`Trusted Computing' Frequently Asked Questions

- TC / TCG / LaGrande / NGSCB / Longhorn / Palladium / TCPA

Version 1.1 (August 2003)

Ross Anderson

---

1. What is TC - this `trusted computing' business?

The Trusted Computing Group (TCG) is an alliance of Microsoft, Intel, IBM, HP and AMD which promotes a standard for a `more secure' PC. Their definition of `security' is controversial; machines built according to their specification will be more trustworthy from the point of view of software vendors and the content industry, but will be less trustworthy from the point of view of their owners. In effect, the TCG specification will transfer the ultimate control of your PC from you to whoever wrote the software it happens to be running. (Yes, even more so than at present.)

The TCG project is known by a number of names. `Trusted computing' was the original one, and is still used by IBM, while Microsoft calls it `trustworthy computing' and the Free Software Foundation calls it `treacherous computing'. Hereafter I'll just call it TC, which you can pronounce according to taste. Other names you may see include TCPA (TCG's name before it incorporated), Palladium (the old Microsoft name for the version due to ship in 2004) and NGSCB (the new Microsoft name). Intel has just started calling it `safer computing'. Many observers believe that this confusion is deliberate - the promoters want to deflect attention from what TC actually does.

2. What does TC do, in ordinary English?

TC provides a computing platform on which you can't tamper with the application software, and where these applications can

communicate securely with their authors and with each other. The original motivation was digital rights management (DRM): Disney will be able to sell you DVDs that will decrypt and run on a TC platform, but which you won't be able to copy. The music industry will be able to sell you music downloads that you won't be able to swap. They will be able to sell you CDs that you'll only be able to play three times, or only on your birthday. All sorts of new marketing possibilities will open up.

TC will also make it much harder for you to run unlicensed software. In the first version of TC, pirate software could be detected and deleted remotely. Since then, Microsoft has sometimes denied that it intended TC to do this, but at WEIS 2003 a senior Microsoft manager refused to deny that fighting piracy was a goal: `Helping people to run stolen software just isn't our aim in life', he said. The mechanisms now proposed are more subtle, though. TC will protect application software registration mechanisms, so that unlicensed software will be locked out of the new ecology. Furthermore, TC apps will work better with other TC apps, so people will get less value from old non-TC apps (including pirate apps). Also, some TC apps may reject data from old apps whose serial numbers have been blacklisted. If Microsoft believes that your copy of Office is a pirate copy, and your local government moves to TC, then the documents you file with them may be unreadable. TC will also make it easier for people to rent software rather than buy it; and if you stop paying the rent, then not only does the software stop working but so may the files it created. So if you stop paying for upgrades to Media Player, you may lose access to all the songs you bought using it.

For years, Bill Gates has dreamed of finding a way to make the Chinese pay for software: TC looks like being the answer to his prayer.

There are many other possibilities. Governments will be able to arrange things so that all Word documents created on civil servants' PCs are `born classified' and can't be leaked electronically to journalists. Auction sites might insist that you use trusted proxy software for bidding, so that you can't bid tactically at the auction. Cheating at computer games could be made more difficult.

There are some gotchas too. For example, TC can support remote censorship. In its simplest form, applications may be designed to delete pirated music under remote control. For example, if a protected song is extracted from a hacked TC platform and made available on the web as an MP3 file, then TC-compliant media player software may detect it using a watermark, report it, and be instructed remotely to delete it (as well as all other material that came through that platform). This business model, called traitor tracing, has been researched extensively by Microsoft (and others). In general, digital objects created using TC systems remain under the control of their creators, rather than under the control of the person who owns the machine on which they happen to be stored (as at present). So someone who writes a paper that a court decides is defamatory can be compelled to censor it - and the software company that wrote the word processor could be ordered to do the deletion if she refuses. Given such possibilities, we can expect TC to be used to suppress everything from pornography to writings that criticise political leaders.

The gotcha for businesses is that your software suppliers can make it much harder for you to switch to their competitors' products. At a simple level, Word could encrypt all your documents using keys that only Microsoft products have access to; this would mean that you could only read them using Microsoft products, not with any competing word processor. Such blatant lock-in might be prohibited by the competition authorities, but there are subtler lock-in strategies that are much harder to regulate. (I'll explain some of them below.)

3. So I won't be able to play MP3s on my computer any more?

With existing MP3s, you may be all right for some time. Microsoft says that TC won't make anything suddenly stop working. But a recent software update for Windows Media Player has caused controversy by insisting that users agree to future anti-piracy measures, which may include measures that delete pirated content found on your computer. Also, some programs that give people more control over their PCs, such as VMware and Total Recorder, are not going to work properly under TC. So you may have to use a different player - and if your player will play pirate MP3s, then it may not be authorised to play the new, protected, titles.

It is up to an application to set the security policy for its files, using an online policy server. So Media Player will determine what sort of conditions get attached to protected titles. I expect Microsoft will do all sorts of deals with the content providers, who will experiment with all sorts of business models. You might get CDs that are a third of the price but which you can only play three times; if you pay the other two-thirds, you'd get full rights. You might be allowed to lend your copy of some digital music to a friend, but then your own backup copy won't be playable until your friend gives you the main copy back. More likely, you'll not be able to lend music at all. Creeping digital lockdown will make life inconvenient in many niggling ways; for example, regional coding might stop you watching the Polish version of a movie if your PC was bought outside Europe.

This could all be done today - Microsoft would just have to download a patch into your player - but once TC makes it hard for people to tamper with the player software, and easy for Microsoft and the music industry to control what players will work at all with new releases, it will be harder for you to escape. Control of media player software is so important that the EU antitrust authorities are proposing to penalise Microsoft for its anticompetitive behaviour by compelling it to unbundle Media Player, or include competing players in Windows. TC will greatly increase the depth and scope of media control.

4. How does TC work?

TC provides for a monitoring and reporting component to be mounted in future PCs. The preferred implementation in the first phase of TC emphasised the role of a `Fritz' chip - a smartcard chip or dongle soldered to the motherboard. The current version has five components - the Fritz chip, a `curtained memory' feature in the CPU, a security kernel in the operating system (the `Nexus' in Microsoft language), a security kernel in each TC application (the `NCA' in Microsoft-speak) and a back-end

infrastructure of online security servers maintained by hardware and software vendors to tie the whole thing together.

The initial version of TC had Fritz supervising the boot process, so that the PC ended up in a predictable state, with known hardware and software. The current version has Fritz as a passive monitoring component that stores the hash of the machine state on start-up. This hash is computed using details of the hardware (audio card, video card etc) and the software (O/S, drivers, etc). If the machine ends up in the approved state, Fritz will make available to the operating system the cryptographic keys needed to decrypt TC applications and data. If it ends up in the wrong state, the hash will be wrong and Fritz won't release the right key. The machine may still be able to run non-TC apps and access non-TC data, but protected material will be unavailable.

The operating system security kernel (the `Nexus') bridges the gap between the Fritz chip and the application security components (the `NCAs'). It checks that the hardware components are on the TCG approved list, that the software components have been signed, and that none of them has a serial number that has been revoked. If there are significant changes to the PC's configuration, the machine must go online to be re-certified: the operating system manages this. The result is a PC booted into a known state with an approved combination of hardware and software (whose licences have not expired). Finally, the Nexus works together with new `curtained memory' features in the CPU to stop any TC app from reading or writing another TC app's data. These new features are called `Lagrande Technology' (LT) for the Intel CPUs and `TrustZone' for the ARM.

Once the machine is in an approved state, with a TC app loaded and shielded from interference by any other software, Fritz will certify this to third parties. For example, he will do an authentication protocol with Disney to prove that his machine is a suitable recipient of `Snow White'. This will mean certifying that the PC is currently running an authorised application program - MediaPlayer, DisneyPlayer, whatever - with its NCA properly loaded and shielded by curtained memory against debuggers or other tools that could be used to rip the content. The Disney server then sends encrypted data, with a key that Fritz will use to unseal it. Fritz makes the key available only to the authorised application and only so long as the environment remains `trustworthy'. For this purpose, `trustworthy' is defined by the security policy downloaded from a server under the control of the application owner. This means that Disney can decide to release its premium content only to a media player whose author agrees to enforce certain conditions. These might include restrictions on what hardware and software you use, or where in the world you're located. They can involve payment: Disney might insist, for example, that the application collect a dollar every time you view the movie. The application itself can be rented too. The possibilities seem to be limited only by the marketers' imagination.

5. What else can TC be used for?

TC can also be used to implement much stronger access controls on confidential documents. These are already available in a primitive form in Windows Server 2003, under the name of `Enterprise rights management' and people are experimenting with them.

One selling point is automatic document destruction. Following embarrassing email disclosures in the recent anti-trust case, Microsoft implemented a policy that all internal emails are destroyed after 6 months. TC will make this easily available to all corporates that use Microsoft platforms. (Think of how useful that would have been for Arthur Andersen during the Enron case.) It can also be used to ensure that company documents can only be read on company PCs, unless a suitably authorised person clears them for export. TC can also implement fancier controls: for example, if you send an email that causes embarrassment to your boss, he can broadcast a cancellation message that will cause it to be deleted wherever it's got to. You can also work across domains: for example, a company might specify that its legal correspondence only be seen by three named partners in its law firm and their secretaries. (A law firm might resist this because the other partners in the firm are jointly liable; there will be many interesting negotiations as people try to reduce traditional trust relationships to programmed rules.)

TC is also aimed at payment systems. One of the Microsoft visions is that much of the functionality now built on top of bank cards may move into software once the applications can be made tamper-resistant. This leads to a future in which we pay for books that we read, and music we listen to, at the rate of so many pennies per page or per minute. The broadband industry is pushing this vision; meanwhile some far-sighted people in the music industry are starting to get scared at the prospect of Microsoft charging a percentage on all their sales. Even if micropayments don't work out as a business model - and there are some persuasive arguments why they won't - there will be some sea-changes in online payment, with spillover effects for the user. If, in ten years' time, it's inconvenient to shop online with a credit card unless you use a TC platform, that will be tough on Mac and GNU/linux users.

The appeal of TC to government systems people is based on ERM being used to implement `mandatory access control' - making access control decisions independent of user wishes but based simply on their status. For example, an army might arrange that its soldiers can only create Word documents marked at `Confidential' or above, and that only a TC PC with a certificate issued by its own security agency can read such a document. That way, soldiers can't send documents to the press (or email home, either). Such rigidity doesn't work very well in large complex organisations like governments, as the access controls get in the way of people doing their work, but governments say they want it, and so no doubt they will have to learn the hard way. (Mandatory access control can be more useful for smaller organisations with more focused missions: for example, a cocaine smuggling ring can arrange that the spreadsheet with this month's shipment details can be read only by five named PCs, and only until the end of the month. Then the keys used to encrypt it will expire, and the Fritz chips on those five machines will never make them available to anybody at all, ever again.)

6. OK, so there will be winners and losers - Disney might win big, and some smartcard makers might go bust. But surely Microsoft and Intel are not investing nine figures just for charity? How will they make money out of it?

For Intel, which started the whole TC thing going, it was a defensive play. As they make most of their money from PC

microprocessors, and have most of the market, they can only grow their company by increasing the size of the market. They were determined that the PC will be the hub of the future home network. If entertainment is the killer application, and DRM is going to be the critical enabling technology, then the PC has to do DRM or risk being displaced in the home market.

Microsoft, who are now driving TC, were also motivated by the desire to bring entertainment within their empire. But they also stand to win big if TC becomes widespread. There are two reasons. The first, and less important, is that they will be able to cut down dramatically on software copying. `Making the Chinese pay for software' has been a big thing for Bill; with TC, he can tie each PC to its individual licenced copy of Office and Windows, and lock bad copies of Office out of the shiny new TC universe.

The second, and most important, benefit for Microsoft is that TC will dramatically increase the costs of switching away from Microsoft products (such as Office) to rival products (such as OpenOffice). For example, a law firm that wants to change from Office to OpenOffice right now merely has to install the software, train the staff and convert their existing files. In five years' time, once they have received TC-protected documents from perhaps a thousand different clients, they would have to get permission (in the form of signed digital certificates) from each of these clients in order to migrate their files to a new platform. The law firm won't in practice want to do this, so they will be much more tightly locked in, which will enable Microsoft to hike its prices.

Economists who have studied the software industry concluded that the value of a software business is about equal to the total costs of its customers switching out to the competition; both are equal to the net present value of future payments from the customers to the software vendor. This means that an incumbent in a maturing market, such as Microsoft with its Office product, can grow faster than the market only if it can find ways to lock in its customers more tightly. There are some ifs and buts that hedge this theory around, but the basic idea is well known to software industry executives. This explains Bill G's comment that `We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains'.

7. Where did the technical ideas come from?

The TC concept of booting a machine into a known state is implicit in early PCs where the BIOS was in ROM and there was no hard drive in which a virus could hide. The idea of a trusted bootstrap mechanism for modern machines seems to have first appeared in a paper by Bill Arbaugh, Dave Farber and Jonathan Smith, ``A Secure and Reliable Bootstrap Architecture'', in the proceedings of the IEEE Symposium on Security and Privacy (1997) pp 65-71. It led to a US patent: ``Secure and Reliable Bootstrap Architecture'', U.S. Patent No. 6,185,678, February 6th, 2001. Bill's thinking developed from work he did while working for the NSA on code signing in 1994, and originally applied to rebooting ATM switches across a network. The Microsoft folk have also applied for patent protection on the operating system aspects. (The patent texts are here and here.)

There may be quite a lot of prior art. Markus Kuhn wrote about the TrustNo1 Processor years ago, and the basic idea behind a trustworthy operating system - a `reference monitor' that supervises a computer's access control functions - goes back at least

to a paper written by James Anderson for the USAF in 1972. It has been a feature of US military secure systems thinking since then.

8. How is this related to the Pentium 3 serial number?

Intel started an earlier program in the mid-1990s that would have put the functionality of the Fritz chip inside the main PC processor, or the cache controller chip, by 2000. The Pentium serial number was a first step on the way. The adverse public reaction seems to have caused them to pause, set up a consortium with Microsoft and others, and seek safety in numbers. The consortium they set up, the Trusted Computer Platform Alliance (TCPA), was eventually incorporated and changed its name to TCG.

9. Why call the monitor chip a `Fritz' chip?

It was named in honour of Senator Fritz Hollings of South Carolina, who worked tirelessly in Congress to make TC a mandatory part of all consumer electronics. (Hollings' bill failed; he lost his chairmanship of the Senate Committee on Commerce, Science and Trasportation, and he's retiring in 2004. But the Empire will be back. For example, Microsoft is spending a fortune in Brussels promoting a draft Directive on IP enforcement which is seriously bad stuff.)

10. OK, so TC stops kids ripping off music and will help companies keep data confidential. It may help the Mafia too, unless the FBI get a back door, which I assume they will. But apart from pirates, industrial spies and activists, who has a problem with it?

A lot of companies stand to lose out directly, such as information security vendors. When it first launched TC as Palladium, Microsoft claimed that Palladium would stop spam, viruses and just about every other bad thing in cyberspace - if so, then the antivirus companies, the spammers, the spam-filter vendors, the firewall firms and the intrusion detection folk could all have their lunch stolen. That's now been toned down, but Bill Gates admits that Microsoft will pursue the computer security market aggressively: "Because it's a growth area, we're not being that coy with them about what we intend to do."

Meanwhile, the concerns about the effects on competition and innovation continue to grow. The problems for innovation are well explained in a recent New York Times column by the distinguished economist Hal Varian.

But there are much deeper problems. The fundamental issue is that whoever controls the TC infrastructure will acquire a huge amount of power. Having this single point of control is like making everyone use the same bank, or the same accountant, or the same lawyer. There are many ways in which this power could be abused.

11. How can TC be abused?

One of the worries is censorship. TC was designed from the start to support the centralised revocation of pirate bits. Pirate software won't run in the TC world as TC will make the registration process tamper-resistant. But what about pirated songs or videos? How do you stop someone recording a track - if necessary by putting microphones next the speakers of a TC machine, and ripping it into an MP3? The proposed solution is that protected content will contain digital watermarks, and lawful media players that detect a watermark won't play that song unless it comes with an appropriate digital certificate for that device. But what if someone hacks a Fritz chip and does a transaction that `lawfully' transfers ownership of the track? In that case, traitor tracing technology will be used to find out which PC the track was ripped from. Then two things will happen. First, the owner of that PC will be prosecuted. (That's the theory, at least; it probably won't work as the pirates will use hacked PCs.) Second, tracks that have been through that machine will be put on a blacklist, which all TC players will download from time to time.

Blacklists have uses beyond music copying. They can be used to screen all files that the application opens - by content, by the serial number of the application that created them, or by any other criteria that you can program. The proposed use for this is that if everyone in China uses the same copy of Office, you do not just stop this copy running on any machine that is TC-compliant; that would just motivate the Chinese to use normal PCs instead of TC PCs. You also cause every TC-compliant PC in the world to refuse to read files that have been created using this pirate program. This will put huge pressure on the Chinese. (The precedent is that when spammers started using Chinese accounts, many US ISPs simply blackholed China, which forced the government to crack down on spam.)

The potential for abuse extends far beyond commercial bullying and economic warfare into political censorship. I expect that it will proceed a step at a time. First, some well-intentioned police force will get an order against a pornographic picture of a child, or a manual on how to sabotage railroad signals. All TC-compliant PCs will delete, or perhaps report, these bad documents. Then a litigant in a libel or copyright case will get a civil court order against an offending document; perhaps the Scientologists will seek to blacklist the famous Fishman Affidavit. A dictator's secret police could punish the author of a dissident leaflet by deleting everything she ever created using that system - her new book, her tax return, even her kids' birthday cards - wherever it had ended up. In the West, a court might use confiscation doctrine to `blackhole' a machine that had been used to make a pornographic picture of a child. Once lawyers, policemen and judges realise the potential, the trickle will become a flood.

The modern age only started when Gutenberg invented movable type printing in Europe, which enabled information to be preserved and disseminated even if princes and bishops wanted to ban it. For example, when Wycliffe translated the Bible into English in 1380-1, the Lollard movement he started was suppressed easily; but when Tyndale translated the New Testament in 1524-5, he was able to print over 50,000 copies before they caught him and burned him at the stake. The old order in Europe collapsed, and the modern age began. Societies that tried to control information became uncompetitive, and with the collapse of the Soviet Union it seemed that democratic liberal capitalism had won. But now, TC has placed at risk the priceless inheritance that Gutenberg left us. Electronic books, once published, will be vulnerable; the courts can order them to be unpublished and the

TC infrastructure will do the dirty work.

The Soviet Union attempted to register and control all typewriters and fax machines. TC similarly attempts to register and control all computers. The problem is that everything is becoming computerised. We have absolutely no idea where ubiquitous content control mechanisms will lead us.

12. Scary stuff. But can't you just turn it off?

Sure - unless your system administrator configures your machine in such a way that TC is mandatory, you can always turn it off. You can then run your PC as before, and use insecure applications.

There is one small problem, though. If you turn TC off, Fritz won't hand out the keys you need to decrypt your files and run your bank account. Your TC-enabled apps won't work as well, or maybe at all. It will be like switching from Windows to Linux nowadays; you may have more freedom, but end up having less choice. If the TC apps are more attractive to most people, or are more profitable to the app vendors, you may end up simply having to use them - just as many people have to use Microsoft Word because all their friends and colleagues send them documents in Microsoft Word. By 2008, you may find that the costs of turning TC off are simply intolerable.

This has some interesting implications for national security. At a TCG symposium in Berlin, I put it this way: in 2010 President Clinton may have two red buttons on her desk - one that sends the missiles to China, and another that turns off all the PCs in China - and guess which the Chinese will fear the most? (At this point, a heckler from the audience said, `What about the button that turns off the PCs in Europe?') This may be an exaggeration, but it's only a slight one. Technology policy and power politics have been intertwined since the Roman empire, and prudent rulers cannot disregard the strategic implications of TC. It would be rather inconvenient for a government to have to switch all its systems from Windows to GNU/linux, and at the height of an international crisis.

13. So politics and economics are going to be significant here?

Exactly. The biggest profits in IT goods and services markets tend to go to companies that can establish platforms and control compatibility with them, so as to manage the markets in complementary products. A very topical example comes from computer printers. Since the Xerox N24 appeared in 1996, printer makers have been putting authentication chips in ink cartridges, so that printers can recognise third-party or refilled cartridges and refuse to work with them. Cartridge tying is now leading to trade conflict between the USA and Europe. In the USA, a court has granted Lexmark an injunction preventing the sale of cartridges with chips that interoperate with Lexmark's printers. Meanwhile, the European Commission has adopted a Directive on waste electrical and electronic equipment which will force member states to outlaw, by the end of 2007, the circumvention of EU

recycling rules by companies who design products with chips to ensure that they cannot be recycled.

This is not just a printer issue. Some mobile phone vendors use embedded authentication chips to check that the phone battery is a genuine part rather than a clone. The Sony Playstation 2 uses similar authentication to ensure that memory cartridges were made by Sony rather than by a low-price competitor. The Microsoft Xbox is no different. But up until now, everyone who wanted to engage in product tying had to come up with his own hardware technology. This could be cheap for hardware product vendors, but was too expensive for most software companies.

TC will enable application software vendors to engage in product tying and similar business strategies to their hearts' content. As the application vendor will control the security policy server, he can dictate the terms under which anyone else's software will be able to interoperate with his own. In the old days, software innovation was fast and furious because there were millions of PCs out there, with data in formats that were understood. So if you thought up a cool new way to manipulate address books, you could write an app that would deal with the half-dozen formats common in PCs, PDAs and phones, and you were in business: you had millions of potential clients. In the future, the owners of these formats will be very strongly tempted to lock them down using TC (`for your privacy') and charge third parties rental to access them. This will be bad for innovation. It's possible because the app policy server enforces arbitrary rules about which other applications will be allowed to use the files a TC app creates.

So a successful TC application will be worth much more money to the software company that controls it, as they can rent out access to their interfaces for whatever the market will bear. So most software developers will enable their applications for TC; and if Windows is the first operating system to support TC, it in turn will get a further competitive advantage over GNU/Linux and MacOS with the developer community.

14. But hang on, doesn't the law give people a right to reverse engineer interfaces for compatibility?

Yes, and this is very important to the functioning of IT goods and services markets; see Samuelson and Scotchmer, ``The Law and Economics of Reverse Engineering,'' Yale Law Journal, May 2002, 1575-1663. In Europe, the EU Software Directive allows EU companies to reverse engineer their competitors' products in order to produce compatible, competing products. But such laws in most cases just give you the right to try, not to succeed. Back when compatibility meant messing around with file formats, there was a real contest - when Word and Word Perfect were fighting for dominance, each tried to read the other's files and make it hard for the other to read its own. But with TC that game is over; without access to the keys, you've had it.

Locking competitors out of application file formats was one of the motivations for TC: see a post by Lucky Green, and go to his talk at Def Con to hear more. It's a tactic that's spreading beyond the computer world. Congress is getting upset at carmakers using data format lockout to stop their customers getting repairs done at independent dealers. And the Microsoft folk say they want TC everywhere, even in your watch. The economic consequences could be globally significant.

15. Can't TC be broken?

The early versions will be vulnerable to anyone with the tools and patience to crack the hardware (e.g., get clear data on the bus between the CPU and the Fritz chip). However, in a few years, the Fritz chip may disappear inside the main processor - let's call it the `Hexium' - and things will get a lot harder. Really serious, well funded opponents will still be able to crack it. But it's likely to go on getting more difficult and expensive.

Also, in many countries, cracking Fritz will be illegal. In the USA the Digital Millennium Copyright Act already does this, while in the EU we will have to deal with the EU Copyright Directive and (if it passes) the draft enforcement directive. (In some countries, the implementation of the Copyright Directive already makes cryptography research technically illegal.)

Also, in many products, compatibility control is already being mixed quite deliberately with copyright control. The Sony Playstation's authentication chips also contain the encryption algorithm for DVD, so that reverse engineers can be accused of circumventing a copyright protection mechanism and hounded under the Digital Millennium Copyright Act. The situation is likely to be messy - and that will favour large firms with big legal budgets.

16. What's the overall economic effect likely to be?

The content industries may gain a bit from cutting music copying - expect Sir Michael Jagger to get very slightly richer. But I expect the most significant economic effect will be to strengthen the position of incumbents in information goods and services markets at the expense of new entrants. This may mean a rise in the market cap of firms like Intel, Microsoft and IBM - but at the expense of innovation and growth generally. Eric von Hippel documents how most of the innovations that spur economic growth are not anticipated by the manufacturers of the platforms on which they are based; and technological change in the IT goods and services markets is usually cumulative. Giving incumbents new ways to make life harder for people trying to develop novel uses for their products is a bad idea.

By centralising economic power, TC will favour large companies over small ones; and TC apps will enable large companies to capture more of the spillover from their economic activities, as with the car companies forcing car-owners to have their maintenance done at authorised dealerships. As most employment growth occurs in the small to medium business sector, this could have consequences for unemployment.

There may also be distinct regional effects. For example, many years of government sponsorship have made Europe's smartcard industry strong, at the cost of crowding out other technological innovation in the region. Senior industry people to whom I have spoken anticipate that once the second phase of TC puts the Fritz functionality in the main processor, this will hammer smartcard sales. Senior TC company people have admitted to me that displacing smartcards from the authentication token market is one of

their business goals. Many of the functions that smartcard makers want you to do with a card will instead be done in the Fritz chips of your laptop, your PDA and your mobile phone. If this industry is killed off by TC, Europe could be a significant net loser. Other large sections of the information security industry may also become casualties.

17. Who else will lose?

There will be many places where existing business processes break down in ways that allow copyright owners to extract new rents. For example, I recently applied for planning permission to turn some agricultural land that we own into garden; to do this, we needed to supply our local government with six copies of a 1:1250 map of the field. In the old days, everyone just got a map from the local library and photocopied it. Now, the maps are on a server in the library, with copyright control, and you can get a maximum of four copies of any one sheet. For an individual, that's easy enough to circumvent: buy four copies today and send a friend along tomorrow for the extra two. But businesses that use a lot of maps will end up paying more money to the map companies. This may be a small problem; mutiply it a thousandfold to get some idea of the effect on the overall economy. The net transfers of income and wealth are likely, once more, to be from small firms to large and from new firms to old.

One well-known UK lawyer said that copyright law is only tolerated because it is not enforced against the vast majority of petty infringers. And there will be some particularly high-profile hard-luck cases. I expect that copyright regulations due out later this year in Britain will deprive the blind of the fair-use right to use their screen scraper software to read e-books. Normally, a bureaucratic stupidity like this might not matter much, as people would just ignore it, and the police would not be idiotic enough to prosecute anybody. But if the copyright regulations are enforced by hardware protection mechanisms that are impractical to break, then the blind may lose out seriously. (There are many other marginal groups under similar threat.)

18. Ugh. What else?

TC will undermine the General Public License (GPL), under which many free and open source software products are distributed. The GPL is designed to prevent the fruits of communal voluntary labour being hijacked by private companies for profit. Anyone can use and modify software distributed under this licence, but if you distribute a modified copy, you must make it available to the world, together with the source code so that other people can make subsequent modifications of their own.

IBM and HP have apparently started work on a TC-enhanced version of GNU/linux. This will involve tidying up the code and removing a number of features. To get an evaluation certificate acceptable to TCG, the sponsor will then have to submit the pruned code to an evaluation lab, together with a mass of documentation showing why various known attacks on the code don't work. (The evaluation is at level EAL3 - expensive enough to keep out the free software community, yet lax enough for most commercial software vendors to have a chance to get their lousy code through.) Although the modified program will be covered by the GPL, and the source code will be free to everyone, it will not work in the TC ecosystem unless you have a certificate for it

that is specific to the Fritz chip on your own machine. That is what will cost you money (if not at first, then eventually).

You will still be free to make modifications to the modified code, but you won't be able to get a certificate that gets you into the shiny new TC world. Something similar happens with the linux supplied by Sony for the Playstation 2; the console's copy protection mechanisms prevent you from running an altered binary, and from using a number of the hardware features. Even if a philanthropist does a not-for-profit secure GNU/linux, the resulting product would not really be a GPL version of a TC operating system, but a proprietary operating system that the philanthropist could give away free. (There is still the question of who would pay for the user certificates.)

People believed that the GPL made it impossible for a company to come along and steal code that was the result of community effort. This helped make people willing to give up their spare time to write free software for the communal benefit. But TC changes that. Once the majority of PCs on the market are TC-enabled, the GPL won't work as intended. The benefit for Microsoft is not that this will destroy free software directly. The point is this: once people realise that even GPL'led software can be hijacked for commercial purposes, idealistic young programmers will be much less motivated to write free software.

19. I can see that some people will get upset about this.

And there are many other political issues - the transparency of processing of personal data enshrined in the EU data protection directive; the sovereignty issue of whether copyright regulations will be written by national governments, as at present, or an application developer in Portland or Redmond; whether TC will be used by Microsoft as a means of killing off Apache; and whether people will be comfortable about the idea of having their PCs operated, in effect, under remote control - control that could be usurped by courts or by government agencies without their knowledge.

20. But hang on, isn't TC illegal under antitrust law?

In the USA, maybe not. Intel has honed a `platform leadership' strategy, in which they lead industry efforts to develop technologies that will make the PC more useful, such as the PCI bus and USB. Their modus operandi is described in a book by Gawer and Cusumano. Intel sets up a consortium to share the development of the technology, has the founder members put some patents into the pot, publishes a standard, gets some momentum behind it, then licenses it to the industry on the condition that licensees in turn cross-license any interfering patents of their own, at zero cost, to all consortium members.

The positive view of this strategy was that Intel grew the overall market for PCs; the dark side was that they prevented any competitor achieving a dominant position in any technology that might have threatened their dominance of the PC hardware. Thus, Intel could not afford for IBM's microchannel bus to prevail, not just as a competing nexus of the PC platform but also because IBM had no interest in providing the bandwidth needed for the PC to compete with high-end systems. The effect in

strategic terms is somewhat similar to the old Roman practice of demolishing all dwellings and cutting down all trees close to their roads or their castles. No competing structure may be allowed near Intel's platform; it must all be levelled into a commons. But a nice, orderly, well-regulated commons: interfaces should be `open but not free'.

This consortium approach has evolved into a highly effective way of skirting antitrust law. So far, the FTC and the Department of Justice do not seem to have been worried about such consortia - so long as the standards are open and accessible to all companies. They may need to become slightly more sophisticated.

As for Europe, the law does explicitly cover consortia, and is being tightened up. There was a conference on TC in Berlin, organised by the German ministry for economics and labour, which heard speakers from the pro- and anti-TC camps state their cases. If you read German, there is a very thorough analysis of the competition policy aspects by Professor Christian Koenig; the executive summary is that TC appears to break European competition law on a number of grounds. Standards groups are allowed as an exemption to cartel law only if they're non-binding, open and non-discriminatory. TCG isn't. It discriminates against non-members; its high membership fees make it hard for small businesses to join; and its use of paid rather than free licensing discriminates against free software. There are also many issues with market power and market interdependence. The EU is about to find Microsoft guilty of trying to extend its monopoly in PCs to servers by keeping interfaces obscure. If interfaces can be locked down by TC mechanisms, that will be worse. TC may also enable Microsoft to extend its monopoly in operating systems to the provision of online music services, or to mobile phone software.

However, law is one thing, and enforcement another. By the end of 2003, the EU should have convicted Microsoft of anti-competitive behaviour over Netscape and over server interfaces. This judgement will come too late to restore Netscape to life or create competition in the browser market. By the time the EU gets round to convicting Microsoft over TC, it will be 2008. By then our society may be addicted to TC, and it may not be politically possible to do anything effective.

21. When is TC going to hit the streets?

It has. The version 1.0 specification was published in 2000. Atmel is already selling a Fritz chip, and you have been able to buy it installed in the IBM Thinkpad series of laptops since May 2002. Some of the existing features in Windows XP and the X-Box are TC features: for example, if you change your PC configuration more than a little, you have to re-register all your software with Redmond. Also, since Windows 2000, Microsoft has been working on certifying all device drivers: if you try to load an unsigned driver, XP will complain. The Enterprise Rights Management stuff is shipping with Windows Server 2003. There is also growing US government interest in the technical standardisation process. TC developers' kits will be available in October 2003, or so we're told. The train is rolling.

22. What's TORA BORA?

This seems to have been an internal Microsoft joke: see the Palladium announcement. The idea is that `Trusted Operating Root Architecture' (Palladium) will stop the `Break Once Run Anywhere' attack, by which they mean that pirated content, once unprotected, can be posted to the net and used by anyone. It will do so by traitor tracing - the technology of ubiquitous censorship.

They seem to have realised since then that this joke might just be in bad taste. At a talk on traitor tracing I attended on the 10th July 2002 at Microsoft Research, the slogan had changed to `BORE-resistance', where BORE standards for `Break Once Run Everywhere'. (By the way, the speaker there described copyright watermarking as `content screening', a term that used to refer to stopping minors seeing pornography: the PR machine is obviously twitching! He also told us that it would not work unless everyone used a trusted operating system. When I asked him whether this meant getting rid of linux he replied that linux users would have to be made to use content screening.)

23. But isn't PC security a good thing?

The question is: security for whom? You might prefer not to have to worry about viruses, but TC won't fix that: viruses exploit the way software applications (such as Microsoft Office and Outlook) use scripting. You might get annoyed by spam, but that won't get fixed either. (Microsoft claimed that it will be fixed, by filtering out all unsigned messages - but you can already configure mail clients to filter out mail from people you don't know and putting it in a folder you scan briefly once a day.) You might be worried about privacy, but TC won't fix that; almost all privacy violations result from the abuse of authorised access, and TC will increase the incentives for companies to collect and trade personal data on you. The medical insurance company that requires you to consent to your data being shared with your employer and with anyone else they can sell it to, isn't going to stop just because their PCs are now officially `secure'. On the contrary, they are likely to sell it even more widely once computers are called `trusted computers'. Economists call this a `social choice trap'. Making something slightly less dangerous, or making it appear less dangerous, often causes people to use it more, or use it carelessly, so that the overall harm increases. The classic example is that Volvo drivers have more accidents.

A mildly charitable view of TC was put forward by the late Roger Needham who directed Microsoft's research in Europe: there are some applications in which you want to constrain the user's actions. For example, you want to stop people fiddling with the odometer on a car before they sell it. Similarly, if you want to do DRM on a PC then you need to treat the user as the enemy.

Seen in these terms, TC does not so much provide security for the user as for the PC vendor, the software supplier, and the content industry. They do not add value for the user, but destroy it. They constrain what you can do with your PC in order to enable application and service vendors to extract more money from you. This is the classic definition of an exploitative cartel - an industry agreement that changes the terms of trade so as to diminish consumer surplus.

24. So why is this called `Trusted Computing'? I don't see why I should trust it at all!

It's almost an in-joke. In the US Department of Defense, a `trusted system or component' is defined as `one which can break the security policy'. This might seem counter-intuitive at first, but just stop to think about it. The mail guard or firewall that stands between a Secret and a Top Secret system can - if it fails - break the security policy that mail should only ever flow from Secret to Top Secret, but never in the other direction. It is therefore trusted to enforce the information flow policy.

Or take a civilian example: suppose you trust your doctor to keep your medical records private. This means that he has access to your records, so he could leak them to the press if he were careless or malicious. You don't trust me to keep your medical records, because I don't have them; regardless of whether I like you or hate you, I can't do anything to affect your policy that your medical records should be confidential. Your doctor can, though; and the fact that he is in a position to harm you is really what is meant (at a system level) when you say that you trust him. You may have a warm feeling about him, or you may just have to trust him because he is the only doctor on the island where you live; no matter, the DoD definition strips away these fuzzy, emotional aspects of `trust' (that can confuse people).

During the late 1990s, as people debated government control over cryptography, Al Gore proposed a `Trusted Third Party' - a service that would keep a copy of your decryption key safe, just in case you (or the FBI, or the NSA) ever needed it. The name was derided as the sort of marketing exercise that saw the Russian colony of East Germany called the `German Democratic Republic'. But it really does chime with DoD thinking. A Trusted Third Party is a third party that can break your security policy.

25. So a `Trusted Computer' is a computer that can break my security?

That's a polite way of putting it.

Ross Anderson

- See also the Economics and Security Resource Page which gives a lot of background to the issues raised here.
- Here are translations into German, Spanish, Italian, Dutch, Chinese, Norwegian, Swedish, Finnish, Hungarian, Greek, Hebrew and French.

Further reading (roughly in chronological order from July 2002 onwards)

- Here is a link to the first online version of this FAQ, version 0.2, and a link to version 1.0, which was online from July 2002 to August 2003.
- Initial publicity, from late 2002, included articles on ZDNet, the BBC, Internetnews, PBS, O'Reilly, , Salon.com, and

Extremetech. Larry Lessig's comments in a seminar at Harvard are also relevant. There was a story allegedly by a former Microsoft employee about how Palladium was launched, and two blog entries (here and here) by Seth Schoen on a Palladium briefing my MS to EFF. The European Union started to take note, and the fuss we managed to stir up depressed PC market analysts in Australia. There was a speech by Bush's CyberCzar Richard Clark praising TCPA (see p 12); at the same conference, Intel CEO Craig Barrett said that government should let industry do DRM rather than mandating a solution (p 58). That may make some sense out of this story story about Intel opposing the Hollings bill, at the same time as they were pushing TCPA. There is also an email from Bill.

- Many TC issues had already been anticipated by Richard Stallman in his famous article The Right to Read.
- TC inventor Bill Arbaugh had second thoughts, and made some proposals about how TC could be changed to mitigate its worst effects, for example by letting users load their own trusted root certificates or turn the Fritz chip off entirely.
- Lucky Green was also an early TC insider, who later repented. The slides from his Def Con talk are now available at his site.
- In this exchange from the cryptography list, Peter Biddle, technical director of TC within Microsoft, explains some of the changes between TC version 1.0 and 1.2. (Executive summary: in TC 1.0, a machine that was running a trusted process and that started an untrusted process was supposed to close down the trusted process and clear memory. This would have made TC unusable in practice with modern ways of working. It was therefore necessary to expand the spec and get Intel to bring in curtained memory, so that trusted and untrusted apps could run simultaneously on the same PC.
- A post from John Gilmore to the cypherpunks list, and further commentary by Adam Back, Seth Schoen and others.
- An opinion from Bruce Schneier; some controversy stirred up by Bill Thompson, who really does appear to believe that the world of trusted computing will be spam- and virus-free, and allow you to exercise your fair use rights; and some reaction ...
- Microsoft released a Palladium FAQ in August 2002 in which they backed off from their initial claims that Palladium will stop spam and viruses.
- In September 2002, Intel announced LaGrande. This chip will be the successor to the Pentium 4 and will support the `curtained memory' mode needed for TC version 1.2 et seq. It was named after a town in Eastern Oregon. The initial reaction was hostile. Civil liberties groups started to wake up; there appeared a web page at EPIC, for example.
- October 2002 saw an article in Linux devices on the problems TCPA may cause for embedded systems, and an article in German in c't magazine. But the highlight of the month was that Richard Stallman denounced TC. Two French translations appeared overnight, here and here. France started to pay attention.
- On the 7th November, there was a public debate on TCPA between the suits (Microsoft, HP, Infineon) and the geeks (Alan Cox and me). We got TV coverage (now unfortunately pulled from the web by Channel 4), and a shorter debate in Cambridge the following day as one of our regular security group meetings.
- In November, TC also made its way into science fiction - in the latest short story by Cory Doctorow.
- French interest continued to grow through January 2003, with this article in Le Monde.
- The main event in January, though, was that Microsoft's TC offering, Palladium, got renamed. The first rule of spin-

doctoring is that when you have a problem on your hands, rename it! So Palladium is now officially knows as NGSCB - for `Next Generation Secure Computing Base'.

- In February 2003, Microsoft announced that it would ship many of the application-level TC features with Windows Server 2003 later in the year, including Rights Management mechanisms that will allow you make an email evaporate on the recipient's machine after 30 days. This is still software-based; it won't work unless the recipient also has a compatible client or server from Microsoft, and can be defeated by patching the software (though this may be illegal in the USA). However, it will start getting this lock-in functionality out into the marketplace and pave the way for full TC later. Comment in places like Geek News, VNUnet and Zdnet has been mixed but is still muted.
- In April, distinguished cryptographers Whit Diffie and Ron Rivest denounced TC at the RSA conference.
- In May, TCPA was relaunched as TCG (the Trusted Computing Group, which announced that it's working on version 1.2 of the Fritz chip, with systems shipping late 2004 or early 2005, and that the scope of TC is to be extended from PCs to PDAs and mobile phones. See the story in EE Times, and the followup; and read about how Chairman Bill struck back at the Windows Hardware Engineering Conference when NGSCB was finally unveiled.
- In July 2003, The Times reported various abuses by printer manufacturers, including setting their toner cartridges to show `empty' when only about two-thirds of the ink has been used up. This is the sort of business model that will become pervasive throughout the IT world if TC succeeds, and the devices that you can use to unlock printer cartridges that still have ink in them will be outlawed in Europe by the enforcement directive - as will technical workarounds for TC mechanisms that undermine competition and exploit consumers.
- Also in July,Bill Gates admitted to the New York Times that Microsoft would pursue the computer security market aggressively: "Because it's a growth area, we're not being that coy with them about what we intend to do." He stressed that the company's biggest bet is on the next version of Windows - code name Longhorn - in other words, the technology formerly known as Palladium and now known as NGSCB. You have been warned.
- In September, we saw the first Intel presentations of LaGrande Technology, reported here and here.

I spoke in public about TC on the 2nd July in Berlin at the "Trusted Computing Group" Symposium; then in Brussels on the 8th July at an event organised by DG Infosoc; then on the 14th July at PODC; then at the Helsinki IPR workshop in August. I'm sure there will be many more. Meanwhile, a version of my economic study of TC has appeared a special issue of Upgrade that deals with IP and computing issues (June 2003). A longer version of the paper deals in detail with many of the issues raised here about competition policy.

Ross Anderson

Cambridge, England
