Trusted Computing Group: Goals, Achievements and Controversies

Joe Pato, Hewlett-Packard Labs
Exploiting a Trusted Platform Framework for Safe Appliance-Based Computing: The Evolution of Security Mechanisms Must Preserve Choice and Diversity

Security mechanisms should not constrain end users to a limited selection of appliances. In particular, personal preference and functional rather than presumed security capabilities should drive the choice between special-purpose dedicated devices, general-purpose appliances, or a dissociated federation of devices to accomplish a task. Security capability should be available for each of these approaches, and a trust infrastructure must be created so that all relying parties can measure the operational trust capabilities.

This talk will examine the role of trusted computing fundamentals in creating diversity for appliance-based systems. It will also examine the controversy around the Trusted Computing Group and how to preserve diversity in secure environments from a variety of perspectives.

Brian LaMacchia, Microsoft
Next-Generation Secure Computing Base (NGSCB)

This talk will present a technical overview of the architecture and key features of Microsoft's Next-Generation Secure Computing Base (NGSCB). NGSCB is new security technology for the Microsoft Windows operating system that leverages TCG components plus other unique hardware and software elements to create isolated processing spaces inside the PC that can give people greater security and privacy in the ways they use computers. Microsoft is building base-level software components that will enable more secure interaction with applications, peripheral hardware, memory, and storage by adding four new security services to today's PCs: curtained memory, secure input and output, sealed storage and attestation. Together, these features provide a high-assurance execution environment running in parallel with the "traditional" kernel- and user-mode stacks. The goal of NGSCB is to help protect software from software; that is, to provide a set of features and services that a software application can use to defend against malicious software also running on the machine (viruses running in the main operating system, keyboard sniffers, frame grabbers, etc.). NGSCB is not designed to provide defenses against hardware-based attacks that originate from someone in control of the local machine.

Ernie Brickell, Intel
Cryptographic Functionality of the Trusted Platform Module 1.2

The Trusted Computing Group (TCG) has defined the Trusted Platform Module 1.2 (TPM) to support the cryptographic functionality needed for a trusted platform. In this talk, I will describe the cryptographic protocols used for this functionality and the purpose and implementation of the cryptographic protocols. In particular, I will discuss the protocols for sealing secrets, creating and using an endorsement key, creating and using an Attestation Identity Key, resetting and extending a platform configuration register and locality.

Jan Camenisch, IBM Zurich Research Lab.
Achieving Privacy in Remote Authentication

This talk discusses the direct anonymous attestation scheme (DAA). This scheme was adopted by the Trusted Computing Group as the method for remote authentication of a hardware module, called trusted platform module (TPM), while preserving the privacy of the user of the platform that contains the module. Direct anonymous attestation can be seen as a group signature without the feature that a signature can be opened, i.e., the anonymity is not revocable. Moreover, DAA allows for pseudonyms, i.e., for each signature a user (in agreement with the recipient of the signature) can decide whether or not the signature should be linkable to another signature. DAA furthermore allows for detection of "known" keys: if the DAA secret keys are extracted from a TPM and published, a verifier can detect that a signature was produced using these secret keys. The scheme is provably secure in the random oracle model under the strong RSA and the decisional Diffie-Hellman assumption.

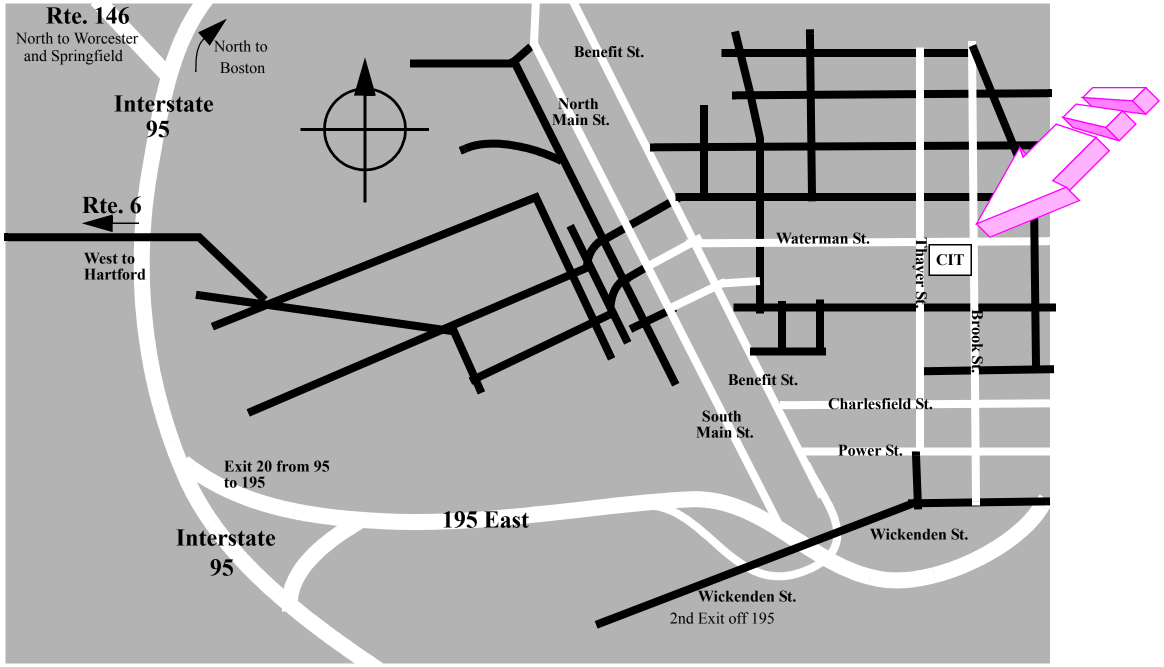
Anna Lysyanskaya, Brown University
Trusted Computing: Academia Meets Industry

I will give an overview of how fundamental problems in theoretical cryptography have found applications in practice, and in particular, in the TCG efforts. I will then review some current key research challenges.

continued ⟶

SCHEDULE

8:30	BREAKFAST and Registration 4th floor, CIT Building
9:00	**Introduction** Eli Upfal, CS Chairman John Savage, Michael Black, IPP Co-Directors
9:15	**Exploiting a Trusted Platform Framework for Safe Appliance-Based Computing** Joe Pato, Hewlett-Packard Labs
10::00	**Next-Generation Secure Computing Base (NGSCB)** Brian LaMacchia, Microsoft
10:45	BREAK
11:00	**Cryptographic Functionality of the Trusted Platform Model 1.2** Ernie Brickell, Intel
12:00	BUFFET LUNCH
1:30	**Achieving Privacy in Remote Authentication** Jan Camenisch, IBM Zurich
2:15	**Trusted Computing: Academia Meets Industry** Anna Lysyanskaya, Brown
3:00	BREAK
3:30	DISCUSSION PANEL Simson Garfinkel, MIT John Jannotti, Brown University Brian LaMacchia, Microsoft Seth Schoen, EFF Audience members are welcome to join the discussion
5:00	RECEPTION (5th floor)



The question I will then discuss in more detail is who trusts whom in trusted computing. Is a user of a given application a friend who needs protection from malicious software, or a foe from whom this application needs to be protected? I will outline the pros and cons of both approaches, and explain why I believe this question to be important for the computer industry and intriguing for academia.

This symposium is a benefit of membership in our **Industrial Partners Program**.

Our Partners and Sponsors include Microsoft Research, Sun Microsystems, Intel, nVIDIA, Pixar and Siemens Corporate Research.
There is no charge.

EMAIL REGISTRATION

To: sjh@cs.brown.edu
By: Friday, March 19, 2004
Please include the following:
Name, title
Company, Department
Postal address
Phone/Fax

DIRECTIONS TO THE CIT BUILDING

- From I-95 N or S, take Exit 20 to I-195E.
- From I-195E take Exit 2, Wickenden St.
- Go LEFT on Wickenden, LEFT again at the 2nd light onto Brook St.
- The red-brick CIT Building (Center for Information Technology) is on the left at the intersection of Brook and Waterman (1st light).
- *Registration is on the 4th floor.*

PARKING

Because most of the visitor parking has been assigned to University employees, I'm afraid we're unable to provide parking. Street parking is usually available for early birds, but watch out for newly designated 2- and 3-hour zones, which used to be all-day spots. You might try the residential area NW of the CIT.

The 32nd IPP Symposium
Dept. of Computer Science
BROWN UNIVERSITY

Trusted Computing Group: Goals, Achievements and Controversies

Thursday
March 25, 2004
Hosted by Professor
Anna Lysyanskaya

INDUSTRIAL
PARTNERS
PROGRAM