Trusted Computing White Paper

A proven security paradigm in use today and already deployed for improved Online Security

The Internet has become an essential fabric in today's society. From home and school to government and industry we depend on an intertwined network of networks – the Internet. Today our use of the Internet is at risk and under daily attack by criminals and other countries representing an advanced persistent threat. Other technologies have leveraged device identity to improve security and the user experience. The computer industry has addressed this need by implementing Trusted Computing.

Cell phones, cable television and even iPods have solved their user authentication and security challenges by securely and uniquely identifying each device.

> In the early years of the cell phone industry, cell phone numbers were hijacked by criminals. Those numbers was sold permitting people to make bogus cell phone calls which were billed to the cell phone owner. Today, with over 4.6 billion users worldwide, cell phone hijacking is unheard of. The cell phone industry recognized the problem and created an international standard to securely and uniquely identify each cell phone. Built into every phone (or its SIM card) is an electronic serial number which is securely part of each call. Imagine if you had to enter your user name and password every time you changed cell phone towers.
>
> The cable TV industry faced a similar challenge in its early days. Bootleg cable boxes could be purchased and people could pirate service without paying for it. Fast forward to today where cable boxes have a unique serial number and pirated service has virtually evaporated. Device identity permits subscriber-based cable services, which like cell phones, eliminates the requirement to enter user name and password every time you change channels.
>
> Imagine only entering your user name and password when you start your computer and then just using the Internet…. securely.

The computing industry has many times rallied around international standards either to reduce cost or to improve usability. Prior to Windows 95 a number of competing network protocols was available with various digital formats and physical cable connectors. With the release of Windows 95 computers were required to support Ethernet and to have RJ-45 jacks. This ended the debate on networks; Ethernet is available today worldwide. Consumers and business can be confident regardless of where they are in the world that everyone uses Ethernet and has cables and jacks based on this standard. Likewise, people are confident that purchasing a computer or laptop today will have an Ethernet jack and an OS that supports the protocol.

Trusted Computing represents the Ethernet for cyber security. Trusted Computing is a user–friendly, powerful tool to increase computer and Internet security; just like device identity has increased the usability and security for cell phones, cable systems and the entertainment industry. Simply put, the heart of Trusted Computing consists of a Trusted Platform Module (TPM) which is a highly secure chip with a unique serial number on the motherboard of personal computers (PC).

Over the past few years over 350 million Trusted Platform Modules have been shipped on virtually every business class PC. TPMs are based on an open, international industry standard shared by leading manufacturers through an industry association, the Trusted Computing Group. TPMs are manufactured by a number of leading chip companies including; AMD, Infineon and Intel. All the leading PC manufacturers incorporate TPMs in business class machines including; Dell, HP, Toshiba, Acer, Lenovo, Samsung, Sony, Gateway, Panasonic.

TPMs have now reached a tipping point. Due in large part to refresh rates of less than five years for PCs, estimates suggest that nearly every business, doctor's office and most government PCs have TPMs inside. The Department of Defense has required all PCs purchased since 2007 to include a TPM, if possible. The National Security Agency (NSA) is supporting the use of TPMs by the DoD to secure their network. Civil agencies and NIST recognize that device identity is a high priority in network security.

The President and the government are in a unique position and have a responsibility to provide leadership for issues too large for any one company to address. Several examples of the President stepping forward and leading change can be seen in the Americans with Disabilities Act (ADA) and the Occupational Safety and Health Act (OSHA).

> For example, The Americans with Disabilities Act generally requires owners of buildings to provide equal access to wheel chair bound people. Without ADA many building owners would not incur the additional expense to provide access but the legislation requires it and provides new freedom. Additionally, others have benefited as an unintended consequence of the ADA, such as the delivery driver who now uses a ramp to a building or a cut in a sidewalk.
>
> Another example of a President providing leadership was the enactment of OSHA improving employee safety. While no employer would desire their employees to be injured many would not enact the safety standards required by OSHA due to competitive pressures on overall cost. OSHA provided an equal playing field raising in effect the cost on all businesses equally. Countless thousands of workers have been saved death or disability by this act and society has benefited.

While industries like Cellular phones and cable TV networks have a compelling business case to implement device authentication the computer industry has evolved differently creating the cyber security challenge we face today. While some, especially hackers, believe that we should support any computer, any time, on any network, we probably could all agree that running a nuclear power plant on our daughter's laptop is not a good idea. Only a known machine should be able to connect to the network operating that nuclear power plant or to networks which contain sensitive data.

As the Internet and computing have become elements of the essential fabric in today's government, business and personal lives, the security of cyber space becomes more and more crucial. The President and Congress can help government, business and consumers by incorporating two tenets into future legislation which will encourage the migration to Trusted Computing. We would suggest two key positions be adopted in Cyber Security and other legislation.

Sensitive Data: Only "Known Computers" should be connected to "Sensitive Networks." Known Computers are computers that have tamper resistant identities that are held in a Trusted Platform Module or similar hardware device that is designed as part of the computer. A Sensitive Network is any network that transmits Personally Identifiable Information (PII) or confidential data where there is a duty to protect that information. Examples of Sensitive Data include;

- Health records
- Financial Records
- Critical infrastructure information e.g. utilities

Critical Institutions Should Support Known Devices: Critical institutions which transmit PII or confidential data should be required to accept credentials from Known Computers. For example, as a consumer you may wish to limit access to your bank accounts to only your two computers with TPMs, but you are not in a position to compel the bank to accept your credentials. Likewise, as a doctor you may wish to register your computers with your insurance providers, but you are not in a position to compel them to support the standard. Examples of Critical Institutions include;

- Insurance Companies
- Doctors
- Banks and Financial Institutions
- Government Services with sensitive information (e.g. VA, IRS, HHS)

Society Benefits: Trusted Computing, using highly secure TPMs, provides significant benefits to society as we seek a simple, affordable solution to improve cyber security and maintain confidence in the ability to conduct Online Transactions Securely.

- TPMs are based on a **free and open** industry standard supported by the leaders in the PC industry
- TPMs are **already deployed** and currently available on 350 million computers
- TPMs are **inexpensive** - costing only about one dollar
- Known devices on networks is a **proven security solution** for the Cellular phone and Cable TV networks
- Known devices can **solve the consumer and business nightmare** of user name password authentication