EFF Comments on LT Policy on Owner/User Choice and Control 0.8

Seth Schoen
Electronic Frontier Foundation

December 31, 2003

Abstract

Trusted Computing technologies like LaGrande Technology have the potential to be abused to diminish computer owners' choice and control even when deployed on an opt-in basis. They may also be used to diminish privacy by disclosing both PII and non-PII information. The present Intel policy sets forth useful best practices, but cannot prevent abuses of LT.

1 Introduction

The Electronic Frontier Foundation (EFF) is pleased to submit these comments on the LaGrande Technology Policy on Owner/User Choice and Control, version 0.8 ("the Policy").[1]

Our general views on trusted computing are described in "Trusted Computing: Promise and Risk", which refers to LT features in general terms along with other trusted computing technologies. There, we focus on the question of why computer owners would desire an attestation feature and suggest that more attention should be paid to conflicts of interest between computer owners and recipients of attestations. In the long run, rational computer owners might prefer that the PC architecture not include an attestation capability that is easy to use against them.[2]

Broadly speaking, the ways in which LT may undermine "owner choice and control" have to do with giving new leverage to third parties who want to coerce computer owners into making particular choices. Among other things, LT changes the balance of power between consumers and service providers and may let market-dominant publishers and service providers more effectively use their market power to diminish consumer choice.

[1] We thank Intel for briefing us on LT technology and privacy issues on several occasions and for its willingness to discuss these questions, and we look forward to future conversations with TC technology developers.

[2] See "Trusted Computing: Promise and Risk", available from EFF at http://www.eff.org/Infra/trusted_computing/20031001_tc.php.

2 Computer owner control is compromised by attestation

Even today, some entities want to influence end-users' software choices by punishing the use of disapproved software (that is, by deliberately increasing the costs of using software alternatives). In the face of this, computer owners routinely benefit because

- third parties can't know for certain the identity of code on the owner's machine (because they have to guess);
- third parties can't punish the computer owner for not using "approved" software (because they don't know); and
- third parties can't punish the computer owner for not disclosing the identity of code running on the owner's machine (because the owner has no ability to disclose it in a convincing way)

In effect, the inability to prove code identity frees the computer owner from the possibility of extortion, just as the secret ballot precludes threats or promises that might influence a voter's electoral choices.[3]

If computer owners had a way to prove the identity of code they were running, they could be punished for running "disapproved" code or for concealing their choice of operating environments. (Only features that are at least potentially visible can be a basis for discrimination.) There is reason to believe that current attestation schemes are detrimental to consumer welfare and that an environment in which they were ubiquitous and ubiquitously used would tend to disadvantage consumers, by forcing consumers to give up choice and control they enjoy today. An early TCPA white paper described this very ubiquity as a goal of trusted computing:

> [A]chieving ubiquity in trusted computing is no exception. It implies that at some point, all PCs will have this ability to be trusted to some minimum level – a level that is higher than possible today – and to achieve this level of trust in the same way.
>
> The objective of the TCPA is to make trust just as much a part of the PC platform as memory and graphics. Every PC will have hardware-based trust, and every piece of software on the system will be able to use it.[4]

[3] "It is interesting that political democracy itself relies on a particular communication system in which the transmittal of authentic information is precluded: the mandatory secret ballot is a scheme to deny the voter any means of proving which way he voted. Being stripped of his power to prove how he voted, he is stripped of his power to be intimidated. Powerless to prove whether or not he complied with a threat, he knows – and so do those who would threaten him – that any punishment would be unrelated to the way he actually voted." Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960).

[4] Trusted Computing Platform Alliance, "Building a Foundation of Trust in the PC: The Trusted Computing Platform Alliance", January 2000.

The Policy suggests that, despite the ubiquity of attestation capabilities, they will need to be provided on an opt-in basis. But opt-in alone can't repair these disadvantages, because people who fail to opt in may actually be concretely disadvantage relative to the status quo. For instance, a person who uses a minority OS or application (or an "aftermarket" application such as an independent implementation of an instant-messaging protocol) may be locked out of on-line services, *even those that are currently available.* This is a consequence of *other people's* decision to opt in, and not of anything the minority OS or application user did, chose, or opted for.

In fact, TCPA previously suggested that this was a desirable use of attestation by publishers and service providers:

> For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform is trustworthy. The service provider's platform (the "challenger") queries the remote platform. [...] When it receives a query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. [...] If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy. If so, the challenger, in this case the service provider, can then deliver the content. [... TCPA] lets the challenger make the final decision regarding the trustworthiness of the platform.[5]

Computer owners are likely to have a different view of the desirability of this scenario, since it explicitly reduces their power to choose what software they will use by creating new third-party leverage over that choice.

The Policy emphasizes that computer owners and users should be able to opt in to LT features; for example, it provides that the

> PC owner must have a choice whether they want to "opt-in" to LT protections, and, to the degree feasible, maintain control over the various functions.

But the Policy goes on to consider owner control only as the ability to turn LT and particular LT features on and off; no other form of owner control is explicitly considered. Clearly, the ability to turn systems and features on and off is far from the only kind of control that a device owner might logically exercise. No one would suggest that a computer purchaser enjoys reasonable "control" over her computer merely because she can decide whether to turn it on and off! Instead, her ability to install, delete, upgrade, or downgrade software, to add and remove hardware, to run firewall software, debuggers, and emulators, to create backups, and to perform many other tasks are considered a normal and customary part of what we understand as "control" over a personal computer. The control of the platform itself plainly does not stop at the power

[5] *Ibid.*

switch, for the PC is not a sealed appliance with fixed functions whose user merely turns it on and off. In the same way, the idea of "control" of LT features is impoverished when it is applied solely to the power to opt-in to using them. This essentially binary choice forecloses other important possibilities.[6]

3 Attestation will harm interoperability

Attempts to block software interoperability already occur, but their efficacy is constrained by the properties of the current PC platform. The traditional legal right in many jurisdictions to create interoperable software and products is constantly exercised by technology developers – to the substantial benefit of competition and of consumers.[7]

Many vendors continue to express the view that they may, for business reasons, prevent interoperability through legal or technical measures. Regardless of their aspirations, they ultimately seem to lack the technical means to enforce their vision of limited interoperability cost-effectively on the PC platform. Ubiquitous attestation could give them their first opportunity to implement their radical vision.

PC customers are hardly clamoring for more and better lock-in, or for a more lock-in-friendly platform, but assuring software interoperability is already difficult enough in the present environment. The PC platform should not be altered in any way that subjects the interoperability of systems to the whims of publishers.

[6] For instance, "Trusted Computing: Promise and Risk" refers to the prospect of compter owners' control over the *content* of attestations, not merely over whether attestations are to be provided. Letting owner determine the content of attestations is a more concrete and substantial form of control than merely letting them decide whether to offer attestations. The difference between a per-transaction binary decision "attest!" or "do not attest!" and a per-transaction decision "attest to the following PCR values" is substantial. The Policy's principle that owners should exercise control "to the degree feasible" does not clearly resolve whether owners should determine the content of attestations, because of possible differences of opinion about whether this is "feasible". For example, LT users in a closed corporate environment may well consider it "feasible" where commercial service providers might deplore the prospect. Even without considering proposals like Owner Override, major questions about key management remain. We discuss below, for example, some of the privacy concerns Intel has previously recognized with respect to the linkability of transactions. As Intel and other TCG members are aware, architectural decisions related to mitigating privacy concerns present complexities that cannot be dismissed as a simple matter of "opt-in" and "opt-out".

[7] The U.S., E.U., and many European jurisdictions have all adopted explicit protections for the reverse engineering of computer software to create new interoperable products. For instance, the U.S. Congress specifically sought to preserve the results of the past decade's pro-reverse engineering court decisions – many of them related to the reverse engineering of video games and video game console systems – in order to protect competition and innovation; the U.S. Senate sought "to ensure that the effect of current [reverse engineering] case law [...] is not changed [...] for certain acts of identification and analysis done in respect of computer programs. See, *Sega Enterprises Ltd. v Accolade, Inc.*, 977 F.2d 1510, 24 U.S.P.Q.2d 1561 (9th Cir. 1992.). The purpose of this [protection] is to foster competition and innovation in the computer and software industry." The policy considerations supporting reverse engineering for software interoperability are discussed at length by legal commentators and will not be rehearsed here.

A use of an LT-like architecture to limit software interoperability is depicted in Figure 1.[8]

4 Computer owner privacy may also be compromised by attestation

We will consider three ways in which computer owners' and users' privacy may be compromised by LT and systems based on LT. In two of the three cases, personally-identifiable information (PII) may be disclosed.

4.1 Disclosure of PII through LT: linking transactions

Linkability of transactions is a major category of PII-related privacy concern – for example, it's the basis for all privacy concerns about cookie support in web browsers.[9]

The original TCPA attestation scheme used third parties as pseudonymizing proxies to protect privacy. But since an attestation recipient could choose which proxies it would trust, and could choose to trust only those proxies that did not adequately protect privacy, the real privacy benefit of this system is dubious.

TCG members, including Intel, subsequently presented to us the Direct Anonymous Attestation (DAA) technology as a privacy-enhancing alternative to the earlier "privacy CA" or "trusted third party" proposal.[10] In DAA, an attestation is made directly to the party receiving it in a way that is nonetheless not necessarily linkable to other attestations.

DAA is a theoretical improvement over privacy CAs but suffers from a similar problem: the linkability characteristics of transactions are partly subject to the choices made by the recipients of attestations. If recipients want to link transactions, they can do so.[11] DAA appears to have the advantage that end-

[8] This diagram and the super-spyware diagram in Figure 2 are extracted from "How to Abuse Trusted Computing", an unpublished set of presentation slides on problematic uses of attestation. These slides are available from EFF upon request and should be published in the near future.

[9] See Netscape Communications Corporation, "Persistent Client State HTTP Cookies", available at http://wp.netscape.com/newsref/std/cookie_spec.html (attempting to forbid cookies to be shared with sites that did not originally produce them: "Only hosts within the specified domain can set a cookie for a domain and domains must have at least two (2) or three (3) periods in them"); note that the anti-linkability countermeasure initially specified by Netscape turned out to be inadequate to protect privacy and led to substantial, ongoing concern about the privacy implications of cookies. One privacy problem that Netscape did not initially address is that even transactions *with a single site* have linkability concerns, because users may want to have several pseudonyms or simply not disclose details of their reading or purchasing patterns.

[10] Our understanding of DAA's privacy implications is informed by the Trusted Computing Group presentation "TCG and Privacy: Direct Anonymous Attestation", dated August 18, 2003. We do not know whether this presentation has been published. "Building a Foundation of Trust in the PC" appears to use the older term "AAWS" for a privacy CA.

[11] We refer to the "Named Base" DAA model, where two attestations can be determined to have been made by the same TPM when they are made using the same Named Base. As

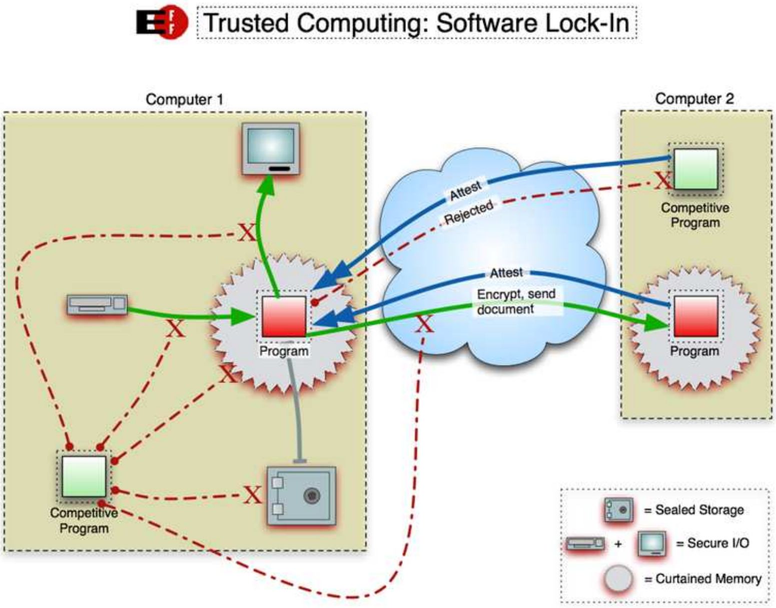


Figure 1: A program uses attestation to control interoperability (from "How to Abuse Trusted Computing".

users can deduce when transactions are potentially linkable[12], but many end-users engage in on-line activities that may compromise privacy *even when they have been warned* that their privacy is threatened.

As we understand it, this means that privacy protections against linkability in DAA are not substantially better than in the privacy CA scheme: attestation recipients determine whether to insist on linkability, and then end-users decide whether or not to accept this condition.[13] DAA does, however, add useful *transparency* by revealing which transactions could in principle be linkable.

4.2 Surreptitious disclosure of PII by LT-enabled applications

Even if LT itself tries to avoid disclosing PII, software built using LT might disclose PII in ways that can presently be blocked or detected.

Computer users want to detect and disable spyware; fortunately, they are generally able to do so today. A wide variety of anti-spyware programs is becoming available, and the availability of anti-spyware software may in time parallel the availability of anti-virus software. Like anti-virus researchers, anti-spyware researchers use reverse engineering techniques to see how spyware programs work and to develop techniques for detecting them and for removing them or blocking their functionality. Despite the prospect of an "arms race" between spyware and anti-spyware programmers (akin to the familiar "arms race" between virus and anti-virus programmers), the current PC computing environment at least permits anti-spyware developers to produce effective detection measures and countermeasures. Spyware cannot readily conceal its presence or its transmissions of PII from a knowledgeable researcher.

LT and operating systems built on LT could change this situation in two ways. First, LT could make it qualitatively harder to tell whether a program is a spyware program or what kind of information it is disclosing. Second, LT could make it qualitatively harder to block spyware functionality without losing other software functionality. Both of these possibilities depend on spyware developers

a result, multiple attestation recipients using the same Named Base for their transaction, or the same recipient using the same Named Base for multiple transactions, can determine whether the transactions were made by a single TPM. Attestation recipients who want to link transactions can thus deliberately choose to use a single Named Base, eliminating privacy protections at the supposed cost of incurring public displeasure.

[12] "TCG and Privacy" says: "Privacy groups can detect that verifiers are using the same name"; presumably the privacy groups would then warn consumers that their transactions could be linked.

[13] "TCG and Privacy" appears to recognize that users might not have much bargaining power to protect their privacy: "User can choose not to use his TPM with different verifiers that are using the same name. Yes, but..." This is qualitatively different from the linkability properties of HTTP cookies, where an end-user can create an unlimited number of intrinsically unlinkable personae, even if all the websites in the world openly collude to try to link them. This difference follows from the fact that a TCG TPM contains a limited quantity of pre-loaded uniqueness and that, as "TCG and Privacy" recognizes, platform owners may try to attack the TPM to extract this uniqueness. It remains unclear to us whether it is desirable to deploy TPMs that give their owners a motive for attacking them.

producing a new generation of spyware programs that specifically rely on LT platform features.

We have described this behavior as “super-spyware”, and one model of such hidden spyware functionality is depicted in Figure 2.

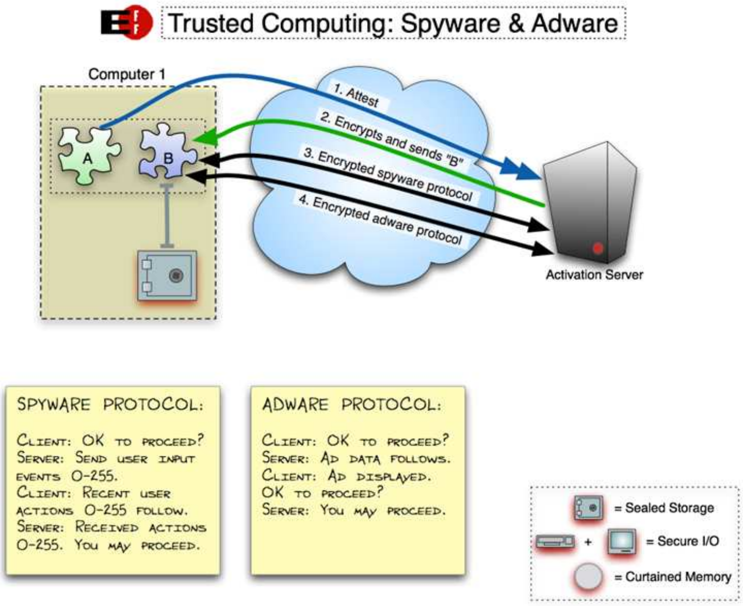
Here, a program “phones home” and uses attestation to establish an encrypted and authenticated channel to its original developer (secured with a session key that is guaranteed to be unavailable to all other software). The program transmits various PII over this channel at the request of the original spyware developer. The presence of the channel is not itself secret, but the channel achieves both confidentiality and authentication against attacks from the computer owner and other software (such as anti-virus or anti-spyware software). If the channel is disrupted, the program can deliberately shut down or malfunction to punish the computer owner for blocking the channel. Thus, the computer owner knows only that some possible transmission of sensitive information is taking place, but not specifically what information – and the flow of such information can’t be blocked without losing other functionality. (None of this would be possible in the current PC environment without attestation, because no session key could be exchanged in a way that would be secure against the computer owner; thus, the computer owner could successfully attack both the confidentiality and integrity of the spyware program’s conversations. Of course, this is precisely what anti-spyware researchers have of late been learning to do!)

Super-spyware need not arouse suspicion by constantly phoning home. Instead, it can store sensitive PII in sealed storage and disclose it only at rare intervals (under the guise, for example, of checking for software updates, or DRM or product activation license renewals). For example, a privacy-invading program could record all user interactions, keep that data in sealed storage, compress it, and leak it over an encrypted channel a few kilobits at a time. Since the program can be protected against reverse engineering by LT platform features, this functionality might be extremely difficult to discover. Platforms that are good at keeping secrets from their owners create risks that are not easily mitigated.

4.3 Disclosure of non-PII sensitive information

The routine automated disclosure of code identity can also be seen as a privacy problem, even though code identity is not usually personally identifiable. The creation of a technology to disclose this information may thus threaten privacy interests.[14]

[14] Andrew Odlyzko suggests that consumers may view the disclosure of any information about them as having privacy implications so long as it permits price discrimination, even if it is general non-personally-identifiable information. Odlyzko does not necessarily think this is a bad thing, but observes considerable consumer backlash against price discrimination. See Andrew Odlyzko, “Privacy, Economics, and Price Discrimination on the Internet”, available at http://www.dtc.umn.edu/ odlyzko/doc/privacy.economics.pdf. Perhaps consumers’ reasons for feeling protective of such information are substantially financial. Whereas the disclosure of sensitive personally identifiable information might expose people to social stigma, or make


Trusted Computing: Spyware & Adware
Computer 1
A
B
1. Attest
2. Encrypts and sends "B"
3. Encrypted spyware protocol
4. Encrypted adware protocol
Activation Server
= Sealed Storage
+
= Secure I/O
= Curtained Memory

SPYWARE PROTOCOL:

CLIENT: OK TO PROCEED?
SERVER: SEND USER INPUT EVENTS 0-255.
CLIENT: RECENT USER ACTIONS 0-255 FOLLOW.
SERVER: RECEIVED ACTIONS 0-255. YOU MAY PROCEED.

ADWARE PROTOCOL:

CLIENT: OK TO PROCEED?
SERVER: AD DATA FOLLOWS.
CLIENT: AD DISPLAYED. OK TO PROCEED?
SERVER: YOU MAY PROCEED.

Figure 2: A spyware program uses attestation to conceal PII as it "phones home" (from "How to Abuse Trusted Computing").

Being able to say – and thus being routinely asked to say – what sort of computer or OS or browser or media player I use may not be a very personally intrusive question. But it may be of fairly great economic import, as for example when someone tries to use the information to force me to upgrade.

5 Nothing compels OEMs or service providers to protect privacy

The Policy frankly emphasizes its own voluntary nature:

> At the same time, we recognize that many aspects of successful policy implementation depend on software and hardware development from third party providers whose implementations are outside Intel's direct control.

It isn't clear that anyone can be compelled to comply with any part of the Policy or to use LT in privacy-respecting ways rather than in privacy-invasive ways. In light of this, the relevance of the Policy to achieving real-world privacy protections is presently limited.

While we commend Intel's forthrightness on this point, there is still a problem here. By the terms of the Policy, any adopter is free to ignore it and suffer no penalty other than Intel's disapproval (and EFF's).

In other contexts, Intel and other technology developers have exercised elaborate control over how technologies they license are applied. As we have previously observed, Intel is a licensor of the DTCP DRM technology. Intel's agent, the Digital Transmission Licensing Administrator (DTLA), undertakes to contractually bind users of DTCP to elaborate and specific compliance rules far more detailed than the Policy.[15] It is instructive to contrast the DTCP contract with the Policy; the DTCP contract is over a dozen times as long and,

them feel physically threatened or intruded upon, or put them at risk of being confronted with information in an unwelcome context, the disclosure of information such as marketing data can undermine their bargaining power. A close analogy might be the disclosure of what someone is actually willing to pay for some product or service. While this could conceivably reveal her income level or other sensitive demographic information, it has the most obvious effect of weakening her ability to bargain. That is a very real harm. It is not a harm rooted in personal autonomy or identity, but it is a concrete harm nonetheless.

[15] See, for example, Digital Transmission Licensing Administrator, "Digital Transmission Protection License Agreement: Evaluation License Convertible to Protection License", July 30, 2003, available at http://www.dtcp.com/data/DTCP_Adopters_Agreement010730.PDF. This document is a bilateral contract between Intel's agent DTLA and any third-party adopter. It was obviously prepared by an attorney, and it is 49 pages long. Presumably, DTLA believes that it can be enforced in court; it provides that "THIS AGREEMENT, AND ALL THIRD-PARTY BENEFICIARY CLAIMS BROUGHT PURSUANT HERETO, SHALL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW YORK". The contract requires very specific steps to be taken by adopters, who must expressly certify their compliance to DTLA in considerable technical detail.

unlike the Policy, is legally binding on adopters of Intel's technology.[16] It is hard to see why it should be feasible to require DTCP technology adopters to restrict consumers' enjoyment of entertainment works, yet impossible to require LT technology adopters to protect consumers' privacy.

6 Conclusion

While all parties should be held accountable for their own bad behaviors, Intel may be able to find ways to make its technologies less susceptible to abuse – above and beyond the promulgation of best-practices statements. We have previously suggested the inclusion of an "Owner Override" feature in trusted computing systems, to make sure that platforms are not used against their owners' interests. Intel and other trusted computing developers should make explicit how their technologies will be used in case of conflicts of interest between computer owners and third parties. As long as TC platforms are capable of enforcing policies against their owners, they are susceptible to abuse to subvert owners' and users' privacy, choice, and control.

The Policy in its present form is conspicuously lacking an enforcement mechanism. Since third parties have much to gain by abusing LT, Intel's disapproval alone is not enough to deter their abuses.

[16] DTCP was co-developed by Toshiba, Hitachi, Sony, and Matsushita, who, together with Intel, make up the "5C Group". "Intel is one of the '5C' companies that developed and administers DTCP." http://www.intel.com/technology/1394/.