Grenoble INP

Ensimag

SecurIMAG

2011-12-06

Questions asked during interview

- **Description:** ideas of possible answers
- **Lecturer:** Guillaume Jeanne

WARNING: *SecurIMAG is a security club at Ensimag. Thoughts, ideas and opinions are not related to Ensimag. The authors assume no liability including for errors and omissions.*

Context

- **Prototypage d'un chiffreur léger et bas coût**

- Le stage consistera en la conception d’un prototype de passerelle IPsec qui devra satisfaire des exigences fortes de sécurité, en particulier l'intégrité logique et physique de l'équipement, tout en réduisant l’encombrement et le coût individuel des chiffreurs.

Context

- IPsec ? Rfc 2401, 3168, 4301

- L'utilisation de passerelles IPsec (chiffreurs) permet de transmettre de manière sécurisée des données sensibles à travers un canal de communication non sûr. La mise en oeuvre d'un tunnel sécurisé permet notamment de couvrir des besoins en confidentialité et en intégrité sur les communications. Cependant, le recours à de tels équipements augmente le coût et l'encombrement du système d'information, ce qui peut être inacceptable pour certaines conditions d'emploi

Intern's work

- étudier les technologies de chiffrement de flux.
- porter un système d’exploitation durci sur une carte de développement.
- étudier les mécanismes de protection de l’intégrité du démarrage, et implanter un tel mécanisme sur la
- plate-forme.
- tester le fonctionnement de la maquette dans le cas d’un réseau de passerelles nomades.
- fournir une documentation complète du système ainsi que son étude théorique.

Question 1

- Qu’est ce qu’un chiffreur léger à bas coût, dans quel contexte on l’utilise ?

Question 2

- Lors d'un voyage en train, je me rends aux toilettes après avoir éteint mon ordinateur mais l'ayant laissé sur ma tablette, à mon retour, comment savoir s'il n'a pas été corrompu ?

- Quels mécanismes avais-je mis en place pour empêcher cela ?

Pieces of answer

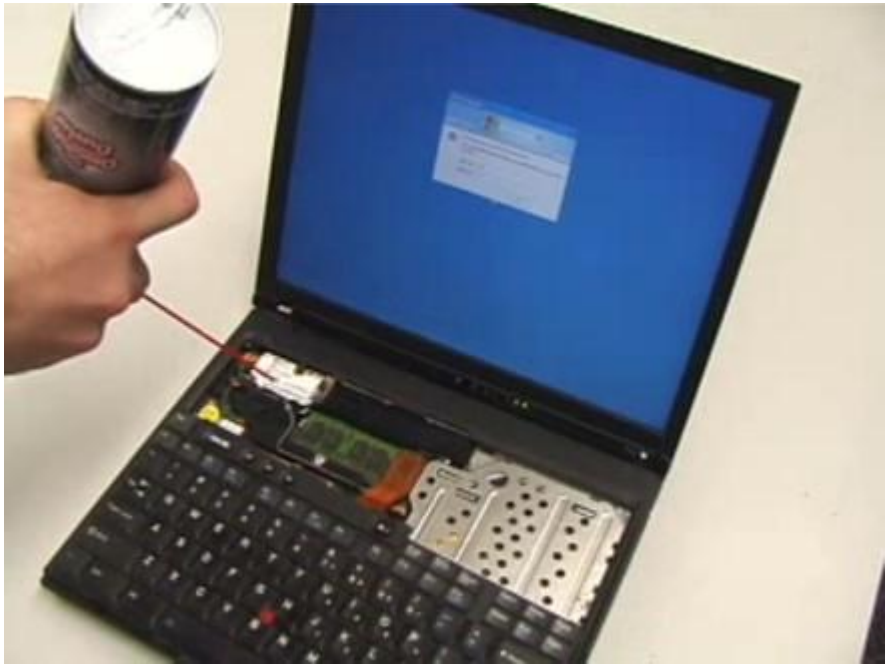
- Encrypted Hard Drive
- Encrypted file system
- Secure boot system
  - Software
  - Hardware (crypto proc TPM)
- Authentication system
- Bios password
- …

Question 3

- Lors d'un voyage en train, un passager se rend aux toilettes, comment je peux attaquer son ordinateur ? sachant qu'il dispose :
  - D'un boot sécurisé avec calcul d'empreinte sur les fichiers systèmes
  - D'un disque de données chiffrées via un mot de passe demandé lors de l'authentification

Pieces of answer

- Cold boot attacks



- http://www.usenix.org/events/sec08/tech/full_papers/halderman/halderman.pdf

Pieces of answer

- Hash collision and raimbow tables

- http://www.sstic.org/2011/presentation/rainbow_tables_probabilistes/

Pieces of answer

- Use a Keylogger/Keygrabber
  - Hardware
  - Software

Pieces of answer

- Malware injection
  - corrupt system files
  - Retrieve hash
  - Change the hash calculation function

Good Luck !