.

There are other components for secure collaboration – and I recognize ***clean slate*** doesn’t address all of the challenges.

For example, we will need revolutionary local area network protocols, architectures, and devices to eliminate other advantages the adversary has on today’s client/server networks.

However a secure workstation is the foundation to build from and

solutions to these other challenges should be incorporated with clean slate for holistic, secure tactical and garrison environments..

The Department of Defense has invested a significant amount of financial and intellectual resources in the quest for securing commercial off-the-shelf systems and high-end secure devices.

Despite these heroic efforts, the average soldier is still vulnerable, from 15-year-old hackers to far more dangerous and determined adversaries.

We learned a great deal over the past few decades, and technology has evolved at a tremendous rate.

We have pieces that may be used in a clean slate machine – such as the Trusted Computing Group and several secure microkernels projects.

But it's also time to begin looking for answers in new directions.

It may be time to revisit the 60-year-old Von Neuman architecture from which personal computers are still designed.

I seek your ideas on how to bring ***clean slate*** and secure networking to our warfighters.

I want to tap into your expertise for revolutionary ideas to design and build a secure host that, in the long run, is no more costly than commercial systems and requires less administrative overhead.

In short, it's time to step back and rethink some basic premises – to build new structures for which no enemy can exploit the blueprint,

attack-proof computing devices that are inexpensive, disposable, tamper-proof and efficient.

With our best efforts,  
and with yours, I am confident it can be done.

Thank you.

I'll be followed by  
Brian Pierce.