Insecurities within automatic update systems

Can patching let a cracker in?.

Peter Ruissen
Robert Vloothuis

RP2 Project OS3 System and Network Engineering
University of Amsterdam

June 28, 2007

Onderzoeksvraag

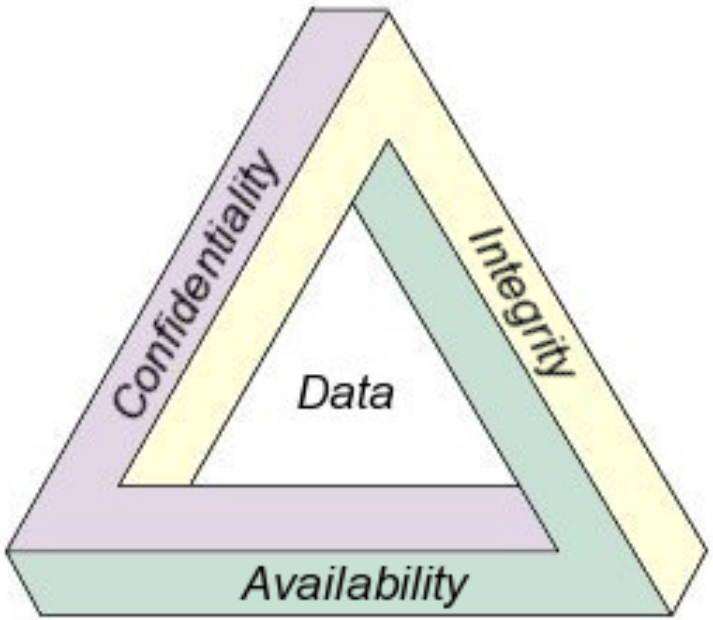
Welke eisen zijn er nodig voor een veilig update mechanisme en in welke mate voldoen de huidige besturingssystemen en applicaties hieraan?

Abstract model

ISO 9126-1

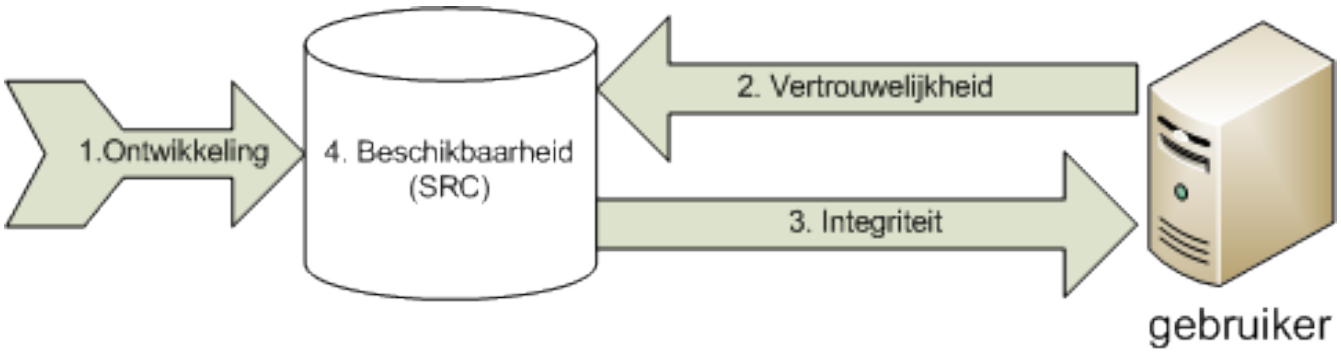
- Functionality
  - security
- Reliability
- Usability
- Efficiency
- Maintainability
- Portability

CIA Triad

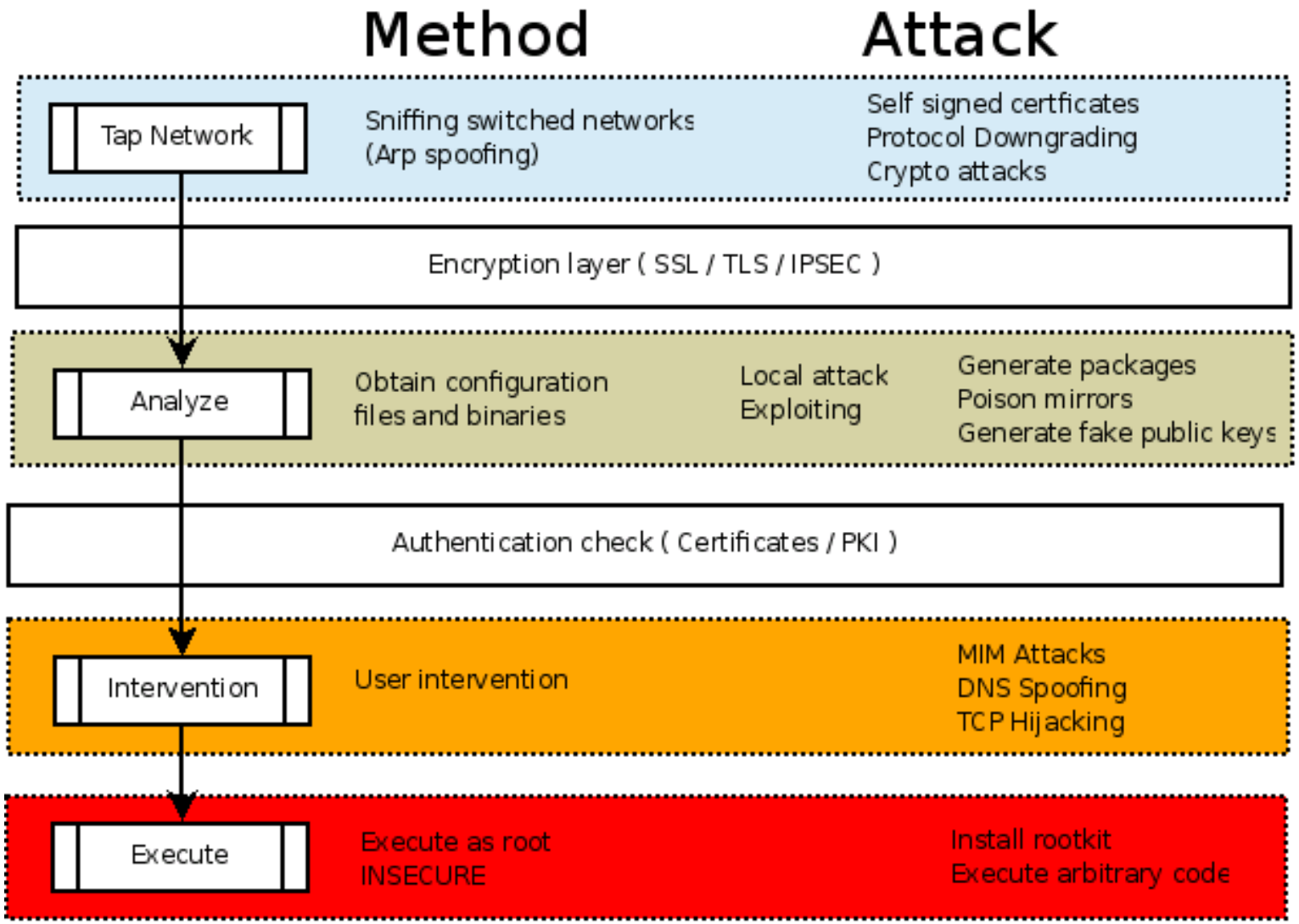


1. Integriteit
   - CRC/HASH
   - Certificaten
   - Ontwikkeling
2. Vertrouwenlijkheid
   - Beveiligde verbinding (SSL/TLS)
3. Beschikbaarheid
   - Meerdere update bronnen

Proces model



1. Ontwikkeling
2. Vertrouwelijkheid
3. Integriteit
4. Beschikbaarheid


Method
Attack
Tap Network
Sniffing switched networks
(Arp spoofing)
Self signed certficates
Protocol Downgrading
Crypto attacks
Encryption layer (SSL / TLS / IPSEC)
Analyze
Obtain configuration
files and binaries
Local attack
Exploiting
Generate packages
Poison mirrors
Generate fake public keys
Authentication check (Certificates / PKI)
Intervention
User intervention
MIM Attacks
DNS Spoofing
TCP Hijacking
Execute
Execute as root
INSECURE
Install rootkit
Execute arbitrary code

Windows XP/Vista

- Windows XP
  - Windows update versie 6
  - Automatische updates
- Windows Vista
  - Ongeveer hetzelfde als XP
  - Gentegreerde update mechaniek
  - Update meer Microsoft applicaties
- Update beveiliging
  - Certificaten
  - TLS v1.0 - Vertrouwelijkheid
  - BITS - Integriteit
  - Centrale update server - Beschikbaarheid

Acrobat Reader 8

- Certificaten
- Inc. Revocation List
- Public Acrobat key in installatie package
- Geen beveiligde verbinding
- Centrale update server

Command & conquer 3

- Download update lijst van EA server in plain tekst
  - FTP server
  - File list
  - File size (FTP command SIZE)
  - Onbekende(?) Hash over bestanden
- GEEN certificaten
- GEEN encryptie
- ÉÉN enkele update server

Linux update (on)veiligheden

- Redhat yellow dog updater (YUM): Mirror chaining: (rsync en CVS) gevaarlijk.. Automatisch ophalen public keys slechte gewoonte....
- Debian Advanced Packaging tool (APT) 2003: GNU en Savannah FTP mirrors gekraakt:
- Gentoo Portage (Emerge and ebuild class files) 2003: enkele trojans vrijgegeven voor Portage: Signed Ebuilds
- Gebruiken allemaal GnuGPG om de host te authenticeren met signed binaries. GnuPG versie 1.4.6 is kwetsbaar.

Java Runtime Environment updates

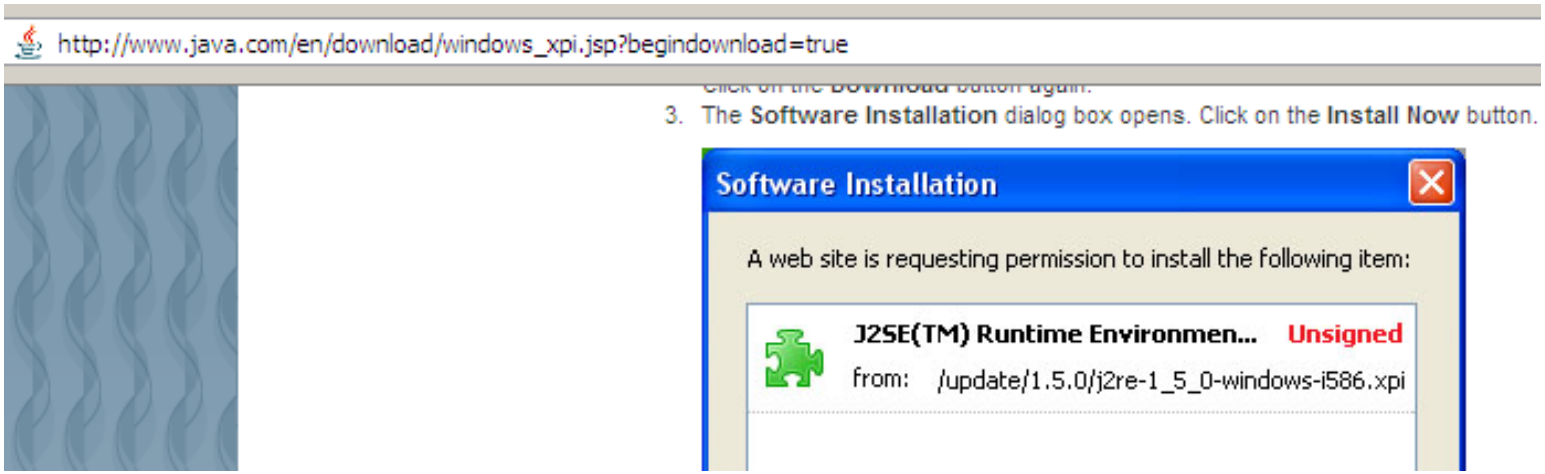


Figure: Sun raad onveilige updates aan...

- Online Java update unsigned, Sun raad aan om dit te negeren
- Java update gebruikt certificaten met SHA1 signatures
  Windows gebruikers zullen warnings negeren (lijkt op third party driver warning)

Java update exploit

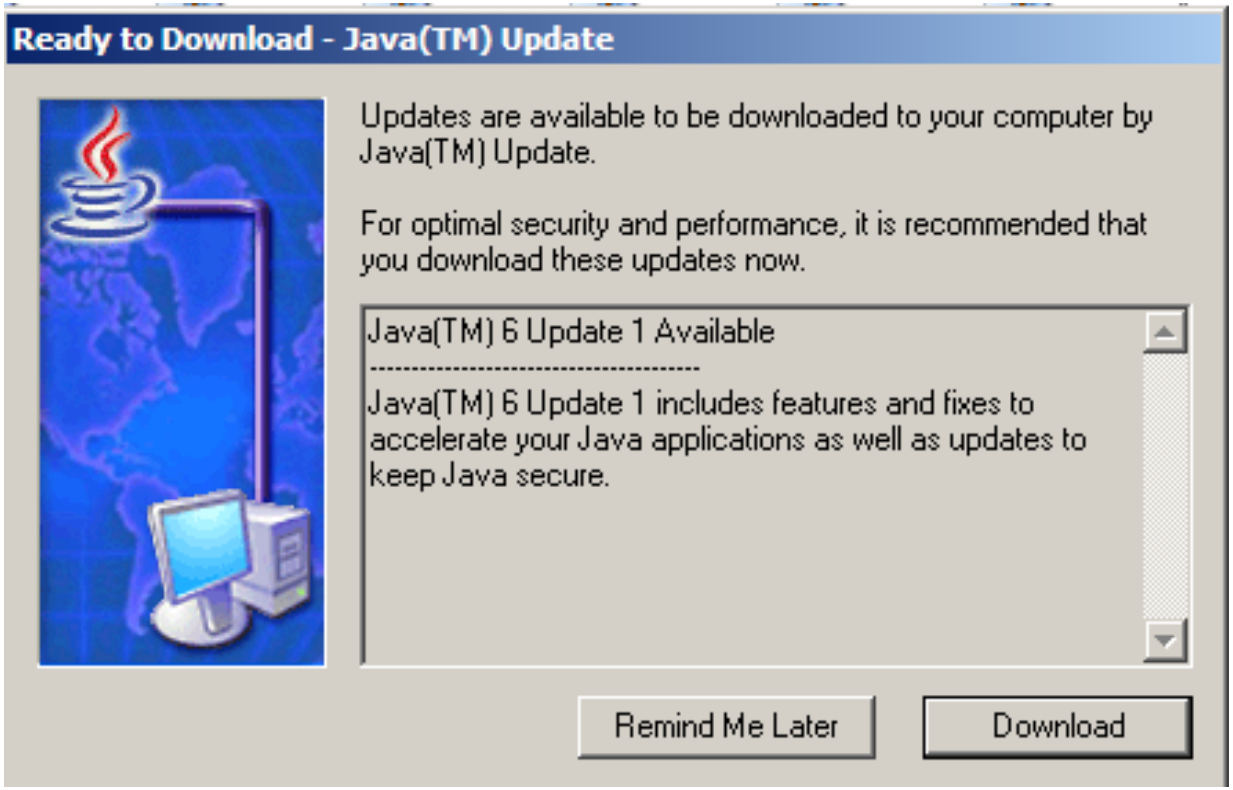


Figure: Simpele Java update spoofing aanval: (Download)

Java update exploit

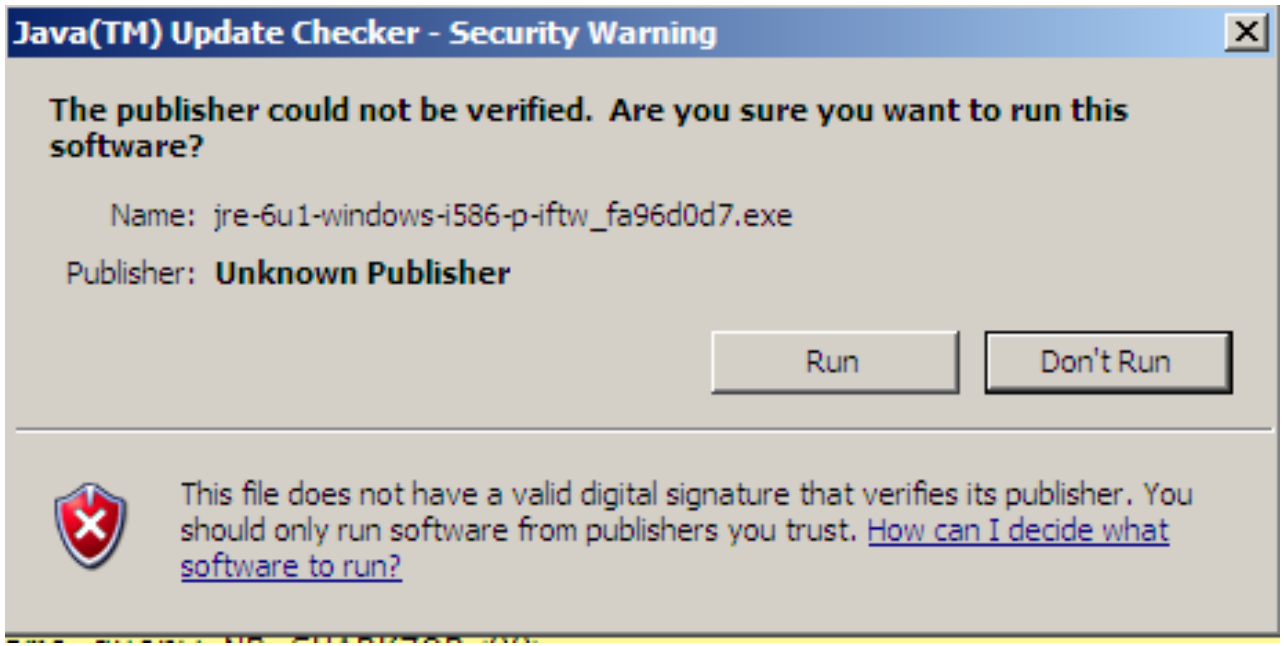


Figure: Simpele Java update spoofing aanval: (Run)

Java update exploit

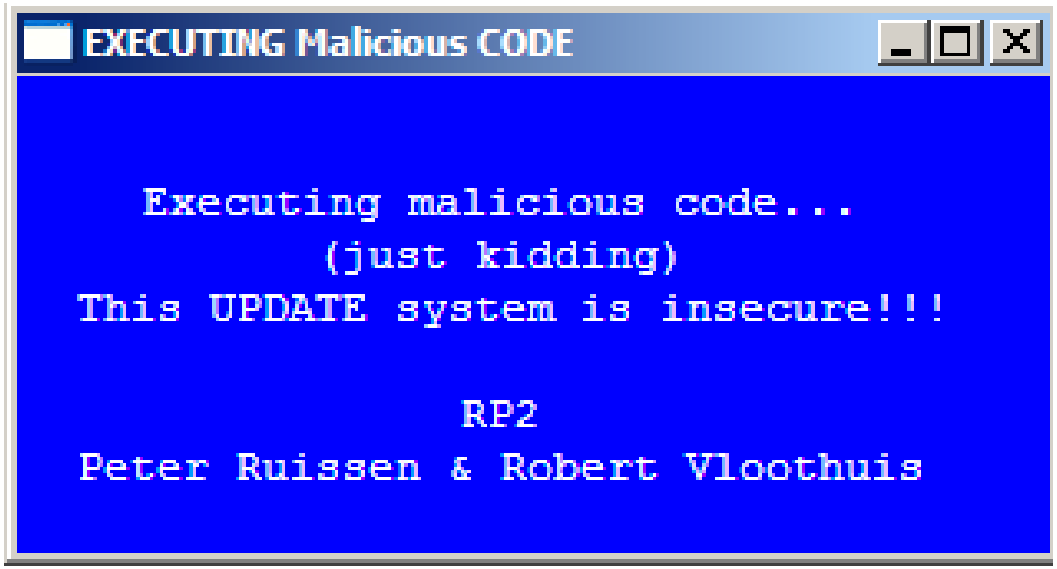


Figure: Simpele Java update spoofing aanval: (Hacked!)

- Juni 2007: Meerder trojans uitgebracht voor alle java versies (image buffer overflow): oude versie worden NIET gedeinstalleerd.

Mozilla & plugins

- Mozilla geprogrammeerd met beveiliging in gedachte (SSL, Manifest files, SHA2 hash; beloning voor vinden van critical security bugs)
- Zwakheden in "third party" plugins
- Automatic install XPI (Cross platform install) packages
- GEEN SSL: Google toolbar, Yahoo, Facebook, AOL en anderen
- Fake update response with malicious data.

Risico model

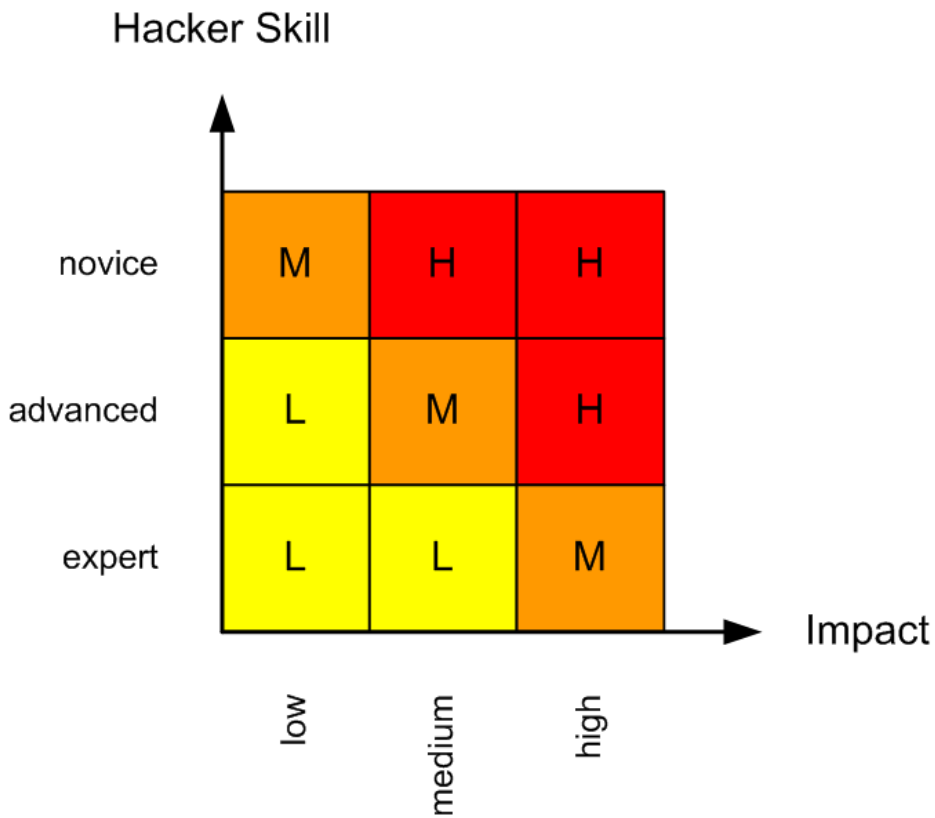


Figure: Simpele risico analyse gebaseerd op impact en hacker skills

Risico overzicht

App/OS	Flaw	Risk
Windows XP/Vista	Denial of updates	MEDIUM
Adobe Acrobat	Denial of updates	MEDIUM
Linux distros	Hacking one GPG mirror compromises all	LOW
Firefox	extensions not using SSL	HIGH
Java Updates	MIM attack, ignore warnings	MEDIUM
Java plugin Firefox	unsigned	MEDIUM
CNC3	MIM attack crack hashing algorithm	MEDIUM

Conclusie

- De laatste jaren is veel gesleuteld aan de beveiliging van update mechanismen
- Er zijn nog steeds applicaties en bedrijven die veel concepten verkeerd toepassen
- Onwikkeling van een standaard en het toepassen risico analyse kan helpen bij het oplossen van deze issues.