

The Trusted Computing Revolution

To arms, Comrades! To arms!

Bruce Potter

gdead@shmoo.com

Don't Believe Anything I Say

- "Do not believe in anything simply because you have heard it. Do not believe in anything simply because it is spoken and rumored by many. Do not believe in anything simply because it is found written in your religious books. Do not believe in anything merely on the authority of your teachers and elders. Do not believe in traditions because they have been handed down for many generations. But after observation and analysis, when you find that anything agrees with reason and is conducive to the good and benefit of one and all, then accept it and live up to it." - Buddha
- By Day, Senior Associate for Booz Allen Hamilton
- By Night, Founder of The Shmoo Group and restorer of hopeless Swedish cars

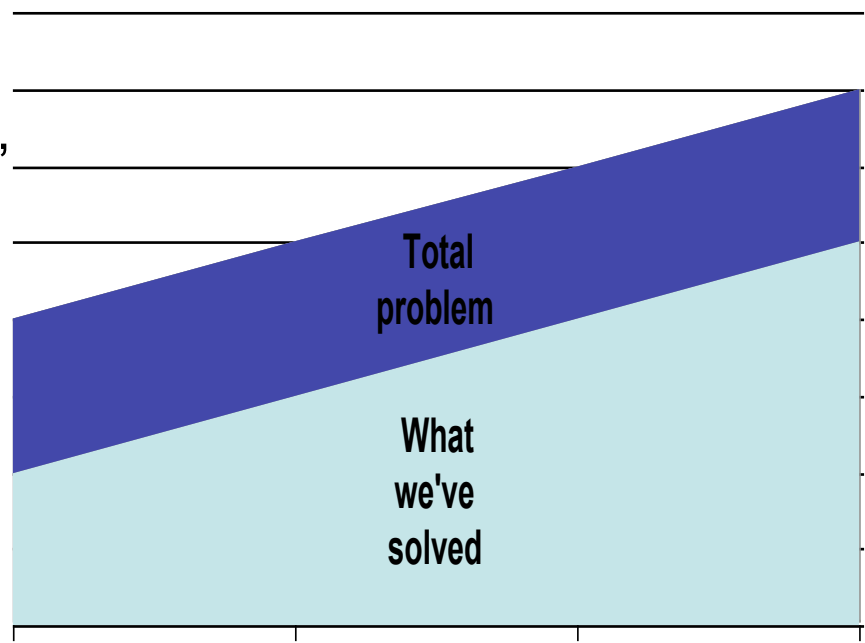
Overview

- History of InfoSec and Trusted Computing
- Current Trusted Computing technologies
- How Trusted Computing changes everything
- Tool Releases
- Sprinkle in some good arguments, and we've got ourselves a party

A Brief History of InfoSec

- For at least 50 years, we've been trying to solve the information security problem
 - However, at the same time, the problem keeps getting more complex
 - In the meantime, it's made security a profitable and sustainable industry (funny what happens when you chase an impossible dream)

InfoSec History - Nutshell



Current InfoSec Trends

- Defense in Depth
 - The core problem is currently unsolvable... So why not throw a giant pile of bandaids at it
 - With a slick phrase like “defense in depth” it even sounds responsible
- Access to systems == Access to data
 - Boot disks are amazing things
 - David Hulton et al have even taken malicious slave devices to a new level
- Transactions are trusted at a network level
 - End to end security only exists in controlled environments

So, How Did We Get Here?

- The roadmap for secure systems is described in Butler Lampson's "Protection" paper
 - <http://research.microsoft.com/~lampson/09-Protection/WebPage.html>
 - "The original motivation for putting protection mechanisms into computer systems was to keep one user's malice or error from harming other users. Harm can be inflicted in several ways: 1. By destroying or modifying another user's data. 2. By reading or copying another user's data without permission. 3. By degrading the service another user gets" (sounds pretty good, even though this was 1971)
 - The paper goes on to describe (basically) multilevel security, the need for hardware security to enforce data separation, and object-based access control (again, pretty good for 1971)

Guesses on when this was written?

- “Another major problem is the fact that there are growing pressures to interlink separate but related computer systems into increasingly complex networks”
- “Underlying most current users’ problems is the fact that contemporary commercially available hardware and operating systems do not provide adequate support for computer security”
- “In addition to the experience of accidental disclosure, there has also been a number of successful penetrations of systems where the security was ‘added on’ or claimed from fixing all known bugs in the operating system. The success of the penetrations, for the most part, has resulted from the inability of the system to adequately isolate a malicious user, and from inadequate access control mechanisms built into the operating system”
- Computer Security Technology Planning Study - October 1972, Electronic Systems Division, Air Force

The Search for the Holy Grail (MLS)

- The road is littered with corpses
 - <http://www.cs.stthomas.edu/faculty/resmith/r/mls/m2assurance.html> has some examples
- Some not so surprising results:
 - Operating systems are complicated
 - Software developers don't know how to write secure code
 - Without a piece of trusted hardware onto which you can layer security assertions, the best you can do it a layered defense... aka: "defense in depth"

Fast Forward... 2000ish

- Digital Rights Management emerges on the scene
 - Content is King.. Or so the saying goes
 - DRM is a mechanism for cryptographically protecting the rights of the content creator
 - Microsoft is including DRM-like capability into Office to prevent unauthorized sharing of data
- DRM is not perfect
 - Can be subverted easily when it is software only
 - Even hardware-based systems can be subverted, especially when they're badly designed
 - Thanks DVD Jon

Guess what? DRM is Cool

- According to a recent survey, iPods are cooler than beer
- Apple made DRM sexy and cool
 - The iPod begat ITMS
 - ITMS was made possible because Apple came up with a rights management scheme that the content providers could deal with at a \$1 a pop
 - In Feb 2006, the 1 billionth song was downloaded from ITMS
 - 1 billion songs means people things ITMS is cool
 - Through transitivity, Apple made DRM cool
- What does Apple have to do with Trusted Hardware?

Funny You Should Ask

- Apple just made trusted hardware sexy and cool
 - And you didn't even realize
- Enter the MacBook Pro
 - When Apple switched to Intel, they developed Rosetta... an emulator that dynamically translates PPC opcodes to x86
 - Apple is using the TPM to protect Rosetta from starting unless the TPM is there
 - This ensures Apple proprietary software only runs on Apple hardware
 - Maxxuss repeatedly bypassed this protection

Backing up a Step

- The Trusted Computing Group
 - Used to be the Trusted Computing Platform Alliance
 - An industry group (read: you have to buy your way in) that sets standards for trusted computing systems and architectures
- Used to be focused solely on the development of a trusted piece of hardware (TPM)
 - Now has broader scope, including networks, servers, storage, mobility applications, and software API's
- 135 Members, including most of the Big Boys TM

TCG on Privacy...

From <https://www.trustedcomputinggroup.org/faq/>

What has the TCG done to preserve privacy?

- TCG believes that privacy is a necessary element of a trusted system. The system owner has ultimate control and permissions over private information and must "opt-in" to utilize the TCG subsystem. Integrity metrics can be reported by the TCG subsystem but the specification will not restrict the choice and options of the owner preserving openness and the ability of the owner to choose.
- The TCG specification will support privacy principles in a number of ways:
 - The owner controls personalization.
 - The owner controls the trust relationship.
 - The system provides private object storage and digital signature capability.
 - Private personalization information is never exposed.
 - Owner keys are encrypted prior to transmission.
- It is also important to know what the solutions are not:
 - They are not global identifiers.
 - They are not personalized before user interaction.
 - They are not fixed functions—they can be disabled permanently.
 - They are not controlled by others (only the owner controls them).

Trusted Platform Module

- Chips manufactured by a variety of manufactures
 - Assured cryptographic operations
 - Trusted keystore
 - Integrity attestation
- The TPM, on it's own, does not do anything
 - Higher level systems (boot managers, operating systems, applications) must use the TPM to do something
- The TPM spec says that the user must have the ability to turn of the TPM chip
 - That means the user always has control of their device
 - However, that doesn't mean that all software will still work

Trusted Network Connect

- Rather than solving the MLS problem from the beginning, TCG is taking baby steps
- Network access is a problem in nearly every enterprise
 - Accessing the network should involve three parties authenticating themselves; the user, the user's device, and the infrastructure
 - Oftentimes, the device does not strongly authenticate itself
 - With a TPM, a device can have a unique cryptographic key to authenticate itself to the infrastructure
- TNC is basically 802.1x
 - Juniper and others already have solutions
 - Couple TNC with patching policies, and you can really put a dent in internal network security issues

Other Capabilities

- Microsoft's BitLocker
 - Vista has the ability to use a TPM for key storage and implements a secure container (ie: an encrypted file that is protected by the TPM)
 - No real documentation of interface to the TPM in Vista Beta
- Remote Attestation
 - The ability to tell a remote system about the local system with some assurance
 - Basically, you can attest to the integrity or configuration of a machine and cryptographically sign the whole thing
- Crypto API
 - No more confusion as to whether a crypto algorithm is implemented properly

Where Trusted Computing is Going

- Trusted computing is going to happen
 - Many systems shipping with TPM's already... just not much software that supports it
 - HUGE capability for InfoSec... Even if we don't reach the holy grail of MLS, there are still many positive features
 - However, if all we do is focus on the privacy concerns and don't figure out a way to use trusted computing to build more secure software, we'll fail before we even get out of the gate
 - /rant

Examining the Apple TPM

- All Intel-based Mac's make use of an Infineon TPM
- No real interface from Apple to examine/use TPM chip
- But never fear, we've got code to examine the TPM
- <http://tpm.shmoo.com/>



Demo of TPM software

Questions?

- Bruce Potter
- gdead@shmoo.com
- <http://tpm.shmoo.com/>