atbusiness

Onko sovelluksissasi madon mentäviä reikiä?

Tietoturva ry
11.11.2003

Jari.Pirhonen@atbusiness.com
Tietoturvallisuuspäällikkö ja -konsultti, CISSP, CISA
AtBusiness Communications Oyj

www.atbusiness.com
www.iki.fi/japi/

Sisältö - pohdiskelua kysymyksiin

atbusiness

- Mitä olemme oppineet vuosien varrella?
- Miten sovellusmaailma on muuttunut?
- Miten sovellusten tietoturvaa voitaisiin parantaa?
- Mitä sovellusprojektit voivat tehdä nyt?
- Web Services – mahdollisuuksia vai matoja?

"We already have enough fast, insecure systems. We don't need another one."

-- Ferguson, Schneier

Christma Exec

- Levisi sähköpostin välityksellä joulutervehdykseksi naamioituneena
- Käyttäjän suorittaessa ohjelman, näytölle ilmestyi joulutervehdys ja samalla mato lähetettiin käyttäjän osoitekirjan sisältämiin osoitteisiin
- Yksinkertainen, REXX-kielellä kirjoitettu mato
- Levisi erityisesti IBM:n sisällä
- Madon poistamiseen kehitettiin ”vastalääke”, anti-Christma Christma
- Madon leviäminen edellytti käyttäjän houkuttelemista suorittamaan haittaohjelma
- Vrt. Love Letter, väärennetyt ”Microsoft-päivitykset”

Lähde: http://www.computer.org/security/v1n5/j5cap.htm

Britney vs. Tietoturva

Alaston Britney Spears tuhoaa tiedostoja

Britney Spears kylvää tuhoaan internetissä. Poptähti on joutunut tahtomattaan epämiellyttävän ilkivallan kohteeksi, sillä Britney-virus on levinnyt internetissä sunnuntaista lähtien.

Tietokoneviruksen kylväjä on keksinyt varman tavan levittää virusta varsinkin miesten tietokoneisiin. Britney Spearsin alastonkuvasta haaveileva surffaaja saa poptähden sijasta koneeseensa madon, joka tuhoaa tiedostoja. Tiedoston nimi *britney.jpg* viittaa aitoon kuvaan, mutta sen sisältä paljastuukin tiedostoja tuhoava virus.

– On todella tavallista, että viruksen levittäjä houkuttelee avaamaan tiedoston julkkiksen alastonkuvalla, viruksien torjuntaan erikoistunut Per Hellqvist kertoo sanomalehti *Aftonbladetin* nettisivulla.

Asiantuntija uskoo, että tämänkertaisen Britney-viruksen alkulähde on saatu tuhottua, mutta koko ajan löytyy uusia vastaavanlaisia yrityksiä. Ennen virukset levisivät lähes ainoastaan sähköpostin välityksellä, mutta esimerkiksi britney.jpg levisi keskustelukanavan kautta.

Britneyn nakukuva sisältää viruksen.

Morris Worm

- Levisi käyttäen hyväkseen sovellus- ja konfigurointivirheitä
  - Luottamuksen väärinkäyttö: Unix *rsh*
  - *Sendmail* debug-option väärinkäyttö
  - Unix *fingerd* puskuriylivuoto
- Saastutti BSD-pohjaisia Unix-järjestelmiä (VAX, SUN)
- Vrt. IE-, SSH ja MS RPC-ongelmat
- Tapahtumasta saadut opit
  - Järjestelmissä ja sovelluksissa annettava vain välttämättömiä oikeuksia
  - Järjestelmien monimuotoisuus on hyvästä
  - Vastalääke ei saa olla ongelmaa pahempi
  - Vastatoimet verkkotasolla eivät riitä
  - Tietoturvakorjausten keskittäminen ja käyttäjien kouluttaminen tietoturvakorjausten tärkeyteen auttaa
  - Hätäisiä vastareaktioita kannattaa välttää

Lähde: http://sunsite.org.uk/packages/athena/virus/mit_ieee.PS

Maailma muuttuu…

	1970	1980	1990	2000
Sovellus	Suurkone-sovellus	PC, funktiot	Client-server, n-kerros sovellus, Web-sovellus, objektit	Service Oriented Architecture, Web Services, palvelut
GUI	ASCII	GUI, ikkunointi	Erikokoiset näytöt, selainversiot, pluginit	päätelaitteiden kirjo, vaihteleva verkon kapasiteetti
Tietoturva	**Tietoturvan hallinta keskitettyä**	**Käyttäjille valtaa ja vastuuta, virukset,**	**Yritysten verkottuminen, client-sovelluksen luotettavuus, sovelluskäyttö rajoitettua, ”linnakemalli”, päämääränä suojautuminen**	**Sovellusten verkottuminen, palveluiden luotettavuus, sovelluskäyttö aina ja kaikkialta, ”tori- tai lentokenttämalli”, päämääränä luotettavuus ja selviytyminen**

…tai sitten ei

- Puskuriylivuodot yleisiä
- Sendmail edelleen käytössä
- Tietoturvaa ei yleensä huomioida sovellusprojekteissa
- Sovellusten ominaisuudet, helppokäyttöisyys, suorituskyky, jne. menevät tietoturvallisuuden edelle
- Tietoturvatuotteet ja -ratkaisut tähtäävät ongelmien paikkaamiseen ja hyödyntämisen minimointiin
- Tietoturvatuotteet eivät ole yhteensopivia
- Ad hoc vastatoimet

Microsoftin turvateesit

Tuotekehityksen uudet teesit:

- ”Secure by design”
- ”Secure by default”
- ”Secure in deployment”


Windowsin paikkaamiseen uponnut sata miljoonaa

Microsoft nostaa tietoturvaa myyntivaltiksi

Tietoturva ennen ominaisuuksia:

”When we face a choice between adding feature and resolving security issues, we need to choice security. Our products should emphasize security right out of the box”
- Bill Gates

”We’re going to tell people that even if it means we’re going to break some of your apps, we’re going to make things more secure. You’re just going to have to go back and fix it”
- Craig Mundie

Bill Gates: You don't need perfect code…

You don't need perfect code to avoid security problems. There are things we're doing that are **making code closer to perfect**, in terms of tools and security audits and things like that. But there are two other techniques: one is called **firewalling** and the other is called **keeping the software up to date**. None of these problems (viruses and worms) happened to people who did either one of those things. If you had your firewall set up the right way — and when I say firewall I include scanning e-mail and scanning file transfer -- you wouldn't have had a problem. But did we have the tools that made that easy and automatic and that you could really audit that you had done it? No. Microsoft in particular and the industry in general didn't have it.

The second is just the updating thing. Anybody who kept their software up to date didn't run into any of those problems, because the fixes preceded the exploit. Now the times between when the vulnerability was published and when somebody has exploited it, those have been going down, but in every case at this stage we've had the fix out before the exploit. So next is making it easy to do the updating, not for general features but just for the very few critical security things, and then reducing the size of those patches, and reducing the frequency of the patches, which gets you back to the code quality issues. We have to bring these things to bear, and the very **dramatic things that we can do in the short term have to do with the firewalls and the updating infrastructure**.
-- Bill Gates, ITBusiness.ca interview 29.10.2003
Lähde:http://www.itbusiness.ca/index.asp?theaction=61&sid=53897

Bill Joy: We need an evolutionary step…

Seriously, though, I'm interested in figuring out how we can build a Net that is a lot less prone to viruses and spam, and **not just by putting in filters** and setting up caches to test things before they get into your computer. **That doesn't really solve anything**. We need an evolutionary step of some sort, or we need to look at the problem in a different way.

I'm not convinced there's not something modest we can do that would make a big difference. You have to find a way to structure your systems in a safer way. Writing everything in Java will help, because stuff written in antique programming languages like **C is full of holes. Those languages weren't designed for writing distributed programs to be used over a network**. Yet that's what Microsoft still uses. But even Java doesn't prevent people from making stupid mistakes.

Nature deals with breakdowns in a complex system with evolution, and a very important part of evolution is the extinction of particular species. It's a sort of backtracking mechanism that corrects an evolutionary mistake. The Internet is an ecology, so if you build a species on it that is vulnerable to a certain pathogen, it can very well undergo extinction. By the way, the species that go extinct tend to have limited genetic diversity.
-- Bill Joy, Fortune interview 29.9.2003

Lähde: http://www.interesting-people.org/archives/interesting-people/200310/msg00034.html

S. Bellovin : IPv4 Header “evil” bit ☺

Firewalls, packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. The problem is that making such determinations is hard. To solve this problem, we define a security flag, known as the "evil" bit, in the IPv4 [RFC791] header. Benign packets have this bit set to 0; those that are used for an attack will have the bit set to 1.
-- RFC 3514 (1.4.2003), S. Bellovin

Lähde: http://www.ietf.org/rfc/rfc3514.txt

Tietoturvatavoitteiden huomioiminen

Tietoturvatavoitteet

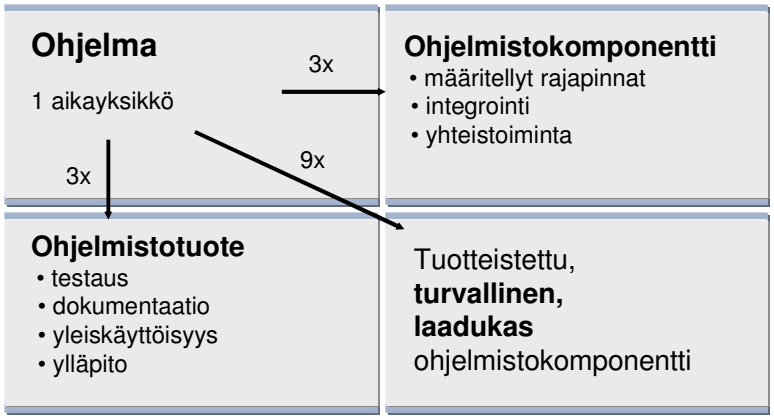
- **Käytettävyys (availability)**
  - käyttökatkosten välttäminen
- **Eheys (integrity)**
  - tiedot ja järjestelmät
- **Luottamuksellisuus (confidentiality)**
  - tiedot vain oikeille henkilöille
- **Jäljitettävyys (accountability)**
  - kuka teki mitä ja milloin?
- **Luotettavuus (assurance)**
  - mistä tiedän riittävän turvallisuuden tason toteutuvan?

Sovellusprojektin tavoitteet

- **Toiminnallisuus (functionality)**
  - usein tärkein (ainoa) kriteeri
- **Käytettävyys (usability)**
  - tietoturva vaikeuttaa…
- **Tehokkuus (efficiency)**
  - tietoturva hidastaa ja maksaa…
- **Oikea-aikaisuus (time-to-market)**
  - kiire, kiire – missä oikaistaan…
- **Yksinkertaisuus (simplicity)**
  - hyvä!

The Mythical Man-Month

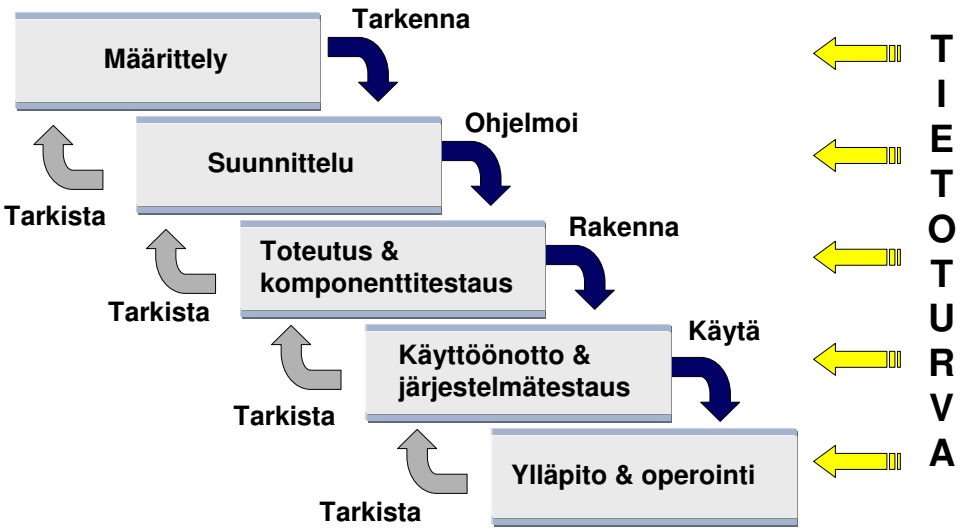
atbusiness



Frederick P. Brooks

Vesiputousmalli

atbusiness



Sovellusten haluttu tietoturvataso on määriteltävä

Suuri osa tietoturvaongelmista voidaan poistaa määrittely- ja suunnitteluvaiheessa.

tietoturvaongelman luokka	tietoturvaongelman sisältäviä sovelluksia (n=45)	suunnitteluvirheiden osuus	vakavien suunnitteluvirheiden osuus
hallintaliittymä	31%	57%	36%
tunnistus/valtuutus	**62%**	**89%**	64%
konfiguroinnin hallinta	42%	41%	16%
salausalgoritmit	33%	**93%**	61%
tiedon keräys	**47%**	51%	20%
syötteen tarkistus	**71%**	50%	32%
parametrien manipulointi	33%	81%	73%
luottamuksellisen tiedon käsittely	33%	70%	41%
istunnon hallinta	40%	**94%**	79%

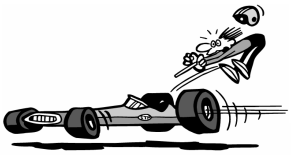
http://www.atstake.com/research/reports/atstake_app_unequal.pdf

Erityistä huomioitavaa

- Riskiarviointi
- Murphy's computer vs. Satan's computer
  - use case vs. mis-use case
- Ohjelmoijan näkökulmat
  - toiminnallinen koodi
  - virhekoodi
  - tietoturvakoodi
- Tekniset vs. loogiset virheet
- Olettamukset
- Sovelluksen testattavuus
- Koodikatselmointi

Web Services haasteita

- Kypsymättömyys
- Monimutkaisuus
- Tuotteiden yhteensopivuus
- Tietoturvafokuksen muuttuminen
- PKI
- Sovelluskehittäjien osaamistaso
- Luottamuksen hallinta



SOAP-madon todennäköisyys?

- Useimpia uusia protokollia on jossain vaiheessa väärinkäytetty
- SOAP tietoturvaa mietitään vasta jälkikäteen
- SOAP mahdollistaa binaari-liitteet
- SOAP-liikennettä ajetaan tyypillisesti HTTP/HTTPS:n yli
- Valtaosa palomuureista ei osaa suodattaa SOAP-liikennettä
- MS Office XP:ssä Web Services ja SOAP-tuki

Quality = Security

We start confusing quality with elegance, brightness, weight, and other subjective things. Then even those get compared when we talk about good quality, bad quality, high and low quality, and all those things. So far today we've used the word quality fifteen or twenty times, and each meaning has been different. If we're going to have a quality improvement program, we have to agree on what the word means. We don't want an elegance improvement program, do we?

-- Philip B. Crosby, Quality is Free