

Re: secure client-side platform

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-09/0021.html>

From: Keith Oxenrider (*koxenrider_at_sol-biotech.com*)

Date: 09/01/05

Date: Thu, 01 Sep 2005 16:41:42 -0400

To: <liudieyu@umbrella.name>, <bugtraq@securityfocus.com>

Something I have discussed with a friend but not explored wrt technical feasibility is a micro kernel residing in the system bios that emulates the hardware it is residing on. I believe under those circumstances it would be impossible to prove you had a secure system without having an external way of verifying the bios instructions. This idea came to me when I read about some bios chip that had 8 MB of memory; plenty to fit a micro Linux kernel with room to spare.

Keith Oxenrider, CISSP

At 03:24 AM 9/1/2005 +0000, liudieyu@umbrella.name wrote:

>#1, we are talking about how to do critical secret communication in a secure
>way, right? so forget about those putting win9x 24/7 on DSL ... let them
>continue contributing to the spam and zombie business ;-)
>
>imagine i'm going to access an e-gold account of \$1M ...
>first i unplug the network cable and remove harddrive;
>then boot with a clean livecd;
>later start firewall and then plug the network cable;
>run "mozilla-firefox about:blank";
>directly go to HTTPS-secured website;
>once done, reboot.
>i cannot figure out what could go wrong in the above process ...
>
>clean read-only OS is a solution against "once owned, stay owned" (trojan
>stays in system until next format)
>
>it does not solve the problem of the vulnerabilities in client software like
>mozilla (as joxean and keith suggested)
>
>if we only have encryption-secured connection to trusted server,
>assuming enemy do not have control over the trusted server itself,
>our computer can only be compromised if:
>* enemy have total control over the communication channel
>between us and the trusted server
>* AND

SecurityFocus Bugtraq: Re: secure client-side platform

> – *there is a vulnerability in the certificate/publickey*
> *verification process of client software like mozilla*
> – *OR the mathematic foundation of publickey-privatekey*
> *sign/encrypt trick got a problem.*
> – *OR we clicked YES in the*
> *certificate-is-invalid-continue-or-not dialog*
> ** AND*
> *enemy got vulnerability to exploit after going thru the*
> *certificate verification process taken in our side.*
>
> *chances are rare, hum? the very last sentence of my trooseid article is:*
> *Never touch any not-encryption-secured connection during a*
> *secret-communication op.*
> *you read it, right?*
>
> *Q: can you really trust Google?*
> *A: it's really up to you which server you choose to store and transfer*
> *encrypted secrets. in my view, the Gmail service of google is just a good*
> *example here ... you got service better than google's gmail, of course go*
> *ahead ...)*
>
> *honestly, i have not used the tools mentioned in the "why not ... " part*
> *below. it gonna take some time to evaluate those solutions by myself.*
>
> *#####*
>
> *"you got a problem"*
> **** 1 ****
> *Joxean Koret <joxeankoret@yahoo.es>*
> *[+] I think this is a bad idea. What about client software vulnerabilities?*
> *You can have a system that were secure but*
>
> *currently it's not.*
> *[+] Various applications, such as web browsers, mail clients, etc...*
> *needs to*
> *be constantly updated to fix the newest*
>
> *vulnerabilities.*
> **** 2 ****
> *"Keith Oxenrider" <web10198@sol-biotech.com>*
> *[+] I am sure you will be hearing this from many others, but basically it is*
> *impossible to secure client side computing if*
>
> *the client every goes outside of your control (one presumes that if it remains*
> *inside your control you have effective*
>
> *controls). Clearly, server side computing is entirely within the control of*
> *whomsoever owns (or Owns) the server, so there*
>
> *is implicit trust when you connect (can you really trust Google to protect*
> *your content?).*

SecurityFocus Bugtraq: Re: secure client-side platform

> [+]
> While your recommendations, if used, will obviously increase the
> baseline
> security of the average person, you can't
>
> guarantee anything. Smart card developers run into many of these issues and
> they don't have to deal with buggy commodity OSs
>
> and browsers. Since the vast majority of users don't even bother to keep
> their machines patched (people STILL use Win9x
>
> connected 24/7 to DSL, btw), offering suggestions on how to make their
> computer even more difficult to use is unlikely to win
>
> any converts.
> [+]
> Those of us who are already paranoid and have done their homework know
> there is no way to ensure on-line security
>
> besides never doing anything on-line.
> [+]
> Something to keep in mind, a read-only OS is only as good as its patch
> level when it was written and will decay with
>
> time eventually (soon) reaching an insecure state that can easily be
> penetrated.
>
>
> "why not ..."
> *** 1 ***
> Joxean Koret <joxeankoret@yahoo.es>
> Why not use a system like LTSP (Linux Terminal Server Project) or any other
> "Think Client" based system?
> *** 2 ***
> "Beauford, Jason" <jbeauford@EightInOnePet.com>
> Tinfoil Hat linux ..silly. <http://tinfoilhat.shmoo.com/>
> *** 3 ***
> "Gustavo Paredes" <gustavo.paredes@internet-solutions.com.co>
> Do you know secuware? www.secuware.com
>
> #####
>
> how to have a secure client-side platform for secret communication?
> ... transferring and storing secret messages, online banking, etc
>
> i got some fresh ideas in mind, and would like to share it here:
> 0. watch network with sniffer, so be sure no byte is sent to weird
> destinations
> 1. read-only operating system(knoppix, etc), so every boot is a fresh start
> 2. get every secret processed in memory and stored as encrypted in remote
> server
>
> any suggestion or fresh idea on this topic is welcome
>

SecurityFocus Bugtraq: Re: secure client-side platform

>*this document for ordinary people on the street:*

><http://umbrella.name/upid/trooseid>

>

>*bugtraq guys can directly go to the conclusion part:*

>http://umbrella.name/computer/trooseid/trooseid_online/#conclusion