## Poll

**Versleutel jij je vertrouwelijke bestanden?**

- Ja, altijd
- Nee
- Soms
- Versleuteling?

## Insight

Win IPv6 naslagwerk "Running IPv6"

Reageer [2]

## Insight

TrueCrypt: Gratis en eenvoudige encryptie voor USB sticks

USB stick wéér verloren? Zelfs als je bij

# OV-chipkaart, skipas en huisdier kwetsbaar voor virus

Door Redactie op woensdag 15 maart 2006 11:39

Is uw hond of kat besmet met een computervirus? Dat zou zo maar kunnen. Bij veel huisdieren en vee is namelijk een kleine chip geïnjecteerd die de dieren kan identificeren als ze zoekraken of besmet blijken te zijn met een ziekte. Omdat de geheugenruimte op deze chips beperkt is, nam iedereen tot nu toe aan dat deze niet geïnfecteerd konden worden met een computervirus. Promovenda Melanie Rieback en haar begeleider prof. dr. Andrew Tanenbaum hebben echter ontdekt dat dit wel degelijk mogelijk is om virussen over te brengen op OV-chipkaarts, skipassen en bagagelabels op vliegvelden. Rieback geeft vandaag op de jaarlijkse IEEE Conference on Pervasive Computing and Communications in Pisa een demonstratie hiervan.

Gelukkig kan de virusdreiging met gangbare maatregelen worden tegengegaan. Rieback benadrukt dan ook dat ontwikkelaars hun RFID- systemen moeten controleren en veiligheidsprocedures en veilige programmeertechnieken moeten toepassen. Deze tegenmaatregelen kunnen de dreiging van RFID-virussen beperken, maar er zal tijd, geld en menskracht moeten worden geïnvesteerd om deze in te voeren. Daarom is het noodzakelijk dat ontwikkelaars en gebruikers van RFID- systemen de veiligheid van hun systemen nu controleren, voor deze op grote schaal worden gebruikt.

Meer informatie over RFID-virussen is te vinden op www.rfidvirus.org. Het IEEE PerCom paper van Melanie Rieback (Is Your Cat Infected with a Computer Virus?) is beschikbaar op via deze link. Het onderzoeksteam van de VU heeft ook onderzoek gedaan naar beveiliging en privacyaspecten van RFID technologie. Dit heeft geleid tot de RFID Guardian, een draagbaar apparaat voor RFID-privacybeheer. De homepage van het RFID Guardian project is te vinden op www.rfidguardian.org.

## Login

E-mail:

Wachtwoord:

Login of registreer

## Stelling

Microsoft moet onderzoekers betalen voor security lekken

Reageer [16]

## Forum

20:50 DR-DoS. Nieuwe
20:16 incidenten?
19:17 lancelot
19:08 Backdoor Haxdoo
17:05 akamaitechnolog
16:25 p2p, of torrent
16:20 Keylogger

## Insight

Interview met IPv6-expert Iljitsch van Beijnum

overheid of defensie werkt hoeft dit niet het einde van je carrière te betekenen.

Reageer [13]

Hebben we in de toekomst nog wel privacy? [16]

Veilig bellen met Philip Zimmermann's Zfone [6]

Reageer [9]



## Zoeken

Zoek

## Pine Virus Top 5

Laatste 24 uur

1.W32/Netsky-P 20%

2.W32/Nyxem-D 9%

3.W32/MyDoom-AJ 8%

4.W32/Mytob-FO 6%

5.HTML.Phishing.B... 4%

1 op de 107.8 mailtjes bevat een virus

Door Pine Digital Security

## Windows Security Bulletins

MS06-012 14-03-2006
MS06-011 14-03-2006
MS06-010 01-01-1970
MS06-009 14-02-2006
MS06-008 14-02-2006
MS06-007 14-02-2006
MS06-006 14-02-2006

Verberg 5 anonieme reacties

Door SirDice op woensdag 15 maart 2006 13:24

Volgens mij is de definitie van een virus: code die zichzelf kan vermenigvuldigen.. Ik zie niet in hoe dit kan met RFID tags.. Een RFID heeft zelf weinig tot geen intelligentie.. Je zou er hooguit wat malware in kunnen stoppen die een eventuele reader kan exploiten.. Maar dan nog ben je afhankelijk van de gebruikte reader.. Beetje in dezelfde trend als WMF bestanden.. Afhankelijk van welk programma je gebruikt om het te lezen ben je wel of niet vatbaar..

Maar stel, in een hypothetisch geval, dat de reader geinfecteerd zou kunnen worden door een dergelijke malicious RFID, hoe kan deze reader dan andere RFID's infecteren?

Kortom, malware in RFID's zou kunnen, virussen echter niet...

Reageer met quote

Door Anoniem op woensdag 15 maart 2006 13:31

Ik vind dit geen ontdekking, laat staan wetenschap. Daarnaast is de presentatie onder de maat die je van een universiteit mag verwachten. Blijkbaar is goedkoop scoren ook tot de Nederlandse universiteiten doorgedrongen. Misschien moeten we ons troosten met het feit dat het hier om een amerikaanse gaat.

## Reacties



## Spam Statistieken

Spam statistieken gegenereerd door Pine Digital Securi

Anti-virus software

Firewall software

Anti-spyware software

Hushmail

US-CERT Technical Cyber Security Alerts

MS06-005 14-02-2006

## Linux Advisories

RedHat: Important...
RedHat: Important...
Gentoo: Sylpheed,...
Gentoo: Scorched ...
Debian: New phpsy...
Debian: New ftpd-...
Debian: New uim p...
Debian: New AbiWo...
Debian: New acidl...
Gentoo: linux-ftp...

Wat is het geval? Als je in de achterliggende applicatie ongeldige data voert dan krijg je heel misschien foutief gedrag.

Niets nieuws dus, in 1 simpele zin te vatten.

Het is al sinds jaar en dag bekend dat hackers langs dit soort wegen systemen aanvallen. Het foutief invullen van formulieren, aankruizen van extra vakjes, het kiezen van niet bestaande voiceresponse opties, het bellen van niet bestaande nummers, het wijzigen van magneetstrips, het plaatsen van extra barcodes of streepjes, etc. etc...

Reageer met quote

Door Anoniem op woensdag 15 maart 2006 16:49

Deze onderzoek slaat nergens op.

Je neemt een programmeerbare rfid tag.
Je neemt een rfid tag lezer die hierbij past.
Je maakt een applicatie die SQL van die tag accepteerd.
Je presenteerd ongenuanceerd dat RFID lek is.
Je vergeet te vermelden dat meeste gebruikte RFID tags niet aan enige ISO norm voldoen maar gebruik maken van private protocols, om te voorkomen dat klanten zomaar naar concurrent kunnen overstappen.
Je vergeet te vermelden dat je meestal geen toegang hebt tot sourcecode of applicatie waar je eventjes een aanvals vector (zoals een buffer overflow) in vind.
Je zet in je eigen rapportage wel de condities aan, maar nuanceerd in je communicatie naar buiten niets.

Ik denk dat ik bij meneer Tanenbaum (jammer dat hij hieraan ze naam heeft geleend) een rapport ga in dienen dat auto's schadelijk zijn voor mens en milleu. Onder het mom, "can my cat die while driver a car?" en zo ook een titel krijgen.....

Immers elke auto onder bepaalde specifieke condities is gevaarlijk voor mens en millieu.

Zie voor meer genuanceerde comments:

FreeBSD advisories

Sun Security Alerts

Waarschuwings dienst

Debian Security Advisories

http://www.webwereld.nl/comments/40249

Reageer met quote

Door Anoniem op woensdag 15 maart 2006 16:56

Input verification anyone?

RFID is net zo kwetsbaar voor een virus als een editbox...

Reageer met quote

Door Anoniem op woensdag 15 maart 2006 17:27

> quote:
>
> Dit heeft geleid tot de RFID Guardian, een draagbaar apparaat voor RFID-privacybeheer.

Die vind ik persoonlijk wel OK...

Kocht laatst een sweatertje bij de V&D met aan de binnenzijde (op een plek waar je dit niet verwacht en ook geen "last" van zou hebben tijdens het dragen) een RFID gestikt waarop aan de achterzijde vermeld stond 'Voor Gebruik Verwijderen' . Op zich goed, zij het niet dat bij het verwijderen de stiksels beschadigd raken....

Reageer met quote

Door Anoniem op woensdag 15 maart 2006 21:08

[quote]Door SirDice
Volgens mij is de definitie van een virus: code die zichzelf kan vermenigvuldigen.. Ik zie niet in hoe dit kan met RFID tags.. Een RFID heeft zelf weinig tot geen intelligentie..
Je zou er hooguit wat malware in kunnen stoppen die een eventuele reader kan exploiten.. Maar dan nog ben je afhankelijk van de gebruikte reader.. Beetje in dezelfde trend als WMF bestanden.. Afhankelijk van welk programma je gebruikt om het te lezen ben je wel of niet vatbaar..

Maar stel, in een hypothetisch geval, dat de reader geinfecteerd zou kunnen worden door een dergelijke malicious RFID, hoe kan deze reader dan andere RFID's infecteren?

Kortom, malware in RFID's zou kunnen, virussen echter niet...[/quote]
Omtrent virussen, spyware en malware heeft de industrie nieuwe definitievoorstellen gedaan waarin de werking maar zeker ook het soort schade onderdeel uitmaakt van de definitie. Volgens deze definities (waarvan eerdere artikelen op security.nl) is het onderzoek wel degelijk relevant. Individuele gevallen zijn misschien niet nieuw maar wel het algehele kader wat men presenteert heeft toegevoegde waarde.

RFID-virussen bestaan wel degelijk en leveren ook een nieuw soort gevaar. Daarvoor moet je wel de gehele keten in ogenschouw nemen:
- de RFID-tag is te beschouwen als een stukje data.
- RFID-software die de tag uitleest kan gecompromiteerd worden.

De metafoor van WMF is op zich een goede omdat hier dezelfde symmetrie in zit: WMF = data ; software om WMF te viewen kan gecompromiteerd worden.

Gevaar is wel degelijk aanwezig en kan leiden tot zelfs levensgevaarlijke situaties.

Reageer met quote

Door frits danon op donderdag 16 maart 2006 10:17

quote:

---

Door SirDice
Volgens mij is de definitie van een virus: code die zichzelf kan vermenigvuldigen.. Ik zie niet in hoe dit kan met RFID tags.. Een RFID heeft zelf weinig tot geen intelligentie..

---

Klopt deels SirDice.
Als je een computervirus vergelijkt met een echt virus klopt het wel.
Een echt virus is alleen maar een pakketje informatie, b.v. het AIDS-virus is slechts DNA informatie, het vermenivuldigt zichzelf niet. Maar in een systeem, de mens, is het in staat zichzelf te laten vermenigvuldigen.
En helaas, de mens is net windows, niet helemaal perfect ;-).

E.e.a. geldt dus voor een RFID-tag ook zo.

Frits

Reageer met quote

Reageer

Naam: Anoniem

Let op: Omdat u niet bent ingelogd wordt uw reactie eerst gemodereerd.

Reactie:

Lees uw reactie goed door en controleer op spelfouten / zinsopbouw.

Verstuur regels voor het plaatsen van een reactie | vb codes

De security.nl headlines in RSS formaat